Universal quantum computing models: a perspective of resource theory*

Wang Dong-Sheng[1)2)†]

1) (*CAS Key Laboratory of Theoretical Physics, Institute of Theoretical Physics, Chinese Academy of Sciences, Beijing 100190, China*)

2) (*School of Physical Sciences, University of Chinese Academy of Sciences, Beijing 100049, China*)

Abstract

Quantum computing has been proven to be powerful, however, there are still great challenges for building real quantum computers due to the requirements of both fault-tolerance and universality. There is still no systematic method to design fast quantum algorithms and identify the key quantum resources. In this work, we develop a resource-theoretic approach to characterize universal quantum computing models and the universal resources for quantum computing.

Our theory combines the framework of universal quantum computing model (UQCM) and the quantum resource theory (QRT). The former has played major roles in quantum computing, while the later was developed mainly for quantum information theory. Putting them together proves to be 'win-win': on one hand, using QRT can provide a resource-theoretic characterization of a UQCM, the relation among models and inspire new ones, and on the other hand, using UQCM offers a framework to apply resources, study relation among resources and classify them.

In quantum theory, we mainly study states, evolution, observable, and probability from measurements, and this motivates the introduction of different families of UQCMs. A family also includes generations depending on a hierarchical structure of resource theories. We introduce a table of UQCMs by first classifying two categories of models: one referring to the format of information, and one referring to the logical evolution of information requiring quantum error-correction codes. Each category contains a few families of models, leading to more than one hundred of them in total. Such a rich spectrum of models

* Project supported by the National Natural Science Foundation of China (Grant Nos. 12047503, 12105343).

† Corresponding author. E-mail: wds@itp.ac.cn

include some well-known ones that people use, such as the circuit model, the adiabatic model, but many of them are relatively new and worthy of more study in the future. Among them are the models of quantum von Neumann architectures established recently. This type of architecture or model circumvents the no-go theorems on both the quantum program storage and quantum control unit, enabling the construction of more complete quantum computer systems and high-level programming.

Correspondingly, each model is captured by a unique quantum resource. For instance, in the state family, the universal resource for the circuit model is coherence, for the local quantum Turing machine is bipartite entanglement, and for the cluster-state based, also known as measurement-based model is a specific type of entanglement relevant to symmetry-protected topological order. As program-storage is a central feature of the quantum von Neumann architecture, we find the quantum resources for it are quantum memories, which are dynamical resources closely related to entanglement. In other words, our classification of UQCMs also serves as a computational classification of quantum resources. This can be used to resolve the dispute over the computing power of resources, such as interference, entanglement, or contextuality. In all, we believe our theory lays down a solid framework to study computing models, resources, and design algorithms.

Keywords: Universal quantum computing, Quantum resource, Quantum error correction

1 Introduction

1.1 Classical and Quantum

The field of quantum information and quantum computing has made tremendous progress in recent decades [1]. It is also referred to by other names, such as quantum information science. The core focus of this field is the study of the properties and applications of quantum information [2], encompassing research directions such as quantum communication, quantum computing, quantum simulation, quantum sensing, and quantum metrology [3]. It is not only a new branch of modern fundamental quantum physics but also an interdisciplinary field that integrates physics, information science, computer science, and more, with significant potential for practical applications.

As an intersection of classical information science and quantum physics, quantum information science emerged in the 1980s. Following foundational contributions by J. Bell [4], K. Kraus [5], and A. Holevo [6], the mathematical frameworks for quantum information and general quantum evolution became increasingly well-defined. R. Feynman and others recognized that using a controllable quantum system (i.e., a quantum computer) to solve quantum problems would likely surpass the capabilities of classical electronic computers, which were still evolving at the time [7]. D. Deutsch took a crucial step by proving the existence of a universal quantum computer [8], which spurred further research by theoretical computer scientists such as A. Yao [9] and U. Vazirani [10]. The field experienced rapid growth following the development of Shor's algorithm in 1994 [11].

In Fig. 1, key stages of development in both classical and quantum computing are briefly outlined. When comparing the two, it becomes evident that the quantum field is still in the stage of developing quantum chips. There remains a significant distance to cover before achieving fully functional quantum computers, network systems, and practical applications across various industries.

The development of classical information science provides valuable insights and a strong reference for the quantum field [12]. Pioneers such as A. Turing and C. Shannon laid the theoretical foundations of computation and information, while J. von Neumann proposed the architecture for general-purpose computers [13,14]. With the invention of semiconductor technology, particularly transistors, companies like Intel and AMD were able to mass-produce integrated circuits. Drawing inspiration from theories such as cybernetics and systems theory, modern computing systems—including computers, smartphones, and other devices—adopt a hierarchical design, as illustrated in Fig. 2. At the lowest level are basic components such as circuits and transistors, which enable the storage of bits. Above this are digital and analog circuits that implement fundamental operations, including Boolean logical gates, amplifiers, and rectifiers. Further up are circuits that perform basic functions, such as adders and memory units. On this foundation, a microarchitecture (i.e., the von Neumann architecture) is constructed, incorporating control, storage, communication, and computing units. Finally, at the software level, there are assembly languages for controlling microcomputers, operating systems for managing devices, and various applications built using high-level programming languages. This hierarchical, modular, and regular structure [12] highlights the importance of both hardware and software design in computing systems.

In a physical system, the two states of classical bits (denoted as 0 and 1) can be effectively represented by properties such as magnetization direction, voltage levels, or wavelength magnitudes. In contrast, qubits allow for superposition states of 0 and 1 [2]. This superposition, along with multi-qubit quantum entanglement, offers significant advantages for quantum computing. However, the inherent instability of qubits, manifested as decoherence, remains a fundamental challenge [2]. Quantum error-correcting code theory has been developed to address decoherence [15], but practical implementation of error correction and fault-tolerance remains a work in progress.

In terms of basic physical devices, significant technological advancements have been made in areas such as superconductivity, photonics, ion traps, and cold atoms [16]. However, when compared to classical devices, it is still unclear whether a quantum counterpart to the transistor exists—a single quantum device capable of simultaneously performing signal amplification, data storage, and logical operations. Additionally, extensive research has been conducted on quantum algorithms, leading to the discovery of several algorithms with quantum advantages, such as Shor's algorithm, Grover's algorithm, and the Harrow-Hassidim-Lloyd algorithm [11,17–20]. Despite these breakthroughs, challenges such as decoherence and limited computational scale prevent the rigorous implementation of these algorithms. Consequently, compared to classical computers—

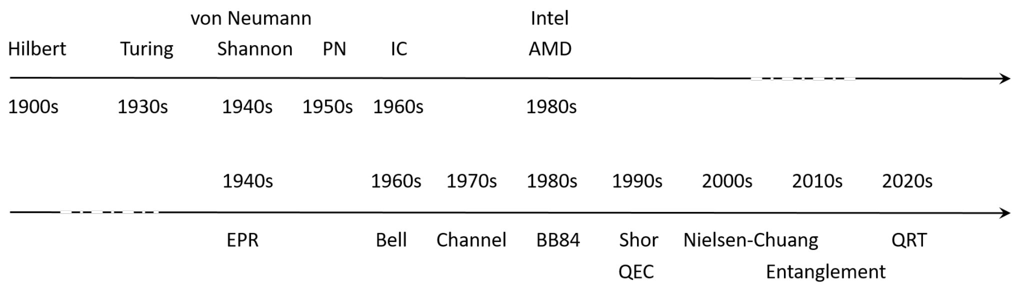

图 1: Development of classical and quantum information science. Classