Issues of Control and Causation in Quantum Information Theory

Thesis submitted for the degree of D.Phil. in Mathematics

Chiara Marletto

Merton College,

University of Oxford

Supervisor: Prof. Artur Ekert

Professor of Quantum Physics,

Mathematical Institute, University of Oxford

Dedicated to my parents, Piera and Giuseppe

Aknowledgements

I have greatly benefited from the illuminating conversations with Simon Benjamin, David Deutsch, Artur Ekert, Alan Grafen, Alastair Kay, Minhyong Kim, Mario Rasetti and Vlatko Vedral. I would like to thank all of them.

I am grateful to Alastair Kay for providing helpful advice and suggesting several useful improvements to the thesis; to Artur Ekert for his fruitful criticism, particularly about my thoughts on the no-cloning and the self-replication issues. I am also grateful to Alex Schekochihin for conversations about classical information theory.

I wish to thank especially David Deutsch, for insightful discussions and incisive criticism of the thoughts presented in this thesis; for providing inspirational ideas about Science and the Multiverse; for his constant encouragement and support.

My research work was supported by the Istituto Superiore Mario Boella (ISMB), EPSRC and Merton College.

Contents

Chapter 1

Introduction

Until very recently, issues of control and causation were considered to be not relevant to fundamental Physics. They appeared here and there, at an emergent level, in thermodynamics, in engineering, in chemistry; but never referred to explicitly by the laws of fundamental Physics. For the latter are expressed, in the *prevailing conception*, exclusively in terms of initial conditions and laws of motion.

A completely different scenario, where issues of control and causation are in fact of the essence, has emerged in the Quantum Theory of Computation, one of the most fruitful branches of fundamental physics. Indeed, the most general scheme of a computation includes a program *causing* some computation to happen on the workspace; by the equivalence between the dynamical evolution of a physical system and a computation, [1], this always corresponds to a physical substrate instantiating the program causing some transformation on the physical system corresponding to the workspace. Hence, in this scenario any dynamical process, at any scale, can be interpreted as an event

in which control and causation occur, whereby a physical system acts on another physical system to cause a transformation to happen. The question therefore arises, whether this approach could be adopted to set a new and more fruitful way of describing the physical reality.

The newly proposed Constructor Theory, [2], which is intended to generalise the Quantum Theory of Computation, provides a description of the world revolving around issues of control and causation. According to Constructor Theory, all scientific theories are expressible as statements about which physical transformations can or cannot be caused, and why. This audacious idea of expressing everything fundamental in terms of the possible-impossible dichotomy is a departure from the prevailing conception of fundamental physics, which only distinguishes between what happens and what does not via initial conditions and laws of motion.

This thesis presents the first applications of this theory, and, among other things, makes the case that this theory allows one to formalise concepts and formulate laws that are not expressible in the prevailing conception.

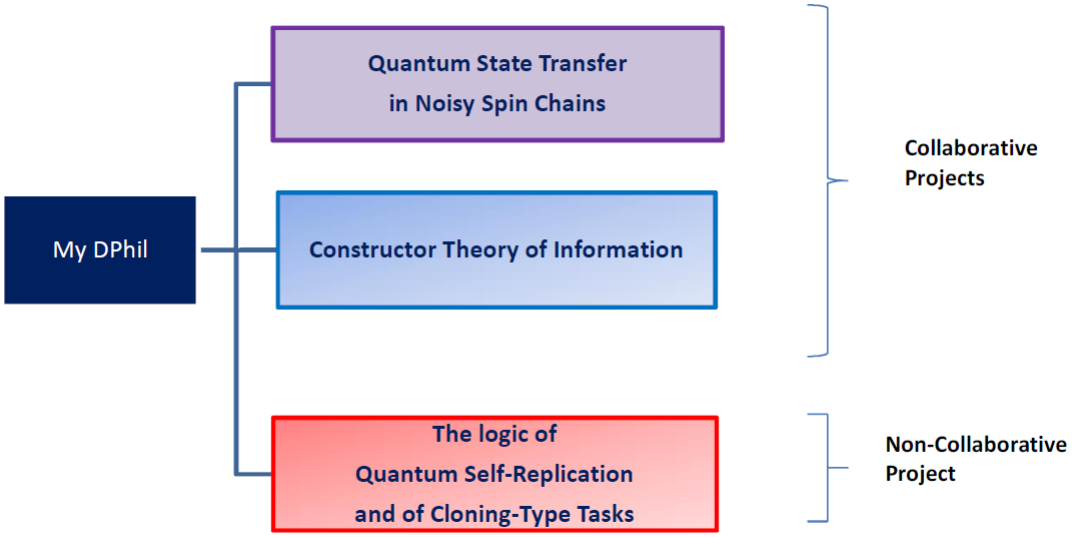
This is the case with the first very promising result of Constructor Theory, the Constructor Theory of Information, [3], developed in collaboration with David Deutsch (chapter 2 and 3). This theory of information, expressed solely in constructor-theoretic terms, permits the formulation of the notion of information within physics which does not suffer from the circularity at the foundations of existing information theory. Moreover, without invoking any laws of Quantum Theory, it explains the relationship between classical and quantum information, revealing a single underlying origin of the most distinctive phenomena associated with the latter, (the unpredictability of

some measurement outcomes in the presence of determinism, the lack of in-principle distinguishability of some states, the impossibility of cloning, the irreducible perturbation caused by measurement and entanglement (as locally inaccessible information)).

The second section of the thesis (chapters 4 and 5) aims to apply the conceptual tools of Constructor Theory and of the Quantum Theory of Computation to assess whether one particular task, self-replication (as it occurs in living entities), is consistent with quantum mechanics. This problem, raised by Schrödinger [4], has been controversial ever since: some physicists [5, 6, 7], notably Wigner [8], argued that self-replication is forbidden by Quantum Mechanics, thus claiming that the latter is not a universal theory and needs to be completed by ad hoc laws [9]. In this thesis I provide a model of the logic of self-replication that updates von Neumann's [10, 11] and is provably consistent with Quantum Theory, thus rebutting those claims and understanding self-replication explicitly within physics. This analysis requires one, among other things, to distinguish carefully self-replication from the task of cloning a quantum state, chapter 5, as the two are often confused with each other. Note, in passing, that I propose a conceptual scheme where the possibility of quantum coherence playing a role in the process of self-replication is allowed. This is rather interesting in the context of the recently-developed discussion on quantum biology, which has received much attention since theories about quantum coherence making photosynthesis more efficient have provided good explanations of experiments in which light-harvesting proteins within algae have been probed using laser beams [12],[13].

The third section of the thesis (chapter 6) presents a protocol (developed

in collaboration with Alastair Kay and Artur Ekert, [14]), to accomplish the task of transferring perfectly a quantum state along a spin chain, in the presence of systematic errors. This third part has two main points of connection with the first two: it investigates the task of transferring perfectly a quantum state from one location to another, which is closely related to the copying issues investigated in the previous chapters; also, it develops formal tools that may be useful to address the related problem, now central in quantum-biology, of how to implement coherent quantum transfer of energy in the presence of noise [15]. The structure of the thesis is summarized in the figure for the reader's convenience.



Three main ideas permeate the structure of this polymorphic thesis.

One is the counterintuitive concept, first developed by Karl Popper [16], that the content of a scientific theory is in what it forbids. In the Constructor Theory of Information it emerges explicitly that it is the impossibility

of performing certain tasks (such as, the task of cloning quantum states) that makes it possible to develop a rich set of effects, such as unpredictability arising from determinism, irreducibly perturbing measurements, and the possibility of storing locally inaccessible information. More generally, Constructor Theory formalises that concept by making the possible-impossible dichotomy play a fundamental role.

Another fundamental idea that will be recurrent in this thesis is that information (particularly knowledge in the Popperian sense, without a knowing subject [16]) can be conceived as an abstract "constructor": something that can cause transformations to happen, while retaining its ability to do so. A closely related idea is that anything that is not forbidden by the laws of physics, can be attained, given the right amount of knowledge [2]. This is precisely what underlies my rebuttal of Wigner's argument: the possibility of encoding the set of instructions to build an organism out of raw material is what permits self-replication, and indeed any specialised construction, to happen in a world that does not contain the design of that specific construction. The protocol to counteract systematic errors is another instance of this: the reason why the class of errors in question can be perfectly counteracted is that one can extract knowledge about them via repeated experiments on the transfer system and then use it to encode in a protected subspace.

The third leading theme of the thesis is the quest for unifications. The Constructor Theory of Information tends towards a unified explanation of quantum (super) information and information, which is intended to clarify the relation between the two, thereby showing that there is no abrupt, mysterious jump from the latter to the former. It also advocates the idea that

the theory of information can be incorporated, without circularities, within physics; it provides a route to showing that control and causation (which rely on causal information processing, locality and causality) are completely compatible with Quantum Theory.

And yet another unification is provided by my formulation of the no-cloning theorem, that is not rooted in any specific picture; and by my model of self-replication, which defends the compatibility of the emergent phenomenon of self-replication in living entities and the (quantum) laws ruling their elementary constituents.

Chapter 2

Constructor Theory

Abstract[1]

Constructor Theory [2] has recently been proposed as the ultimate generalisation of the Quantum Theory of Computation. Its mathematical structure is a necessary tool both for expressing the principles of the theory and for performing the translation of current physical theories into constructor-theoretic terms. In this Chapter I shall introduce the algebra of tasks necessary to develop the discussion about the Theory of Information (Chapter 3). I shall also outline some of the most promising future applications of the theory.

2.1 Introduction

There are several possible approaches to Constructor Theory, [2], but I think the most fruitful one in this context is to consider it as the ultimate generalisation of the Quantum Theory of Computation.

[1]This Chapter is part of a wider joint project with David Deutsch about the Mathematical structure of Constructor Theory.

Let me now consider the reason why the Quantum Theory of Computation has to be generalised. The Quantum Theory of Computation has proven to be a fundamental branch of Physics. In particular, we know that a program is in the Universal Quantum Computer's repertoire if and only if it simulates, to some accuracy, a physical system that could exist [17]. However, the study of all such programs, i.e., the Quantum Theory of Computation, cannot be the whole of Physics [18].

That is because, although according to the Quantum Theory of Computation any given program in the repertoire of the universal quantum computer simulates (at least) one real physical system to some accuracy ϵ, nothing in the Quantum Theory of Computation allows one to say which system it simulates. Indeed, given two different interpretations of the constants of that program, one claiming that the program simulates a real physical system (i.e., one permitted by the laws of physics) and the other one claiming that it simulates another quantum computer, running some other program for the emulation of some imaginary physical system, one can make a distinction between the two interpretations only by bringing to bear some knowledge of laws of physics, additional to those contained in the Quantum Theory of Computation. Constructor Theory was proposed by David Deutsch as the theory which shall generalise the Quantum Theory of Computation.

I shall use the term *principle* for a law of physics that expresses constraints on other laws rather than on the behaviour of physical objects directly. The principle of the conservation of energy is an example: one can check mathematically whether a proposed law of motion for a particular species of particle satisfies it or not; but one cannot test experimentally whether the motion

of the particle obeys the principle unless one is given its supposed laws of motion. (For instance, early observations of beta decay satisfied the principle of the conservation of energy under the assumption that neutrinos were emitted, but refuted it under the assumption that no undetected particle was emitted.)

The laws of Constructor Theory are all principles. They are supposed to apply to all other theories expressing laws of physics, which therefore are called, in this context, *subsidiary theories*.

The prevailing conception of fundamental physics, as defined in [2], is based on explanations via prediction, i.e., on predicting the dynamical evolution of a physical system, or of the whole world, given the laws of motion of its elementary constituents and the initial conditions. However, physical processes consist of *transformations* where two (kinds of) systems are interacting one with the other, each behaving in a fundamentally different way from the other. One system is the physical object causing the transformation, which I shall refer to as the **constructor**. It is distinguished by the fact that it remains unchanged in its ability to cause the transformation again. The other one is the physical system undergoing the transformation, which I shall call **the substrates** of the construction:

$$\text{Input states of substrates} \overset{\text{Constructor}}{\Longrightarrow} \text{Output states of substrates},$$

where the constructor and the substrates **jointly constitute an isolated system**.

Note that the above framework is very general. It perfectly describes the pattern of chemical reactions, thermodynamical transformations, computa-

tions; moreover, it can also describe spontaneous processes, if one considers them as special kinds of transformations where the constructor causing them is a clock [2].

Constructor Theory is precisely the theory of which transformations (intended as above) can or cannot be caused, and why. Its main objects are in fact the **abstract** specifications of the input/output pairs of the transformations, with the constructor itself abstracted away:

$$\text{Input states of substrates} \implies \text{Output states of Substrates} \ .$$

I call these **construction tasks**, or **tasks** in short.

A constructor is **capable** of performing a task T if whenever presented with the substrates in one of the legitimate input states it delivers them in one of the corresponding output states. A task is said to be **impossible** if the laws of physics forbid the existence of a constructor performing it with arbitrary accuracy short of perfection; possible otherwise. So Constructor Theory is not the theory of constructors (this would mean to apply the prevailing-conception approach), but the theory of *tasks*.

The *basic principle of Constructor Theory* is that all subsidiary theories must be expressible entirely in terms of statements about which physical transformations are possible and which are impossible, and why. This is in sharp contrast with the prevailing conception of fundamental physics, whose basic dichotomy is between what happens and what does not. In the case of stochastic theories, there is a continuum of probability rather than a dichotomy, but the basic principle of Constructor Theory rules out

[2] Unless otherwise stated, it is sufficient, for present purposes, to confine attention to stationary substrates (i.e., stationary except when acted on by a constructor).

any reference to probability in laws in physics: they have to be deterministic. Probability can arise only at an emergent level of description. For how this happens in Quantum Theory, see [19] and [20].

The reason why Constructor Theory is a generalisation of the Quantum Theory of Computation becomes now clear. In fact, in constructor-theoretic language, a computer is a constructor whose substrates of interest are considered only as information-carrying media. In other words, the transformation caused by a computer always consists of some information processing, transforming some abstractions (in input) to some other abstractions (in output). While the theory of computation is limited to the description of such transformations, Constructor Theory is going to unify the study of this class of transformations with the study of all transformation, that involve not just abstract substrates, but also physical ones. (This is precisely what allows Constructor Theory to accommodate a consistent physical theory of information, as explained in chapter 3.) A universal constructor is also expected to exist, generalising the notion of universal quantum computer, whose repertoire includes that of the latter, but also all possible physical transformations, involving both abstract and physical substrates.

Further explanation is needed to understand why Constructor Theory should be expected to be a more fruitful mode of explanation than the prevailing conception of physics. There are in fact several converging motivations for expecting this to be true [2]. I think the most appropriate to mention here is that some constructor-theoretic principles are already taken for granted in existing physics (though not all of them are currently acknowledged as principles of *physics*). For instance, the *principle of testability* (that scientific

theories be testable by experiment) and the principles of thermodynamics. Hence our most fundamental laws are already expressible as statements about tasks being possible or impossible: those principles mean that various classes of constructors *could* be constructed, not that they will be.

However, the prevailing conception does not allow tasks to appear explicitly in laws of physics. For it does not and cannot distinguish between the fundamentally different roles played by the constructor and the substrates in a construction: the best it can do is to describe the process of interaction between constructor and substrate given the universal laws governing their constituents. Hence, the aforementioned fundamental laws are not naturally expressible in the prevailing conception. But they are in Constructor Theory: they are, in fact, constructor-theoretic statements.

Hence, Constructor Theory has to be intended as a new conceptual framework, whose language can be used to express without ambiguities all existing theories in physics. In this respect, one can speculate that the statements which are naturally expressed within the prevailing conception of fundamental Physics can be converted into a constructor-theoretic language; also, the statements which are notorious for being difficult or impossible to express in the language of the prevailing conception, such as the principles mentioned above (along with the Turing Principle and the principle of testability) can be naturally expressed in the language of Constructor Theory. However, there is more to Constructor Theory that just this. For Constructor Theory is not a contentless framework: there are some constructor-theoretic principles (i.e., laws about laws), which constrain all other theories and can be formulated

only within Constructor Theory. [3]

Therefore, Constructor Theory is a theory at a deeper level of explanation than that of the existing deepest fundamental physical theories (Quantum Theory and General Relativity). In fact, not only does it accommodate those theories (along with some other existing theories, perhaps less fundamental, such as thermodynamics, and presumably also the laws of motion of quantum fields) expressing them in a homogeneous language; it contains also additional laws. Those laws, combined with the laws of subsidiary theories, are expected to allow one to formulate non-trivial statements, which have no equivalent, and cannot be expressed, in the present theories. (An example of a fruitful application of the laws of Constructor Theory is provided in chapter 3, where the Constructor Theory of Information is presented.)

The status of Constructor Theory is therefore summarised as follows (see figure 2.1):

- Constructor Theory is a unifying language where all subsidiary theories can be *expressed*;
- Constructor theory is a theory with its own principles, constraining subsidiary theories: only some subsidiary theories will be compatible with the principles of Constructor Theory. These principles, combined with the laws of the subsidiary theories compatible with them, will produce a *new, unified mode of explanation* and will allow one to formulate new laws of Physics.

[3] For example, the Composition Principle, stating that the composition of two tasks (defined in a suitable sense) is always a possible task; or the Interoperability Principle for information, see Chapter 3.

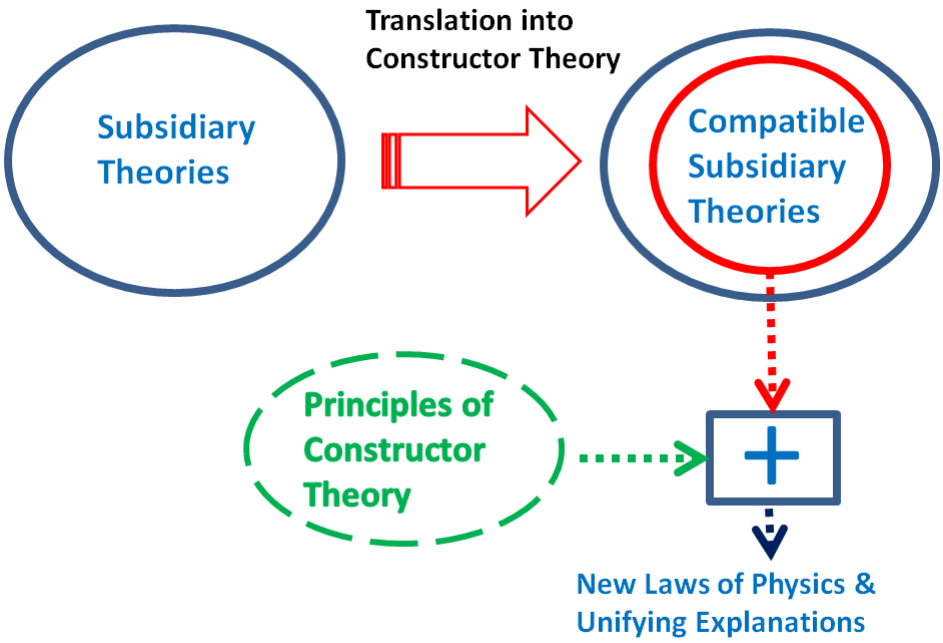


Figure 2.1: The reach of Constructor Theory.

2.2 The mathematical structure

2.2.1 Definition of a construction task

The **state** of a system **S** is a specification of everything that is objectively in **S** [4]. An **attribute** x_1 is a set of states $x_1 = \{s_1, s_2, \dots\}$: the substrate **S** has the attribute x_1 if it is guaranteed to be in any of the states belonging to x_1 [5]. I shall consider tasks that specify only some of the attributes of the substrates.

A physical **variable** X is any set of two or more disjoint attributes, $\{x_1, x_2, \dots\}$, each of which is labelled. If **S** has the attribute with label x_1 in X, then X is

[4] For a discussion of how the notion of quantum state is compatible with this framework, see section 2.3.1

[5] Note that the state s of a substrate $\mathbf{S}_1$ can be identified with the attribute $\{s\}$ of any composite system, $\mathbf{S}_1 \oplus \mathbf{S}_2$, i.e., $\{s\} = \bigcup_y \{(s, y)\}$ over all states y of $\mathbf{S}_2$

said to be *sharp*, and to have the *value* x_1. Special kinds of variables that will play a central role in this thesis are computation variables (section 3.2), information variables (section 3.3) and a subclass of the latter, i.e., observables (section 3.5).

In general, a **construction task** A is a set of ordered pairs of attributes of some substrates:

$$\mathrm{A} = \{x_1 \to y_1, \quad x_2 \to y_2, ..., \quad x_N \to y_N, ...\} \ .$$

I define the set $\{x_i\} \equiv \mathrm{In(A)}$ as the legitimate input attributes of A (and the states with those attributes as its legitimate input states), and likewise for the legitimate output attributes $\{y_i\} \equiv \mathrm{Out(A)}$.

A constructor is capable of performing a task A if, whenever presented with substrates having an attribute in In(A), it delivers them with one of the corresponding attributes from Out(A), while retaining its ability to do so again. A task always refers to an isolated system of constructor and substrates, so, for instance, heating a kettle of water is not a possible task on the water, but only on the combined system of the water plus a power supply, for which the kettle is then a constructor. Since the constructor must retain its ability to perform the task, the distinction between substrates and constructor is very sharp and their roles are not interchangeable [6]: given the dynamics on a certain isolated system $\mathbf{S} = \mathbf{S_1} \oplus \mathbf{S_2}$, $\mathbf{S_1}$ corresponds to a constructor for a certain (possible) task on $\mathbf{S_2}$ if and only if, after $\mathbf{S_2}$ has undergone the

[6] In general – though see chapter 5 for the additional issues that arise in regard to self-replication, when the output of a constructor is itself required to be a constructor of the same type

transformation specified by the task, $\mathbf{S_1}$ can cause the transformation again, when presented with another instance of $\mathbf{S_2}$ in any of the legitimate input attributes of the task.[7]

A task that can be expressed in such a way that each of its input attributes appears only once as an input and each of its output attributes only once as an output is *logically reversible* (or 1:1) with respect to those attributes. Note that each x_i, y_i, can occur more than once in a given task, in which case the task is not $1:1$. I define the set of legitimate input attributes of A as $\mathrm{In(A)} = \{x_i\}$ and the set of the output attributes of T as $\mathrm{Out(A)} = \{y_i\}$.

No perfect constructors exist in nature. Approximations to them, such as catalysts or robots, have non-zero error rates and also deteriorate with repeated use. However, a task A is *possible* (which one writes as $\mathrm{A}^{\checkmark}$) if the laws of nature impose no limit, short of perfection, on how accurately A could be performed, nor on how well things that are capable of approximately performing it could retain their ability to do so again. Otherwise A is impossible (which one writes as $\mathrm{A}^{\times}$).

In other words, a task A is possible if and only if for any positive number ϵ representing the desired accuracy there can exist a constructor capable of performing A within that accuracy. How "accuracy" is defined is set by the subsidiary theory, via an appropriate measure of "distance" between states. In quantum theory this would be in terms of the inner product, for instance. Consequently the basic principle of Constructor Theory requires every subsidiary theory to define a measure of the accuracy with which any

[7] How this is formalised in quantum theory, for a special kind of tasks, is explained in section 2.3.1.

constructor described by that theory performs any task; and it must give a meaning to whether an infinite sequence of tasks $\mathrm{A}_1, \mathrm{A}_2, \ldots$ on a system $\mathbf{S} \oplus \mathbf{E}$ (where E might be the environment of S, and the effect of the A_i on E tends to zero as i increases) converges to a limiting task A on S.

Note that, according to the definition of a constructor being capable of performing a task, a given pair of attributes can be regarded either as a constraint or as an option. For example, in $A = \{x_1 \to y_1, x_2 \to y_2\}$ each pair is a constraint, i.e., a requirement to be met by the constructor. In $B = \{x_1 \to y_1, \quad x_1 \to y_2\}$ each pair is an option. Therefore, a constructor capable of performing $C = \{x_1 \to y_1\}$ is also capable of performing B, but may not be capable of performing A.

Since tasks are sets, one can define the union of two tasks A and B as the set union of A and B. Note that taking the union of a task with another task does not always mean adding a constraint: using the example above, $\mathrm{A} \cup \mathrm{C}$ is less constrained than A, because In(C) and In(A) have a non-empty intersection. Note also that if a task $\mathrm{T} = \bigcup \mathrm{A}_i$ is $1:1$ and it is possible, then A_i are possible $\forall i$. For if $\mathrm{T}^{\checkmark}$, then there is a constructor that performs it, and hence that constructor can be used to perform each of the A_i's. On the other hand, if each A_i is possible, their union might not be.

2.2.2 Task algebra

Given a set of attributes V, I shall denote the set of all tasks defined on V as $\mathcal{T}(V)$. The tasks in $\mathcal{T}(V)$ can be composed via the following operations.

Serial composition

The *serial composition* of two tasks A and B is the task whose net effect is that of performing A and then B on the same substrate:

$$\mathrm{BA} = \{\, x \to y \mid \quad \exists z \;:\; \quad (x \to z) \in \mathrm{A} \quad \& \quad (z \to y) \in \mathrm{B} \} \;,$$

The above definition means that the serial composition of two tasks A and B is a task that specifies the net effect of performing A and then B on the same substrate. However, if BA is possible, this does not imply that so are both A and B: the constructor performing BA might achieve its effect without performing either A nor B. In fact, the most interesting cases (as we shall see) are those where A and B are impossible, but their serial (or parallel) composition is a possible task.

The serial composition has the following properties:

- Associativity: $(\mathrm{AB})\,\mathrm{C} = \mathrm{A}\,(\mathrm{BC})$
- Existence of the unit task $I_V = \bigcup_{x \in V} x \to x$ such that

$$I_V A = A = A I_V, \forall A \in \mathcal{T}(V) \;.$$

- Existence of the local unit: $\forall A \in \mathcal{T}(V)$ the local output unit is: $I_{Out(A)} = \bigcup_{y \in Out(A)} y \to y$, such that $I_{Out(A)} A = A, \forall A$ and the local input unit is $I_{In(A)} = \bigcup_{x \in In(A)} x \to x$, such that $A I_{In(A)} = A, \forall A$. Since they are in $1:1$ correspondence with the states of a given substrate, and hence they could be the route to express the concept of a attribute

purely in terms of tasks.

- Existence of the empty task $e = \{\}$ such that $Ae = e = eA, \forall A \in \mathcal{T}(V)$. The empty task represents the task which does not impose any constraint on the constructor. (Hence, anything could be a constructor for the empty task.)

Parallel composition

Let me now consider the composite system $\mathbf{M} \oplus \mathbf{N}$ of two substrates $\mathbf{M}$, $\mathbf{N}$, with sets of attributes V and W. The parallel composition $\mathrm{A} \otimes \mathrm{B}$ on a composite system $\mathbf{M} \oplus \mathbf{N}$ is the task whose net effect is that of performing A on $\mathbf{M}$ and B on $\mathbf{N}$:

$$\mathrm{A} \otimes \mathrm{B} = \{(x, z) \to (y, w) \ , \ \ \forall \ (x \to y) \in \mathrm{A} \quad \& \quad (z \to w) \in \mathrm{B}\} \ .$$

where (x, z) and (y, w) denote the attribute of $\mathbf{M} \oplus \mathbf{N}$.

A construction task specifies only *intrinsic attributes* of the combined system of all its substrates such as their individual shapes or mutual orientations attributes that do not refer to any object other than them. For example, "change the colour of the substrate to that of the sun" is not a valid task because it refers specifically to the sun as well as the substrate. But "change the colour of substrate 1 to that of substrate 2" is a valid task on the composite system of two suitable substrates, because "having the same colour" is an intrinsic property of the combined system. Thus, it may be that a task $\mathrm{A} = \{(x, z) \to (y, w)\}$ cannot be decomposed into $\{x \to y\} \otimes \{z \to w\}$ because the individual attributes are not intrinsic and therefore the arguments

of that parallel composition are not valid tasks. However, if both A and $\{x \to y\}$ are valid tasks, then $\{z \to w\}$ must be a valid task too.
Parallel composition has the following properties:

- $e \otimes A = e = e \otimes A$
- $(A \cup B) \otimes C = (A \otimes C) \cup (B \otimes C)$
- $(A \otimes B)(C \otimes D) = AC \otimes BD$

The transpose of a task

The transpose of a task is defined, $\forall A \in \mathcal{T}(V)$, as the task $A^{\sim}$, satisfying the following axioms:

- If $A = \{x_1 \to y_1, x_2 \to y_2, ..., x_N \to y_N, ...\}$, $T^{\sim}$ is (in terms of states):

$$A^{\sim} = \{y_1 \to x_1, y_2 \to x_2, ..., y_N \to x_N, ...\} .$$

  Hence, for $1:1$ tasks the transpose task is a proper inverse.

- $(A^{\sim})^{\sim} = A$, $(AB)^{\sim} = B^{\sim} A^{\sim}$ and $(A \otimes B)^{\sim} = A^{\sim} \otimes B^{\sim}$

2.2.3 Possibility with side effects allowed

In constructor theory tasks always refer to an isolated system of constructor and substrates: hence all substrates must be included in their specification. But one is also often interested in possibilities or impossibilities that hold regardless of the resources applied. So one introduces another category of possibility: a task A is *possible with side-effects*, which I write as $A^{\underline{\checkmark}}$, if

$(\mathrm{A} \otimes \mathrm{T})^{\checkmark}$, for some task T on some possible substrate. A *possible substrate* is one whose construction is possible from naturally occurring ones. For present purposes, one can assume that these substrates exist in unlimited numbers, and the attribute of being such a substrate is called g, for "generic". This will be referred to as the "generic resources" assumption. Thus, for example, for every task A,

$$\mathrm{A}^{\checkmark} \Rightarrow \{(g, g, \ldots) \rightarrow \mathbf{C}_{\mathrm{A}}\}^{\underline{\checkmark}}\,, \tag{2.1}$$

where "$\Rightarrow$" denotes implication and $\mathbf{C}_{\mathrm{A}}$ is some constructor for A. This implies that there are naturally occurring (approximations to) constructors too. Under these assumptions, one also has

$$\mathrm{A}^{\underline{\checkmark}} \Leftrightarrow (\exists h)\,(\mathrm{A} \times \{(g, g, \ldots) \rightarrow h\})^{\checkmark}\ , \tag{2.2}$$

where $\times$ denotes the Cartesian product of sets. One could also replace $(g, g, \ldots)$ by g in (2.1) or (2.2), since a collection of any finite number of generic substrates is a generic substrate.

2.2.4 The Composition Principle

Because of the principle of locality, an arbitrary network without loops whose nodes are tasks and whose lines are their substrates is necessarily a task too (if the substrates are unchanged between tasks). The serial composition C = BA of two tasks is regular if

$$\forall x \in \mathrm{In}\,(C)\,, \forall y : x \rightarrow y \in A,\ \ BI_{\{y\}} \neq e.$$

Let me first define a regular *network* of construction tasks as a network in which tasks are composed either via parallel composition or via regular serial composition. Hence a *regular network* of tasks is one where the set of legitimate input states at the end of each such line is the set of legitimate output states at its beginning. Loops are excluded because a substrate on a loop is necessarily a constructor. The **Composition Principle for Tasks**, conjectured in [2], is stated as follows: any *regular* finite network of possible tasks is a possible task. (For irregular serial composition the composition principle may not apply: if $A = \{a \rightarrow b, a \rightarrow d\}^{\checkmark}$ and $B = \{d \rightarrow e\}^{\checkmark}$, $BA = \{a \rightarrow e\}$ might be impossible, as A might be possible even if $\{a \rightarrow d\}$ is impossible.)

By the composition principle, if there are possible tasks at all, the unit task and any of the local unit tasks must be possible: when confining attention to stationary states, the unit task is a task which can be performed by "doing nothing" to the substrate. I shall refer to the constructor capable of performing the unit task as the null constructor. As a consequence, the null constructor can perform any $A^{\sim}$ A and $AA^{\sim}$. The empty task contains no constraints, so any constructor is capable of performing it.

2.2.5 Algorithms

Constructor theory includes the theory of **programmable constructors**. For the purpose of this thesis, all I need from that theory is the concept of construction algorithm, and hence I shall provide its basic definition. A **construction algorithm** (which I shall call algorithm for short) represents a

procedure to perform *transformations*. One can define algorithms recursively. First, one defines some convenient class of elementary algorithms, whose details it is not necessary to investigate in the discussion in question, in terms of tasks. All of those are going to be possible tasks. Hence, formally one says that any possible task can be considered as an elementary step of an algorithm.

An algorithm is possible if its elementary tasks are all possible. The overall task specified by a possible algorithm is a possible task. Note that while a network of algorithms specifies *a way* of performing a given task, a network of tasks does not. Hence, an algorithm might be impossible, but the task specified by it might be possible (might be performable in a different way than the one specified by the algorithm). Note that in a network of algorithms there might be logical operations, such as *if*, which are in fact based on the notion of (classical) information. In the next chapter I shall provide a notion of (classical) information expressed in purely constructor-theoretic terms.

2.3 Future perspectives

In this section I present an overview of some possible future applications of the theory just discussed, whose complete development goes beyond the purpose of this thesis. I mention them here to provide context to the issues I shall consider later on.

Recall that a subsidiary theory about a physical system is translated into constructor-theoretic terms via providing the set $\mathcal{T}(V)$ of conceivable tasks having that system as a substrate, their algebraic relations and a function

$P : \mathcal{T}(V) \rightarrow \{\text{possible, impossible}\}$. Such a function is provided by the subsidiary theory, along with an informal explanation of what the system is. The subsidiary theory is compatible with Constructor Theory if and only if the assignments of possible and impossible that it makes obey the principles of Constructor Theory.

2.3.1 Quantum Theory as a Subsidiary Theory

An intriguing problem is how to translate Quantum Theory into constructor-theoretic terms.

Let me first make a preliminary remark about locality. Constructor theory requires subsidiary theories to satisfy a locality principle: given two substrates $\mathbf{S_1}$, $\mathbf{S_2}$, there must exist, within any subsidiary theory compatible with the structure of constructor theory, a description of reality with the property that the change in the "real factual situation" of the composite system is completely specified by the change in each of the descriptors of $\mathbf{S_1}$ and of $\mathbf{S_2}$. [8]

As explained in [22, 23], and further developed in [24], Quantum Theory, when expressed in the Heisenberg picture, is manifestly consistent with this requirement (even in the presence of entanglement). In this picture the descriptor of the state of the i-th qubit of an N qubit system is a triplet $\hat{q}_i \doteq (q_{ix}, q_{iy}, q_{iz})$ such that $[q_{i\alpha}, q_{j\beta}] = 0$ when $i \neq j$, $q_{i\alpha}^2 = \mathbb{1}$ and $q_{ix} = iq_{iy}q_{iz}$ (and cyclic permutations). Such descriptors can be represented by $2^N \times 2^N$

[8] This formal requirement can be interpreted as the constructor-theoretic expression of the principle of locality, as stated by Einstein: for any two spatially separated physical systems S_1 and S_2 , "the real factual situation of the system S_1 is independent of what is done with the system S_2" [21].

matrices. This descriptor plus the Heisenberg state determine, at any one time, the state of the qubit. *Since the Heisenberg state never changes, the change in the real factual situation of the composite system is completely specified by how the local descriptors change.* This happens both when the two qubits are entangled and when they are not: for instance, one can trace back whether qubit 1 and qubit 2 have undergone an entangling interaction by considering the commutation relations between observables in the sets $\{\hat{q}_1$ before interaction, $\hat{q}_2$ before interaction$\}$, $\{\hat{q}_1$ after interaction, $\hat{q}_2$ after interaction$\}$.

Quantum Theory is therefore compatible with the locality requirement of Constructor Theory and the Heisenberg picture holds promise for being the most suitable picture for the translation of quantum theory into constructor-theoretic terms.

Note however that for the results presented in this thesis (specifically, the constructor theory of information) to apply in the case when Quantum Theory is the subsidiary theory only the *formal* compatibility of Quantum Theory with the locality requirement of Constructor Theory is required. Hence the worries about interpretations of this formal locality, as well as those in regard to underdetermination of the state stemming from the Heisenberg-based description proposed by [22] (raised in [25]) need not concern us in this context. Note also that this is an example of the fact that Constructor Theory poses strong constraints on subsidiary theories: for example, variants of Quantum Theory relying on non-linear Schrödinger equations would generically not be compatible with the principles of Constructor Theory. I think this is very promising.

Constructors for projector-type tasks

I shall now discuss the properties of a particular class of tasks, that will be relevant in the following chapters: **projector-type tasks**. Let me consider the composite system of two physical systems, **C** and **S**, respectively with Hilbert spaces $\mathcal{H}_C$ and $\mathcal{H}_S$, so that the Hilbert space of the two systems will be $\mathcal{H} = \mathcal{H}_C \otimes \mathcal{H}_S$. Let U be the unitary law of motion (set by Quantum Theory, in the event) which describes the interaction between **C** and **S**.

Let me denote by $\Sigma(X)$ the $+1$-eigenspace of the projector X and let me introduce the notation $B^{(C)} = B \otimes \mathbb{1}$, $B^{(S)} = \mathbb{1} \otimes B$ for a generic operator B. A projector-type task on the substrate **S** is defined as

$$A_t = \{g \to t\}$$

for some attributes of **S**, g and t, associated with the orthogonal projectors G and T. Each of these attributes can be thought of as the set of (pure and, possibly, mixed) states of **S** in which the corresponding projector is sharp with value 1.

In this type of task the identity of the substrate is not changed (**S** remains an **S** throughout the process), but its attributes are. I shall now define the necessary and sufficient conditions for **C** to be a constructor for A_t under the laws of Quantum Theory.

Consider the set of states of **C**

$$V_t = \{|\psi\rangle \in \mathcal{H}_C \ : \ \forall\, |g\rangle \in \Sigma(G^{(S)}) \ , \ \ U(|\psi\rangle\, |g\rangle) \in \Sigma(T^{(S)})\}.$$

If V_t is non-empty, then it is straightforward to check that it is a vector space. When **C** is initialised in one of the states in V_t, and presented with the substrate **S** in the state $|g\rangle \in \Sigma(G)$, it delivers the substrate in a state with attribute t. Note that in the final state **C** and **S** can be entangled. Also, in that final state **C** may no longer be able to cause the transformation again upon being presented with another instance of **S** in with attributed g. The states of **C** that correspond to **C** being a constructor must have the property that **C** can cause the transformation again. Hence we need the following definition.

The sufficient and necessary conditions for C to be a constructor for the task A_t are:

- V_t is non empty;
- There exists a subspace $W_t \subseteq V_t$ such that

$$U\left(W_t \otimes \Sigma(G^{(S)})\right) \subseteq W_t \otimes \Sigma(T^{(S)}) \ .$$

  These states of **C** are the ones that retain their property of being capable of causing the transformation T over and over again. I shall denote by Π_{W_t} the orthogonal projector onto the smallest subspace $W_t \subseteq \mathcal{H}_C$ with that property.

If the above two conditions are satisfied, one can define the (non-empty) set

$$V_{C_t} = \{|\psi\rangle \in \mathcal{H}_C \ : \ \forall\, |g\rangle \in \Sigma(G^{(S)}) \ , \ \ U(|\psi\rangle\, |g\rangle) \in \Sigma(\Pi_{W_t}^{(C)} T^{(S)})\},$$

which is easily proven to be a vector space. States in this subspace either

belong to W_t or they are brought into that space after one application of U. The projector Π_{C_t} onto this subspace is the **projector for being a constructor** for A_t. Hence, being a constructor for a projector-type task is in principle a measurable property.

Under the laws of motion, represented by the unitary U, the system **C** may be a constructor for different tasks on the same substrate **S** initialised to a generic, fixed attribute $G^{(S)}$ (that can be thought of as a blank state). For instance, let Π_1 be the projector for being a constructor for the task A_{t_1} defined by the projector T_1, and Π_2 be the projector for being a constructor for the task A_{t_2} associated with the projector T_2. In this case, **C** can be considered as a programmable constructor with two kinds of programs in its repertoire, one to produce objects with the property T_1, the other to produce objects with the property T_2. (For example, **C** could be the register of a quantum computer, **S** its workspace.) Indeed, programs are (abstract) constructors.

An interesting question to consider is whether quantum coherence in the programming phase of this programmable constructor could possibly widen its repertoire: i.e., if, given any two programs for two different projector-type tasks, T_1 and T_2, their superposition could be a program for something "new". Although this question goes beyond the purpose of this thesis, it is interesting to provide a hint to the answer, as follows.

I shall first prove that in the case when the two tasks are specified by unambiguous attributes, i.e, $\Sigma(T_1) \cap \Sigma(T_2) = \{0\}$, the attributes of being programs for the two tasks are bound to be distinguishable from each other, i.e., $\Pi_1\Pi_2 = 0$.

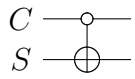
Proof

By hypothesis, U has the property that, for states $|P_i\rangle \in \Sigma(\Pi_i)$

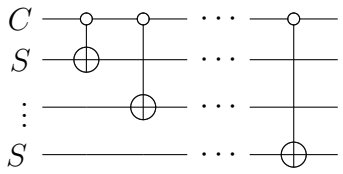
$$U(|P_1\rangle\,|g\rangle) \in \Sigma(\Pi_1^{(C)} T_1^{(S)}) \tag{2.3}$$

$$U(|P_2\rangle\,|g\rangle) \in \Sigma(\Pi_2^{(C)} T_2^{(S)})\,. \tag{2.4}$$

Let me denote by



the network performing U. The following network acting on the composite



system $\mathbf{C}\oplus\mathbf{S}^{(n)}$, including n replicas of the substrate $\mathbf{S}$, $\mathbf{S}^{(n)} = \underbrace{\mathbf{S}\oplus\mathbf{S}\oplus\cdots\oplus\mathbf{S}}_{n}$, performs the unitary:

$$\begin{aligned} |P_1\rangle\,|g\rangle^{\otimes n} &\rightarrow \left|\psi_1^{(n)}\right\rangle \\ |P_2\rangle\,|g\rangle^{\otimes n} &\rightarrow \left|\psi_2^{(n)}\right\rangle \end{aligned} \tag{2.5}$$

where $\left|\psi_i^{(n)}\right\rangle \in \Sigma\left(\Pi_i^{(C)}\hat{T}_i^{(n)}\right)$, where $\hat{T}_i^{(n)} = \mathbb{1}\otimes\underbrace{T_i\otimes T_i\otimes\cdots\otimes T_i}_{n}$. For, at the end of each transformation, the property of being a constructor for that specific task is preserved.

Let me introduce the operator norm, $||A|| = \mathrm{Sup}\{|A\,|v\rangle\,| \;:|\,|v\rangle\,| = 1\}$. On the one hand, by the properties of the operator norm, $||T_1^{(n)}T_2^{(n)}|| \leq ||T_1T_2||^n$.

On the other hand, $0 \leq ||T_1 T_2|| < 1$ because the intersection between $\Sigma(T_1)$ and $\Sigma(T_2)$ is empty.[9]

Hence, in the limit $n \to \infty$ one has that

$$||\hat{T}_1^{(n)} \hat{T}_2^{(n)}|| = ||T_1 T_2||^n \to 0$$

which implies that

$$\lim_{n\to\infty} \hat{T}_1^{(n)} \hat{T}_2^{(n)} = 0 \, .$$

This means that the states $\lim_{n\to\infty} \left|\psi_1^{(n)}\right\rangle$, $\lim_{n\to\infty} \left|\psi_2^{(n)}\right\rangle$ are orthogonal, and so must be $|P_1\rangle$ and $|P_2\rangle$, because for arbitrary n the transformation performed by the above network on $\mathbf{S}^{(n)}$ is unitary. Picking the two pure states $|P_1\rangle$ in the $+1$-eigenspace of Π_1 and $|P_2\rangle$ in the $+1$-eigenspace of Π_2 with the property that $|\langle P_1|P_2\rangle|^2$ is maximal, the above result shows that $|\langle P_1|P_2\rangle|^2 = 0$, thus proving that $\Pi_1 \Pi_2 = 0$. In other words, the network asymptotically works as a distinguisher between the two constructor subspaces. (This is an instance of what we shall describe in chapter 3 as using redundancy to obtain a sharp outcome from a non-sharp input.) ∎

The condition $\Sigma(T_1) \cup \Sigma(T_2)$ includes the noteworthy case where $T_i = |\psi_i\rangle \langle\psi_i|$ - i.e., it applies to quantum computers that have in their repertoire different quantum states. (This was pointed out in [27], using a different method of proof.) Also, it trivially holds when T_1 and T_2 are orthogonal to each other (for instance, when they represent two different macrostates, such as a dog

[9] The projector onto $\Sigma(T_1) \cap \Sigma(T_2)$ is $\lim_{n\to\infty} (T_1 T_2)^n$, [26]: if that intersection is empty, there can be no non-zero states $|v\rangle$ with the property that $T_1 T_2 |v\rangle = |v\rangle$ (otherwise they would be in the intersection). This fact, together with $||T_1 T_2|| \leq ||T_1||\, ||T_2|| = 1$ implies that $||T_1 T_2|| < 1$.

and a tiger, see chapter 5).

Considering **C** as a non-universal programmable constructor with the programs Π_1 and Π_2 in its repertoire, the above result implies that coherence in the programming phase does not add any new projector-type task to the repertoire. For suppose one programs the constructor with the coherent superposition of a program from the range of Π_1 and another program from the range of Π_2: $|P_{1,2}\rangle = \alpha |P_1\rangle + \beta |P_2\rangle$. Then, the unitary evolution U acts as follows:

$$(\alpha |P_1\rangle + \beta |P_2\rangle) |g\rangle \rightarrow \alpha |\psi_1\rangle + \beta |\psi_2\rangle \ ,$$

where $\Pi_i^{(C)} |\psi_i\rangle = |\psi_i\rangle$ for $i \in \{1, 2\}$. The information that is accessible locally on the substrate is represented by the reduced density matrix on the substrate subspace, i.e. by the operator:

$$\rho^{(S)} = \mathrm{Tr}_C[|\alpha|^2 |\psi_1\rangle \langle\psi_1| + |\beta|^2 |\psi_2\rangle \langle\psi_2| + \bar{\alpha}\beta |\psi_2\rangle \langle\psi_1| + \alpha\bar{\beta} |\psi_1\rangle \langle\psi_2|] \ .$$

Upon noticing that, since $\Pi_1^{(C)}\Pi_2^{(C)} = 0$ and $\Pi_i^{(C)} |\psi_i\rangle = |\psi_i\rangle$,

$$\mathrm{Tr}_C[|\psi_1\rangle \langle\psi_2|] = 0 = \mathrm{Tr}_C[|\psi_2\rangle \langle\psi_1|] \ ,$$

one sees that the reduced density operator on the substrate is the same as the one obtained by programming the constructor in a decoherent way, i.e. with the mixture program $|\alpha|^2 |P_1\rangle \langle P_1| + |\beta|^2 |P_2\rangle \langle P_2|$.

This means that programming the constructor with a mixture of two different programs gives the same result as programming it with their coherent superposition. Hence, coherence in the programming phase does not add any

new object to the ones that the machine can construct when programmed in a decoherent way (i.e., with states belonging to an orthogonal basis and their mixtures). To put it another way, the tape of a non-universal constructor with two non-ambiguous tasks in its repertoire can be measured any number of times and this does not restrict its repertoire. It is to be expected that that this is true in the case of constructors with ambiguous tasks in their repertoire too; but investigating this goes beyond the purpose of this thesis.

In the case of a universal constructor the issue about ambiguous tasks does not arise. Indeed, every projector-type task in the repertoire of a universal machine can be coded for by programs that are members of an orthogonal basis. Suppose indeed there was some property T not achievable by the computational basis programs, but only via a superposition $|\psi_T\rangle$ of those basis states. Since the constructor in question is universal, there must be one program in its repertoire that codes for constructing the program $|\psi_T\rangle$, which can be used to produce T thereby. Such a program must be a member of the orthogonal basis, which means that anything achievable by a superposition of basis programs must be achievable by the basis programs too. Hence, in the case of universal machines coherent programming for (ambiguous and unambiguous) projector-type tasks does not add anything new to the repertoire of the machine. An interesting question (that arises both for universal and not universal machines) is whether coherence in the programming phase could improve the efficiency of performing a given task. An indicative argument along the following lines suggests that it cannot. Suppose we have a constructor with two orthogonal programs $|P_1\rangle$ and $|P_2\rangle$ in its repertoire, to perform the tasks defined by the projectors T_1 and T_2. Coherence in the program-

ming phase would make it possible to increase efficiency if and only if the program $|\alpha|^2 |P_1\rangle \langle P_1| + |\beta|^2 |P_2\rangle \langle P_2|$ was slower than $|P_{1,2}\rangle = \alpha |P_1\rangle + \beta |P_2\rangle$. This would mean that $|P_{1,2}\rangle$ is faster than both $|P_1\rangle$ and $|P_2\rangle$. But this is impossible, as $|P_{1,2}\rangle$ cannot be faster than the slower of $|P_1\rangle$ and $|P_2\rangle$, just like the mixture program. As a side remark, the mixture can be produced by a randomizer, while the coherent superposition requires a coherent transformation to be generated, which implies it is much more onerous than the mixture to begin with.

2.3.2 Conservation Laws

Suppose that a given subsidiary theory claims there is a conservation law for an (additive, for simplicity) quantity Q. The informal expression of a conservation law, in constructor-theoretic terms, is that there is no constructor that can change the Q of its substrates. [10] One could wonder what structure the presence of a conservation laws induces in the algebra of tasks of the system under consideration. In short, the existence of the conservation law in the theory of a given substrates *implies that the set of pairwise tasks on that substrates is partitioned into classes*. Tasks in the same class, if impossible, are impossible for the same reason, and are equivalent under an equivalence relation (called "is-like").

We say that $A \sim B$ (read: "A is like B") if and only if

$$A \sim B \leftrightarrow [(A^{\sim} \otimes B)^{\checkmark} \wedge (A \otimes B^{\sim})^{\checkmark}] .$$

[10] This statement expresses more thoroughly the notion of conservation law than the prevailing-conception statement, which, in fact, is a weaker one [2].

Theorem 2.3.1 *"is-like" is an equivalence relation for all 1:1 tasks.*

Proof By definition, "is-like" is symmetric. It is reflexive because $A \otimes A^{\sim}$ is just the unit task, and hence it is possible (and so is its inverse task). The relation is transitive too. For one has that $(A \sim B) \wedge (B \sim C)$ implies $(A \otimes B^{\sim})^{\checkmark} \wedge (B \otimes C^{\sim})^{\checkmark}$, which, in turn, implies that

$$[(A \otimes B^{\sim} \otimes I)(I \otimes B \otimes C^{\sim})]^{\checkmark}$$

is possible, by the composition law (which can be applied since the latter is always a regular network, as I am dealing with pairwise tasks). This is equivalent to $[(A \otimes B^{\sim}\ B \otimes C^{\sim})]^{\checkmark}$. Since $B^{\sim}\ B$ is just the unit task on the output attribute of B, one has $[(A \otimes \underbrace{B^{\sim}\ B}\otimes C^{\sim})]^{\checkmark} \Rightarrow (A \otimes C^{\sim})^{\checkmark}$ where use has been made of the fact that, for $1:1$ tasks, the bracketed task is perfomed by the null constructor, so that its substrates can be interpreted as being part of the constructor performing $A \otimes C^{\sim}$. The proof for $(A^{\sim} \otimes C)^{\checkmark}$ is analogous. Therefore, if $A \sim B$ and $B \sim C$ then $A \sim C$. ∎

This equivalence relation partitions therefore the set of all $1:1$ tasks into equivalence classes.

The hint about how to interpret the equivalence classes comes from noticing that there are three kinds of task classes. Notice first that $A \sim B$ implies that A is possible if and only if B is possible.

If $A = B$, this is trivially true. Otherwise, $B^{\checkmark} \Leftrightarrow (\mathbb{I} \otimes B)^{\checkmark}$ and $A \sim B$

implies that $(A \otimes B^{\sim}\ )^{\checkmark}$. By the composition law, this implies:

$$[(I \otimes B)(A \otimes B^{\sim}\ )]^{\checkmark} \Leftrightarrow [(A \otimes \underbrace{BB}^{\sim}\ )]^{\checkmark} \Leftrightarrow A^{\checkmark}$$

(I have again used the fact that, since I am dealing with pairwise tasks, $B^{\sim}\ B$ is just the unit task.) Hence, if $A \sim B$, $B^{\checkmark} \Rightarrow A^{\checkmark}$ The same argument, by symmetry of is-like, allows one to prove that $A^{\checkmark} \Rightarrow B^{\checkmark}$. In order to discover what the three possible kinds of classes are, suppose first that A is like the identity. Then, $(A^{\sim}\ \otimes I)^{\checkmark} \wedge (I \otimes A^{\sim}\ )^{\checkmark} \Leftrightarrow A^{\checkmark} \wedge (A^{\sim}\ )^{\checkmark}$. Recall that $A \sim\ B \Rightarrow A^{\checkmark} \Leftrightarrow B^{\checkmark}$, so that any other $B\ :\ A \sim\ B$ has the same property: $B^{\checkmark} \wedge B^{\sim\ \checkmark}$. The tasks in this class are all possible, and so are their transposes.

If A is not like the identity, then at least one between A and $A^{\sim}$ must be impossible. Therefore, I am left with the three following cases: $[A^{\checkmark} \wedge (A^{\sim}\ )^{\times}]$ or $[A^{\times} \wedge (A^{\sim}\ )^{\checkmark}]$ or $[A^{\times} \wedge (A^{\sim}\ )^{\times}]$. Since $A \sim\ B \Rightarrow A^{\checkmark} \Leftrightarrow B^{\checkmark}$, the same holds for any other $B\ :\ A \sim B$. Hence, the classes under is-like are further partitioned into three classes of classes: K_1, containing is-like classes each one of which is such that its representative element A and its transpose $A^{\sim}$ are both possible (there is only one such class, the one containing the unit task); K_2, containing is-like classes each one of which is such that its representative element A is possible, but $A^{\sim}$ is not; and K_3 containing is-like classes each one of which is such that its representative element A is impossible, and so is $A^{\sim}$.

Suppose that the subsidiary theory provided us with a multiplication table of the tasks on a given substrate such that an is-like pattern of classes was

present. How should we interpret it? It is conjectured that the classes in K_3 correspond to the existence of a conservation law in the subsidiary theory. For suppose only one conservation law is present: then a task is impossible if and only if it violates the conservation laws of some amount. It is therefore possible to parametrise the pairwise tasks by q, so that T_q means "increase the conserved quantity by q". Because of the conservation law, tasks with $q \neq 0$ are impossible, and the only composed tasks of the form $T_{q_1} \otimes T^{\sim}_{q_2}$ that are possible are those for which $q_1 = q_2$. Hence, the set of pairwise impossible tasks can be partitioned into classes, such that each class is labelled by the "amount" q by which tasks in that class call upon the constructor to change the conserved quantity Q. [11] Those classes precisely correspond to the is-like classes in the class K_3. A similar argument can be made to associate the classes in K_2 with the classes induced by the existence of a principle such as the second law of thermodynamics; in this specific case tasks in the same class would require the constructor to change entropy of the same amount. Some intriguing questions that shall be addressed deal with the problem of finding the constructor-theoretic statement of Noether's theorem is in this picture, thereby translating a concept in the prevailing conception (that of a symmetry group in the laws of motion) into constructor-theoretic terms.

[11] q could be a scalar, a vector or a multi-component object.

Chapter 3

Constructor Theory of Information

Abstract[1]

I present here a theory of information expressed *solely* in terms of which transformations of physical systems are possible and which are impossible, i.e., in constructor-theoretic terms. It permits the formulation of laws of physics that are directly about information, solving the circularity at the foundations of existing information theory. This theory explains also the relation between classical and quantum information. It reveals the single property underlying the most distinctive phenomena associated with the latter, particularly the unpredictability of the outcomes of some deterministic processes, the lack of in-principle distinguishability of some states, the irreducible perturbation caused by measurement and the possibility of storing locally inaccessible information in composite systems (entanglement).

[1]The content of this chapter is part of a collaboration with David Deutsch, [3].

3.1 Introduction

The equivalence between the dynamical evolution of a physical system and a computation, [1], provided a route to a far-reaching unification in Physics. Building on that idea, we understood that the theory of computation is not a set of a priori truths, as it had been deemed for long, but it is a branch of Physics: what computations can be performed in a certain world is set solely by its laws of motion T. Inspired by that, we then discovered the Quantum Theory of Computation, [17] and we started considering enthralling ideas, such as that discovering new laws of physics would allow new modes of computation to be achieved.

New, enthralling questions are suggested by the fact that *all* possible theories of computation, corresponding to different laws of motion T, express their laws in terms of the *same* entity, "information"[2]. Is "information" itself a physical entity, as one would expect if the equivalence between dynamical evolution and computation lies at fundamental laws of nature? In other words, is it possible to formulate a *theory of information* consistently within Physics?

In some respect, information is very different from any of the entities in terms of which Physics has in the past described the world. It does not look like a quantum mechanical observable or a function of tensor fields only on spacetime. Moreover, the equivalence between computation and dynamics seems to break down at some level, because the "information states" via

[2] Although information in this sense is instantiated by systems obeying a discretised, idealised version of classical physics, it is misleading to call it "classical" information, because it underlies all models of computation. (As we know, a quantum computer does manipulate ("classical") information.)

which each theory of computation expresses its statements do not correspond to dynamical states of the laws of motion. Loosely speaking, a dynamical state by itself does not carry information: for it to do so, it must be possible to choose it among a set of possible states (and this is what makes the nature of information *counterfactual*[3]).

Yet in other respects, information closely resembles physical quantities, such as energy and momentum, that appear in fundamental principles of physics. It can be moved from one medium to another while retaining all its properties qua information. (This is what I shall call its *interoperability property*). Also, the laws of the theory of computation refer directly to information without regard to the specific media in which it is stored or processed. I call that the *substrate-independence* of information.

What does one mean, therefore, by a "physical theory of information"? Such a theory should provide an explanation of how information (with its substrate-independence, interoperability and independence from any specific dynamical law T) can be associated to the description of a given physical system. This can be accomplished by providing the criterion for a physical system (described by *any* of the laws of motion T) to support computation, to instantiate information and to allow different modes of information processing, (including what is now loosely referred to as "quantum-information processing"). Hence this theory of information could not be formulated within any of the particular physical theories T, for it must apply to systems obeying any T.

[3] A counterfactual statement is one that asserts something about entities/events that do not exist/happen (but "could").

In this work Constructor Theory is proposed as a candidate to provide this theory of information. Indeed Constructor Theory exists at a deeper level of abstractions than any of the (subsidiary) theories T.

It is illuminating to point out that the two information theories that already exist in Physics (namely, Shannon's classical theory and quantum information theory) would not serve our aim.

Shannon's theory, [28], was set up in order to analyse the physics of communication. The scenario includes a *receiver* receiving a *message* from a *transmitter* through a *medium* of communication. Essential to this concept of communication is that *a message instantiates information* only if it is one of at least two *possible* messages (here is that counter-factual element); the receiver can then become a transmitter of the same information to a further receiver; that information can be *shared* by communication (i.e. the transmitter can retain a copy of the message); and receiving the message entails being capable of *distinguishing* it from all the other possible messages.

Shannon's theory does not attempt to define distinguishability. It merely assumes that information is embodied in states that are distinguishable. That did not prevent the theory from being useful when applied to classical information, because in classical physics it is self-consistent (albeit unrealistic) to assume that *any* two states are distinguishable, and copiable without perturbing them, in which case it is unnecessary to model the distinguishing process performed by the receiver as a physical process. But that assumption is inconsistent with the case where the medium of communication is ruled by Quantum Theory: there are degrees of distinguishability between quantum states, and there is a new possibility in addition, namely that of

entanglement. Also, acquiring information about some attributes of a system necessarily changes other attributes. So Shannon's theory is rooted in a discretised version of classical physics, thereby leaving us with the unsolved problem of providing a definition of "distinguishable" that is not rooted in any particular subsidiary theory T.

To do so, one needs to understand distinguishability as an operational property: the states in a given set are distinguishable if some physical process could distinguish between them. So what does a physical process have to do, in order to be a distinguishing process?

As I shall explain in the next section, I shall only need to consider processes that deliver an unambiguous outcome. So, for example, in Quantum Theory, suppose that a quantum system $\mathbf{S}_1$ can be in one of two states $|a\rangle$ and $|b\rangle$. An instrument distinguishes which of those two states $\mathbf{S}_1$ is in, while leaving that information unchanged in $\mathbf{S}_1$, if it effects a transformation of the form

$$\left\{\begin{array}{lcl} |a\rangle\,|0\rangle & \rightarrow & |a\rangle\,|\alpha\rangle \\ |b\rangle\,|0\rangle & \rightarrow & |b\rangle\,|\beta\rangle \end{array}\right\} \tag{3.1}$$

where $|\alpha\rangle$ and $|\beta\rangle$ are themselves distinguishable states of another substrate $\mathbf{S}_2$, and $|0\rangle$ is some initial state of $\mathbf{S}_2$. Evidently this is a recursive criterion, but it already allows us to deduce the condition (valid in Quantum Theory) that only a set of orthogonal states can be mutually distinguishable: since the unitarity of the laws of motion requires all inner products to be preserved, we have $\langle a|b\rangle = \langle a|b\rangle\,\langle\alpha|\beta\rangle$, and so and since $\langle\alpha|\beta\rangle \neq 1$ (merely by virtue of $|\alpha\rangle$ and $|\beta\rangle$ being different states), it follows that $\langle a|b\rangle = 0$. By the same argument, we must have $\langle\alpha|\beta\rangle = 0$ for onward transmission of the

information to be possible. It is easily verified that this remains a necessary condition even if the transmission is allowed to delete the information in the original transmitter, so long as it is required to be copiable by *some* eventual recipient. However, it is not a sufficient condition: not all orthogonal pairs of states are distinguishable by some instrument.

And so, without a base for the recursion to specify what it means for the outputs $|\alpha\rangle$ and $|\beta\rangle$ themselves to be distinguishable, the criterion is circular. Indeed, existing theories of information and computation provide no non-circular account of what it means for a set of physical states to be mutually distinguishable, and therefore to be capable of instantiating information or communication in Shannon's sense. The theory that I shall present here does.

In regard to "quantum information theory", the latter is usually presented as the generalisation of Shannon's theory to the case where the medium in question is a quantum medium. However it is not, despite the name, a theory about a new type of information (that is, the entity that is loosely called "quantum information"). Rather, it consists of the combination of the language of classical information theory with *ad hoc* application of the laws of Quantum Theory to phenomena that involve *information*, but violate the laws of classical information theory: for instance, channel capacity doubling [29], quantum parallelism in computation, the impossibility of cloning, and the existence of public-key cryptography invulnerable to attack with arbitrarily large computer power, all of which violate the classical theory of information. All this makes the theory not even self-contained qua theory of information. Indeed, it never gets round to specifying what quantity or

property it is referring to as "quantum information", nor its relation to "information". The absence of a unified framework in which to compare the former with the latter prevents us from giving satisfactory answers to questions that are crucial to applications, such as what resource that quantum computers use to allow new modes of computation is.

The Constructor Theory of Information will, among other things, explain what relates the various properties of quantum information to each other, and what relates classical and quantum types of information, by expressing their laws as special cases of underlying purely constructor-theoretic laws.

3.2 Computation

The key to avoiding circularity at the foundations of information theory is to understand information in terms of computation and not vice-versa as is usually done. It is computation that will provide the base for the recursive criterion in our discussion in section 3.1. Hence we must first understand computation in terms of intrinsic properties of physical systems which, in Constructor Theory (see chapter 2), means in terms of the possibility and impossibility of tasks.

To minimise clutter in our notation, I shall use the same symbol for a physical attribute, for the label attached to it in a given context, and for the information that one may interpret that label as representing. (For instance the attribute might be "having a spin component $\frac{1}{2}\hbar$ in the z-direction", the label might be "true", the information might be "the number was prime", and one might refer to all those as "1", with the context resolving the ambiguity.) I

shall also assume that unlimited resources are available for information processing. This is expressed in constructor-theoretic terms as the conjectured *composition principle* [2]: *every regular network of possible tasks is a possible task* (though here I need only assume that it holds for information-processing tasks).

Without loss of generality, I confine attention to reversible computations, because an irreversible computational task on a computer's memory $\mathbf{M}$ can be regarded as part of a reversible computation on some memory $\mathbf{M} \oplus \mathbf{N}$, where $\mathbf{N}$ is an additional substrate that will contain waste products. Furthermore, for simplicity of exposition, I am not addressing here issues of error correction, as the latter add nothing fundamental to the theory.

One needs only consider tasks for which the set of input substrates is the same as the set of output substrates, and only their states are transformed. Also, one needs only consider constructions on static attributes of substrates: attributes that are unchanging except when acted on by a constructor, so that every unit task is trivially possible.

Definition 3.2.1 *A* **reversible computation** $\mathrm{C}_{\Pi}(X)$ *is the task of performing a permutation* Π *over some set of at least two attributes of some substrate:*

$$\mathrm{C}_{\Pi}(X) = \bigcup_{x \in X} \{x \to \Pi(x)\} \ .$$

It follows that the attributes in any such X *are all disjoint, so one can define a computation variable as a set* X *for which* $\mathrm{C}_{\Pi}^{\checkmark}$ *for all permutations* Π *over* X*. A* **computation medium** *is a substrate with at least one computation variable.*

Reversible computations thus defined are intrinsic to the substrate: simply swapping two pure quantum states constitutes a reversible computation under the definition, even if they are not orthogonal. Whether a particular substrate is a computation medium, and if so, with respect to which computation variable or variables, therefore depends on what interactions are available in nature i.e. on which tasks are possible and impossible. For example, the term qubit is currently used for several types of computation media. It could be a quantum system whose computation variable is the set of all pure and mixed states on a two-dimensional Hilbert space, and whose computations are unitary transformations on that space (plus resetting to a particular pure state). Or it could be a subsystem of a quantum register containing N such systems, which can be caused to undergo unitary transformations on the 2^N-dimensional Hilbert space, which is a much richer class of computations that those available on N qubits of the first type. Or it could be an object capable of being one of the latter types of qubit for any N. Such a qubit can exist if and only if arbitrarily scalable universal quantum computer technology can exist (something which it is not known how to prove or disprove from todays best subsidiary theories).

3.3 Information

Information enters the picture when a computation medium is usable by some other system to provide inputs for further computations or preparations. I first consider tasks involving two or more instances of the same substrate **M**.

Definition 3.3.1 *The* **replication task** *of a set X of possible attributes of X is defined as the task*

$$\mathrm{R}_X\left(x_0\right) = \bigcup_{x \in X} \left\{(x, x_0) \rightarrow (x, x)\right\} ,$$

on $\mathbf{M} \oplus \mathbf{M}$*, where* x_0 *is some possible attribute of* $\mathbf{M}$*. A set X is* **replicable** *if* $\mathrm{R}_X(x_0)^{\checkmark}$*. An* **information variable** *is a computation variable that is replicable. An* **information medium** *is a substrate some of whose attributes constitute an information variable.*

If X is the set of all states of some substrate, then the replication task is called **cloning***. If the second substrate is of a different type, and its labels x refer to some 1-1 mapping between its attributes and those of X (I shall always assume such labellings wherever relevant in what follows), then the task is called* **copying***.*

Thus I have provided the promised non-circular, purely constructor-theoretic notion of information: a substrate **S** instantiates information if it has an attribute in an information variable A of **S**, and if giving it any of the other attributes in A was a possible task (with side effects allowed). One can define the information capacity of **S** as the logarithm of the cardinality of its largest information variable, for then the principle of locality implies the convenient property that the combined information capacity of disjoint substrates is the sum of their capacities. For simplicity, I shall assume that *unlimited resources* are available in nature for conversion into information storage devices. In constructor-theoretic terms I express this as: *any information medium, in*

any one of its information attributes, is preparable from naturally occurring (i.e., generic) substrates. Hence, all information attributes are preparable (from generic resources).

A qubit qualifies as an information medium with the set of eigenstates of the z-component of the spin, $\{\{|0\rangle\}, \{|1\rangle\}\}$ (or with the set of eigenstates of the x-component of the spin $\{\{|+\rangle\}, \{|-\rangle\}\}$); it also qualifies as a computation medium with the set $\{\{|0\rangle\}, \ \{|+\rangle\}\}$, even though the latter is not an information variable.

The interoperability of ("classical") information is currently taken for granted in the theories of information and computation, though it cannot even be stated in the prevailing conception of fundamental physics. But it has an elegant expression in Constructor Theory as the **interoperability principle**: *the composite system of two media with information variables X_1 and X_2 is an information medium with information variable $X_1 \times X_2$*. Note that this is not a property following from the definitions: it is a proposed law of physics. From this principle it follows that the composite system of any substrate $\mathbf{Q}$ and of an information medium $\mathbf{M}$ with variable X is an information medium with variable $X \times q$, where q is an arbitrary fixed attribute of $\mathbf{Q}$.

It also follows that the information in a given information medium **can be copied** into a medium of the same or higher capacity. For instance, consider the two information media, $\mathbf{M}_1$ with information variable $\{0, 1\}$ and $\mathbf{M}_2$ with information variable $\{0', 1'\}$. By the Interoperability Principle, $\mathbf{M}_1 \oplus \mathbf{M}_2$ is an information medium with set $S_1 \times S_2 = \{00', 10', 01', 11'\}$. By the definition of information medium, all permutations over $S_1 \times S_2$ are possible. Hence, in particular, so is the task $\{00' \to 00' \ , \ 10' \to 11' \ , \ 01' \to 01' \ , \ 11' \to 10'\}$,

which one interprets as copying *information* from $\mathbf{M}_1$ to $\mathbf{M}_2$ when the latter is initialised to the state $0'$.

Definition 3.3.2 *A set X of attributes of a substrate $\mathbf{S}_1$ is a* **distinguishable set** *if*

$$\left(\bigcup_{x\in X}\{(x, s_0) \to \psi_x\}\right)^{\checkmark} \tag{3.2}$$

where the $\{\psi_x\}$ constitute an information variable of $\mathbf{S}_1 \oplus \mathbf{S}_2$, $\mathbf{S_2}$ is an information medium and s_0 is some (fixed) possible attribute of $\mathbf{S_2}$.

If two attributes x and y are distinguishable I shall write: $x \perp y$. We propose a *principle* of Constructor Theory, that a set of pairwise distinguishable attributes is a distinguishable set. (Once more, this is a proposed law of Physics. Even if $x \perp y$ for every pair of elements x and y of S, it does not follow logically that S is a distinguishable set, because the definition allows the process that distinguishes x from y to change the original state of the substrate.)

The above definitions are satisfied by the notions of information and distinguishability that appear in the classical theories of information and computation, and so in that sense what I have just defined is "classical" information. But it is now emancipated from its dependence on classical physics, and its circularity has been cured. I shall refer to it simply as information because, as I commented on in the introduction, the notion of information is not rooted in any particular subsidiary theory. Indeed this construction is not theory-laden, and therefore meets the criteria set in section 3.1. As I shall show, a quantum information medium is a special case of an information medium.

3.4 Measurement

Having expressed information and computation in constructor-theoretic terms, one can now do the same for measurement and testing.

Definition 3.4.1 *Under the simplifying assumption that the identities of substrates are unchanged during constructions, one can rewrite the condition for a set of attributes to be distinguishable as the condition for a variable X to be* **measurable***:*

$$\left(\bigcup_{x\in X}\{(x,x_0)\to(y_x,x)\}\right)^{\underline{\checkmark}} \tag{3.3}$$

where the second substrate (the target) is a pre-existing information medium that has been prepared with an initial, "receptive" attribute x_0. The measurement process changes the attribute x to y_x , but accurately reports that it had been x. The attribute x is called "outcome" of the measurement and it belongs to an information variable O of the target substrate (with the same cardinality as X), that I shall call the "output variable". X will be called the "input variable" of the measurement.

A constructor is a **measuring instrument** for X if it is capable of performing the task in (3.3). If $y_x \equiv x$, the measurement of X is *non-perturbing*. That is the type of measurement that is typically needed in communication.

From the interoperability principle, it follows that **any information variable X can be non-perturbatively measured** (see the appendix, theorem 3.10.1, for the proof).

The term "measurement" is also used to describe processes where a measuring instrument for a variable X is presented with a substrate which does not

hold a sharp values of X. The output of such a process is specified by the subsidiary theories, but we shall see that in such case the output variable O cannot always be sharp at the end of the measurement.

A **test** of a scientific theory is a measurement one of whose possible outcomes would imply that that theory is false. To satisfy the principle of testability, "imply" here must mean more than logical implication: it must also be possible to enact the implication as a computational process, which then controls events such as rejection or non-rejection of the theory, or its use or non-use in the design of future measuring instruments and experiments and so on. Hence, *a test is a measurement whose output is guaranteed to be in a state in which the output variable for that measurement is sharp* (by all subsidiary theories describing the process, including those whose predictions are being tested). The truth value of a theory is not a variable: by the laws of Physics, it is guaranteed to have only one particular value, either true or false. This is precisely what makes tests different from other measurements. Much of the theory of measurement, computation and testability is concerned with how to obtain outputs holding a sharp value, in situations in which some of the variables of interest are not sharp.

3.5 Observables

When a measurer of X is presented with a substrate prepared in one of the attribtue in X, so that the input variable is sharp, there is necessarily an outcome (i.e. the output variable O is necessarily sharp). But the converse is not true, in constructor theory. The output variable can be sharp with a

given value even if the input variable X was not sharp. To take an example from quantum theory, consider the variable $X = \{\{|a\rangle, |b\rangle\}, \{|c\rangle\}\}$ where $|a\rangle$ and $|b\rangle$ are mutually orthogonal states and degenerate with eigenvalue 0, and $|c\rangle$ is orthogonal to both and has eigenvalue 1. If the state of the system is a superposition $2^{-\frac{1}{2}}(|a\rangle + |b\rangle)$, X is not sharp but any measurement of X will yield an output in which the output variable is sharp with value 0. In quantum theory, if every measurement of a particular *observable* would have outcome x, then the system has the attribute x. In constructor theory, we define a class of variables which we call *observables* (because quantum observables are examples), of which that is true:

An information variable X is an observable if all attributes $x \in X$ have the following property: If the subsidiary theories say that every measurement of X performed on a substrate with attribute y would have outcome x, then y is the attribute x or a subset thereof.

To the end of providing an instance of the concept of observable, we need first to define the notion of the *complement* of an attribute x.

Definition 3.5.1 *The* **complement** $\bar{x}$ *of an attribute* x *of a substrate* **S** *is the set of all attributes that are distinguishable from* x*.*

One can prove that $\bar{\bar{\bar{x}}} = \bar{x}$, as follows. First notice that $x \subseteq \bar{\bar{x}}$, by definition. Hence $\bar{\bar{x}} = x \cup \tilde{x}$ for some $\tilde{x}$. Similarly, $\bar{\bar{\bar{x}}} = \bar{x} \cup z$ for some set of attributes z. By definition of complement, the above implies that z contains attributes that are distinguishable from $\bar{\bar{x}}$, and, hence, from x. But this is a contradiction with the fact that $\bar{x}$ is the set of all attributes that are distinguishable from x, unless z is empty or it is a subset of $\bar{x}$. Hence $\bar{\bar{\bar{x}}} = \bar{x}$.

The attribute $\bar{\bar{x}}$ will be called the *completion* of x. It is the largest attribute having $\bar{x}$ as its complement. Referring to the example from quantum theory presented at the beginning of the chapter, the completion of $\{|a\rangle, |b\rangle\}$ would correspond to the whole subspace spanned by $\{|a\rangle, |b\rangle\}$.

In regard to the complement of an attribute x that is *preparable* from generic resources, we state the following *axiom*: *for any preparable attribute x, the variable $\{x, \bar{x}\}$ is an information variable.*

Given a preparable attribute x, there is a special class of such information variables, that have the form $P_x = \{x, \bar{x}\} \ : \ x = \bar{\bar{x}}$. We shall call them **Boolean Observables**. That they are observables can be proven, as follows. Suppose that a preparable attribute y had the property that a measurement of P_x, performed on a substrate with attribute y, would deliver the target substrate with attribute x, so that the output variable would be sharp with value x. Then $y \subseteq \bar{\bar{x}} \equiv x$ by definition of complement and of boolean observable. Hence, y would have to be contained in one of the attributes in P_x, i.e., P_x would have to be sharp in y. Similarly, if the output variable was sharp with value $\bar{x}$, then it would follow that $y \subseteq \bar{x}$. This shows that P_x is an observable.

Boolean observables will play a central role for the discussion about superinformation.

3.6 Redundancy and ensembles

I denote by $\mathbf{S}^{(n)}$ a physical system $\overbrace{\mathbf{S} \oplus \mathbf{S} \oplus \ldots \mathbf{S}}^{n \text{ instances}}$ consisting of n instances of $\mathbf{S}$, and I denote by $x^{(n)}$ the attribute $\overbrace{(x, x, \ldots x)}^{n \text{ terms}}$ of $\mathbf{S}^{(n)}$.

Evidently the set $\left\{x^{(n)}\,|x \in X\right\}$ is an information variable of $\mathbf{S}^{(n)}$ whenever X is an information variable of $\mathbf{S}$, and each $x^{(n)}$ is a redundant instantiation of the information x. In classical information theory, if X is a discrete set and each instance of $\mathbf{S}$ has a probability $p < \frac{1}{2}$ of having been changed from the correct value x by random, uncorrelated perturbations, the probability that a plurality of the values stored in n instances will not instantiate x falls exponentially with n. Constructor theory requires all subsidiary theories to be deterministic, and so probability plays no role at the fundamental level in constructor information theory. Nevertheless, redundancy does, in following way. Let me denote by $\mathbf{S}^{(\infty)}$ an unlimited supply of instances of $\mathbf{S}$. Suppose that they all have the same attribute; and let me call a sequence of experiments on $\mathbf{S}^{(n)}$, as n increases without limit, an "experiment on $\mathbf{S}^{(\infty)}$". Recall from chapter 2 that a possible task is one for which the laws of nature impose no limit, short of perfection, on how well the task can be performed. Since our assumptions about generic resources imply that there is no limit on n, it follows the **property** that for any two attributes x and y of a substrate $\mathbf{S}$, that are preparable from generic resources, $x^{(\infty)}$ and $y^{(\infty)}$ are either interchangeable in all experiments on $\mathbf{S}^{(\infty)}$ (using generic resources), or distinguishable. For given such a supply, performing all possible experiments on (instances of) $\mathbf{S}$, infinitely often, is a possible task. So if that cannot tell the difference between x and y , nothing (that uses only generic resources) can. If something can, i.e., if $x^{(\infty)} \perp y^{(\infty)}$, x and y are **ensemble distinguishable**. Otherwise, they are operationally the same and they are the **same attribute**. This means that *any two different attributes, each preparable from generic resources, are ensemble-distinguishable.*

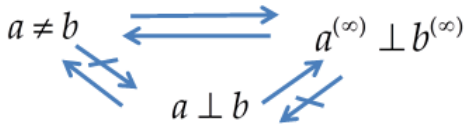


Figure 3.1: The relations between the notions of different attributes preparable from generic resources ($a \neq b$), ensemble-distinguishable attributes ($a^{(\infty)} \perp b^{(\infty)}$), and distinguishable attributes ($a \perp b$).

Remarkably, in classical physics the notions of physically different attributes, ensemble-distinguishable attributes and distinguishable attributes coincide, but in general they do not. For instance, consider the attributes $\{|0\rangle\}, \{|+\rangle\}$ of a qubit: they are not distinguishable. However, the set $\{\{|0\rangle^{\otimes n}\}, \{|+\rangle^{\otimes n}\}\}$ becomes a distinguishable set as approaches infinity. Hence the two attributes $\{|0\rangle\}$ and $\{|+\rangle\}$ are ensemble-distinguishable.

3.7 Superinformation

It follows from the definition of information variables that for any information variable X, every subset of X with at least two members is also an information variable. But the converse does not hold: the union of two information variables is not necessarily an information variable, even if all their attributes are mutually disjoint. This turns out to be the key to explain quantum information in terms of information.

Definition 3.7.1 *A* **superinformation medium** *is an information medium with two or more information variables X_i whose attributes are mutually disjoint but whose union $X = \bigcup_i X_i$ is not an information variable.*

S instantiates *superinformation* if it has one of the attributes in X but could have had any of the others. For example, in quantum physics the variables $X_1 = \{\{|0\rangle\}, \{|1\rangle\}\}$ and $X_2 = \{\{|+\rangle\}, \{|-\rangle\}\}$ are each an information variable, but their union is not: its members are not all distinguishable from each other. The condition that with respect to the union of the X_i, the medium is not an information medium means that it has some tasks impossible that would be possible if it were an information medium. As we shall see, with respect to each of the X_i, the medium is an information medium with additional properties precisely induced by the constraint on the union of them.

I shall now prove that super-information media have many of the distinctive features of quantum-information media: unpredictability arising in the presence of determinism, no-clonability, and non-distinguishability. A further property, the ability to store locally inaccessible information in composite systems, will be proven to arise in the presence of a property that I shall call "coherence", that is the generalisation of quantum coherence.

3.7.1 Some information attributes of a superinformation medium are not distinguishable

Let **S** be a superinformation medium and let X and Y be two of its non-overlapping information variables. I want to show that, as consequence, that there must exist at least one pair of attributes $x \in X,\ y \in Y$ with the property that x *is not distinguishable from* y.

Let us suppose that $\forall x \in X,\ \forall y \in Y,\ x \perp y$. This implies that all states in

$X \cup Y$ are pairwise distinguishable. Recall that it is a principle of constructor theory that a set of pairwise distinguishable attributes is a distinguishable set. Hence, this implies that $X \bigcup Y$ is a distinguishable set, which, as shown below, implies that $X \bigcup Y$ is an information variable, thus implying a contradiction with the defining condition of superinformation medium.

I first prove that, since each attribute in $X \bigcup Y$ is preparable from generic resources, $\mathrm{C}_\Pi^{\checkmark}$ for all permutations C_Π on $X \bigcup Y$. For, given $\mathbf{S}$ with an arbitrary attribute z of $X \bigcup Y$, one would first distinguish which attribute that is, thereby preparing some ancillary information medium (used in the distinguishing process) with an information attribute that, by our convention, I may label z. Then one would compute $\Pi(z)$ on the ancilla (that computation must be possible because it is a permutation and the ancilla is an information medium.) Then one would use the result $\Pi(z)$ to prepare, from naturally-occurring substrates, another instance of $\mathbf{S}$ with the attribute $\Pi(z)$. This is possible because the attributes in an information variable are preparable from generic resources. Then one discards the ancillary information medium, the original instance of $\mathbf{S}$, and the computer used to perform $\Pi(z)$. This proves that the set $X \bigcup Y$ can be permuted, with side effects, as promised. Hence, one condition for $X \bigcup Y$ to qualify as information variable has been met.

I then show that the other condition is met: the replication task is possible (with side-effects). Since $X \bigcup Y$ is a distinguishable set of $\mathbf{S}$, $(X \bigcup Y) \times (X \bigcup Y)$ is a distinguishable set of $\mathbf{S} \oplus \mathbf{S}$: one can distinguish its members by performing a distinguishing operation on each instance of S in parallel and then combining the results with a logical "or" operation, as shown in 3.10.2.

Moreover, $X \times X$, $X \times Y$, $Y \times X$ and $Y \times Y$, are all information variables of $\mathbf{S} \oplus \mathbf{S}$, by the interoperability principle. Therefore the attributes in their union are, each one, preparable from generic resources.

These two facts imply, by the argument that I developed above, that all permutations of $(X \bigcup Y) \times (X \bigcup Y)$ are possible with side-effects. Since those permutations include the replication tasks on $X \bigcup Y$, it follows that $X \bigcup Y$ is an information variable, which contradicts the condition for S to be a superinformation medium.

So there must exist at least one pair of attributes $x \in X$ and $y \in Y$, with the property that they are not distinguishable.

3.7.2 Impossibility of measuring which variable is sharp, while leaving it sharp

If the above-mentioned super-information medium **S** is known to have an attribute in $X \cup Y$, but it is not known which, no non-perturbing measurement can determine which of X and Y the attribute is in. For if such a measurement were possible, one could first perform it and then, depending on that outcome, either perform the task that distinguishes the attributes in X or the one that distinguishes the attributes in Y. Hence $X \cup Y$ would be a distinguishable set, contrary to our previous result.

3.7.3 Sets of attributes of a superinformation medium cannot be cloned

Suppose that $\forall x \in X$ and $y \in Y$, the pair $\{x, y\}$ could be cloned. It would then follow that any pair $\{x, y\} \subseteq X \bigcup Y$ is clonable. Then, given our generic resources assumption, for any $z \in \{x, y\}$, one could apply the cloning operation for that pair any number of times, resulting in a composite medium $\mathbf{S} \oplus \mathbf{S} \oplus \mathbf{S} \ldots$ with the attribute $(z, z, z \ldots)$. The cloner could therefore be used to get arbitrarily close to preparing the set $\left\{\left(z^{(\infty)}\right) : z \in \{x, y\}\right\}$. The attributes z are each, separately, preparable from generic substrates and are different (because X and Y are supposed to be non-overlapping); hence the attributes must be pairwise ensemble-distinguishable: one has $x^{(\infty)} \perp y^{(\infty)}$. Hence, upon preparing the set $\left\{\left(z^{(\infty)}\right) : z \in \{x, y\}\right\}$ from the set $\{x, y\}$ (via repeated cloning) and distinguishing the ensembles thus obtained, one achieves the effect of distinguishing the attributes in the pair $\{x, y\}$. So, if all such pairs are clonable, it would then follow that all attributes in $X \bigcup Y$ are pairwise distinguishable. But, as I have proven in the previous section, this is contrary to the defining property of superinformation media, so the assumption that all pairs $\{x, y\} : x \in X,\, y \in Y$ are clonable must be false.

3.7.4 Superinformation media with boolean observables

Let $\mathbf{S}$ be a superinformation medium and let X and Y be two of its non-overlapping information variables that have the property that each of their attributes is its own completion: $\bar{\bar{z}} = z$. I have proven above that there must exist at least one pair of attributes $x \in X$ and $y \in Y$ that have

the property that x is not distinguishable from y. Let us consider the sets $P_x = \{x, \bar{x}\}$, $P_y = \{y, \bar{y}\}$. In the section 3.5 I proved that P_x and P_y are two boolean observables: they are information variables with the property that if a measurer of P_x, when presented with some preparable attribute z, delivers the outcome x (respectively $\bar{x}$), then $z \subseteq x$ (respectively, $z \subseteq \bar{x}$). Similarly for P_y. This property, together with the the fact that $x \cap y$ is empty (non-overlapping hypothesis), implies that $\forall a \in P_x$ and $b \in P_y$, $\{a, b\}$ is not a distinguishable set, as follows. Suppose that, $x \perp \bar{y}$. This would imply, by definition of complement and by the properties of Boolean Observables, that $x \subseteq \bar{\bar{y}} \equiv y$, thus violating the non-overlapping condition. A similar reasoning leads one to the same contradiction when supposing $\bar{x} \perp y$ or $\bar{x} \perp \bar{y}$. Hence *no pair of states $x \in P_x$, $y \in P_y$ is distinguishable*, which implies that $P_x \bigcup P_y$ is *not* an information variable. Hence, **S** is a superinformation medium with respect to the Boolean Observables P_x and P_y.

Unpredictability of deterministic processes

I shall now prove that not all outcomes of measurements on **S** are predictable. That is, superinformation media with boolean observables (of which quantum information media are a special case) can exhibit the astounding property of evolving **deterministically yet unpredictably**. This is a consequence of some of the computations on $P_x \bigcup P_y$ being impossible tasks.

Consider any instrument M that is capable of performing a non-perturbing measurement of the observable P_x, storing the result in the output variable O. What will happen if M is presented with an instance of **S** prepared to have the attribute $y \in P_y$, so that P_x need not be sharp?

That is up to the relevant subsidiary theories, and might be different for different instruments M. But the principles of constructor theory place constraints on what the subsidiary theories can say. Because of the determinism required by the basic principle of constructor theory, the effect of M when presented with y must always be the same:

$$\begin{aligned} (x, x_0) &\rightarrow (x, x) \\ (\bar{x}, x_0) &\rightarrow (\bar{x}, \bar{x}) \\ (y, x_0) &\rightarrow (f(y), g(y)) \end{aligned}$$

where $f(y),\ g(y)$ are (not necessarily intrinsic) attributes.

We first note that the *output variable must not always be sharp*, when the input observable X is not: $g(y) \notin O$. For, if $g(y) \subseteq x \in O$, y would be distinguishable from $\bar{x}$, contrary to our previous result that no pair of attributes $x \in P_x$, $y \in P_y$, is distinguishable. Similarly if $g(y) \subseteq \bar{x}$.

Recall now that the value of an observable X is *predictable* (supposing a given subsidiary theory to be true) if some statement of the form "X will have value x" is consistent with the relevant subsidiary theory. What we have just proven implies therefore that the value of the output variable O of a measurement of X is unpredictable when the input variable X is not sharp.

That raises the issue: when a subsidiary theory predicts that the outcome of a measurement will be non-sharp and indeed non-predictable then, given the requirement that a test must have a sharp outcome, how is that prediction

to be tested?

By repeated measurements on multiple instances of the substrate. For example, the Born rule in operational Quantum Theory assigns a probability to the outcomes of individual measurements. Repeated measurements on independent systems have uncorrelated probabilities, and hence the predicted aggregate outcome can always be made as sharp as desired (short of perfection). The same holds in the general case in Constructor Theory: because of the results of Section 3.6, Constructor Theory requires a sequence of identical experiments starting from generic substrates to converge to a sharp outcome.

Irreducible perturbation caused by measurement

Can the measurement M of P_x, as defined in the above section, be guaranteed to be non-perturbing when $y \in P_y$ is the input? Suppose it were, so that $f(y) = y$. By applying M an unlimited number of times to the same instance of $\mathbf{S}_1$, recording the output in successive instances of $\mathbf{S}_2$, one would approach arbitrarily closely the effect of performing

$$\begin{aligned} \left(x, x_o^{(\infty)}\right) &\rightarrow \left(x, x^{(\infty)}\right) \\ \left(\bar{x}, x_o^{(\infty)}\right) &\rightarrow \left(\bar{x}, \bar{x}^{(\infty)}\right) \\ \left(y, g(y)^{(\infty)}\right) &\rightarrow \left(y, x_o^{(\infty)}\right) \end{aligned} \tag{3.4}$$

By the property of ensembles, for each of the $z \in O$, we have only two possibilities. Either $g(y)^{(\infty)}$ is distinguishable from $z^{(\infty)}$, thus implying, by the possibility of the above task, that y is distinguishable from the corresponding attribute $z \in P_x$, which, as I showed in the previous section, is a contradic-

tion; Or $g(y)^{(\infty)}$ is not distinguishable from $z^{(\infty)}$, so that, by the properties of ensembles, it follows that $g(y) \subseteq z$, thus implying that y is distinguishable from the attribute $\bar{z}$: this, once more, is a contradiction. Hence *it is impossible for any instrument that would perform an accurate, non-perturbing measurement of P_x to leave the attributes in P_y unchanged.*

Moreover, the change must be *irreducible*: i.e., y cannot be restored while keeping the measurements result unchanged. Were it reducible, while keeping the measurement outcomes unchanged, the overall effect of the measurement plus the effect of the reducing operation would constitute a measurement of the kind just proved impossible.

3.8 Coherent computation in superinformation media

Definition 3.8.1 *Let* **M** *be a superinformation medium with information variables X and Y. A supercomputation is a physical transformation that maps the union $S = X \cup Y$ to itself. A computation Γ on any subset S' of S is* **coherent** *with respect to S if it is performed in a way that is reversible on S, i.e. where there exists a $1:1$ task A whose restriction to the domain S' is Γ and whose legitimate input set contains S, with both A and its transpose possible with side-effects: $\mathrm{A}^{\swarrow}$ and $\big(\tilde{\mathrm{A}}\big)^{\swarrow}$.*

Thus, given a super-information medium **M** with variables X and Y, the computation Π on X can be performed coherently with respect to $X \cup Y$ if there exists a pair of constructors, one capable of performing a logically

reversible (i.e., 1:1) task on the union $X \cup Y$ that contains the permutation Π, and the other its transpose task. These tasks are coherent supercomputations. For example, in a universal quantum computer all the reversible classical computations in some computation basis can be performed; and the quantum computer is capable of performing certain coherent supercomputations (quantum computations) on the set of all pure states of the qubits.

Performing a coherent computation with respect to a variable S of a substrate $\mathbf{M}$ means performing it without irreversibly modifying any other physical substrate $\mathbf{A}$. Any such modification would constitute a *decoherent* interaction between $\mathbf{M}$ and $\mathbf{A}$, which would make some degrees of freedom of $\mathbf{A}$ come to depend on those of $\mathbf{M}$, and hence, in our picture, some information about $\mathbf{M}$ be copied into $\mathbf{A}$, or vice-versa. Such an interaction would therefore be, in our information theory, a kind of process that distinguishes the states of $\mathbf{M}$. (Indeed, decoherence processes in quantum systems can be regarded as measurements of the quantum system by the environment [30]).

3.8.1 Locally inaccessible information

When considering the composite system of two instances of superinformation medium $\mathbf{M}$ on which coherent computation can be performed, an *additional notion of distinguishability* becomes relevant. For two distinguishable attributes of $\mathbf{M} \oplus \mathbf{M}$ may not be distinguishable by "local means" only. I therefore introduce a purely constructor-theoretic notion of "locally distinguishable" attributes. Note that this will turn out to be interestingly different from the notion of "distinguishable by local measurements and classical

communication" that is used in existing quantum information theory.

Definition 3.8.2 *The information variable* $\Sigma = \bigcup_j Q_j$ *of the medium* $\mathbf{M}_A \oplus \mathbf{M}_B$ *is* **locally distinguishable** *if and only if the following condition holds (or the same with* A *and* B *exchanged): there exist distinguishable sets* X *of* $\mathbf{M}_A$ *and* Y_x *of* $\mathbf{M}_B$*,* $\forall x \in X$*, with the property that*

$$\Sigma = \bigcup_{x \in X} \bigcup_{y \in Y_x} (x, y) \ .$$

Note that X and Y_x in general have cardinality smaller than Σ, and different attributes $y \in Y_x$ and $w \in Y_{x'}$ are not distinguishable when $x \neq x'$.
If the information variable Σ is locally distinguishable, it is possible to distinguish between its attributes even in a situation where direct interaction between $\mathbf{M}_A$ and $\mathbf{M}_B$ is forbidden and *only information* can travel between A and B. I shall explicate this by restricting attention to the situation where the distinguishable sets X and $\{Y_x\}$ are measurable (but not necessarily in a non-perturbing way). This simplifies the notation and, as I shall note, does not lose any generality. Under these conditions, the network in figure 3.8.1 is possible (with side effects), where:

- Between time $T = 0$ and $T = 1$ the preparation of the set Σ takes place, controlled by the information held at location C: at time T=1 the information medium $\mathbf{M}_A \oplus \mathbf{M}_B$ is in one of the states Q_j, selected according to the value j stored in the information medium $\mathbf{M}_C$.

- The arrow labelled by X represents the task of measuring the variable X using a target information medium $\mathbf{N}_A$ with information variable

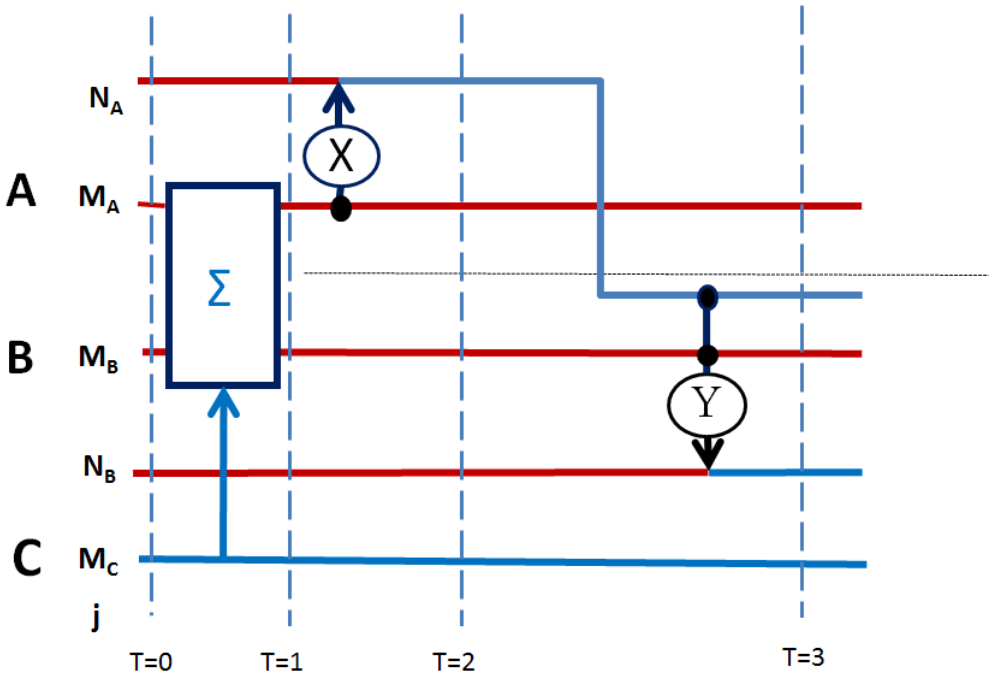


Figure 3.2: Network to distinguish locally the set Σ. The blue lines represent information media holding a sharp value of an information variable. The circled arrows represent tasks whose input and output are states holding a sharp value of an information variable. After $T = 1$ direct interaction between $\mathbf{M}_A$ and $\mathbf{M}_B$ is forbidden.

X_2:

$$\bigcup_{x \in X} \{(x, x_0) \to (s_x, x)\}$$

where x_0 is a generic receptive attribute.

- The arrow labelled by Y represents the algorithm of measuring the variable Y_x if the ancilla $\mathbf{N}_A$ holds the value x, $\forall x \in X$, i.e. of performing, for each x, the task:

$$\bigcup_{y \in Y_x} \{(y, x_0) \to (s_y, y)\}$$

where Y_{x2} is the information variable of the target medium $\mathbf{N}_B$ which stores the outcome y of the measurement.

The network distinguishes between the states in $\Sigma \doteq \{Q_j\}$ via first performing the task X locally on $\mathbf{M}_A$, and then via causing, by communicating the attribute x in the **information variable** X, the (local) task Y_x to be performed on $\mathbf{M}_B \oplus \mathbf{N}_B$[4]. The substrate $\mathbf{N}_A \oplus \mathbf{N}_B$ emerges from the network in the attribute (x, y_x) corresponding to the attribute Q_j prepared at the outset, thereby holding the information to distinguish the set Σ.

It is illuminating to highlight the difference between **communication via an information variable**, which is used in our definition of "locally distinguishable", and what in Quantum Theory is known as "classical communication", that I shall refer to as "communication via a decoherent channel" (such as the one that is used in teleportation). To explicate the difference, let me consider the algorithm 3.8.1 in Quantum Theory.

Each of the above information media at location A and B are qubits, initialised to a fixed blank state that is the simultaneous +1-eigenstate of their z-component operators. One of a set of orthogonal states $\Sigma = \{\ |Q_j\rangle\}$ of the two qubits $\mathbf{M}_A$ and $\mathbf{M}_B$ is prepared the according to the information j held at location C .

The conditions for local distinguishability via an information set require the qubit $\mathbf{N}_A$ to hold, after the measurement X, a value that **is predictable** by an agent that knows the information stored at location C. In quantum-mechanical terms, the ancilla $\mathbf{N}_A$ must hold a sharp value of the observable

[4]Note that one can perform the same analysis supposing distinguishability (instead of measurability), by adding one copy operation from the medium $\mathbf{M}_A \oplus \mathbf{N}_A$ to another ancilla $\bar{\mathbf{N}}_A$ and using the latter to perfom the communication via an information set.

used to control the unitary corresponding to Y: the state of the medium must be an eigenstate of the observable instantiating the information being communicated. (States that are not eigenstates, but are imagined to "collapse" to them, do not of course qualify, as I shall explain). The information about which of the states was prepared is then retrieved **by measuring a physical variable of the joint system $\mathbf{N}_A \oplus \mathbf{N}_B$**, after $T = 3$.

Instead, in the usual discrimination protocol "via local operations and classical communication" (LOCC) the ancilla $\mathbf{N}_A$ is only required to be a generic decoherent channel (i.e., the protocol is required to work no matter how many times the substrate $\mathbf{N}_A$ is measured), as distinct from holding a sharp value of the observable used to control the measurement on the other party.

The difference between the two kinds of decoherent communications is manifest when one considers the task of discriminating two orthogonal states of a bipartite system, describing entangled qubits. As explained in [31] it is always possible for any two orthogonal states to be discriminated via LOCC, and so is it in the case considered. Indeed, it is always possible to write the two orthogonal states as

$$|Q_1\rangle = |0_X\rangle\,|0_{Y_0}\rangle + |1_X\rangle\,|0_{Y_1}\rangle \ , \ |Q_2\rangle = |0_X\rangle\,|1_{Y_0}\rangle + |1_X\rangle\,|1_{Y_1}\rangle$$

where $\langle 0_p|1_p\rangle = 0$ (and the states are not necessarily normalised), with $p \in \{\mathrm{X},\ \mathrm{Y}_0,\ \mathrm{Y}_1\}$ denoting some appropriate basis.

One could therefore discriminate the two states by the algorithm represented in figure 3.8.1.

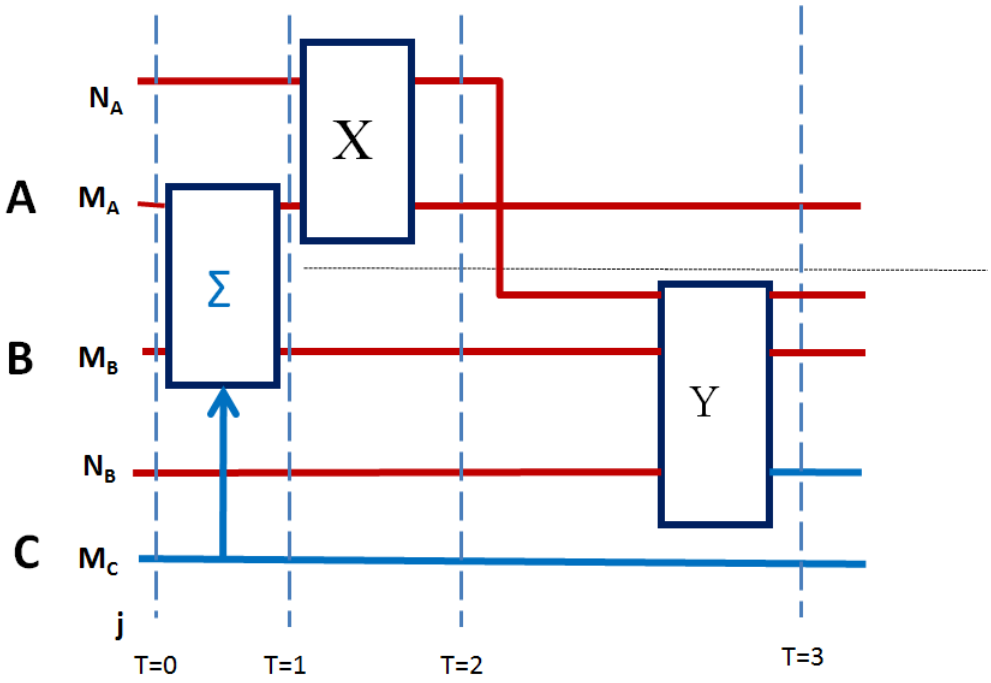


Figure 3.3: Network to distinguish the set Σ by sending a qubit $\mathbf{N}_A$ via a decoherent channel. No direct interaction between $\mathbf{M}_A$ and $\mathbf{M}_B$ is allowed after $T = 1$.

In that algorithm one first performs the measurement X in the basis $\{0_X,\ 1_X\}$: the qubit $\mathbf{M}_A$ is the source and $\mathbf{N}_A$ is the target. This operation is denoted by a rectangle because it is involves, unlike in 3.8.1, a physical substrate, not information: the observable of qubit $\mathbf{M}_A$ corresponding to X is **not** sharp. Then the qubit $\mathbf{N}_A$ is sent to location B, where one performs the measurement Y in the basis $\{0_{Y_x}, 1_{Y_x}\}$ of $\mathbf{M}_B$ with $\mathbf{N}_B$ as a target, controlled by value x of the z-component of the ancilla $\mathbf{N}_A$. Once more, this unitary operation has in input a physical substrate, not information: the z-component of the ancilla $\mathbf{N}_A$ is not sharp at $T = 2$. However, the z-component of the qubit $\mathbf{N}_B$ is sharp at time $T = 3$, with value 1 if the initial state was Q_1 and 0 otherwise.

However, those two states cannot be locally distinguished under the constraint that the communication happen via an information variable: indeed, when applying the LOCC protocol, the ancilla $\mathbf{N}_A$ holds, for a fixed state $|Q_j\rangle$, a value that is unpredictable even to an agent in C, who knows which state $|Q_j\rangle$ that has been prepared. In other words, $\mathbf{N}_A$ is not in an information state: it does not instantiate one bit of information (but, in the language of [22], it carries the physical key to retrieve it). It is interesting to point out that this subtle difference between communication via a decoherent channel, used in teleportation, and communication via an information variable breaks the analogy between teleportation and superdense coding, which has from time to time been proposed (see, for instance, [32]). In super-dense coding two bits of information are used, while in teleportation what is communicated are not two bits of information, but two qubits in a decoherent channel.

Definition 3.8.3 *Distinguishable sets that are* **locally not distinguishable** *contain* **locally inaccessible information**.

By showing that super information media, when involved in appropriate coherent computations, can contain locally inaccessible information, I shall now attain our objective of showing that super-information media exhibit many of the distinctive properties of quantum-information media. Note that it is possible to prove that when two quantum systems are entangled then they contain locally inaccessible information [22]. More generally, all phenomena that have been purported to exhibit the feature of quantum non-locality in composite quantum systems (such as teleportation and the Bell experiment) can be demonstrated to be due to the existence of locally inaccessible infor-

mation, that is "stored in the correlations between the subsystems" of the quantum system [22] in the context of Everettian Quantum Theory. Also the phenomenon known as " non-locality without entanglement", [33] can be understood in terms of locally inaccessible information.

Coherent measurement of a non-sharp boolean observable produces locally inaccessible information

Consider the super-information medium $\mathbf{M}$ with the two boolean observables $P_x = \{x, \bar{x}\}$ and $P_y = \{y, \bar{y}\}$, as defined in the section 3.7.4 (recall, in particular, that $\bar{\bar{x}} = x$, $\bar{\bar{y}} = y$, and that we proved that no pair of attributes $a \in P_x$, $b \in P_y$ can be distinguishable).

Consider the computation $T_{M_{P_X}}$ on the information variable $P_x \times O$ of the medium $\mathbf{M} \oplus \mathbf{N}$ corresponding to the perfect measurement of P_x, where $\mathbf{N}$ is the target ancilla holding the outcome of the measurement in the output variable O. [5] Suppose there is a perfect measurer that performs $T_{M_{P_X}}$ as a coherent computation with respect to the variable $P_x \times O \bigcup P_Y \times O$. I shall now prove that this constructor, when prompted with any attribute $y \in P_Y$, produces two-fold information variables of $\mathbf{M} \oplus \mathbf{N}$ that are not locally distinguishable, and hence contain locally inaccessible information[6].

[5] The task $T_{M_{P_X}}$ can be identified with the the controlled NOT operation on $P_X \times O$

[6] Note that the sets associated with locally inaccessible information without entanglement (containing the (separable) sets of quantum states constructed in[33]), necessarily have two-fold information subsets that are locally distinguishable.

Since the measurement is coherent, the task

$$\begin{aligned} \mathrm{T} = \{(x,x) &\rightarrow (x,x),(\bar{x},x) \rightarrow (\bar{x},\bar{x}), \\ (\bar{x},\bar{x}) &\rightarrow (\bar{x},x),(x,\bar{x}) \rightarrow (x,\bar{x}),(y,x) \rightarrow (f(y),g(y))\} \end{aligned}$$

is possible with side-effects and so is its transpose. Here, $\psi_y \doteq (f(y), g(y))$ is an attribute of the combined system that is distinct from any of the attributes in $P_X \times O$ (by definition of coherent computation). From now on, for simplicity of notation, we shall denote (a, b) simply by ab. The set $A = \{yx, \bar{x}\bar{x}, x\bar{x}\}$ is a distinguishable set. (This follows from the fact that $\{x, \bar{x}\}$ is a distinguishable set.). Also, all the attributes in A can be prepared from generic resources. These two facts imply that A is an information variable. Hence, by theorem 3.10.3, since T and its transpose are both possible with side effects, the set $\Sigma \doteq \{x\bar{x}, \bar{x}x, \psi_y\}$ is an information variable. Consider now the subsets $\{x\bar{x}, \psi_y\}$ and $\{\bar{x}x, \psi_y\}$ of Σ (which are, in turn, information variables). I shall now argue that both of them are locally not distinguishable. Suppose indeed that either of those were locally distinguishable. If the set $\{x\bar{x}, \psi_y\}$ were locally distinguishable, then either $f(y) \perp x$ or $g(y) \perp \bar{x}$. In the former case $\{xx, \psi_y\}$ is a distinguishable set, which by the possibility of T implies that $\{x, y\}$ would be a distinguishable set, which contradicts the assumptions. In the latter case $\{\bar{x}\bar{x}, \psi_y\}$ would be distinguishable, and hence $\{\bar{x}, y\}$ is a distinguishable set, which, once more, is a contradiction with the assumptions.

By symmetry, the same contradiction is reached when $\{\bar{x}x, \psi_y\}$ is supposed to be locally distinguishable. Hence, the assumption must be false: both

$\{\bar{x}x, \psi_y\}$ and $\{x\bar{x}, \psi_y\}$ are information variables that are not locally distinguishable. Hence, they can be used to store locally inaccessible information. This proves the thesis.

Note that the situation just described is realized in Quantum Theory in the production of entanglement by the measurement of a non-sharp observable of a qubit. A fuller Constructor Theory is expected to implement further relations between attributes, which arise in Quantum Theory, such as that of y being an "equally weighted" superposition of x and $\bar{x}$, which would lead to a full correspondence with entanglement.

3.9 Concluding remarks

The Constructor Theory of Information I have just presented has expressed self-consistently the notion of information within physics, emancipating it from particular subsidiary theories. It has expressed its interoperability with an elegant principle, and explained how substrate-independence is reconciled with the fact that information must be instantiated in physical systems. Moreover, it has provided a beautiful unification between the theories of quantum and classical information (see figure 3.9); it has shown how unpredictability can arise from a deterministic theory, and has delivered a promising insight into concepts such as locally inaccessible information.
This theory relies only on the principles postulated for Constructor Theory itself (which are proposed laws of nature). I summarise below the definitions and principles upon which the theory of information relies:

- **Definitions in Constructor Theory**: Attribute, Variable, Task;

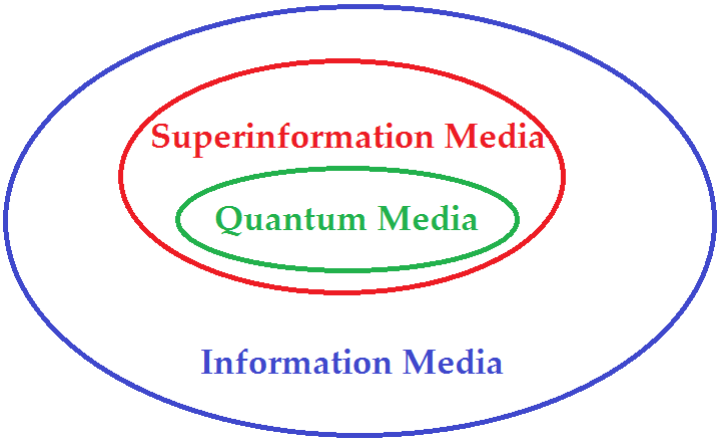


Figure 3.4: The hierarchy of Information Media according to the Constructor Theory of Information

Union, Serial and Parallel Compositions; Possibility (with side effects allowed); Generic Resources;

- **Principles of Constructor Theory**: Principle of Locality, Principle of Testability, The Composition Principle, the Interoperability Principle for Information; the principle about pairwise distinguishable sets being distinguishable; the principle that a preparable attribute and its complement form an information variable;

- **Definitions in the Constructor Theory of Information**: Permutation Task (as reversible computation); Replication Task; Computation, Information Variable; Computation, Information Medium; Distinguishable, Measurable; Complement; Observable, Boolean Observable; Locally Distinguishable; Ensemble; Ensemble-distinguishable; Superinformation Medium; Coherent Computation;

- **Principles of other branches of Physics** (subsidiary theories):

None.

The insight into the phenomenon of locally inaccessible information, conceived as analogues of quantum entanglement, seems to be particularly promising. Of course more elements have to be introduced in the theory to investigate the nature of quantum information. The first step would be to understand how to incorporate a full analogue of the notion of superposition of states, in order for different degrees of local not-distinguishability (corresponding to different degrees of entanglement) to be represented in our theory; furthermore, it will be important to develop the theory of observables, and investigate under what conditions observables of arbitrary cardinality can be constructed. I expect to address these issues in the developments of this thesis.

Within our theory of information one can speculate to be able to address new problems that in the current framework are impossible to even formulate rigorously. I mention here a few of these problems, as possible future developments, by way of providing context and motivation to this thesis (but they go well beyond its purposes).

Information is of the essence in preparation and measurement, both of which are necessary for testing scientific theories. (The output of a measurement is information specifying an attribute of the input system; the input of a preparation is information specifying an attribute and its output is a physical system with that attribute.) One therefore expects our theory to provide a foundation for expressing a theory of measurement within Physics, and ultimately to incorporate the principle of testability into it. Furthermore,

expressing quantum information as a special case of a generalisation of information would provide the tools to compare the former to the latter, in order to pin down the feature that makes quantum information-processing more powerful than classical information processing. It would also provide tools to address far-reaching questions, such as whether it is possible to simulate a universal quantum computer under any other dynamical laws than Quantum Theory, and how would those laws be different from Quantum Theory.

3.10 Appendix

Theorem 3.10.1 *If S is an information variable of an information medium* $\mathbf{M}$*, it is a measurable variable.*

Proof Let me consider the combined system $\mathbf{M} \oplus \mathbf{N}$ where $\mathbf{N}$ is another information medium with information variable $Z = \{z_i\}$, whose cardinality is at least that of S. By the Interoperability Principle, $\mathbf{M} \oplus \mathbf{N}$ substrate is an information medium too, with variables $S \times Z$. Hence, all permutation tasks over $S \times Z$ are possible with side-effects. Given that

$$M_S \doteq \bigcup_{x \in S} \{(x, s_0) \to (x, s_x)\}$$

is a 1:1 subtask of one of such permutation tasks, $\mathbf{M}_S$ is possible too. Hence the set S is measurable. Since $\{(x, s_x)\}$ is an information variable of the medium $\mathbf{M} \oplus \mathbf{N}$, from the definition of distinguishable set it follows that S is a distinguishable set too. ∎

Theorem 3.10.2 *If a set S_1 of states of a substrate $\mathbf{M}_1$ is a distinguishable set and a set S_2 is a distinguishable set of $\mathbf{M}_2$, then so is the set $S_1 \times S_2$ of states of the substrate $\mathbf{M}_1 \oplus \mathbf{M}_2$.*

Proof Let me pick the information media $\mathbf{N}_i$, $i = 1, 2$, with information variable Z_i, whose cardinality is, respectively, greater than or equal to that of S_i. Since S_i is a distinguishable set, the task

$$D_{S_i} \doteq \bigcup_{x \in S_i} \{(x, \bar{s}) \rightarrow (\psi_x^{(i)})\}$$

is possible with side-effects, where, for each $i = 1, 2$, $\{\psi_x^{(i)}\}$ is an information variable of $\mathbf{M}_i \oplus \mathbf{N}_i$. Hence, for all states $(x, y) \in S_1 \times S_2$, the task

$$D^* \doteq D_{S_1} \otimes D_{S_2} = \bigcup_{(x,y) \in S \times S} \{(x, \bar{s}, y, \bar{s}) \rightarrow (\psi_x^{(1)}, \psi_y^{(2)})\}$$

is possible. Since by the Interoperability Principle $\{\psi_x{}^{(1)}\} \times \{\psi_x{}^{(2)}\}$ is an information variable of the medium $\mathbf{M}_1 \oplus \mathbf{N}_1 \oplus \mathbf{M}_2 \oplus \mathbf{N}_2$, the possibility of D^* shows that $S_1 \times S_2$ is a distinguishable set. ∎

Theorem 3.10.3 *If X is an information variable of an information medium $\mathbf{M}$ and both T and $T^{\tilde{}}$ are possible (with side effects), where T is a 1:1 task that is defined as $T \doteq \bigcup_x \{x \rightarrow \psi_x\}$ for some set of states $\Sigma \doteq \{\psi_x\}$ of $\mathbf{M}$, then Σ is an information variable of X.*

Proof

Consider an arbitrary permutation Π, which is possible because X is an information variable. Since T is 1:1 and it is possible , $T\Pi T^{\tilde{}}$ is a permutation

task over the set $\{\psi_x\}$, and it can be performed by composing the corresponding constructors . The same applies to the cloning task $R_X[x_0]$: since the latter is possible, so is the replication task $(T \otimes T)R_X[x_0](T \otimes T)^{\tilde{}}$ over $\Sigma \otimes \Sigma$. Hence Σ is an information variable.

∎

Chapter 4

A Network Analysis of Cloning-Type Tasks

Abstract

I propose a unifying account of the notion of cloning a quantum state using the general method of analysis of quantum networks. This provides a deeper and more fundamental understanding of why the universal cloning is impossible in Quantum Theory, as well as a formulation of the no-cloning theorem that is not rooted in any particular picture.

4.1 Introduction

The fact that unitarity of Quantum Theory forbids the existence of a universal cloner, as stated by the no-cloning theorem [34], has always been considered as a distinctive, fundamental property of quantum systems. (Indeed, we have seen in chapter 3 that restrictions on the cloning task are what

provides superinformation media with additional properties.) Proofs of the no-cloning theorem and all the subsequent analysis have been carried out in the Schrödinger picture, and seem therefore to be rooted in that picture.

Inspired by the philosophy underlying Constructor Theory and the theory of information, I will provide an account of cloning which is not rooted in any particular picture, using the method of quantum networks. This analysis is unifying, because it provides an alternative proof of the no-cloning theorem which is suitable to both the Heisenberg and the Schrödinger picture.

This analysis will also be useful for the discussion about the quantum logic of self-replication, because the no-cloning theorem has been often mistaken for being a fundamental obstacle to the compatibility of the logic of self-replication (as it occurs in living entities) with quantum mechanics. As we shall see in chapter 5, this is not the case.

Furthermore, giving this task-oriented formulation of cloning is interesting in view of the plan of translating Quantum Theory into constructor-theoretic terms. Indeed, this chapter can be considered as developing some of the conceptual and formal tools to perform that translation.

4.2 The cloning task

Without loss of generality, let me restrict attention to the case of a 2-qubit system: indeed, if a universal cloner is possible, it must be - in particular - possible for a qubit.

I shall denote the descriptors (using the terminology of [22]) of the n-th qubit by $\hat{q}_n \doteq (q_{nx}, q_{ny}, q_{nz})$, $n = 1, 2$, where $q_{n\alpha}$ is the descriptor of the

α-component of the n-th spin, satifying the following relations: $q_{n\alpha}^2 = \mathbb{1}$, $q_{nx}q_{ny} = iq_{nz}$, and cyclic permutations, $[q_{n\alpha}, q_{m\beta}] = 0, \;\; n \neq m$.

Let me consider the rotation by ϕ about the axis $m = (m_x, m_y, m_z)$ of the i-th qubit, $M[q_i] = \exp(i\phi/2\; m.\hat{q}_i)$. As m,ϕ vary, this unitary applied to any state of qubit i, *considered as a single qubit*, describes all its possible non-entangled states. From now on M will be used as a multi-index, denoting the pair (ϕ, m).

As explained in chapter 3, the cloning task is always defined with respect to a set $S = \{M\}$. I am here interested in the universal cloning, i.e. in the case where M varies over all its possible values.

Consider the network in figure 4.1.

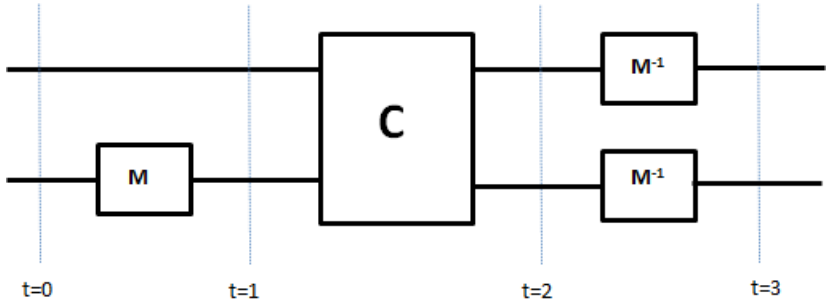


Figure 4.1: The operational definition of the cloning gate for a single qubit.

The universal cloning of a single qubit is possible if and only if there is a unitary transformation $C[\hat{q}_1, \hat{q}_2]$, whose functional form does not depend on M, that satisfies the network of constructions 4.1 with the constraint that the projector for both qubits to hold the value 1 must be sharp at time 0 and 3. I shall refer both to the unitary transformation specified by the above network and to the network itself as $M[C]$. The requirement that C not depend on M means that the state of the source qubit is unknown, and hence that C

must work for all M.

In order to intepret the network, let me analyse it in the Schrödinger picture. The conditions on the projectors can be expressed as:

$$\langle\psi(0)|\, q_{1x}\, |\psi(0)\rangle = \quad 1 \quad = \langle\psi(0)|\, q_{2z}\, |\psi(0)\rangle \tag{4.1}$$

$$\langle\psi(3)|\, q_{1z}\, |\psi(3)\rangle = \quad 1 \quad = \langle\psi(3)|\, q_{2z}\, |\psi(3)\rangle \ . \tag{4.2}$$

Thus, since 1 is an extreme eigenvalue of both q_{1z} and q_{2z} , condition (4.1) requires the initial state $|\psi(0)\rangle$ to be a simultaneous eigenstate of both q_{1z} and q_{2z} with eigenvalues 1: $|\psi(0)\rangle = |\mathbf{0}\rangle$.

Then, at time 1, the preparation of the source qubit takes place: $|\psi(1)\rangle = M[\hat{q}_2]\,|\mathbf{0}\rangle$. As M varies in the specified range, the rotation gate prepares the source qubit in the single-qubit states belonging to the set to be cloned. The receptive qubit remains in the 0 state.

At the other end of the network, condition (4.2) requires $|\psi(3)\rangle = |\mathbf{0}\rangle$, so that $|\psi(2)\rangle = M[\hat{q}_1]M[\hat{q}_2]\,|\mathbf{0}\rangle$. Therefore, $C[\hat{q}_1, \hat{q}_2]$ satisfies the network if and only if it performs the task $M[\hat{q}_2]\,|\mathbf{0}\rangle \longrightarrow M[\hat{q}_1]M[\hat{q}_2]\,|\mathbf{0}\rangle$, for all M, which resembles the usual formulation of the cloning task. [1] Note that, even though the analysis has been carried out in the Schrödinger picture, this network formulation is picture-independent, as it relies only on constraining projectors. Hence, the same analysis can be carried out in the Heisenberg picture.

[1] I am here concerned with presenting a particular method of analysis of the cloning task, and hence one can restrict the analysis to cloning transformations that do not use ancillas.

It is also worth mentioning that condition (4.1) requires the initial state to be a pure state. This does not lose any generality, because this is precisely the situation that is of interest in the no-cloning theorem. For if the two qubits are entangled at the outset, then the receptive qubit contains already an explicit dependence on the descriptors of the source qubit.

Note also that fixing the intial state of the receptive qubit to a particular state $|0\rangle$ does not lose any generality. Since the initial state is independent of M, the possibility of C does not depend on which particular state that is. For if a cloner C existed for that particular intial state, then $U^\dagger CU$ would be a cloner for the state of the receptive qubit obtained acting with U on that particular initial state $|0\rangle$.

4.2.1 No-Cloning theorem revisited

At time $t = 0$, the projector $P_{0,0} \doteq \frac{1}{4}(\mathbb{1} + q_{1z})(\mathbb{1} + q_{2z})$ is sharp with value 1. Let me denote by $U \doteq U[\hat{q}_1, \hat{q}_2]$ the unitary that expresses the form of state of the qubit at time 3 as functions of the state at time 0:

$$|\psi(3)\rangle = U\,|\psi(0)\rangle$$

Equations (4.1),(4.2) are equivalent to requiring that

$$U[\hat{q}_1, \hat{q}_2]P_{0,0} = P_{0,0}\ .$$

This condition, plus the requirement that U be unitary, constrains the func-

tional form of U as a function of the operators of the Pauli group on 2 qubits. Let me define the space of solutions of the above equation

$$\mathcal{S} \doteq \{U \ : \ UP_{0,0} = P_{0,0}\} \ .$$

By picking the representation $\hat{q}_{1\alpha} = \sigma_\alpha \otimes \mathbb{1}_2$, $\hat{q}_{2\alpha} = \mathbb{1}_2 \otimes \sigma_\alpha$, $\alpha \in \{x, y, z\}$, where the σ_α are the standard Pauli matrices, one has that $U \in S$ must be of the form

$$U \equiv \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & w_{11} & w_{12} & w_{13} \\ 0 & w_{21} & w_{22} & w_{23} \\ 0 & w_{31} & w_{32} & w_{33} \end{pmatrix}$$

where the matrix W is required to be unitary. In this form, it is manifest that the unitaries in $\mathcal{S}$ are all the ones which preserve the state $|\mathbf{0}\rangle$.

A universal cloner exists if there is a unitary C, whose functional form does not depend on M, such that $M[C] \in \mathcal{S}$ for all M.

It is immediate to prove that a fixed unitary C satisfying that equivalence for all q-values of M cannot exist, thereby proving the no-cloning theorem. Suppose such a unitary C existed. It would satisfy $M[C] \in \mathcal{S}$ for all M, and, in particular, it should satify it for $M = \mathbb{1}$, which would immediately imply $C = U$ for some $U \in \mathcal{S}$. Hence, for all M, one should also have $M[U] = U'$ with $U, U' \in \mathcal{S}$. However one can easily show that there are M that do not preserve the space $\mathcal{S}$. For example, one can consider $M[\hat{q}_i] = \frac{1}{\sqrt{2}}(q_{ix} + q_{iz})$ (i.e., the Hadamard gate on qubit i): using the standard representation, one

can see that $M^\dagger[\hat{q}_2]M^\dagger[\hat{q}_1]UM[\hat{q}_2]$ does not belong to $\mathcal{S}$, for a generic $U \in \mathcal{S}$, unless U is explicitly chosen to meet the criterion for that particular M. But this would mean that C contains an M dependence, which is not allowed. Hence a unitary C that satisfies this network for all M cannot exist.

4.3 Concluding remarks

This operational, task-like formulation of the concept of cloning has provided a unified description of the cloning tasks: both the universal and the restricted cloning (i.e., when one is interested in cloning only a restricted set of states M) can be defined by the same network. Also, since it is picture-independent, it can be readily translated in the Heisenberg picture.

As future work, one could ask, in this framework: what is maximal set of M such that there is a unique gate C that satisfies the conditions (4.1),(4.2) ? More specifically, suppose that there were a unitary gate C that satisfies the network for a set of rotations $\{M_i\}_{i\in Z}$ (that do not preserve the state $|0\rangle$): using the notation introduced above, one would have $M_i(C) = U_{M_i}$, $\forall i \in Z$, for some (not necessarily distinct) $U_{M_i} \in \mathcal{S}$. What are the permitted $\{M_i\}$? Answering this question requires to classify the unitaries in $\mathcal{S}$. I conjecture that they can be described by the identity, the swap gate, and the perfect-measurement gate of qubit 1, by qubit 2 (and viceversa), up to some unitary transformation: the only clonable sets of M_i's correspond either to single states or to orthogonal pairs.

Chapter 5

The Logic of Self-replication under Quantum Theory

Abstract

The logic of self-replication as it occurs in living entities has been claimed to be incompatible with quantum mechanics, notably by Wigner. Were these claims true, quantum mechanics would not be a universal theory and it would need to be complemented with additional laws. I argue here that the arguments in support of these claims are invalid and I provide a proof that the logic of self-replication is, of course, compatible with quantum mechanics.

5.1 Introduction

The question of whether the characteristic properties of living entities are compatible with Quantum Theory, one of our most fundamental theories,

was first posed by Schrödinger [4]. It is remarkable that, even in the scientific community, this question has sometimes been addressed via what Dawkins called "arguments by incredulity" [35]; that is to say, arguments based on the amazement before the contrast between the simplicity of the elementary components of inert matter and the appearence of design in living entities. As we know, this contrast has been explained by Darwin's theory of evolution, but the "incredulity-driven" attitude is still quite popular. This attitude has affected, in particular, the debate about whether one specific feature of living entities, i.e., the ability to self-replicate, is compatible with Quantum Theory.

Specifically, Wigner, [8], and other quantum physicists , [5],[6], [7], have proposed arguments to support the claim that the logic of self-replication, as it occurs in living entitites, is incompatible with Quantum Theory. Different meanings have been given to the term incompatible, as I shall explain later. But no matter what shade of meaning, those claims, if true, constitute a serious challenge to the universality of Quantum Physics. Were those claims true, a set of different laws from quantum mechanics would be needed to explain the observed existence of living entities; or, to put it in another way: living entities would be a counterexample to quantum mechanics being a universal theory. In fact, this is how they have been interpreted [1]. This issue has also bearing on the question of whether quantum coherence could be exploited by biological systems, which has recently come to the fore after compelling empirical evidence, [12], [13]. To make progress in this process

[1]For example, in 1974 H. Yockey quoted Wigner to support the claim that "for all physics has to offer, life should never have appeared and if it ever did it would soon die out." [9]. See also the article [36].

of unification between biology and fundamental physics it is necessary to assess the validity of these alleged no-go theorems about the compatibility of self-replication, and quantum physics.

In this work I show that the proposed arguments are invalid, or irrelevant to the question, and that the logic of self-replication, as envisaged by von Neumann, [10], [11] is in fact permitted by Quantum Theory.

The recently proposed Constructor Theory gives the conceptual framework in which to formulate and fruitfully address this problem.

5.2 The algorithm of self-replication

The logic of self-replication as it occurs in living organisms is available in theoretical biology [37], [38, 39], [40]. I will refer to that specific notion, confining the present analysis, without loss of generality, to organisms that do not rely on the existence of other organisms in their environment to reproduce themselves. In fact, life is possible if and only if such organisms are possible. For the sake of exposition, I shall consider a simplified world that is a collection of replicas of the same elementary unit, a physical system **Q**. The ambient space of self-replication is divided into three parts: 1) the constructor space **C**, where the parent self-replicator lives, composed of d units **Q**; 2) the substrates space $\mathbf{S} \oplus \mathbf{A}$ made of a cluster of d units, **S**, (that will contain the child instance of the self-replicator) and another cluster of a units, **A**, (that will contain the waste product of the self-replication process); 3) the rest of the world, which is a reservoir containing a number of **Q** that, in order for self-replication to continue over many generations, will be generically

supposed to be very large compared to $d + a$.

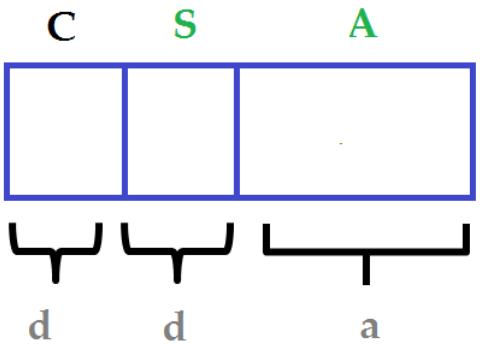


Figure 5.1: Partition of the ambient space into the constructor space (C) and the substrates space (S, A).

I shall only consider processes which do not change the identity of the elementary constitutents of the world (each **Q** remains a **Q**), but change their attributes. This assumption is acceptable because I want to analyse only the logic of self-replication.

Let M denote the attribute of being a particular constructor. I shall loosely refer to the subsystem **C** with the attribute M as "the machine M". The **replication task** on the system $\mathbf{C} \oplus \mathbf{S} \oplus \mathbf{A}$ is defined as

$$R_M = \bigcup_W \{(M, G, G) \to (M, M, W)\} \tag{5.1}$$

for some fixed attribute G of $\mathbf{S} \oplus \mathbf{A}$, and any attribute W of **A**, representing waste products. The above attributes should be intended as defined in chapter 2, as sets of states. In particular, when specialising to quantum systems, we shall see that those attributes are associated to projectors; also, the attribute (M, M, W) may correspond to the situation where the constructor, the substrates and the waste are entangled.

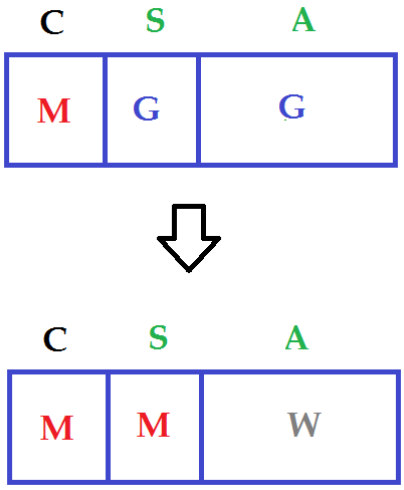


Figure 5.2: The replication task R_M. Self-replication of M is a particular mode of performing this task, where: $\mathbf{S} \oplus \mathbf{A}$ is a generic environment; the laws of motion do not contain the design of M; M contains adaptations; $\mathbf{C} \oplus \mathbf{S} \oplus \mathbf{A}$ may be isolated.

The task R_M of replicating the machine M can be performed in many ways: the substrates of the transformation may contain a copier for an M, for instance. However, *self-replication* is the algorithm of performing the replication task with the constraint that the construction of the new instance of M is caused by M only, and by nothing else in the environment. More specifically, self-replication is an algorithm to perform the task R_M, with the following constraints:

- The tranformation (5.1) can happen when $\mathbf{C} \oplus \mathbf{S} \oplus \mathbf{A}$ is isolated. In constructor-theoretic terms, this means that it is caused by a clock, which can be considered as a timer, set to some finite time t. Its being required to be the only constructor for the process is equivalent to requiring that the whole transformation be spontaneous.

- The network is embedded in a world whose laws do not contain the

design of M. This means, for example, one cannot have a law of the form "and now an M appears".

- The substrates contain the raw materials necessary to construct M, but *do not contain any knowledge*[2] (or artifacts embodying knowledge) about how to construct an M. For instance, they cannot contain a copier. This requires the attribute G to be generic, in the sense defined in chapter 3 [3].

As explained in chapter 2, requiring this algorithm to be possible implies requiring that each step of that algorithm can be performed *with arbitrary accuracy* and it *can be stabilised* under the laws of Physics in question.

At the end of the process there must be at least two instances of M: in the case of binary fission, there would be the parent and the offspring plus some waste W[4].

I am interested in the case where M contains adaptations: in other words, most of the objects containing small variations with respect to M would not satisfy the network. Hence, a layer of crystal would not satisfy this definition: for, while the crystal grows, dislocations and imperfections of a crystal layer do not prevent it from being copied, and are passed onto the next layer. On the other hand, in order for evolution to be possible, that process must be allowed not for a single M, but for a set of different machines $\{M\}$, each one

[2]Knowledge here is intended in the sense set by Popper [16]: knowledge without a knowing subject. It could be understood to mean "relevant information".

[3]An unlimited supply of copies of such an attribute are available in nature.

[4]It is sufficient to our purposes to neglect many of the subtleties occurring in actual self-replicating organisms. For instance, in actual organisms semi-conservative replication occurs: each instance of M would contain one DNA strand from the parent, and one newly constructed DNA strand.

differing only slightly from the others. In this work I shall bear this fact in mind, but since I am focusing on the logic of self-replication only, I shall not address the issue of evolution explicitly.

So far I have not yet appealed to any specific subsidiary theory. It is remarkable that the problem of understanding whether this algorithm is compatible with a particular subsidiary theory, specifically Quantum Theory, is a problem that requires an approach that is not theory-laden, for it exists at a deeper level of abstraction than that one pertaining to a specific subsidiary theory. There is a similarity between this problem and, for instance, the problem of understanding what are the theories that allow a computing machine that can emulate a universal quantum computer. These are problems that cannot be addressed within a specific subsidiary theory, but nevertheless pertain to Physics, and hence require Constructor Theory to be rigorously formulated.

The purpose of this work is precisely to show that a specific subsidiary theory, i.e., quantum mechanics, *allows* the algorithm of self-replication to be performed. In order to do so, I shall follow this logic:

- Building on von Neumann's original argument, I shall argue that an evolvable, stable self-replicator must be a programmable (i.e., code-based) one;

- I shall then formalise the algorithm of self-replication in Quantum Theory; explain why Wigner's argument is invalid and show that under Quantum Theory it is possible to accommodate the logic of self-replication. (Note, however, that this does not entail showing that

Quantum Theory *requires* the logic of self-replication to be possible, or to be performed in a particular way.)

5.3 von Neumann's replicator-vehicle logic

To investigate the foundations of theoretical biology, von Neumann set the problem of self-replication in the Hixon Symposium paper [10]. There, he gave an informal definition of self-replicator, as a machine M that can construct a copy of itself within an environment containing all the relevant raw materials. This machine would, in particular, perform the replication task R_M. Building on this definition, he sketched a proof that a self-replicator must be a programmable constructor executing a program P_M with *two steps*: one is to construct a new instance of M with a blank tape, according to the instructions contained in P_M; the other is to copy the program on the tape of the new instance.

I will now provide an argument to support von Neumann's claim relying on the (more accurate) notion of self-replication I defined in the previous section. My argument concurs with von Neumann's one, but aims at being more tight; it also improves on it in some steps, that I shall highlight.

Specifically, I shall argue that if M is a self-replicator then necessarily it is a programmable constructor $M[\ ]$ that is programmed with a program P_M including the two instructions: 1) Copy the content of the tape 2) Construct an $M[\ ]$. Adopting the terminology introduced by Dawkins, [38], this logic will be referred to as the **replicator-vehicle logic**. The program is the replicator, which uses the constructor $M[\ ]$ as a vehicle to accomplish its

replication. The composite object $M[P_M]$ is then said to self-replicate.

Let me first argue that M must be a programmable constructor executing some program P. For in the self-replication algorithm a self-replicator has to be its own user: nothing in the environment can present M with the instructions of what to do, by the definition. Hence, it must contain a program P: $M = M[P]$ for some program P.

It follows that, whatever the content of the program, it must be copied.

I shall now argue that the program must contain *all the knowledge about* M for self-replication to occur in an environment that does not contain the knowledge about how to construct M and under laws that do not contain its design. In other words, the replication happens by following a complete sequence of instructions in the program, and not merely via M looking at itself and constructing a new M on the ground of the information gained by this self-inspection (i.e., by self-copying).

First, notice that the program P may either contain some knowledge about M, or may not do so. Suppose the latter is the case. Then, P will be a simple sequence of instructions executed by a control unit $H[P]$ to the end of coordinating the other parts of M that perform different subtasks:

- K, a copier, which copies the program;
- C, which directly copies the organism, elementary constituent by elementary constituent; for example, one might in principle imagine that it is constituted by something like a (3D) raster scanner, O, that scans the organism, and a constructing arm, A, which constructs the new instance according to the information provided by the scanner.

- F, a unit that fetches raw materials when needed.

Unlike what von Neumann speculated, the problem of this configuration is not that O could not look at $M[P]$ while $M[P]$ is moving, nor that O cannot look at itself. For as a matter of logic, the scanner could do both things by, for example, producing a probe (e.g., a beam) to scan the whole of M[P], including itself (supposing an appropriate scaling of the characteristic times of the motions of $M[P]$, O and of the beam produced by O).

The problem is that this process of construction could not be stabilised and hence could not evolve. Note first that any construction process is, in general, prone to errors. Some errors can be harmful, some others may be neutral or beneficial. Let me consider the harmful ones. From theoretical biology, we know that the rate of harmful mutations in self-replication of actual organisms must be less than about one per genome per generation, otherwise natural selection is not powerful enough to remove them, and so the species suffers an "error catastrophe" [41]. Indeed the mutation rate limits the genome size (and hence the complexity of the species in question). Natural selection alone (without any error correction that keep the mutation rate below the critical value for any length of the genome) would therefore not be enough to achieve boundless evolution, to arbitrarily complex species. Hence, a mechanism of error-correction is needed to ensure (unlimited) evolution.

Could the above construction be reliably error-corrected? No, because the scanning-copying function is analogue. In analogue processes, the output can never be more than partially right, and hence errors cannot be detected

effectively. [5] Hence, the construction must be executed not by scanning and copying, but by executing a sequence of digital instructions, whose copy can be error-corrected.

This means that P must code for these instructions, containing complete knowledge about how to construct a new $M[\ ]$: if it does not, the self-replication may occur once, but it would be unstable - hence M could not satisfy our definition of self-replicator. (The same argument applies in case P contains only partial knowledge about $M[\ ]$, and the rest of the knowledge is instantiated only in the hardware of the vehicle. The latter could not be error-corrected and would be lost in few generations.) Note that in the vehicle there can of course be knowledge - which could be extracted by a process of reverse-engineering [6]. What I argue here is that the vechicle *cannot contain knowledge that is not also included in the program*.

Hence, as promised, P must contain the instructions: 1) Copy what is on the tape and 2) Construct $M[\ ]$. Any P with this logic will therefore be denoted as P_M. As envisaged in theoretical biology, the construction phase and the copy phase have very different tolerances: the copy phase needs to be almost perfect, while the construction phase needs only to create a loose copy of M. How should the copy of the program be performed? The copy must be blind. For, if it was program-specific, a change in the program would prevent the copy from happening again. This is what allows evolution to be achieved:

[5] A system using redundancy and post-selection can always be used to reduce the error-rate, but (unlike in the digital case) there is a limitation for the accuracy to which one can perform the overall construction, set by the accuracy in performing the elementary physical operations involved in that post-selection stage.

[6] as illustrated by the remarkable example of the enzyme reverse-transcriptase in viruses, which infers from RNA strands of the host cell (part of the vehicle) information about its DNA.

occasional variations in the program can be passed on to the next generations. Indeed, it is notable that the replicator-vehicle logic is the only one that allows errors in the construction process not to propagate to the next generations. Only errors in the copy of the program do; but the program can be error-corrected.

Finally (as von Neumann envisaged) the option of P not containing any knowledge about $M[\ ]$ should be ruled out also on the ground of realistic considerations: our laws of Physics would not allow the appropriate time-scales, nor the perfect measurements required by the process of $M[\ ]$ looking at itself. Worse, this option forces $M[\ ]$ to include objects, such as the various components of a raster scanner, that are all adapted to cooperating with each other to performing the raster-scan-and-copy function. Hence, $M[\ ]$ could not be a model of real self-replicators, such as archaea or bacteria. For the latter have come about through a sequence of ancestors (i.e., catalysts that promote the production of further instances of themselves), each of which was a step closer to being a life form, and was only partially implementing the self-replication function. Instead, raster-scan-copying cannot be partially implemented and still partially perform its function. Hence, organisms that have evolved to perform the function of self-replication cannot possibly rely on raster-scanner copying to perform their self-replication.

5.4 The replicator-vehicle logic is compatible with Quantum Theory

In order to present the algorithm of self-replication under Quantum Theory I shall restrict attention to the case where the elementary unit Q is a qubit. It suffices to prove that the logic of the algorithm of self-replication is allowed in this case, in order to show that it is compatible with quantum mechanics.

Let $\mathcal{H}$ be the Hilbert space associated with a single qubit. According to the replicator-vehicle logic, the ambient space of the constructor $\mathbf{C}$ is further partitioned into two parts, the register $\mathbf{R}$, with Hilbert space $\mathcal{H}_R = \mathcal{H}^{\otimes d_R}$ and the vehicle $\mathbf{V}$, with Hilbert space $\mathcal{H}_V = \mathcal{H}^{\otimes d_V}$, so that $\mathcal{H}_C = \mathcal{H}_R \otimes \mathcal{H}_V$. Correspondingly, the substrate that will contain the new instance of the self-replicator, $\mathbf{S}$, is partitioned into two parts: the one that is transformed into a vehicle, $\mathbf{S_V}$ with Hilbert space $\mathcal{H}^{\otimes d_V}$ and the one that is transformed into a program, $\mathbf{S_R}$ with Hilbert space $\mathcal{H}^{\otimes d_R}$, with $\mathcal{H}_S = \mathcal{H}_{S_R} \otimes \mathcal{H}_{S_V}$.

Finally, the ancillary subsystem $\mathbf{A}$ is partitioned into the space of the ancilla used up to copy the program, $\mathbf{A_P}$, and the one of the ancilla used up to construct the vehicle, $\mathbf{A_V}$, so that $\mathcal{H}_A = \mathcal{H}_{A_R} \otimes \mathcal{H}_{A_V}$, where $\mathcal{H}_{A_R} = \mathcal{H}^{\otimes a_r}$ and $\mathcal{H}_{A_V} = \mathcal{H}^{\otimes a_v}$.

I shall adopt the notation by which $B^{(X)}$ denotes the operator $\mathbb{1} \otimes ... \otimes B \otimes ... \mathbb{1}$ acting as the operator B on subsystem X only.

In quantum-mechanical terms, one represents the attribute of being the machine M as the $+1$-eigenspace of a projector (that this attribute is a measurable one follows from empirical considerations). The projector for being the

machine $M[P_M]$ is

$$\Pi_M^{(C)} = P_M^{(R)} M^{(V)} \ ,$$

where I have introduced the projector $P_M^{(R)}$ for being a program containing the instructions to build the machine $M[\ ]$ and the projector for being a vehicle of the M-kind, $M^{(V)}$. The rank of $\Pi_M^{(C)}$ will be denoted by n.

Upon denoting the +1-eigenspace of an operator O by $\Sigma(O)$, the replication task is expressed as:

$$\Sigma(\Pi_M^{(C)} G^{(S,A)}) \to \Sigma(\Pi_M^{(C)} \Pi_M^{(S)}) \tag{5.2}$$

for some projector $G^{(S,A)}$.

Let me introduce the projector $\Pi_g^{(i)}$ for being generic in the Hilbert space of the i-th qubit and let the projector for the region X to contain generic resources be $G^{(X)} = \prod_{i \in X} \Pi_g^{(i)}$.

The self-replication algorithm requires $\Pi_M^{(S)} G^{(S)} = 0$. This guarantees that the environment does not already contain a self-replicator, or the means of building one without the knowledge contained in the system in question. In general, the subspace defined by $G^{(S)}$ is much larger than the subspace defined by $\Pi_M^{(S)}$ as any species of self-replicator contains much more adaptations than the generic resources.

5.4.1 Wigner′s argument is not relevant

Wigner's thesis is that "according to standard quantum mechanics the probability is zero for the existence of self-reproducing states" so that "the present laws and concepts of quantum mechanics will have to undergo modifications

before they can applied to problems of life". As he himself put it, "the question in the foreground is whether the real equation of motions can be expected to give reproduction". I shall now explain why the argument he presents in support of this thesis is not valid.

The argument is about the *replication task*, whose possibility is a necessary condition for self-replication to be possible. Wigner represents the Hilbert space of the constructor plus substrates as the tensor product of three Hilbert spaces: $\mathcal{H}_C \otimes \mathcal{H}_S \otimes \mathcal{H}_A$, respectively accommodating the self-replicator M, the raw materials becoming the new instance of M, and the waste products; $\mathcal{H}_C = \tilde{\mathcal{H}} = \mathcal{H}_S$ and the dimension N of $\tilde{\mathcal{H}}$ is much smaller than the dimension N_A of $\mathcal{H}_A$.

In $\mathcal{H}_C$ there is a "living" subspace V_M that has dimension n much smaller than N. Wigner's statement is that for a **random** unitary S acting on $\mathcal{H}_C \otimes \mathcal{H}_S \otimes \mathcal{H}_A$, there are no subspaces $V_M \subseteq \tilde{\mathcal{H}}$ with dimension $n << N$ and states $|g\rangle \in \tilde{H}_S \otimes \mathcal{H}_A$ with the property that

$$S \ : \ V_M \otimes \mathrm{Span}\{|g\rangle\} \to V_M \otimes V_M \otimes \mathcal{H}_A \ . \tag{5.3}$$

Let Π_M be the projector onto V_M. By setting

$$\Pi_M^{(C)} = \Pi_M \otimes \mathbb{1} \otimes \mathbb{1} \ \ , \quad \Pi_G^{(S,A)} = \mathbb{1} \otimes |g\rangle \langle g| \ \ ,$$

one sees that this is precisely the replication task in (5.2).

Following Wigner's argument, one can fix a basis $\{|\kappa\rangle |\lambda\rangle |\mu\rangle\}$ in the space $\tilde{\mathcal{H}} \otimes \tilde{\mathcal{H}} \otimes \mathcal{H}_A$ with respect to which $V_M = \mathrm{Span}\{v_\kappa^{(j)}\}_{j=1}^n$. If the initial state is $\Phi_{\kappa\lambda\mu}^{(j)} = v_\kappa^{(j)} g_{\lambda\mu}$ the equations corresponding to the replication task become:

$$\sum_{\bar{\kappa}\bar{\lambda}\bar{\mu}} S^{\bar{\kappa}\bar{\lambda}\bar{\mu}}_{\kappa\lambda\mu} v^{(j)}_{\bar{\kappa}} g_{\bar{\lambda}\bar{\mu}} = \sum_{k,\ell} u^{jk\ell}_{\mu} v^{(j)}_{\kappa} v^{(\ell)}_{\lambda}$$

These equations must be satisfied for every λ, κ, μ, and j, so the number of equations is nN^2N_A. The number of unknowns, on the other hand, is given by the u, that are n^3N_A, the v, that are nN, and the g, that are NN_A. So there is a solution if $nN^2N_A = n^3N_A + nN + NN_A$. Since N is much greater than n, the number of equations is much larger than the number of unknowns, which implies that there are no solutions unless the laws of Physics S are infinitely fine-tuned.

This indicative argument, as pointed out by Baez [42], is tantamount to proving that the set of unitaries

$$\{U \in B(H) \ : \ \exists V_M \ , \ \exists \, |g\rangle \ : \ V_M \otimes \mathrm{Span}\{|g\rangle\} \to V_M \otimes V_M \otimes \mathcal{H}_A\}$$

is of zero measure in the space of unitary transformations $B(H)$ defined on $\tilde{\mathcal{H}} \otimes \tilde{\mathcal{H}} \otimes \mathcal{H}_A$.

Wigner interprets this result to mean that "if the laws of physics S are not tailored so as to permit reproduction, it is infinitely unlikely that there be any state of the nutrient that would permit the multiplication of any set of states which is much smaller than all the possible states of the system.". His point could be summarised by the diagram 5.3.

I shall now show that Wigner's argument is invalid qua argument about self-replication, because it would lead to the same conclusion for **any** construction where both the constructor and the target objects are specialised, i.e., when

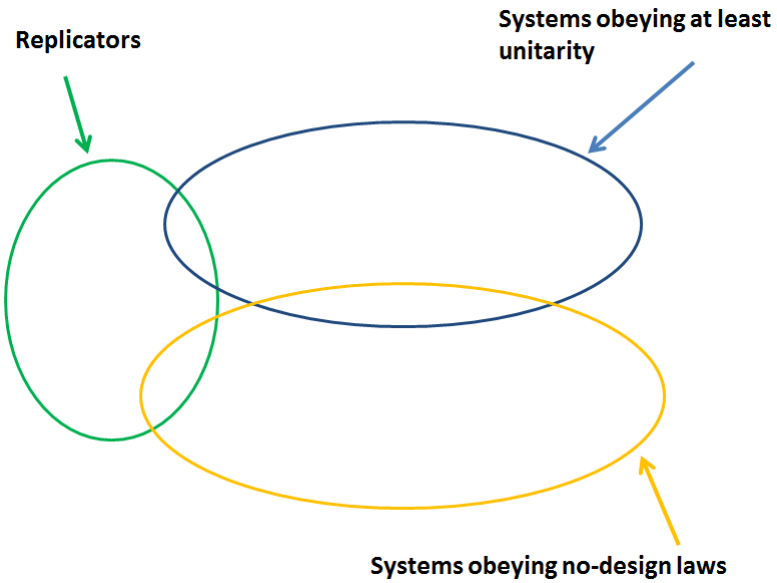


Figure 5.3: Wigner's thesis: replicators that obey unitary laws can occur only under laws that contain the design of the replicator.

the property of being that constructor and that target are associated with subspaces with dimension much smaller than that of the ambient space.

Let me follow Wigner's prescription and pick a random unitary S to represent the laws of motion ruling the interaction between the constructor and the substrates. Suppose one wants to investigate if under such a unitary any specialised construction can be performed, such as the conversion of hydrogen to helium [7]. Let the property of being a certain target be represented by the projector onto the subspace $V_B \subseteq \tilde{\mathcal{H}}$, and the property of being a constructor for it by the projector onto $V_C \subseteq \tilde{\mathcal{H}}$. As explained in section 2.3.1, a necessary condition for $\mathbf{C}$ to be a constructor for the task in question, under S, is that

$$S(V_C \otimes \mathrm{Span}(|g\rangle) = V_C \otimes V_B \otimes \mathcal{H}_A \ ,$$

[7] Note that specialised does not mean that is contains design.

because the constructor must preserve its ability to be a constructor. How many pairs of subspaces V_C, V_B and states $|g\rangle$ can there be that satisfy the above equations?

Upon fixing the basis $\{|\kappa\rangle\,|\lambda\rangle\,|\mu\rangle\}$, with respect to which $V_C = \mathrm{Span}\{v_\kappa^{(j)}\}$ and $V_B = \mathrm{Span}\{b_\kappa^{(j)}\}$, the initial state is denoted by

$$\Phi_{\kappa\lambda\mu}^{(j)} = v_\kappa^{(j)} g_{\lambda\mu}.$$

Then the v, the b, the u and g must satisfy the following equation:

$$\sum_{\tilde{\kappa}\tilde{\lambda}\tilde{\mu}} S_{\kappa\lambda\mu}^{\tilde{\kappa}\tilde{\lambda}\tilde{\mu}} v_{\tilde{\kappa}}^{(j)} g_{\tilde{\lambda}\tilde{\mu}} = \sum_{k,\ell} u_\mu^{jk\ell} v_\kappa^{(j)} b_\lambda^{(\ell)}$$

By the same counting argument, the number of equations is mN^2N_A and the number of unknowns is $mn^2N_A + (m+n)N + NN_A$. Since both n and m are much smaller than N, by following Wigner's interpretation, *one would conclude that almost no construction is allowed under the laws of quantum physics, unless some additional law with the design of both the constructor and the target is postulated.*

This shows that, under Wigner's interpretation, his theorem rules out a lot more than just self-replicators. It rules out **every** specialised construction. One begins to suspect that there is something more wrong with Wigner's interpretation than merely misunderstanding the needs of biology. So, what has gone wrong?

Wigner's theorem only says that the unitary that achieves the net effect of self-replication is special (i.e., there could be some unitaries that performed

the task (5.2), but their number is vanishingly small in $\frac{n}{N}$). Just like the process of constructing, say, a Boeing 787 out of raw materials is an unusual process.

But this gives no indication on whether the **elementary interactions** between the simple constituents of matter must contain the design of a self-replicator (or of a Boeing 787). Indeed, as I shall discuss in the next section, under quantum mechanics the matrix S that he shows must be "special" can nontheless be decomposed into elementary steps that do not contain the design of S, corresponding to the interactions between the elementary constituent of the self-replicator and the substrate. This is possible because (as pointed out by von Neumann and explained in the previous section) the self-replicator in my model, just like real ones, contains a program including all the knowledge about itself. [8]

Likewise, the construction of a Boeing 787, albeit unusual, is not an improbable outcome of the construction process happening in the Boeing company headquarters, in the presence of the knowledge produced by the designers (and that knowledge is present neither in the laws of motion nor the initial state). It is the presence of that knowledge that makes it possible for the Boeing 787 to be constructed out of raw materials, even though the (unitary) laws of Physics ruling the interaction between the elementary components of the factory and the elementary components of the raw materials are not tuned to make a Boeing 787.

[8] Wigner's claim that a confrontation between his model and von Neumann's self-replicating automaton "is not possible because the model used by von Neumann can assume only a discrete set of states whereas all our variables are continuous" is mistaken, because the analysis that Wigner performs could be carried out in exactly the same way using a discrete setting.

In summary, as I shall elaborate later, generic laws plus a knowledge-laden state can perform that role that Wigner assumed can only be played by knowledge-laden laws and a generic state.

There is also another reason why Wigner's argument is invalid, which was first pointed out by Baez, in [42]. Wigner fixes a specific tensor-product structure at the outset, in order to carry out his analysis: his theorem regards how many unitaries would achieve the replication task in a *specific, arbitrarily fixed* tensor-product structure. However, in order to investigate the probability that a unitary dynamics allow replication (that is the problem Wigner is actually interested in), one should in fact consider how many unitaries would achieve the replication of some subspace V_M in *some* product structure (whose choice is allowed to depend on the unitary). For the product structure is not an element of reality: just like the basis, its choice is a matter of convenience. Therefore, as Baez argues, one should investigate the cardinality of the set

$$\begin{aligned} S^* = \{ \quad & U \in B(\mathcal{H}) \ : \ \exists V_M \in \mathcal{H}_C, \quad \exists \, |g\rangle \in \mathcal{H}_S, \exists U^* \in B(\mathcal{H}) \ : \\ & U^{*\dagger} U U^* (V_M \otimes \mathrm{Span}(|g\rangle) \quad = V_M \otimes V_M \otimes \mathcal{H}_A \ \} \ , \end{aligned} \tag{5.4}$$

where $U^* \ : \ \tilde{\mathcal{H}} \otimes \tilde{\mathcal{H}} \otimes \mathcal{H}_{\mathcal{R}} \to \mathcal{H}$ is the unitary isomorphism representing the tensor product structure that self-replication can occur in. Unitaries in this set satisfy a more relaxed criterion than the one Wigner considered.

Baez further showed that, when the dimension n of the subspace V_M is 1,

i.e., $V_M = \text{Span}\{|v\rangle\}$, the set

$$\{U \in B(\mathcal{H}) \ : \ \exists\, |v\rangle \in \mathcal{H}_C, \exists\, |g\rangle \in \mathcal{H}_S, \exists U^*(v,g) \in B(\mathcal{H}) \qquad (5.5)$$
$$U^*(v,g)^\dagger U U^*(v,g)(V_M \otimes \text{Span}(|g\rangle) = V_M \otimes V_M \otimes \mathcal{H}_A \ \}$$

is dense in the set of all unitaries $B(\mathcal{H})$. This means that almost all unitaries would achieve replication of a specific single state $|v\rangle$ in the presence of a specific state $|g\rangle$, in some tensor product structure. I have used the notation $U^*(v,g)$ to highlight the fact that according to Baez's theorem, for the replication of the state $|v\rangle$ to be possible under a particular S (corresponding, say, to the actual laws of Physics) a **specific** initial conditions $|g\rangle$ would be required: any other initial state of the raw materials would make the replication fail. This makes Baez's point no rebuttal of Wigner's claim: for, one could argue, replication (and hence, allegedly, life) requires a very special initial condition to occur; this initial condition is in fact of zero-measure in the set of all possible initial conditions, thus leading to the same conclusion as Wigner's.

Moreover, Baez's theorem regards the replication of a single quantum state, i.e., $V_M = \text{Span}\{|v\rangle\}$ for a fixed $|v\rangle$ (this case was discussed by Wigner too at the outset of his paper). This is too strict a requirement to represent self-replication as it occurs in living entities, as acknowledged by Wigner himself. Indeed, actual self-replicators require the replication of the property of being some species (represented by some projector) to be possible, as opposed to replication of a single, specific quantum state. Were self-replication to occur

only for a single quantum state, it could not permit evolution.[9]

As a side comment, notice that Wigner models only a necessary condition for self-replication, i.e., the replication task. So he does **not** provide a model of self-replication. Indeed, no restrictions are applied to what S and A must be. As pointed out by Baez, in [42], the raw materials could already contain the object with the property V_M; or, for instance, Dr Frankenstein assembling another instance of himself out of raw materials, by mere self-copying, would perform the replication task in Wigner's defintion; so would a bit of paper in a photocopier. In other words, nothing in Wigner's model forces S to acquire the distinctive feature of all real stable and evolving self-replicators: that S must contain a program including all the knowledge about itself.

In the next section I shall prove that quantum mechanics can accommodate self-replication: there can be a unitary that causes the transformation in eq. (5.2) to happen, is stable and does not contain the design of the self-replicator. Before doing that, let me clarify the relation between my model and the one von Neumann proposed.

Would the von Neumann machine suffice?

After the Hixon-Symposium paper, von Neumann focused on the issue of demonstrating a formal model achieving self-replication via the replicator-vehicle logic [11].

There are two of these models. The first one, relying on machines moving

[9] Note also that even in the case when V_M is 1-dimensional, Wigner's theorem differs from the no-cloning theorem. The latter is about the set of unitaries such that there exists a tensor product structure $\mathcal{H} = \mathcal{H}_C \otimes \mathcal{H}_S$ in which, for an arbitrary $|g\rangle \in \mathcal{H}_S$ and $\forall\, |v\rangle \in \mathcal{H}_C, |v\rangle\,|g\rangle \to |v\rangle\,|v\rangle$. This set is empty, for any dimension of the Hilbert space $\mathcal{H}_C$.

in a Euclidean space, turned out to be tremendously difficult to carry out in detail, even if one ignored problems of energy, noise in the environment, and the like. Hence it was abandoned in favour of a simpler model.

The second of the models is based on a deterministic cellular automaton. There is an infinite array of squares in the Euclidean plane; each square or "cell" is capable of being in any of a number of states (twenty-nine possible states for the von Neumann machine). Time moves in discrete steps. A functional relation is defined, such that the state of a cell at time t is a function of its state and that of its four nearest neighbors at $t-1$. As time goes by, this functional relation determines the evolution of the states of all cells. A certain state of the cells is "quiescent" and corresponds to an inactive part of the plane. von Neumann proved that there is a functional relation such that there can be embedded in this 29-state cellular structure an automaton that is a universal Turing machine, a universal constructing machine[10] which is, in particular, a self-replicator. (Self-replication, here, has the meaning that groups of neighbouring "active" cells can cause another group of cells to take on a similar active state.)

One might ask whether the self-replicator (or von Neumann's machine) would provide the model I am seeking. The answer is negative, for the following reasons.

First, the von Neumann's machine does not satisfy the definition of self-replicator as it occurs in living entities. Although it acts according to no-design laws, and its time-evolution could in principle be implemented in a

[10]universal with respect to that model world, whose laws are not our actual laws of Physics

unitary way, its stability relies upon the stability of the (external) universal machine in which that model world is embedded.

Hence, the Turing Machine is an underlying facility upon which the parent von Neumann machine and all its children rely. So, the self-replicator, by itself, would not be stable; to be stable, it resorts to an external entity, a universal classical Turing machine, that performs error-correction but does not undergo self-replication. Consequently, the composite object (von Neumann machine + Turing machine) cannot be considered as a self-replicator. This is also one of the reasons why von Neumann's model is not evolvable, as von Neumann himself aknowledged.

Furthermore, even if one thought of a variant of that model, where stability was achieved without resorting to anything external to the self-replicator itself, that model still would not do. In fact, it would be a self-replicator according to our definition. But the laws under which it acts are imaginary ones, that can be implemented only in classical computational models, but do not exist in reality. Since physical computers conforming to those computational models came into existence as a consequence of the existence of special self-replicators (i.e., living entities) one cannot just assume their existence to investigate the question whether the actual laws of physics (in this particular case, quantum mechanics) allow the existence of self-replicators. Hence, demonstrating that model would still not give any indication as to whether the actual laws of physics, in particular quantum mechanics, permit self-replication - which is precisely what I am trying to assess in this project.

A further reason why it would not suffice is that the subtasks implicitly required by this self-replicator would be exclusively tasks that cannot possibly

require quantum coherence, as they are implemented in a model world based on the laws of discrete classical Physics. On the other hand, my model will allow for quantum coherence to be required.

The same critique applies to a simulation of the von Neumann self-replicator on a quantum computer, which therefore would not serve my aim either.

5.4.2 Modelling the logic of self-replication

I will now complete the rebuttal of Wigner's argument, by showing that quantum mechanics is compatible with self-replication without the need for any additional design-law. The conclusion I shall reach is illustrated by the diagram 5.4.

In order to discuss the model I shall pick a fixed generic state, the simultaneous +1-eigenvector of the z-components of the qubits composing the substrates $S \oplus A$.

Note first that the projectors for being vehicles of different kinds are orthogonal, $M^{(V)}N^{(V)} = 0$. This follows from the fact that different types of vehicles (such as a dog and a tiger) correspond to different (distinguishable) macrostates.

As discussed in section 2.3.1, this implies that the projectors for being programs for different machines, $P_M^{(R)}$ and $P_N^{(R)}$, must be orthogonal to each other. Furthermore, as commented on in chapter 2, one can restrict to a set of orthogonal programs within each subspace, for all programs in that subspace (the basis and its superpositions) code for the same vehicle, by linearity. So I shall restrict, in the specific qubit example, to the computational

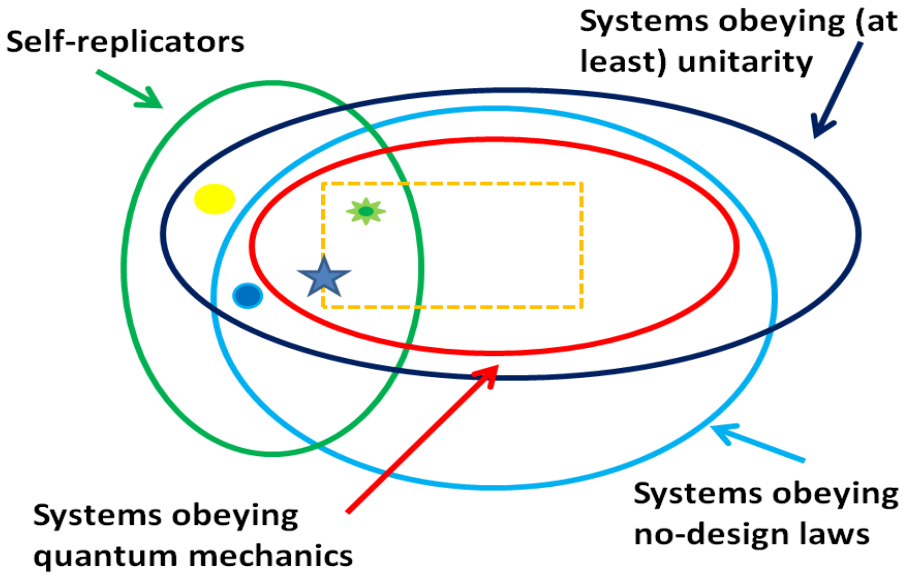
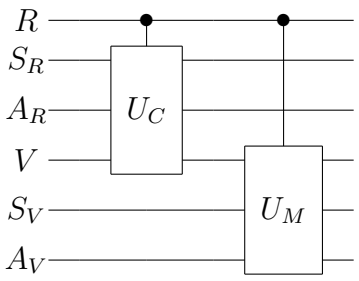


Figure 5.4: The blue star represents the model I argue for. The orange dotted line is the boundary set by the actual laws of physics (i.e., Quantum Theory plus other theories - e.g. General Relativity, thermodynamics, and yet others to be known) and need not be known for present purposes, because here I am concerned with Quantum Theory only. The yellow dot represents the unitary implementation of the von Neumann machine that relies on external error-correction, the blue one the von Neumann machine that does not rely on external error-correction: both self-replicate in an imaginary world whose laws are based on a classical logic. The green asterisk is a real bacterium. Points in the intersection between the light-blue ellipse and the green one each represent a code-based self-replicator.

basis, as defined in chapter 2.

Stable self-replication of a species M is permitted by quantum mechanics with the following logic:



where the first unitary represents the copy phase, and the second one the construction phase. I have used the faculty of moving clusters of qubits together in order to make the representation easier. (This is just a representation and should not be intended as a prescription for the spatial arrangement of real self-replicators.)

- Copying the program

  The unitary controlled-U_C describes the interaction between the vehicle (in $\mathbf{V}$), the program (in $\mathbf{R}$) and the substrates (in $\mathbf{S_R} \oplus \mathbf{A_R}$) which leads to the (in principle, perfect) copying of the program:

$$U_C = M^{(V)} \left(\prod_{i=1}^{d_p} \mathrm{CNOT}_{i \to i+d_p}^{(R,S_R)} \right) + \left(\mathbb{1} - M^{(V)} \right) W^{(R,S_R)}$$

  where the unitary W is arbitrary.

  In this phase the vehicle copies, bit by bit, the program in the register.

The meaning of the projector $M^{(V)}$ is that if a vehicle is there, anything that is on the register (i.e., a valid program whether or not it codes for the particular organism, and invalid programs) is copied. As discussed in the previous section, the vehicle does not execute the program in this phase, but only reads it as data: the copy is blind, to allow changes in the programs to be copied and evolution thereby. The reason why the unitary involves the ancilla A_R in the network is that it may include a process of classical error-correction on the new instance of the program, controlled by the program. This guarantees that the copy phase can be stabilised and brought to the desired precision, up to meet the stringent requirements on fidelity in nature [11].

In order to permit evolution, each machine $M[\,]$ needs to have in its repertoire a *finite* set of programs $\{|P_M\rangle\}$, which code for machines only slightly different from one another - the ones closer to the type M in the evolutionary sequence. Note that "closer" in this context means that the machines are described by very similar programs, not that their projectors are close in the Hilbert-Schmidt norm sense. Since I have explained that the programs are elements of the computational basis, in this phase each program in the repertoire of $M[\,]$ is faithfully copied. Note that real self-replicators are not universal constructors: they are much simpler machines. Hence, having a finite-number of generic resources is not an issue for self-replication as it occurs in living

[11] The copier of DNA is highly accurate, with an intrinsic error rate of less than one error every 10^7 nucleotides added. In eucaryotes, additional proofreading and post-replication mismatch make the replication fidelity of less than one mistake for every 10^9 nucleotides added.[43]

entities, contrary to what has been claimed by [5], [6]. (But in fact it is not an issue either for the universal constructor, as explained in the appendix).

Hence the copy phase can happen in a unitary way, with arbitrary accuracy, and can be stabilised.

- The construction phase

This is the phase where the program is executed in order to build a new vehicle:

$$U_M = P_M^{(R)} C_M^{(V,S_V,A_V)} + (\mathbb{1} - P_M^{(R)}) \tilde{W}^{(V,S_V,A_V)}$$

where $\tilde{W}$ is an arbitrary unitary.

This phase is program-specific: the vehicle executes the program. The unitary C_M must satisfy

$$C_M \quad : \quad \Sigma(M^{(V)} G^{(S_V,A)}) \to \Sigma(M^{(V)} M^{(V)})$$

which can be easily met: if $r_M = \mathrm{Rank}(M^{(V)})$ and $r_g = \mathrm{Rank}(\mathrm{G}^{(\mathrm{S_V,A})})$, one has $r_M r_g << r_M^2 2^{A_V}$ (because $A_V >> r_g$) .

This is of course not enough to conclude that under quantum mechanics, self-replication of the machine M can occur without the need of additional, *ad hoc* design laws. In fact C_M is precisely the kind of unitary that Wigner argued is very special and requires design to happen.

One notices, at this point, that the construction of a vehicle (the unitary C_M) can be performed by an algorithm whose elementary steps are simple operations (such as "pull two atoms closer together"); "simple" in the sense that they can be performed without any information about the design of any organism. Indeed, they are the elementary steps of many algorithms each one intended to perform many other different tasks, most of which do not code for self-replicating machines such as M. This implies that these elementary steps do not contain the design of an M. Also, this algorithm does not contain any loops of indeterminate length and therefore can be efficiently coded for in the program P_M.

This is in particular true under Quantum Theory. Hence, under Quantum Theory it is possible to implement self-replication in a no-design way, i.e., without resorting to special laws containing the design of an M. It is the fact that all the knowledge about V_M is embodied in the program that allows the construction of a vehicle to be possible even in the absence of design.

The condition about the "No-design" of the elementary operations, however, is not necessary to be expressed for the present purposes. It will eventualy be needed to extend the method to answer different questions – e.g. to understand the transition from mere catalysis to self-replication in early manifestations of life. This will be a challenge for complexity theory, which currently has not yet reached the stage where one could impose a "no-knowledge" requirement algebraically.

The best information-theoretic characterisations of 'knowledge' (e.g. Bennett's "logical depth" [44]) are not expressible as algebraic conditions on unitary transformations.

The construction phase can be stabilised by a second error-correction phase. The instructions to perform this error-correction can be encoded in the program too. By realistic considerations, this error-correction phase should be much looser than the one on the copy of the program.

Hence the logic of self-replication is compatible with quantum mechanics: under the laws of quantum mechanics it can be implemented in a way that can be stabilised, without requiring any additional design law.

Demonstrating the specific C_M is outside the scope of this thesis, and it is not relevant to the issue discussed in this chapter. It is enough to show that quantum mechanics allows *one* unitary to be performed in a way that does not include the design of an M. That way corresponds to the blue star in diagram 5.4, and thus refutes Wigner's argument.

This model has been expressed wholly in quantum-mechanical terms and hence it allows for implementations (organisms) using quantum coherence. In particular, the copy-me instruction, despite corresponding to a classical computational task, in real life is performed by physical objects that perform coherent subtasks (just like the physical device that implements the classical computational model of a Turing machine computes the classical functions via performing quantum subtasks). But one must not rule out a priori organisms where the construction phase of the new vehicle may actually require quantum coherence. My formalism accommodates both the

case where the elementary steps of that construction are all decoherent, and the case where they are coherent. This makes my model general enough to accommodate possible future discoveries about the role of coherence in biological processes. Indeed, understanding whether the latter possibility is viable (i.e., if there exists a way to efficiently decompose the C_M into a set of simple *unitary* transformations, controlled by the program, performing each one an elementary step of the construction) is a possible development of this work. However, investigating whether this is possible goes beyond the purpose of the present work. For in this work I aimed at showing that under quantum mechanics a no-design implementation of C_M is permitted; not that pure quantum mechanics (as distinct from particular laws of motion) requires a particular implementation to be possible.

The above model could be extended by incorporating the possibility of evolution. This would entail taking into account what happens when the machine changes from V_M to some variant V_N that can still copy the program P_M; and allowing the vehicle V_M to copy and execute variant programs P_K in its repertoire, to construct a machine K that is only slightly different from M. This can be in principle accommodated in the formalism because the projectors for different vehicles and programs are orthogonal, but goes beyond the purposes of the present work.

5.5 Conclusions

I have therefore shown that Quantum Theory, without the need of any ad-hoc additional law, can accommodate the logic of self-replication. To wit, I

have;

a) proven that the arguments claiming that Quantum Theory cannot accommodate the logic of self-replication are invalid;

b) shown that the logic of self-replication is compatible with quantum mechanics, without the need to postulate any additional law;

c) indicated the route to provide an exact model of a self-replicator under Quantum Theory.

There are some other enthralling points that one could develop using the model presented here:

- Let me define an emulation as a simulation of physical system that is in a suitable sense (e.g., polynomially) efficient and also preserves all the causal relationships between the subsystems of the *simulandum*. By universality, a universal quantum computer can emulate any other physical system with arbitrary accuracy. Consider a quantum computer running an emulation of a real self-replicator. Would the cluster of qubits whose evolution corresponded to that of the actual self-replicator be a self-replicator? I guess this is the case. The reason resides in the fact that being a self-replicator is an abstract property.

- Where could quantum coherence possibly play a role in the construction phase?

- New, open problems emerge in connection with the possibility of the existence of the universal constructor (see my comments in the appendix on how it could possibly self-replicate in a world of finite resources). For

instance, what the shortest description of a procedure to build a Universal Constructor, or indeed any quantum self-replicator, can possibly be.

These are some of the lines along which open problems about Quantum Theory, universal machines and Constructor Theory will find a fruitful unification, and, with any luck, a solution. But this is another story. And shall be told another time.

5.6 Appendix: Critique of Braunstein's argument

Let me consider the model which underlies the proof that "unitarity forbids perfect self-replication" with finite resources ([5], [6]). I shall argue, in the following, that the proof is about the non-existence of constructors which perform a *different* task than the one specified in 5.2. Hence, these results do not apply to self- replication as it occurs in living entities.

The model proposed by the authors is purported to be about a universal constructor, which, among other things, should also be a self-replicator. It includes a quadruple $(|\psi\rangle, |P_U\rangle, |C\rangle, |\Sigma\rangle)$, where $|\psi\rangle \in \mathcal{H}^N$ is the state of the processor of the alleged universal constructor, $|P_U\rangle \in \mathcal{H}^{N^{\otimes m}}$ is the program state that contains the instructions to copy a state $|\psi\rangle$, i.e., to perform the unitary operator $U \;:\; U(|\psi\rangle|0\rangle) = |\psi\rangle|\psi\rangle$, $|C\rangle$ is the state of the control unit, and $|0\rangle^{\otimes n}$ is a collection of nutrient states such that $|0\rangle \in \mathcal{H}^N$. The authors consider a fixed linear unitary operator L acting on the combined

Hilbert space of the input, program, control and $(m+1)$ blank states such that

$$\begin{aligned} L(\quad & |\psi\rangle\,|0\rangle\,|P_U\rangle\,|0\rangle^{\otimes m}\,|C\rangle)\,|0\rangle^{\otimes n-(m+1)} \\ = \quad & |\psi\rangle\,|P_U\rangle\,L(|\psi\rangle\,|0\rangle\,|P_U\rangle\,|0\rangle^{\otimes m}\,|C^*\rangle)\,|0\rangle^{\otimes n-2(m+1)} \end{aligned} \tag{5.6}$$

where $|C^*\rangle$ is the final state of the control unit, $\forall\,|\psi\rangle \in \mathcal{H}^N$. They claim that a quantum universal constructor and, in particular, a self-replicator, is possible if and only if a unitary L that satisfy eq. (5.7) for every state $|\psi\rangle\,|P_U\rangle$ exists; then they show that such an L cannot exist (it would violate unitarity).

The main point to note here is that, once more, this argument is irrelevant to the question of whether real self-replicators are allowed by quantum mechanics. For L does not describe what an actual self-replicator does. First, the unit C is never copied, so the child machine would not be able to self-replicate in turn. Moreover, even thinking of a variant of the above model that included the replication of the unit C, the program P_U above is required to contain the information to reconstruct *each state* of the machine, out of some fixed (blank) state of some raw materials. In other words, in each generation the machine is required to make an exact copy of the program and of its initial state, for all states. But in a self-replicator the program contains the information about the whole organism **architecture**, and it is the program that has to be exactly copied, not each state of the whole machine. As I said, the self-replicator could end up in any of a set of states which satisfy a much weaker condition: being in the +1-eigenspace of the projector for

being capable of performing the transformation again.

As already noticed, also, self-replicators in real life do not rely on universal machines: they are very simple, and have in the repertoire few programs.

So, the model-machine performing the unitary L (which turns out to be impossible because it violates unitarity) does not model self-replication as it occurs in living entities. Therefore this argument does not give any indication about the impossibility of actual self-replicators withing quantum mechanics, and does not have, as claimed by the authors, bearing on explaining life based on Quantum Theory.

In regard to the model *per se*, the model machine in [5], [6] is ruled out by the no-cloning theorem, if the programs are not orthogonal, while the authors deny this. In fact, the existence of a machine performing L would imply the existence of a universal cloner (if the transformation L acted for only one step). And, on the other hand, they overlook the fact that, to achieve the purpose of encoding the unitary that would reconstruct the state $|\psi\rangle$ out of a blank state, a set of orthogonal states suffice, as I have proven in chapter 2. This is because of the Quantum Theory of Computation: the assembler for a set of universal gates works running a set of orthogonal programs. Hence no more than that is needed in order to reconstruct with arbitrary accuracy any unitary U_ψ.

The authors also claim that a universal constructor using orthogonal programs could not possibly self-replicate in the presence of a finite number of blank states available at any one time because the program space would have to be infinite-dimensional. However, the program encoding for the self-replication of a universal constructor (just like any program) occupies only

a finite portion of the tape. Hence copying the program entails copying it onto a *finite* portion of tape, and attaching it to the machine. Indeed, each program in any universal machine has a finite length, hence the copy of the program would not entail performing a never-ending copy.

Chapter 6

How to Counteract Systematic Errors in Quantum State Transfer

Abstract[1]

In the absence of errors, the dynamics of a spin chain, with a suitably engineered local Hamiltonian, allow the perfect, coherent transfer of a quantum state over large distances. Here, I describee encoding and decoding procedures to recover perfectly from low rates of systematic errors. The encoding and decoding regions, located at opposite ends of the chain, are small compared to the length of the chain, growing linearly with the size of the error. I also describe how these errors can be identified, again by only acting on the encoding and decoding regions.

[1] The research work described in this thesis has been developed in collaboration with Artur Ekert and Alastair Kay [14].

6.1 Introduction

The task of transferring a quantum state from one location to another is fundamental in the field of quantum information. This is true not only in the rather explicit case of the quantum communication scenario, where two distant parties have to communicate, but also for quantum computing itself. Indeed, in a quantum computer one needs to transfer quantum states and generate entanglement between different areas of the system. In particular, to achieve large scale quantum computing it is necessary to link several small quantum processors and allow them to communicate. Thus, quantum state transfer is a fundamental subprotocol within a quantum computer.

Since in a quantum computer the interactions are typically local, achieving quantum state transfer between distant qubits is a non-trivial task. One way to perform the task would be to apply a sequence of SWAP gates to bring distant qubits together, but this is a massive source of errors. Another possibility would be to use a 'flying qubit' within the same system to achieve the communication between distant qubits. However, this implementation requires additional information processing (interfacing) when transferring quantum information between dissimilar media. Therefore is more difficult to realize.

Alternatively one can think of using a quantum communication channel which takes a state at one location and outputs it at another. The idea is to design the Hamiltonian of the system realizing the channel in such a

way that its free evolution leads to the transfer of the state.

This approach has many advantages. To begin with, it avoids interfacing, since both the quantum computer and quantum channels may be made by the same physical systems, from the same solid-state technology. Moreover, it minimises the amount of external control, since in principle one should interact just during the initialisation and then at the read-out. Finally, the channel only has to perform the state-transferring task, so it is expected to be easier to fabricate and therefore achievable well before a quantum computer.

The study of this particular implementation of state transfer was initiated by Bose [45], who proposed a scheme employing a uniformly coupled spin chain to perform short distance communication. Then, the scheme was generalised to arbitrary networks and to non-uniform couplings to achieve communication over arbitrary distances, [46, 47]. After that, a plethora of variations have been proposed. However, the simplest and optimal way to do the transfer, minimising the interaction with the system, is still the one that uses a one-dimensional spin chain, [48].

In this thesis I shall therefore focus on state transfer along spin chains. After briefly reviewing perfect state transfer in the ideal case, I shall extend the theory to cover errors. This will lead to the main object of this chapter: encoding and decoding procedures to protect against systematic errors. By systematic errors, as will be clarified later on, I mean errors having the same effect each time one performs the transfer, so that one can learn how to protect against them. This procedure has to be intended as a first step on the way to a more general error-correcting scheme.

6.1.1 Perfect state transfer in spin chains

To set the scene, let me consider a linear chain of N qubits, i.e., spin-$\frac{1}{2}$ particles. The Hilbert space of such a system is $\mathcal{H} \simeq [\mathbb{C}^2]^{\otimes N}$. Let me assume that the dynamics of the system is governed by the following nearest-neighbour Hamiltonian [49]:

$$H \doteq \frac{1}{2}\sum_{n=1}^{N-1} J_n(X_nX_{n+1} + Y_nY_{n+1}) - \sum_{n=1}^{N} B_nZ_n \ , \ J_n \ , \ B_n \in \mathbb{R} \tag{6.1}$$

where X, Y, Z denote the familiar Pauli operators acting on $\mathbb{C}^2$ and $\forall\ A \in \{X, Y, Z\}$, $A_i \doteq \mathbb{1}^{\otimes i-1} \otimes A \otimes \mathbb{1}^{\otimes N-i}$, $i = 1, 2, ...N$ ($\mathbb{1}$ being the identity acting on $\mathbb{C}^2$). I define the state $|\mathbf{0}\rangle \doteq |0\rangle^{\otimes N}$, where all the spins are 'down', and the state $|\underline{i}\rangle = |0\rangle^{\otimes i-1} \otimes |1\rangle \otimes |0\rangle^{\otimes N-i}$, $i = 1....N$, where the spin at site i is 'up' (this represents an excitation). The set $\{|\underline{i}\rangle\}_{i=1}^{N}$ is called the computational basis.

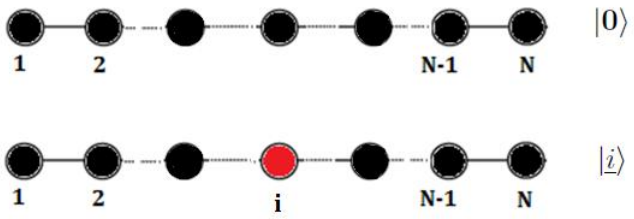


Figure 6.1: The *vacuum* state (top) and an excited state (bottom) of the chain.

The Hamiltonian has a symmetry, since

$$\left[H \ , \ \sum_{n=1}^{N} Z_n\right] = 0 \ .$$

This arises as a consequence of the fact that it is symmetric with respect to

the exchange of X with Y. The unitary time evolution associated with the Hamiltonian preserves therefore the total number of excitations.

This is a very important point, because as a consequence in the ideal case one can restrict the analysis to the subspace:

$$\mathcal{H}_0 \cup \mathcal{H}_1 \ ,$$

where $\mathcal{H}_0 \doteq \mathrm{Sp}\left\{|\mathbf{0}\rangle\right\}$ is the zero-excitation subspace and

$$\mathcal{H}_1 \doteq \mathrm{Sp}\left\{|\underline{i}\rangle \ \right\}_{i=1}^{N}$$

is the single excitation subspace, of dimension N.

In the computational basis the Hamiltonian is a tridiagonal matrix:

$$H_1 \doteq \begin{pmatrix} B_1 & J_1 & 0 & \cdots & 0 \\ J_1 & B_2 & J_2 & \cdots & 0 \\ 0 & J_2 & B_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & J_{N-1} \\ 0 & 0 & \cdots & J_{N-1} & B_N \end{pmatrix}$$

due to its nearest-neighbour-coupling feature. Here, an identity shift of $-\sum_n B_n \mathbb{1}$ was neglected being irrelevant to the dynamics.

Let me now define the protocol to perform a quantum state transfer from site 1 to site N, in the ideal case. Suppose one would like to send the unknown state

$$|\chi\rangle \doteq \alpha\,|0\rangle + \beta\,|1\rangle \ \ , \ \ \alpha, \beta \in \mathbb{C} \ , \ |\alpha|^2 + |\beta|^2 = 1 \ .$$

Then the state transfer process is defined by the following four steps:

1. **Initialization** of the spin system to the state $|\mathbf{0}\rangle$.

2. **Preparation** of the spin system in the quantum state

$$|\psi_I\rangle = |\chi\rangle \otimes |0\rangle^{\otimes N-1} = \alpha\,|\mathbf{0}\rangle + \beta\,|\underline{1}\rangle \ ,$$

   at time $t = 0$.

3. **Time evolution** up to time a certain time, say t_F. If $0 \leq t \leq t_F$, then

$$|\psi(t)\rangle = U(t)\,|\psi_I\rangle = \alpha|\mathbf{0}\rangle + \beta \sum_{n=1}^{N} \beta_{n,1}(t)|\underline{n}\rangle \ ,$$

   where $U(t) \doteq \exp(-iHt)$ and

$$\beta_{n,j}(t) \doteq \langle \underline{n}|U(t)|\underline{j}\rangle \ \ , \ \beta_{1,j}(0) = \delta_{1,j} \ .$$

   Here, use has been made of the fact that $U(t)\,|\mathbf{0}\rangle = |\mathbf{0}\rangle$, up to a phase factor.

4. **Recovery** of the state at site N, given by the reduced density matrix acting on the Hilbert space associated with site N of the chain at time t_F:

$$\rho_N(t_F) \doteq \mathrm{Tr}_{1\ldots N-1}(W\,|\psi(t_F)\rangle\,\langle\psi(t_F)|\,W^\dagger) \ ,$$

   where W is a unitary operator which is used to decode the information. It usually acts non-trivially only over a small number of qubits (the decoding region).

A measure of how good the state transfer has been is given by the **fidelity**:

$$F_N(t_F) \doteq \sqrt{\langle\chi|\,\rho_N(t_F)\,|\chi\rangle}\ .$$

I achieve a **perfect** state transfer iff

$$F_N(t_F) = 1\ , \tag{6.2}$$

for some time t_F. This condition shall be referred to as the perfect state transfer condition [46], [47].

Our aim is to design the coupling coefficients of the Hamiltonian so that it is possible to satisfy this condition for some t_F. More precisely, I shall now try to answer the following question. "Which Hamiltonians in the class defined by (6.1) are capable of performing a perfect state transfer, in the sense just defined?".

A partial answer to this question is that every Hamiltonian H such that

$$\exists t_F, \phi\ \in\ \mathbb{R}\ \mid\ \exp(-iHt_F)\,|\underline{1}\rangle = \exp(i\phi)\,|\underline{N}\rangle\ , \tag{6.3}$$

is capable of performing a perfect state transfer in time t_F, since from (6.3) it follows that

$$|\psi(t_F)\rangle = \exp(-iHt_F)(\alpha\,|\mathbf{0}\rangle + \beta\,|\underline{1}\rangle) = (\alpha\,|\mathbf{0}\rangle + \beta\exp(i\phi)\,|\underline{N}\rangle)\ .$$

which manifestly satisfies the perfect state transfer condition (6.2) with an appropriate choice of $W(\phi)$.

I shall now identify a set of Hamiltonians H (among the ones defined in (6.1)) which satisfy (6.3), following the approach adopted in [49]. In general, it can be proven that a necessary condition for satisfying (6.3) is $J_n^2 = J_{N-n}^2$, $B_n = B_{N-n+1}$. Also, a local unitary transformation transforms any of these coupling schemes into one with $B_n = B_{N+1-n}$ and $J_n = J_{N-n}$. This means they are all equivalent for state transfer, except that the phase ϕ is changed. Moreover, for the class of Hamiltonians whose coupling coefficients satisfy

$$J_n = J_{N-n} \ , \ B_n = B_{N-n+1} \ \ \forall n \ , \tag{6.4}$$

it is possible to give some necessary and sufficient conditions to satisfy equation (6.3). Notice first that condition (6.4) can be considered as a mirror-symmetry property, since it is equivalent to the following:

$$[H_1, S] = 0 \ ,$$

where the symmetry operator S,

$$S \doteq \sum_{i=1}^{N} |\underline{n}\rangle \langle \underline{N-n+1}| \ ,$$

maps a state with an excitation on site n onto a state with an excitation on site $N-n+1$ (its mirror-image state). See figure 6.2. Due to this symmetry the set of eigenstates of H in the single excitation subspace, $\{|\lambda_n\rangle\}$, splits into two classes: the symmetric eigenstates,

$$|\lambda_n^s\rangle \ : \ H_1 |\lambda_n^s\rangle = \lambda_n^s |\lambda_n^s\rangle \ , \ S |\lambda_n^s\rangle = |\lambda_n^s\rangle$$

and the antisymmetric eigenstates

$$|\lambda_n^a\rangle \ : \ H_1 |\lambda_n^a\rangle = \lambda_n^a |\lambda_n^a\rangle \ , \ S |\lambda_n^a\rangle = - |\lambda_n^a\rangle \ .$$

For Hamiltonians in this class, the following lemma holds.

Lemma 6.1.1 *If H_1 satisfies (6.4), then H_1 satisfies (6.3) if and only if there exists a phase ϕ and a time t_F such that*

$$exp(-i\lambda_n^s t_F) = \exp(i\phi) \ , \ \exp(-i\lambda_n^a t_F) = -\exp(i\phi) \ , \tag{6.5}$$

for every eigenvalue λ_n^a, λ_n^s of H_1.

Proof

Let me assume that H_1 satisfies (6.4) and (6.3). From (6.3) and the definition of S it follows that

$$\exp(-iHt_F) |\underline{1}\rangle = \exp(i\phi) |\underline{N}\rangle = \exp(i\phi) S |\underline{1}\rangle \ . \tag{6.6}$$

On the other hand, by (6.4) one can expand the state $|\underline{1}\rangle$ in the eigenstates of the Hamiltonian:

$$|\underline{1}\rangle = \sum_n \alpha_n^s |\lambda_n^s\rangle + \alpha_n^a |\lambda_n^a\rangle \ .$$

Therefore, (6.6) becomes

$$\sum_n \alpha_n^s \exp(-i\lambda_n^s t_F) |\lambda_n^s\rangle + \alpha_n^a \exp(-i\lambda_n^a t_F) |\lambda_n^a\rangle = \exp(i\phi) \left(\sum_n \alpha_n^s |\lambda_n^s\rangle - \alpha_n^a |\lambda_n^a\rangle \right) \ .$$

For every n such that $\alpha_n \neq 0$ this is true iff

$$\exp(-i\lambda_n^s t_F) = \exp(i\phi) \ , \ \exp(-i\lambda_n^a t_F) = -\exp(i\phi) \ \ .$$

Notice that $\alpha_n \neq 0 \ \ \forall n$. [2] This proves the necessity of condition (6.5).

To prove sufficiency, let me now assume (6.4) and (6.5). One has, using again the decomposition in terms of symmetric and antisymmetric eigenvectors, that

$$\begin{aligned} \exp(-iH_1 t_F)\,|\underline{1}\rangle &= \sum_n \alpha_n^s \exp(-i\lambda_n^s t_F)\,|\lambda_n^s\rangle + \alpha_n^a \exp(-i\lambda_n^a t_F)\,|\lambda_n^a\rangle \\ &= \exp(i\phi)\left(\sum_n \alpha_n^s\,|\lambda_n^s\rangle - \alpha_n^a\,|\lambda_n^a\rangle\right) \equiv \exp(i\phi)\,|\underline{N}\rangle \ \ , \end{aligned}$$

where use has been made of (6.5) and of the definition of S. This proves the sufficiency of (6.5). ∎

I shall now translate equation (6.5) into a condition on the eigenvalues of H_1, which is readily testable. Indeed, the following lemma holds [49]:

Lemma 6.1.2 *For tridiagonal matrices, with positive off-diagonal entries and eigenvalues λ_n (n=1...N), the number of sign changes in the eigenvectors $|\lambda_n\rangle$ is $N-n$ (assuming an ordering such that $\lambda_n > \lambda_{n+1}$).*

Since H_1 is a tridiagonal matrix with positive entries, the lemma applies. By noticing that eigenvectors with an odd number of sign changes are anti-

[2] Indeed, for any eigenvector of H_1 with eigenvalue λ_n, $|\lambda_n\rangle = \sum_n \lambda_{n,m}\,|\underline{m}\rangle$, the coefficients $\lambda_{n,m}$ obey the recursion relation $J_m\lambda_{n,m+1} = \lambda_n\lambda_{n,m} - J_{n-1}\lambda_{n,m-1}$ (where I suppose that $J_n \neq 0 \ \forall n$). So, if $\lambda_{n,m-1} = \lambda_{n,m} = 0$ then $\lambda_{n,m+1} = 0$. This shows that if $\lambda_{n,1} = 0$, then $\lambda_{n,2} = 0$ and so on. Since $\alpha_n = \lambda_{n,1}$, if $\alpha_n = 0$, then by induction the eigenvector is 0. Therefore, there is no eigenvector with $\alpha_n = 0$.

symmetric, while the eigenvectors with an even number of sign changes are symmetric, one can rewrite the condition (6.5) as:

$$\lambda_n = \lambda_m + (2\kappa_{n,m} + 1)\frac{\pi}{t_F} \, , \kappa_{n,m} \in \mathbb{N} \, ,$$

where if n is odd m is even and sl vice versa. As a consequence, assuming $\{\lambda_n\}$ to be an ordered set of eigenvalues $\lambda_n < \lambda_{n+1}$, condition (6.5) is equivalent to the following:

$$\lambda_n - \lambda_{n-1} = (2k_n + 1)\frac{\pi}{t_F} \; k_n \in \mathbb{N} \, , \, , \tag{6.7}$$

which is therefore a sufficient and necessary condition for mirror-symmetric Hamiltonians to satisfy equation (6.3). Notice that this implies that the ratio of the differences of different eigenvalues is a rational number. Moreover, this is a remarkably simple condition on the eigenvalues in the single-excitation subspace, which is readily testable. For example, it can be proven [47] that if J_n =const. (uniform coupling, as in [45]) the perfect state transfer cannot be achieved for $N \geq 4$, because in those cases equation (6.7) is not satisfied. As a final remark: if the Hamiltonian satisfies (6.4) and (6.5), then $U(t_F)\,|\underline{n}\rangle = |\underline{N-n+1}\rangle$, $\forall n = 1...N$. See figure 6.2. The proof of this is similar to the one already presented and therefore I shall not elaborate it here.

Finally, it is relevant to observe that if (6.3) and (6.4) holds, $\exp(-iH2t_F)\,|\underline{1}\rangle = \exp(i2\phi)\,|\underline{N}\rangle$. Indeed, due to (6.3) and (6.4), applying $U(t_F)$ twice is equivalent, modulo the phase ϕ, to applying S^2, which equals the identity. The system is therefore periodic, with period $2t_F$. The condition on the eigen-

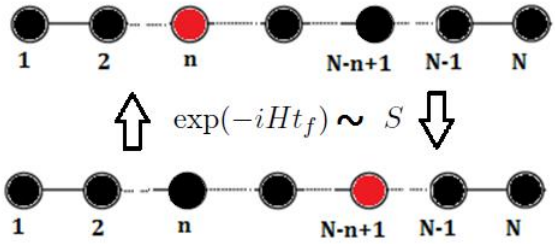


Figure 6.2: The mirror-symmetrical action of the time evolution associated with an Hamiltonian that satisfies (6.3) and (6.4).

values can indeed been thought of as a manifestation of the periodicity of H_1 [47].

An example

Let me now consider a remarkably simple example, which provides an instantiation of the lemmas just introduced. To introduce this example, one can notice that one can associate to the spin chain in the first excitation subspace a fictitious spin $S \doteq \frac{1}{2}(N-1)$ particle, relabelling the states of the computational basis as follows :

$$\{|\underline{i}\rangle\} \longrightarrow \{|m\rangle \ , \ m = S + i - 1\} \ \ \forall i = 1, 2, ...N \ .$$

The state $|m\rangle$ is an eigenvector of S_z, the $z-$component of the angular momentum operator associated with the spin of the fictitious particle.

Now, setting $J_n \doteq \sqrt{n(N-n)}$ then (6.4) is satisfied and moreover $H_1 = S_x$; indeed:

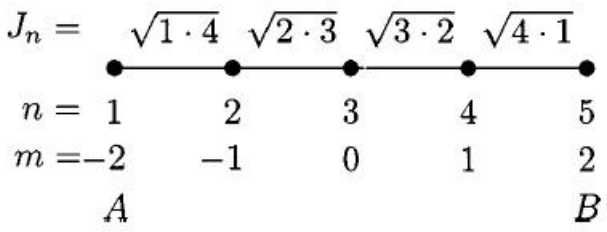


Figure 6.3: Couplings J_n that admit perfect state transfer in a five-qubit chain. Eigenvalues m of the fictitious spin-particle are also shown. (Adapted from [46]).

$$H_1 |m\rangle = \sqrt{S(S+1) - m(m+1)}\, |m+1\rangle + \sqrt{S(S+1) - m(m-1)}\, |m-1\rangle \ .$$

The eigenvalues of H_1 are therefore:

$$\lambda_i = -S + i - 1 \ , \quad i = 1...N$$

so that equation (6.7) is satisfied with $t_F = \pi$ and since the lemma applies perfect state transfer is possible. Notice indeed that $U(t)$ coincides with the rotation of the S-particle around the x axis. Therefore, the matrix elements $\beta_{m,1}(t)$ are well known and the fidelity is easily computed. One finds $F(t) = 1$ when $t = n\pi$, $n \in \mathbb{N}$, [46] .

6.1.2 The Jordan Wigner transformation

Another, equivalent description of the same system is provided by the Jordan-Wigner (JW) transformation [50]. The latter is very useful for describing multiple excitations in the system, providing the ideal formalism when deal-

ing with errors. Indeed one can think of an error as a bit flip, i.e., an excitation introduced in the system, or as dephasing noise (e.g., respectively, X_m or Z_m acting instantaneously at some point during the transfer). In the case of a bit flip the number of excitation is no longer preserved, therefore it is necessary to consider higher excitation subspaces. I shall now briefly summarise the formalism of the Jordan-Wigner transformation.

The JW transformation is defined by:

$$a_n^\dagger = \frac{1}{2} \prod_{m=1}^{n-1} Z_m \left(X_n - iY_n \right)$$

which ensures that

$$\{a_n^\dagger, a_m\} = \delta_{n,m} \text{ and } \{a_n, a_m\} = 0 \, ,$$

i.e., these operators describe fermionic particles. This transformation provides the right anticommutation relations due to the string of Z operators included in the definition. Inverting the transformation, one has:

$$\begin{aligned} X_n &= \prod_{m=1}^{n-1} Z_m (a_n^\dagger + a_n) \\ Y_n &= -i \prod_{m=1}^{n-1} Z_m (a_n^\dagger - a_n) \\ Z_n &= \mathbb{1} - 2a_n^\dagger a_n \end{aligned} \tag{6.8}$$

showing that while Z_m is a local operator, Y_m, X_m are non local, involving

the sites from 1 up to m. The state $|\mathbf{0}\rangle$ is such that $a_n^\dagger|\mathbf{0}\rangle = |\underline{n}\rangle = X_n|\mathbf{0}\rangle$ and $a_n|\mathbf{0}\rangle = 0$; also, $a_n|\underline{n}\rangle = |\mathbf{0}\rangle = X_n|\underline{n}\rangle$ and $a_n^\dagger|\underline{n}\rangle = 0$.

Applying the JW transformation to the Hamiltonian H one obtains:

$$H = \sum_{n=1}^{N-1} J_n(a_n^\dagger a_{n+1} + a_{n+1}^\dagger a_n) + 2\sum_{n=1}^{N} B_n a_n^\dagger a_n \ .$$

This Hamiltonian is bilinear in the fermionic operators and represents the hopping of a spinless fermionic particle along the chain. The most important feature of this Hamiltonian, for our purpose, is that it describes independent fermions [49]. This can be proven by defining the linear transformation

$$b_n^\dagger = \sum_{k=1}^{N} \lambda_{n,k} a_k^\dagger \ , \ \forall n \ ,$$

where

$$\sum_{n=1}^{N} \lambda_{n,m}^* \lambda_{n,k} = \delta_{m,k} \ .$$

The b_n's satisfy

$$\{b_n^\dagger, b_m\} = \delta_{n,m} \ \text{ and } \ \{b_n, b_m\} = 0 \ .$$

The inverse transformation is $a_n^\dagger = \sum_{k=1}^{N} \lambda_{k,n}^* b_k^\dagger$.

Set $H^{'} = \sum_{n=1}^{N} \lambda_n b_n^\dagger b_n$. I aim to show that $H = H^{'}$. To this end, let me write the eigenvectors in the first excitation subspace with eigenvalue λ_n as $|\lambda_n\rangle = b_n^\dagger|\mathbf{0}\rangle$, $\forall n$. Since

$$\langle \mathbf{0}|\, a_m a_k^\dagger \,|\mathbf{0}\rangle = \sum_{n=1}^{N} \lambda_{n,m}\lambda_{n,k}^* = \delta_{k,m} \tag{6.9}$$

One also has: $\langle\lambda_n|\lambda_m\rangle = \delta_{n,m}$, as required. On the one hand, if $|\lambda_n\rangle$ is an

eigenvector with eigenvalue λ_n the following relationship holds

$$\lambda_n \lambda_{n,m} = J_{m-1}\lambda_{n,m-1} + J_m \lambda_{n,m+1} + B_m \lambda_{n,m} \ .$$

On the other hand,

$$H^{'} = \sum_{m,n,k=1}^{N} (B_m \lambda_{n,m} + J_{m-1}\lambda_{n,m-1} + J_m \lambda_{n,m+1}) a_m^{\dagger} \lambda_{n,k}^{*} a_k$$

and making use of the property just introduced as well as of the orthogonality property (6.9) I get:

$$H^{'} = \sum_{m=1}^{N} J_{m-1} a_m^{\dagger} a_{m-1} + J_m a_m^{\dagger} a_{m+1} \ \equiv H \ ,$$

as required.

Since $H = \sum_{j=1}^{N} \lambda_j b_j^{\dagger} b_j$, the "fermionic modes" represented by the operators $b_n^{'}s$ are independent one from the other. Then, one can expect that if one excitation is transferred perfectly, so two are, because the time evolution acts independently on each of them. The following lemma formalizes this intuition.

Lemma 6.1.3 *If H satisfies equation (6.3), then (if $n < m$)*

$$\exp(-iHt_F)|\underline{n}, \underline{m}\rangle = -\exp(2i\phi)|\underline{N-m+1}, \underline{N-n+1}\rangle \ ,$$

where $|\underline{n}, \underline{m}\rangle \doteq X_n X_m |\mathbf{0}\rangle$.

Proof

Suppose $n < m$. Then, by the Jordan-Wigner transformation,

$$\exp(-iHt_F)|\underline{n},\underline{m}\rangle = U(t_F)a_n^\dagger a_m^\dagger|\mathbf{0}\rangle = U(t_F)\sum_{h,k=1,h\neq k}^{N}\lambda_{k,n}^*\lambda_{h,m}^* b_k^\dagger b_h^\dagger|\mathbf{0}\rangle\ .$$

Recall that $U(t_F) = \prod_{j=1}^{N}\exp(-i\lambda_j b_j^\dagger b_j t_F)$. Therefore,

$$\exp(-iHt_F)|\underline{n},\underline{m}\rangle = \sum_{h,k=1,h\neq k}^{N}\lambda_{k,n}^*\lambda_{h,m}^*\exp(-i\lambda_k t_F)\exp(-i\lambda_h t_F)b_k^\dagger b_h^\dagger|\mathbf{0}\rangle\ .$$

Let me make use of (6.7) ($\lambda_n - \lambda_{n-1} = \frac{2\pi}{t_F}m_n + \frac{\pi}{t_F}$) to relate λ_h to λ_k. I get:

$$\lambda_k = \frac{2\pi}{t_F}\sum_{i=k-h+1}^{k}\kappa_i + (k-h)\frac{\pi}{t_F} + \lambda_h \quad (k > h)$$

and

$$\lambda_h = \frac{2\pi}{t_F}\sum_{i=h-k+1}^{h}\kappa_i + (h-k)\frac{\pi}{t_F} + \lambda_k \quad (k < h).$$

The case $h = k$ is not relevant because it contributes zero to the sum. Then:

$$\begin{aligned} &\exp(-iHt_F) \quad |\underline{n},\underline{m}\rangle \\ = \quad &\exp(2i\phi) \quad \sum_{h=1}^{N}\left(\sum_{k<h}(-1)^{h-k}\lambda_{k,n}^*\lambda_{h,m}^* b_k^\dagger b_h^\dagger|\mathbf{0}\rangle + \sum_{h<k}(-1)^{k-h}\lambda_{k,n}^*\lambda_{h,m}^* b_k^\dagger b_h^\dagger|\mathbf{0}\rangle\right) \end{aligned}$$

where use has been made of the fact that $\exp(-2i\lambda_h t_F) = \exp(-2i\lambda_k t_F) = \exp(2i\phi)$. Since $\lambda_{n,k} = (-)^{N-k}\lambda_{N-n+1,k}$ (holding for tridiagonal matrices satisfying (6.3)) the phase in the summation cancels out, and therefore I

obtain

$$\exp(-iHt_F)|\underline{n},\underline{m}\rangle = \exp(2i\phi)\sum_{h=1}^{N}\sum_{k<h}\lambda^*_{k,N-n+1}\lambda^*_{h,N-m+1}b^\dagger_k b^\dagger_h|\mathbf{0}\rangle$$

from which it follows, using the definition of the a_n's, that:

$$\exp(-iHt_F)|\underline{n},\underline{m}\rangle = \exp(2i\phi)a^\dagger_{N-n+1}a^\dagger_{N-m+1}|\mathbf{0}\rangle\ .$$

Since $m > n$,

$$\begin{aligned}
\exp(-iHt_F)|\underline{n},\underline{m}\rangle &= \exp(2i\phi)a^\dagger_{N-n+1}a^\dagger_{N-m+1}|\mathbf{0}\rangle \\
&= -\exp(2i\phi)a^\dagger_{N-m+1}a^\dagger_{N-n+1}|\mathbf{0}\rangle \\
&= -\exp(2i\phi)X_{N-m+1}X_{N-n+1}|\mathbf{0}\rangle \\
&= -\exp(2i\phi)|\underline{N-m+1},\underline{N-n+1}\rangle\ ,
\end{aligned}$$

as required. ∎

Then, two excitations are transferred perfectly in a time t_F, modulo an exchange phase arising from the fact that during the transfer two fermions are swapped. The following lemma, crucial in the following, is based on this property.

Lemma 6.1.4 *For every Hamiltonian of the form*

$$H = \sum_{n=1}^{N-1} M_{m,n}(a^\dagger_m a_n)\ ,\quad M_{m,n} \doteq J_n\delta_{m,n+1} + J_m\delta_{m,n-1} - B_m\delta_{m,n}\ ,$$

the unitary time evolution $U(t) \doteq \exp(-iHt)$ *acts as*

$$U(t)^\dagger a_n^\dagger U(t) = \sum_{m=1}^{N} \langle \underline{n}| \exp(-iH_1 t) |\underline{m}\rangle \, a_m^\dagger \, , \tag{6.10}$$

where H_1 *is the Hamiltonian written in the one-excitation subspace.*

Proof

Upon defining the linear transformation (introducing the so-called Majorana fermion operators) [51]:

$$c_{2n-1} \doteq a_n + a_n^\dagger \, , \quad c_{2n} = i(a_n^\dagger - a_n) \, , \; \{c_\mu, c_\nu\} = \delta_{\mu,\nu}$$

one can rewrite the Hamiltonian as

$$\begin{aligned} H &= \frac{i}{4} \sum_{n=1}^{N-1} J_n (c_{2n-1} c_{2(n+1)} + c_{2n+1} c_{2n}) \\ &- \frac{i}{2} \sum_{n=1}^{N} B_n (c_{2n-1}^2 + c_{2n}^2 - 2i c_{2n} c_{2n-1}) \end{aligned}$$

or also as

$$H = i \sum_{\mu,\nu=1}^{2N} h_{\mu,\nu} c_\mu c_\nu$$

where $h = -\frac{i}{4}(Y \otimes H_1)$. Here, H_1 is the Hamiltonian written in the first excitation subspace, $[H_1]_{n,m} \doteq \langle \underline{n}| \, H \, |\underline{m}\rangle$ so that h is a real and antisymmetric matrix. Recall now the Campbell- Baker- Hausdorff formula [52]:

$$U(t)^\dagger c_\xi U(t) = c_\xi + \sum_{n=1}^{\infty} \frac{(-t)^n}{n!} \underbrace{[iH, \, [iH \, , ...[iH, \, c_\xi]}_{n-times} ...] \,] \, .$$

Due to the fact that H is bilinear in the fermionic opeator, one has a nice closure property by which:

$$[iH, c_\xi] = 4 \sum_{\nu=1\ ,\xi\neq\nu}^{2N} h_{\xi,\nu} c_\nu$$

which allows one to obtain, by recursively evaluating the RHS of the Baker Hausdorff formula,

$$U(t)^\dagger c_\xi U(t) = \sum_{m=1}^{2N} [R]_{\xi,m} c_m \ , \tag{6.11}$$

where $R \doteq \exp(-i(Y \otimes H_1)t)$ (use has been made of the explicit expression for h).

The operator R acts over the Hilbert space $\mathcal{H} \doteq \mathcal{H}_2 \otimes \mathcal{H}_N$ of dimension $2N$. Thus a basis defining a representation for R is

$$\{|0,m\rangle \doteq |0\rangle \otimes |\underline{m}\rangle \ , |1,m\rangle \doteq |1\rangle \otimes |\underline{m}\rangle \ : \ m = 1....N\} \ .$$

Representing the operator R in this basis one has:

$$\begin{aligned} \langle 1,\underline{m}| R |1,\underline{n}\rangle &= \langle \underline{m}| \cos(H_1 t) |\underline{n}\rangle = \langle 0,\underline{m}| R |0,\underline{n}\rangle \\ \langle 1,\underline{m}| R |0,\underline{n}\rangle &= \langle \underline{m}| \sin(H_1 t) |\underline{n}\rangle = -\langle 0,\underline{m}| R |1,\underline{n}\rangle \end{aligned} \tag{6.12}$$

Recall now that $a_n^\dagger = \frac{1}{2}(c_{2n-1} - ic_{2n})$; using equations (6.11) and (6.12) finally I get:

$$U(t)^\dagger a_n^\dagger U(t) = \sum_{m=1}^{N} \langle \underline{n}| \exp(-iH_1 t) |\underline{m}\rangle \, a_m^\dagger \ ,$$

as required. ∎

This lemma has therefore provided a way to write the Heisenberg form of a fermionic operator acting on a given site in terms of a linear combination of the fermionic operators acting on the whole chain.

An alternative encoding

I shall immediately make use of the lemma to prove that perfect state transfer can be achieved by using an encoding which uses two qubits instead of one but allows for an arbitrary state on the rest of the chain. This is important because some of the concepts developed here will be used later on.

Notice first that as a consequence of the lemma, one has:

$$U(t_F)a_nU^\dagger(t_F) = \sum_{m=1}^{N} \beta^*_{m,n}(t_F)a_m = \exp(-i\phi)a_{N-n+1} \ , \tag{6.13}$$

because $\beta_{n,m}(t_F) = \langle \underline{m}| \exp(iH_1t_F) |\underline{n}\rangle = \exp(-i\phi)\delta_{n,N-m+1}$ by the perfect state transfer property of H_1, equation (6.3). From now on I shall drop the phase $\exp(i\phi)$, without loss of generality. For a local unitary at the end of the transfer can correct this phase.

I am going to use the above property to prove that the following encoding allows perfect state transfer:

$$|\psi_I\rangle = (\alpha \left|\bar{Q}_0\right\rangle + \beta \left|\bar{Q}_1\right\rangle) \ ,$$

where:

$$\left|\bar{Q}_0\right\rangle \doteq a_1^\dagger |\psi_0\rangle \ \ , \left|\bar{Q}_1\right\rangle = \ a_2^\dagger |\psi_0\rangle \ .$$

Here $|\psi_0\rangle = L\,|\mathbf{0}\rangle$ where the operator L is defined as

$$L \doteq \sum_{x\in S} \alpha_x \prod_{j=1}^{N} (a_j^\dagger)^{x_j}$$

where $S = \{x \in \{0,1\}^N \;:\; x_1 = 0 = x_2\}$. This means that one has to initialize to the 0 state just the first two qubits. On the rest of the chain the state may contain an arbitrary number of excitations.

More explicitly:

$$|\psi_I\rangle = (\alpha\,|0\rangle_1 \otimes |1\rangle_2 + \beta\,|1\rangle_1 \otimes |0\rangle_2) \otimes |\phi\rangle \;\;,$$

where $|\phi\rangle$ is arbitrary. Also, I require $\langle\psi_0|\psi_0\rangle = 1$. These conditions ensure $\langle\bar{Q}_i|\bar{Q}_j\rangle = \delta_{i,j}$.

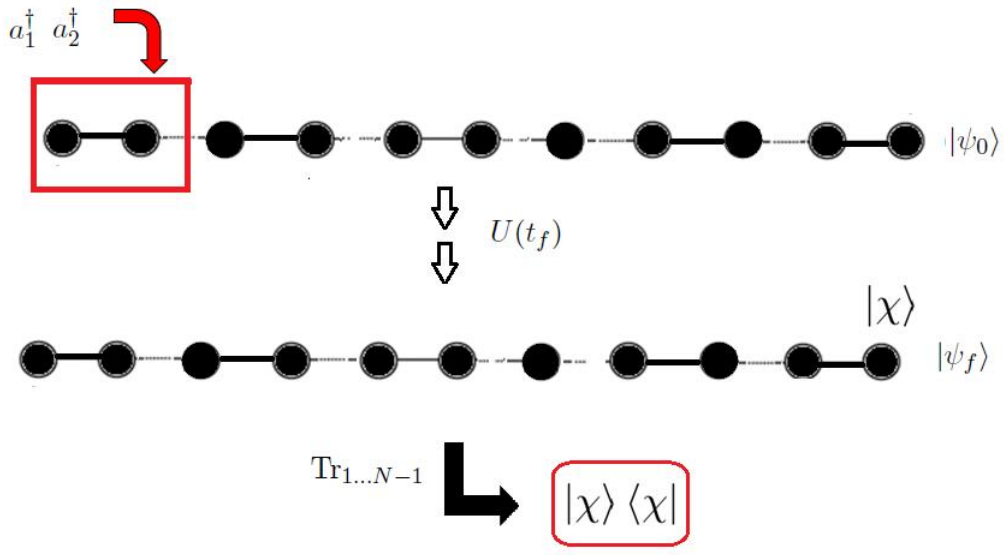


Figure 6.4: The alternative two-qubit encoding. The encoding region is highlighted in red.

The state at the end of the evolution is therefore

$$\begin{aligned} |\psi_f\rangle &= U(t_F)\,|\psi_I\rangle \\ &= [U(t_F)(\alpha a_1^\dagger + \beta a_2^\dagger)U^\dagger(t_F)][U(t_F)LU(t_F)^\dagger]U(t_F)\,|\mathbf{0}\rangle \\ &= (\alpha a_N^\dagger + \beta a_{N-1}^\dagger)L(t_F)\,|\mathbf{0}\rangle \ . \end{aligned} \tag{6.14}$$

Here, use has been made of the property (6.13) and I have defined the operator $L(t_F) \doteq U(t_F)LU(t_F)^\dagger$, whereby

$$L(t_F) = \sum_{x\in S}\alpha_x \prod_{j=1}^{N} U(t_F)(a_j^\dagger)^{x_j}U^\dagger(t_F) = \sum_{x\in S}\alpha_x \prod_{j=1}^{N}(a_{N-j+1}^\dagger)^{x_j} \ .$$

Notice that the fermionic operators appearing in this operator are labeled by the sites between 1 and $N-2$. Therefore, by using the anticommutation relations of the fermionic operators, one has: $L(t_F)a_N^\dagger = a_N^\dagger L'$, $L(t_F)a_{N-1}^\dagger = a_{N-1}^\dagger L'$, where

$$L' \doteq \sum_{x\in S}\alpha_x \prod_{j=1}^{N}(-1)^{w_x}(a_{N-j+1}^\dagger)^{x_j}$$

and w_x is the Hamming weight of the string x counting the number of fermionic operators appearing in each term of the sum. Finally one obtains:

$$|\psi_f\rangle = L'(\alpha a_N^\dagger + \beta a_{N-1}^\dagger)\,|\mathbf{0}\rangle = |\Phi\rangle \otimes (\alpha\,|1\rangle \otimes |0\rangle_N + \beta\,|0\rangle \otimes |1\rangle_N) \ .$$

The explicit definition of the state $|\Phi\rangle$, unimportant to the rest of the reasoning, can be obtained from the L'. Here, the relevant fact is that $\langle\Phi|\Phi\rangle = 1$, because the time evolution is unitary. Then on the last qubit one has the state $|\chi\rangle$, modulo the exchange phase that can be corrected by a local rota-

tion. Hence $\rho_N(t_F) = |\chi\rangle\langle\chi|$ and then the perfect state transfer is achieved. A summary of this encoding-procedure is provided in figure 6.4.

6.1.3 Error analysis: an overview

In a real situation the state transfer is affected by errors, which are inevitably introduced into the system either by imprecisions in the realisation of the quantum channel or by the coupling with the environment. In order to realize the quantum state transfer, it is therefore of the highest importance to develop a theory to describe errors and to define error-correcting strategies, in order to see to what extent the ideal-case results are preserved in the presence of errors. In this section I shall therefore give an overview of the models proposed so far to describe errors. In the end, I shall introduce the problem this chapter is aiming to address, i.e., that of *systematic errors*.

So far, the research has covered only the following classes of errors.

- *Timing errors*

  They arise when the recovery of the state occurs at time $t_F + \delta$. It turns out that a spectrum with minimum spread between the eigenvalues will optimise the fidelity, although of course not perfectly [49]. Moreover, the spectrum with minimum spread is the one defined in [46] and [47], described in the aforementioned simple example.

- *Manufacturing errors*

  Manufacturing errors arise during the fabrication process, since it is

possible to manufactrue the coupling strengths of the Hamiltonian only up to a certain tolerance [49]. These errors have been modeled as random *static* defects in the coupling coefficients, leading to a quantum spin chain with disordered interaction. This case is well-studied: it leads to the phenomenon of the Anderson localization. Roughly speaking, a quantum particle placed anywhere in the chain will diffuse only slightly, even for long times.

More precisely, Osborne, in [53], proposed the following Hamiltonian:

$$H = \sum_{n=1}^{N-1} \mu_n (X_n X_{n+1} + Y_n Y_{n+1}) + \sum_{n=1}^{N} \nu_n Z_n \ .$$

Here μ_j and ν_j are distributed according to some probability distribution, representing the random static perturbation introduced in the coupling strengths as a consequence of the manufacturing imprecision. Assuming that ν_j is distributed as a Cauchy distribution it has been proven that for this system a stronger version of the Lieb-Robinson bound holds, which reflects the presence of the Anderson localisation. According to this bound all information is exponentially attenuated outside a light cone whose radius grows *logarithmically* with time. This implies that two parties having access, respectively, to two bounded regions of the chain cannot use the dynamics of the system to communicate. Indeed, the receiver has to wait for a time which grows *exponentially* (in the size of the region to which the two parties do not have access) before a non-trivial amount of information arrives.

A further step to generalise the theory has been taken by treating

time-varying random perturbations. In particular, Burrel, Eisert and Osborne ([54]) proposed a model to describe a randomly time-varying magnetic field coupled to the Hamiltonian. Two cases have been analysed. In the one case, the magnetic field time-varies randomly both in strength and direction. A Lieb Robinson bound is computed, performing an ensemble-average over all possible realisation of the fluctuating field. Two regimes arise: in the presence of strong disorder, the information is highly localised and the transfer properties are compromised; in the presence of a weaker disorder, the bound seems to indicate the possibility for ballistic transport.

In the other case, the magnetic field aligned in the z direction varies in strength only. It was proven that information (measured in terms of an ensemble-averaged correlation function) propagates along the chain by a distance proportional to $\sqrt{t}$.

Besides, Ronke, Spiller and D'amico [55] analysed numerically the effect of some relevant perturbation factors, discussing the robustness of the state transfer properties in their presence.

Approaching the problem from a different point of view, Burgarth and Bose proposed a protocol for perfect state transfer using two parallel identical spin chains [56]. The encoding is performed over the first qubits of both the chains, and repeated measurements on the receiving end allows for obtaining perfect state transfer. Later on the same authors proposed a modification of the protocol to include the usage of two non-identical chains [57]. This scheme allows a perfect state

transfer also in the presence of errors.In fact, it is not subjected to the limitations imposed by the Lieb-Robinson bounds, since there is no significant probability of success unless you wait a sufficiently long time.

- *Environmental noise*

  In this class there are errors introduced as a result of the coupling with the environment. Although restricting access to the ends of the chain allows one to protect the bulk of the chain to a large degree, one cannot perfectly protect against the environment. Therefore the study of these errors is relevant to the implementation of state transfer.

  The general approach is to consider the chain as an open system. Just a few attempts have been made to describe those errors, the most relevant being that proposed by Wiesniak [58]. He studied the dynamical coupling of the chain with a thermal bath. The author compared different encoding strategies by evaluating their robustness in the presence of the process of thermalization, using both analytical and numerical techniques.

  A less general approach, which has the advantage of being completely analytical, was proposed by Burgarth and Bose [59]. They created an independent bath model where every spin of the chain is coupled to a localized set of spins with similar interactions. The Hamiltonian reads:

$$H^{'} = H + H_I \ , \ H_I \doteq \sum_{m=1}^{N} \sum_{n=1}^{N_m} \frac{1}{2} g_m^n (X_m X_n^{(m)} + Y_m Y_n^{(m)})$$

where g_m^n is the coupling strength of the m-th spin of the chain with the n-th spin of the bath of N_m spins coupled to that particular site.

By restricting to the first excitation subspace it is possible to diagonalize the Hamiltonian and therefore compute the fidelity. It can be proven that the transfer time is doubled, and that an oscillatory term whose frequency is proportional to the coupling strength modulates the fidelity. Thus, it is still possible to achieve the perfect state transfer in this particular case.

A still almost unexplored area is that of addressing *systematic* errors. This class includes all sorts of *predictable* errors affecting the chain. Unlike the vast majority of the errors studied so far, the distinctive feature of systematic errors is that they occur every time one attempts to use the channel, manifesting always the same features (the exact meaning of this statement will become clearer in the next section). Therefore, they have a more controllable nature allowing for a deterministic (or almost deterministic) description. Something close to this scenario was discussed (briefly) by Kay [49], who addressed the problem of describing the effect of the random application of a Z error (dephasing noise) with probability p during the time evolution, on a given site of the chain.

With the aim of digging further into this problem, I propose here encoding and decoding procedures to protect against systematic errors. This shall be discussed in the next section.

6.2 How to protect against systematic errors

One of the promising features of a spin chain is that, in only requiring interactions with the ends of a chain, the majority of the spins can be shielded from the effects of noise. Nevertheless, as we have seen, errors are generated in a practical implementation by manufacturing imprecisions and through coupling with the environment. The main effect of these errors is to compromise the transfer by introducing unwanted excitations and destroying the coherence. In order to reduce this effect, one can consider encoding in an error correcting code. However, applying standard error-correcting codes to state transfer is very inefficient; any error occurring during the transfer, even on a single qubit, is spread over the whole chain by the action of the Hamiltonian. Hence, one expects that a generic error-correcting code would require a large number of encoding qubits per logical qubit, conflicting with the central tenet of the state transfer protocol. It is therefore necessary to design *ad hoc* error correcting codes. In addition to the importance of error correction on the spin chain itself, such studies comprise the essential initial studies of equivalent questions in systems where Hamiltonian dynamics are used in an information processing capacity, such as in a computational architectrue [60].

As explained in the previous section, studies of error correction in state transfer have adopted a cause-based classification that has so far concealed the interesting category of *systematic errors*, by which I mean errors that in each transfer experiment are drawn from a fixed set of possible errors (whose description includes position, time, and type of error). This key feature enables the detection, once and for all, of the set of possible errors, potentially allow-

ing us to protect against them. In the next sections, I present a strategy to recover perfectly from low rates of systematic error on a spin chain, encoding the information in a protected set of states and decoding it accordingly. The number of qubits used for the encoding and decoding scales linearly with the sizes of the errors in the set. The encoding and decoding strategies are presented in the following section, under the assumption that the errors are known, before describing an example of how the errors can be identified in Section 6.2.4, while also indicating that significant efficiency savings can be made over and above the sufficient conditions previously derived.

6.2.1 General Remarks

In the most general case, a systematic error can be described as an error-operator $\mathcal{E}$ which is going to act on the chain at known time t, $0 \leq t \leq t_F$. A way to protect against this error is to define an appropriate encoding which is robust against the error, in the sense that combined with the best possible decoding operation it allows the fidelity of the transfer to be maximised.
Suppose one wants to send the (unknown) state $|\chi\rangle \doteq \alpha\,|0\rangle + \beta\,|1\rangle$, where one can use the parametrisation $\alpha = \cos(\theta)$, $\beta = \sin(\theta)\mathrm{e}^{i\phi}$ (using the Bloch sphere picture). I shall define the encoding operation as the preparation of the system in the state

$$|\psi_I\rangle \doteq \alpha\,|Q_0\rangle + \beta\,|Q_1\rangle$$

where for the moment the only requirement on the encoding states is that $\langle Q_i|Q_j\rangle = \delta_{i,j}$, $\forall i, j = 0, 1$.

The time evolution up to time t_F is

$$M(t) = U(t - t_F)\mathcal{E}U(t)$$

since I suppose that the action of the error-operator is instantaneous, i.e., its characteristic time is by far shorter than the time over which the dynamics of the system takes place. Then the final state will be

$$|\psi_F\rangle = M(t_F)\,|\psi_I\rangle \ .$$

At t_F one applies the unitary decoding operation W and computes

$$\rho_{dec} = \mathrm{Tr}_{\bar{D}}(W\,|\psi_F\rangle\,\langle\psi_F|\,W^\dagger)$$

where D is the decoding region, and $\bar{D}$ its complement.

Upon introducing the average maximal fidelity (over all the input states uniformly spread over the surface of the Bloch sphere)

$$\bar{F} = \int_0^{2\pi}\int_0^{\pi} \max_{\{W\}}\{\langle\chi|\,\rho_{dec}\,|\chi\rangle\}\sin(\theta)\mathrm{d}\theta\mathrm{d}\phi$$

one determines the encoding states so that they maximise $\bar{F}$.

This procedure is rather lengthy. However, if one assumes to know something more about the error, then one can hope for finding the optimal encoding with a more straightforward procedure. In fact, in the next section I shall define a class of errors $\mathcal{E}$ for which it is possible to define encoding and decoding procedures to achieve the maximum fidelity, i.e., $F = 1$ independently of α

and β, by following a rather simple procedure. As we shall see, the error class against which this procedure protects is still rather broad. It includes, indeed, all errors written in the basis provided by the Pauli operators having a sufficiently small support (i.e., acting over a sufficiently small number of sites).

6.2.2 Modelling Systematic Errors

A systematic error is represented by a set of possible errors $\{\mathcal{E}_\ell\}$ acting at times $\{t_\ell\}$. Using the $\{a_i^\dagger\}$ as a basis, each of these $\mathcal{E}_\ell$ can be expanded as

$$\mathcal{E} \doteq \sum_{i=1}^{s} \gamma_i \prod_{j=1}^{m_i} a^\dagger_{k_j^{(i)}} \prod_{j=m_i+1}^{n_i} a_{k_j^{(i)}} \ , \tag{6.15}$$

where $k_j^{(i)}$ are the n_i positions that the creation/annihilation operators act on. For a given i, the sets $\{k_j^i\}_{j=1}^{m_i}$ and $\{k_j^i\}_{j=1}^{m_i}$ may share common sites, and so may $\{k_j^i\}_{j=1}^{n_i}$ and $\{k_j^\ell\}_{j=1}^{n_\ell}$. The $\{\gamma_i\}$ are arbitrary coefficients. For the sake of presenting our results, I shall confine attention here to a unitary operator $\mathcal{E}$. This model includes the bit flips $X_i = \prod_{j=1}^{i-1} a_j^\dagger a_j (a_i + a_i^\dagger)$ and the phase errors $Z_i = (\mathbb{1} - 2a_i^\dagger a_i)$. For simplicity of exposition, I shall work with just one error $\mathcal{E}$ acting at time t, the effect of multiple errors being easily incorporated. The error is assumed to act instantaneously, or, at least, for a time much smaller than t_F, so that otherwise the time-evolution is governed by U [3]. Let me introduce the notation $\hat{a}_i(t) \doteq U(t) a_i U^\dagger(t)$. The state at time t_F is

$$|\psi_F\rangle = \hat{\mathcal{E}}(t_F - t) U(t_F) \, |\psi_I\rangle \ ,$$

[3] I comment on the relaxation of this assumption in the conclusions.

with

$$\hat{\mathcal{E}}(t_F - t) = \sum_{i=1}^{s} \gamma_i \prod_{j=1}^{m_i} \hat{a}^{\dagger}_{k_j^{(i)}}(t_F - t) \prod_{j=m_i+1}^{n_i} \hat{a}_{k_j^{(i)}}(t_F - t) \; . \tag{6.16}$$

The fermionic operators $\hat{a}_i(t_F - t)$'s represent the (possibly non-orthogonal) fermionic modes affected by the error.

6.2.3 How to Counteract Systematic Errors

In order to counteract these systematic errors, I shall encode the information about the state $|\chi\rangle$ in the first D qubits at one end of the chain, called the *encoding region*. The encoding will be defined so that perfect state transfer can be achieved by applying a unitary decoding operator U_D at time t_F, acting just over a *decoding region* of size D at the opposite end of the chain (see Fig. 6.5). I refer to the region outside the decoding region as the complement region, which has size $\bar{D} \doteq N - D$. The size D will be determined by the number of errors that one has to encode against, but should be considered small compared to the transfer distance, N.

State Encoding

I propose to encode the information in the state

$$|\psi_I\rangle \doteq (\alpha Q_0^{\dagger} + \beta Q_1^{\dagger}) \, |\psi_0\rangle \tag{6.17}$$

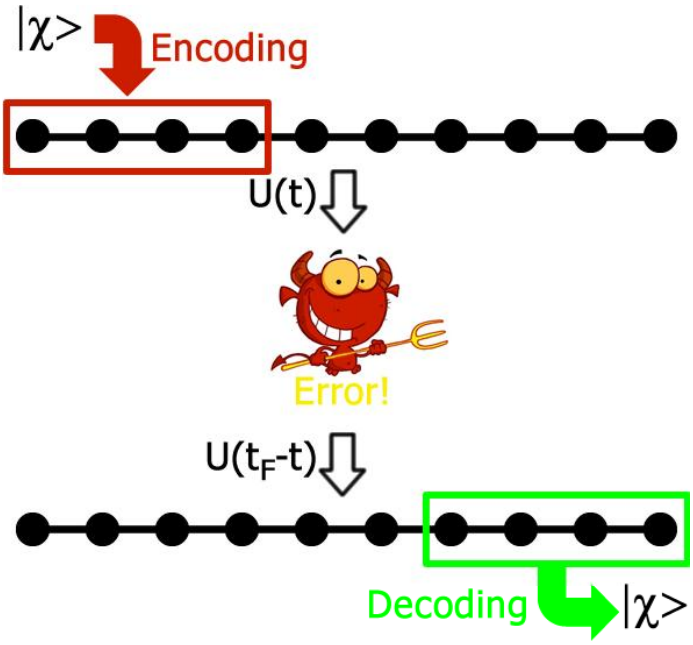


Figure 6.5: General schematic for the operation of a perfect state transfer system in the presence of a systematic error at time t via an initial encoding and corresponding decoding in small regions at either end of the chain.

where the encoding operators

$$Q_\mu^\dagger \doteq \sum_{i=1}^{D} (\epsilon_i^\mu a_i^\dagger + \eta_i^\mu a_i),\ \mu \in \{0,\ 1\}\ ,\quad \epsilon_i^\mu\ ,\quad \eta_i^\mu \in \mathbb{C} \tag{6.18}$$

are to be determined to ensure that the decoding operation U_D exists; the state $|\psi_0\rangle$ fulfils:

$$Q_\mu\,|\psi_0\rangle = 0\ ,\quad \forall\ \mu \in \{0,\ 1\}\ . \tag{6.19}$$

I require the $\{Q_\mu\}$'s to represent two orthogonal fermionic modes, which imposes the conditions

$$\{Q_\mu, {Q_{\mu'}}^\dagger\} = \delta_{\mu,\mu'} \iff \sum_{i=1}^{D} (\epsilon_i^\mu {\epsilon_i^{\mu'}}^* + \eta_i^\mu {\eta_i^{\mu'}}^*) = \delta_{\mu,\mu'}\ ,\ \forall\ \mu \in \{0,\ 1\} \tag{6.20}$$

$$\left\{Q_\mu, Q_{\mu'}\right\} = 0 \iff \sum_{i=1}^{D} (\epsilon_i^\mu \eta_i^{\mu'} + \eta_i^\mu \epsilon_i^{\mu'}) = 0 \;.\; \forall\, \mu \in \{0,\, 1\} \tag{6.21}$$

This ensures that the logical 0, $Q_0^\dagger \left|\psi_0\right\rangle$, and the logical 1, $Q_1^\dagger \left|\psi_0\right\rangle$, are orthogonal, normalised states, $\left\langle\psi_0\right| Q_\mu Q_{\mu'}^\dagger \left|\psi_0\right\rangle = \delta_{\mu,\mu'}$. The idea behind the proposed definition is that if the encoding operators correspond to fermionic modes different from the ones affected by the error, the orthogonality of the encoding states would be unaffected by the error, and so would the encoded information. In addition, since the Hamiltonian describes independent fermions, the transfer of the information-carrying excitations would be independent of the excitations introduced by the error, making it possible to recover the information by applying an appropriate decoding operation at time t_F. I shall now formalise this intuition.

State Decoding

Let me rewrite $\left|\psi_F\right\rangle$, highlighting the action of the time-evolved error and encoding operators on the decoding region. To do this, I describe the action of any given fermionic operator as a product of the part that acts on the decoding region, and the part that acts on its complement.

$$\begin{aligned} a_j^\dagger &= \tilde{f}_j^\dagger \otimes \mathbb{1}^{\otimes D} \;,\; \tilde{f}_j = \frac{1}{2} Z^{\otimes j-1} \otimes \left(X - iY\right) \otimes \mathbb{1}^{\otimes \bar{D}-j} \;,\; \forall j \leq \bar{D} \\ a_j^\dagger &= Z^{\otimes \bar{D}} \otimes f_j^\dagger \;, f_j^\dagger \doteq \frac{1}{2} Z^{j-\bar{D}-1} \otimes \left(X - iY\right) \otimes \mathbb{1}^{N-j} \;\; \forall j > \bar{D} \;, \end{aligned}$$

with $\{f_j^\dagger, f_i\} = \delta_{i,j}$, $\{f_i, f_j\} = 0$ (and similarly for the $\tilde{f}_j$'s). Hence, by lemma 6.1.4, a fermionic operator evolved in time from when it acts up to

the decoding time, t_F, is expressed as

$$\hat{a}_n(t) = \tilde{F}_n(t) \otimes \mathbb{1}^{\otimes D} + Z^{\otimes \bar{D}} \otimes F_n(t) \ ,$$

with $\tilde{F}_n(t) \doteq \sum_{m=1}^{\bar{D}} \beta_{n,m}(t-t_F)\tilde{f}_m$, $F_n(t) \doteq \sum_{m=\bar{D}+1}^{N} \beta_{n,m}(t-t_F) f_m$. The $F_n(t)$ represent the action of the error on the decoding region. We shall see that the error action on the complement of the decoding region (represented by $\tilde{F}_n(t)$) is irrelevant for the recovery of the state. Substituting in Eq. (6.16), one obtains

$$\mathcal{E}(t_F - t) = \sum_{i=1}^{s} \gamma_i \sum_{x \in \{0,1\}^{n_i}} \tilde{P}_{\bar{x}}^{(i)} \Lambda_x \otimes P_x^{(i)} \tag{6.22}$$

summing over the string x in order to convey within the $P_x^{(i)}$ all the different combinations of $F_{k_j^i}$ acting on the decoding region

$$P_x^{(i)} \doteq \prod_{j=1}^{m_i} \left(F_{k_j^i}^{\dagger}\right)^{x_j} \prod_{j=m_i+1}^{n_i} \left(F_{k_j^i}\right)^{x_j} \ , \ \ \Lambda_x \doteq (-1)^{\epsilon_{\bar{x}}} \prod_{j=1}^{n_j} (Z^{\otimes \bar{D}})^{x_j},$$

with $\tilde{P}_x^{(i)}$ (obtained by substituting $\tilde{F}_{k_j^i}$ for $F_{k_j^i}$) conveying the equivalent information for the complement region[4]. The complement of x is denoted by $\bar{x}$. ϵ_x conveys the parity of the ordering of the string x, as arises from imposing a standard ordering of the fermionic operators. Rewriting the encoding operators in the same formalism, one has:

$$U(t_F)\,|\psi_I\rangle = (\alpha \hat{Q}_0(t_F) + \hat{Q}_1(t_F))\,|\psi_{out}\rangle \ , \ |\psi_{out}\rangle \doteq U(t_F)\,|\psi_0\rangle \tag{6.23}$$

[4]The argument t has been omitted for simplicity.

where

$$\hat{Q}^\dagger_\mu(t_F) = Z^{\otimes \bar{D}} \otimes q_\mu \ , \ \ q^\dagger_\mu \doteq \sum_{i=1}^{D} \epsilon^\mu_i f^\dagger_{N-i+1} + \eta^\mu_i f_{N-i+1} \ .$$

To complete the rewriting, note that it is always possible to write $|\psi_{out}\rangle = \sum_i |\phi_i\rangle \otimes |\psi_i\rangle$, where $|\phi_i\rangle$ is any (not normalised) state defined over the complement of the decoding region, and, via Eq. (6.19), $|\psi_i\rangle$ is a solution to

$$q_\mu |\psi\rangle = 0 \ , \mu = 0, 1 \ . \tag{6.24}$$

One can find this state as an eigenstate of the operator $q^\dagger_0 q_0 q^\dagger_1 q_1$ with eigenvalue 1. Provided $D \geq 2$, such eigenstates always exist (the size of the Hilbert space spanned by the solutions of this equation is 2^{D-2}; hence $|\psi_{out}\rangle$ can be chosen in a Hilbert space of dimension 2^{N-2}, i.e., condition (6.19) is not too restrictive). In what follows, I shall work with $|\psi_{out}\rangle = |\phi\rangle \otimes |\psi\rangle$ for the sake of simplicity, and more general states follow by linearity.

The state at time t_F can be rewritten as:

$$|\psi_F\rangle = \sum_{i=1}^{s} \gamma_i \left(\sum_{x \in \{0,1\}^{n_i}} \left|\phi^i_{\bar{x}}\right\rangle \otimes (\alpha \left|\mathbf{0}^{(i)}_x\right\rangle + \beta \left|\mathbf{1}^{(i)}_x\right\rangle) \right) \ , \tag{6.25}$$

with $\left|\mathbf{0}^{(i)}_x\right\rangle \doteq P^{(i)}_x q_0 |\psi\rangle$, $\left|\mathbf{1}^{(i)}_x\right\rangle \doteq P^{(i)}_x q_1 |\psi\rangle$ and $|\phi^i_{\bar{x}}\rangle \doteq \tilde{P}^{(i)}_{\bar{x}} \Lambda_x Z^{\otimes \bar{D}} |\phi\rangle$. I shall now prove that if Eqns. (6.20), (6.21) and (6.24) hold, it is sufficient to

impose that

$$\begin{aligned}\left\{q_\mu^\dagger, F_{k_j^{(i)}}\right\} &= 0 \iff \sum_{l=1}^{D} \beta_{k_j^{(i)},l}(t)\eta_l^\mu = 0 \\ \left\{q_\mu^\dagger, F_{k_j^{(i)}}^\dagger\right\} &= 0 \iff \sum_{l=1}^{D} \beta^*_{k_j^{(i)},l}(t)\epsilon_\ell^\mu = 0 \ , \end{aligned} \tag{6.26}$$

for both encoded states ($\mu = 0, 1$), and each of the possible operators F_j ($j = 1 \dots n_i$) from all possible error strings ($i = 1 \dots s$), to ensure the existence of least one unitary U_D that, applied at time t_F, perfectly recovers the encoded information. Fulfilling these conditions then defines the coefficients of the encoding operators in Eq. (6.18), completely specifying our strategy.

Let me introduce the sets of vectors: $Z_\mu \doteq \left\{ \left| \mu_x^{(i)} \right\rangle \ : \ x \in \{0,1\}^{n_i} \ \ \forall\, i = 1 \dots s \right\}$, $\mu = 0, 1$, representing the domain of U_D . Conditions (6.26) imply the crucial property

$$P_x^{(i)} q_\mu = (-1)^{w_x} q_\mu P_x^{(i)} \ , \quad P_x^{(i)} q_\mu^\dagger = (-1)^{w_x} q_\mu^\dagger P_x^{(i)} \ , \ \forall \mu \ , \ \forall x \ , \ \forall i \ . \tag{6.27}$$

Consequently, via (6.21) and (6.24), no matter what the error, the two logically encoded states remain unambiguously distinguishable, $\left\langle \mathbf{0}_x^{(i)} | \mathbf{1}_y^{(j)} \right\rangle = 0$, $\forall x \in \{0,1\}^{n_i}$, $\forall y \in \{0,1\}^{n_j}$, $\forall i, j$. This is already sufficient to imply the existence of U_D, although I give an explicit construction in the Appendix.

I have just proven that conditions (6.20), (6.21), (6.24) and (6.26) define a fermionic encoding that protects perfectly from the error, allowing the perfect recovery of the information. The extension of the above procedure to the case of errors acting at different times $\{t_i\}$ is straightforward, by defining the sets $\{F_\ell(t_i)\}$ and imposing for each t_i conditions (6.26). Suppose $\bar{n}$ is the number

of distinct sites affected by the error $\mathcal{E}$. There are $4\bar{n}+6$ conditions for the $4D$ parameters defining the q_μ's. The minimal D for which a solution may be found is $D=\bar{n}+2$, with $2 \leq D \leq N$. Under this assumption, conditions (6.26), involving operators representing the error-action just on the decoding region, suffice to define fermionic modes globally unaffected by the error.

In a practical sense, the procedure is worthwhile only if $\bar{n} \ll N$, since this confines the encoding and decoding procedures to the ends of the chain, preserving the central tenet of the state transfer protocol. I therefore take the condition $\bar{n} \ll N$ as defining the concept of a low error rate in this scenario. It is important to emphasise, however, that this counting is in terms of the fermionic description of the error operators. Such counting is favourable for errors such as Z_i or X_iX_{i+1}, but there are other local Pauli errors, such as X_i, which are necessarily described in terms of $O(i)$ fermionic modes, and therefore may not be included in the low rate condition.

As previously mentioned, the typical assumption that the chain is initialised in some global initial state $|\psi_0\rangle$ is not necessary [49, 61, 62]. This is also true of our procedure. Indeed, there are two contexts in which our results apply equally. Either one can choose what the initial state should be, as I have so far assumed, or one is given a fixed initial state, in which case (6.24) gives two additional constraints on the encoding operators, which can be accommodated by our choice of D. The advantage of choosing a particular initial state is that it may reduce the effective number of errors that one has to correct for. The following section provides an illustration of this idea.

6.2.4 Determining the Error

Given a spin-chain affected by an (unknown) error $\mathcal{E}$ acting at time t, conditions (6.26) indicate what knowledge of the error is needed to apply our encoding procedure. What experiment can one perform in order to gain this knowledge? One may, of course, use process tomography [63] to determine $\mathcal{E}(t_F - t)$, but this is extremely inefficient and would provide a lot of redundant information. Our description of the error suggests indeed that there must be more efficient procedures, based on preparing the chain in a suitable set of states and then applying state tomography just on the decoding region to determine the error modes $\{F_k\}$, with little regard for those acting on the complement region, $\{\tilde{F}_k\}$. I shall now define a probing procedure in the case $|\psi_0\rangle = |\mathbf{0}\rangle$, motivating the existence of such procedures by using the most commonly assumed fixed initial state.

In the case where the entire chain is initialised in the state $|\psi_0\rangle = |\mathbf{0}\rangle$, it is only necessary to reconstruct a subset of the error modes. Indeed, observe that the encoding operators contain only creation operators, i.e., $\eta_i^\mu = 0$, $\forall i = 1, \dots D$, hence in (6.26) the equations $\{q_\mu, F_{k_j^i}\} = 0$, $\forall i, j$ are automatically satisfied. Also, note that in $\mathcal{E}$ the fermionic operators are ordered so that the annihilation operators act first. If $|\psi_0\rangle = |\mathbf{0}\rangle$, there are no excitations on the complement region and therefore all error strings with any annihilation operators $\tilde{F}_k$ on the complement region just give a zero-contribution to the final state. In other words, from Eq. (6.25), for any i, $|\phi_{\bar{x}}^i\rangle \neq 0$ if and only if $x \in C$, with $C \doteq \{x : \bar{x}_j = 0 \ , \forall \ j \geq m_i + 1\}$. These x correspond to $\tilde{P}_{\bar{x}}^{(i)}$ including no $\tilde{F}_k$. Furthermore, $\forall x \in C$, since $q_\mu^\dagger |0\rangle^{\otimes D}$

belongs to the 1-excitation subspace, only the error modes containing no more that one annihilation operator F_k acting on the decoding region do not annihilate the encoding state. Namely, $P_x^{(i)} q_\mu^\dagger |\psi\rangle \neq 0$ if and only if $n_i = m_i$ or $n_i = m_i + 1$. Let me define the sets $S_\ell \doteq \{i : n_i - m_i = \ell\}$. I have just shown that to protect against the error it is sufficient to protect against all the $P_x^{(i)}$ such that $i \in S_\ell$, $\ell = 0, 1$, and $x \in C$. So, it is sufficient that the encoding operators satisfy:

$$\begin{aligned} \{q_\mu^\dagger, F_{k_j^i}\} &= 0, \forall j = 1 \ldots n_i, \forall i \in S_0 \\ \{q_\mu^\dagger, F_{k_j^i}\} &= 0, \forall j = 1 \ldots n_i, \forall i \in S_1. \end{aligned}$$

Moreover, $\forall i \in S_1$, the latter reduces to just

$$\{q_\mu^\dagger, F_{k_{n_i}^i}\} = 0, \forall i \in S_1$$

because this implies that $P_x^{(i)} q_\mu^\dagger |0\rangle^{\otimes D} = 0$, $\forall x \in C$, so imposing the conditions for $j = 1 \ldots m_i$ becomes unnecessary.

In order to provide the information relevant to these conditions, one can probe the system with two different initial states, $|\mathbf{0}\rangle = |0\rangle^{\otimes N}$ and $|\mathbf{1}\rangle = |1\rangle^{\otimes D} |0\rangle^{\otimes \bar{D}}$. Note that both of these are prepared using the same fixed initial state outside the encoding region (in which one has the ability to prepare any state), and this fixed state is the same one that will be used for the state transfer protocol. Consider first using $|\mathbf{0}\rangle$. The only error operators that do not annihilate the probing state are the $P_x^{(i)}$ such that $i \in S_0$ and $x \in C$, which indeed do not include any annihilation operators. In order to

reconstruct the information about the corresponding ${F_{k^{(i)}}}^\dagger$, one can therefore post-select on the decoding region being the the one-excitation subspace, and perform tomography to determine the corresponding density matrix. The span of states is described by the set $V_0 \doteq \{F_{k_i}^\dagger |0\rangle^{\otimes D}\}, \forall j = 1 \dots m_i, \forall i \in S_0$. Hence, state tomography [63] applied just to the decoding region allows one to reconstruct Span$\{V_0\}$, which is sufficient information to impose $\{q_\mu^\dagger, F_{k_j^i}\} = 0$, $\forall j = 1 \dots n_i, \forall i \in S_0$.

When one uses the initial state $|\mathbf{1}\rangle$, the only non-zero contribution to the final state is given by all the $P_x^{(i)}$ $\forall x \in C$, $i = 1 \dots s$. Hence, the projection of this state on the $D-1$ excitation subspace of the decoding region at time t_F includes the action of the $P_x^{(i)}$ with $x \in C$ and $i \in S_{w_x+1}$, i.e., the $P_x^{(i)}$ where one more F_k operator acts than $F_j^\dagger$ operators. The span of these states hence includes those I am interested in, $V_1 \doteq \{F_{k_{m_i+1}} |1\rangle^{\otimes D}\}_{i \in S_1}$, but also includes some others, V'. This information is sufficient to impose the remaining conditions $\{q_\mu^\dagger, F_{k_{n_i}^i}\} = 0$, $\forall i \in S_1$, as desired, together with additional (unnecessary) conditions, which would protect from the error-components contributing to $V^{'}$. This redundancy is well tolerated, however, since we have assumed that the number $\bar{n}$ of the single error-modes is small compared to N.

Overall, this procedure gives a method to determine the relevant errors using only operations on the encoding/decoding regions, and requiring a number of measurements that scales as $O(2^D)$, and $D \simeq \bar{n} \ll N$, thereby achieving a significant efficiency saving compared to standard process tomography on the whole chain.

6.2.5 Conclusions

I have presented a protocol, incorporating encoding and decoding procedures, to achieve perfect state transfer in the presence of low rates of systematic errors, whose repeatability allows one to learn about their structure. This procedure may be thought of as an error correction optimally tuned to the error. Indeed, it ensures perfect recovery and, in addition, it has the appealing feature that if the number of sites affected by the error is small compared to the dimension of the whole chain, the encoding and decoding operators involve just a small number of qubits, preserving the central feature of the ideal state transfer protocol.

The low rate limit may be relaxed slightly, by extending the procedure to include errors with a support greater than the upper bound n, by selecting, via the proposed probing procedure, the first n operators F_k having the highest probability of acting on the decoding region and then encoding against them. This would minimise the probability of an unrecoverable error.

Our formalism can also be applied in more general scenarios, where the action of the error is not instantaneous, since it is sufficient to describe the effect of any error just at the output time, t_F. For instance, consider the case of a perturbed Hamiltonian, such as $H = H_0 + \delta V$, where H_0 is the perfect state transfer Hamiltonian while $\delta V(t)$ is a perturbation which acts non-trivially only for a short time interval δ at time t. In the interaction picture, the dynamics is determined by $H^{'}(t) = U(t)\delta V U^{\dagger}(t)$. Hence,

$$\mathcal{E} = U(t_F - t) \exp(-i \int_0^{\delta} H^{'}(\tau) \mathrm{d}\tau) U^{\dagger}(t_F - t) \left|\psi_{out}\right\rangle .$$

For small δ, $\exp(-i\int_0^\delta H'(\tau)\mathrm{d}\tau)$ can be written just like the error (6.15), affecting, according to the Lieb-Robinson bound [64], only a small number of sites localised around the region where the perturbation acts. Therefore, the proposed encoding may equally be applied to recover perfect state transfer in the presence of this class of perturbations.

In the future, it will be interesting to see how the error correcting capabilities can be developed further, either by encoding on a single chain or across multiple chains, or by using different network topologies for communication. It will also be important to understand if errors such as local bit-flips can be corrected for.

Appendix: Construction of the Decoding Unitary

To explicitly construct the decoding unitary, one orthogonalises the vectors belonging to each Z_a via the Gram-Schmidt procedure:

$$|\breve{\mathbf{a}}_{x,j}\rangle \doteq \left|\mathbf{a}_x^{(j)}\right\rangle - \sum_{y,l} \frac{\left\langle \breve{\mathbf{a}}_{y,l}|\mathbf{a}_x^{(j)}\right\rangle}{\langle \breve{\mathbf{a}}_{y,l}|\breve{\mathbf{a}}_{y,l}\rangle} |\breve{\mathbf{a}}_{y,l}\rangle \tag{6.28}$$

The number z of such vectors satisfies $z \leq \sum_{j=1}^{s} 2^{n_j}$ (as some vectors in Z_a may be linearly dependent). Then, U_D can be defined as:

$$U_D = \sum_{w,l}\sum_{a} \left(|w,l\rangle \otimes |a\rangle\right) \langle \breve{\mathbf{a}}_{w,l}| \,,$$

where the sum runs over all the orthogonalised vectors and $\{|w,h\rangle\}$ is any set of orthonormal vectors, defined over all the decoding region but qubit N. To see that the above is the desired unitary, one rewrites $|\psi_F\rangle$ in terms of

the orthogonalised vectors and uses

$$\left\langle \breve{\mathbf{0}}_{w,l} | \mathbf{0}_x^{(j)} \right\rangle = \left\langle \breve{\mathbf{1}}_{w,l} | \mathbf{1}_x^{(j)} \right\rangle \doteq \mu_{w,l}^{(x,j)} \quad \forall j, x, i, y \ ,$$

which holds because (6.20), (6.24) and (6.27) imply

$$\left\langle \mathbf{1}_x^{(i)} | \mathbf{1}_y^{(j)} \right\rangle = \left\langle \mathbf{0}_x^{(i)} | \mathbf{0}_y^{(j)} \right\rangle \ , \ \forall x, \forall y \ , \ \forall i, j \ .$$

Consequently, U_D applied to $|\psi_F\rangle$, gives:

$$|\psi_d\rangle \doteq (\mathbb{1}_{\bar{D}} \otimes U_D) \, |\psi_F\rangle = |\Phi\rangle \otimes (\alpha|0\rangle_N + \beta|1\rangle_N) \, ,$$

where $|\Phi\rangle \doteq \sum_{x \in \{0,1\}^{n_i}} |\phi_{\bar{x}}^i\rangle \otimes \sum_{w,l} \mu_{w,l}^{x,i} \, |w, l\rangle$. Since $\mathcal{E}$ is trace-preserving,

$$\mathrm{Tr}_{1 \ldots N-1}(|\psi_d\rangle \langle\psi_d|) = |\chi\rangle \langle\chi| \, ,$$

i.e., the information has been perfectly transferred to the last qubit, as promised.

Chapter 7

Concluding remarks

In this thesis I have shown that the newly conceived Constructor Theory, which David Deutsch proposed to generalise the Quantum Theory of Computation, not only provides a new, promising mode of explanation, but also the possibility of formulating new scientific theories.

I have presented the Constructor Theory of Information, developed with David Deutsch, that has provided beautiful unifications: it has explained the relationship between classical and quantum information, revealing a single underlying origin of the most distinctive phenomena associated with the latter; it has allowed to incorporate information into physics, curing the circularities that affected the previous theories.

I have then proposed a model of the logic of self-replication that updates Von Neumann's and is provably consistent with Quantum Theory, thus rebutting the alleged incompatibility of self-replication with Quantum Theory, and understanding self-replication explicitly within physics, and distinguishing it from cloning a quantum state.

Finally, I have proposed a protocol to counteract systematic errors in quantum state transfer, in collaboration with Alastair Kay and Artur Ekert, which allows one to recover the most appealing features of the ideal protocol (small control areas at the two ends of the chain, no control required during the transfer, possibility of setting up the protocol once and for all) in the presence of systematic errors.

This thesis has many promising future developments, some of which I mention in the following.

Constructor theory can be used as a language for expressing laws of physics, unifying emergent and microscopic ones (as needed to express e.g. the second law of thermodynamics without coarse-graining). Moreover, expressing Quantum Theory in constructor-theoretic terms is expected to yield some illuminating results about the foundations of Quantum Theory (for instance, about the recent controversy on locality and the role Heisenberg state [25], [23]). The Constructor Theory of Information also shows promise for many applications, such as identifying the resource that makes quantum computation powerful; classifying entanglement [65] and more-than-quantum correlations [66].

My work on self-replication could be extended, on the one hand, to investigate whether the existence of a universal constructor (which generalises the notion of universal quantum computer) follows from the laws of Constructor Theory; on the other, to understand in which scenarios quantum coherence could be useful to self-replicators and, in passing, address the related problem of how to implement coherent quantum communication in the presence of noise.

I very much look forward to setting out on this new quest.

Bibliography

[1] R. Landauer, Physics Today, **44**, 5 (1991).

[2] D. Deutsch, Constructor Theory, Synthese, 10.1007/s11229-013-0279-z, (2013).

[3] D. Deutsch, C. Marletto, "Constructor Theory of Information", in preparation.

[4] E. Schrödinger, *What is life?* (1944).

[5] A. Pati, S. Braunstein, *Quantum Mechanical Universal Constructor*, in *Quantum Aspects of Life*, edited by D. Abbott, P. Davies, A. Pati, with a foreword by Sir R. Penrose, (2008).

[6] I. Chakrabarty, Prashant, B. S. Choudhury, Int. J. Theor. Phys., **46**, 12, 3281-3284 (2004).

[7] A. Pati, Fluctuation and Noise Letters, **4**, pp. R27-R38 (2004).

[8] E.P. Wigner, *On the probability of a self-reproducing unit*, in *The logic of personal knowledge* (edited by M. Polanyi), London (1961).

[9] H.Yockey, J. Theor. Biol. **46**, 369 (1974).

[10] J. von Neumann, *The general and logical theory of automata*, in the Hixon Symposium (edited by L.A. Jeffress), New York, John Wiley and Sons, (1951).

[11] J. von Neumann, A. Burks, *The theory of self-reproducing automata*, Univ. of Illinois Press, (1966).

[12] G. Fleming *et al.*, Science **316**, 1462 (2007).

[13] E. Collini *et al.*, Nature **463**, 644-647 (2010).

[14] C. Marletto, A. Kay, A. Ekert, QIC, **12** , 7 and 8 (2012).

[15] M. B. Plenio and S. F. Huelga, New J. Phys. **10** 113019 (2008).

[16] K. Popper, "Objective Knowledge", Oxford University Press, (1979).

[17] D. Deutsch, Proc. R. Soc. Lond. A, **400**, 1818, 97-117, (1985).

[18] D. Deutsch, *Physics, Philosophy and Quantum Technology*, Proceedings of the Sixth International Conference on Quantum Communication, Measurement and Computing, Shapiro, J.H. and Hirota, O., Eds. (Rinton Press, Princeton, N.J. 2003).

[19] D. Deutsch, Proc. R. Soc. A **455** 312937, (1999).

[20] D. Wallace, Studies in the History and Philosophy of Modern Physics **34**, 41539, (2003).

[21] A. Einstein (1949, p.85) quoted in Albert Einstein: Philosopher, Scientist, P.A. Schilpp, Ed., Library of Living Philosophers, Evanston, 3rd edition (1970).

[22] D. Deutsch, P. Hayden, Proc. R. Soc. A**456** 1759-74, (2000).

[23] D. Deutsch, Proc. R. Soc. A **468** 531-44, (2012).

[24] C. Hewitt-Horseman, V. Vedral, New Journal of Physics, **9**, 5, 135 (2007).

[25] D. Wallace, C. J. Timpson, Found. Phys. **37** 951-5, (2007).

[26] H. Nakano, "Spectral Theory in the Hilbert Space", Japan Society for the Promotion of Science, Tokyo, 1953.

[27] M. Nielsen, I. Chuang, Phys. Rev. Lett., **79**, 2, (1997).

[28] C. E. Shannon, Bell System Technical Journal **27**, 379423, 623656 (1948).

[29] C.H. Bennett, S.J. Wiesner, Phys. Rev. Lett. **69** 2881-4, (1992).

[30] W.K., Wootters,W.H. Zurek, Nature **299** 802-3, (1982).

[31] J. Walgate, A. J. Short, L. Hardy, V. Vedral, Phys. Rev. Lett. **85**, 4972 (2000).

[32] P. Shor, Geom. Funct. Anal., Special Volume, GAF A2000, 816838, (2000).

[33] C.H. Bennett *et al.* Phys. Rev. A **59**, 2, (1999)

[34] Zurek, W.H. (1981) Phys. Rev. D24 1516-25.

[35] R. Dawkins, "The Blind Watchmaker", (1986).

[36] C. Seife, Science **300**, 884, (2003).

[37] C. Darwin, *The Origin of Species*, (1859).

[38] R. Dawkins, *The Selfish Gene*, Oxford University Press, (1976).

[39] R. Dawkins, *The Extended Phenotype*, Oxford University Press, (1982).

[40] R.A. Fisher, *The Genetical Theory of Natural Selection*, Oxford, Clarendon Press, (1930).

[41] M. Ridley, *Mendel's Demon: gene justice and the complexity of life*, Weidenfield and Nicholson, (2000).

[42] J. Baez, Foundations of Physics, **19**, 1 (1989).

[43] S. D. McCulloch , T.A. Kunkel, Cell Res. **18**: 14861, 2008.

[44] C. H. Bennett, "Logical Depth and Physical Complexity", pp. 227-257 in The Universal Turing Machine a Half-Century Survey, edited by Rolf Herken, Oxford University Press (1988)

[45] S. Bose, Phys. Rev. Lett. **91**, 20791, (2003).

[46] M. Christandl, N. Datta, T. Dorlas, A. Ekert, A. Kay and A. Landahl Phys. Rev. A **71**, 032312, (2005).

[47] M. Christandl, N. Datta, A. Ekert and A. J. Landahl, Phys. Rev. Lett. **92**, 187902, (2004).

[48] A. Kay, Phys. Rev. A **73**, 032306, (2006).

[49] A. Kay, Int. J. Quantum Inf. **8**, 641, (2010).

[50] M. A. Nielsen, *The Fermionic canonical commutation relations and the Jordan-Wigner transform*, (2005).

[51] R. Josza, A. Miyake, Proc. R. Soc. A, **464**, 2100, 3089-3106, (2008).

[52] R. Gilmore, *Lie groups, Lie algebras and some of their applications*, Dover Publications, 2005.

[53] C. Burrell and T. J. Osborne, Phys. Rev. Lett., **99**, 16, 167201, (2007).

[54] C. Burrell, J. Eisert and T. J. Osborne, Phys. Rev. A **80**, 052319, (2009).

[55] R. Ronke, T. Spiller and I. D'Amico, Journal of Physics, **286** 012020, (2011).

[56] D. Burgarth and S. Bose, Physical Review A **71**, 052315, (2005).

[57] D. Burgarth and S. Bose, New J. Phys. **7** 135, (2005).

[58] M. Wiesniak, quant-ph/0711.2357 (2007).

[59] D. Burgarth and S. Bose, Phys. Rev. A **73**, 062321, (2006).

[60] A. Kay and P. J. Pemberton-Ross , Phys. Rev. A **81**, 010301(R), (2010).

[61] C. Di Franco, M. Paternostro and M. S. Kim, Phys. Rev. Lett. **101**, 230502, (2008).

[62] C. Di Franco, M. Paternostro, D. I. Tsomokos, and S. F. Huelga, Phys. Rev. A **77**, 062337, (2008).

[63] M. A. Nielsen, I. L. Chuang,*Quantum Computation and Quantum Information*, Cambridge University Press, (Cambridge), (2000).

[64] E. H. Lieb and D. W. Robinson, Commun. Math. Phys. **28**, 251, (1972).

[65] R. Horodecki, Rev. Mod. Phys., **81**, (2009).

[66] S. Popescu, D. Rohrlich, Found. Phys. **24**, 379 (1994).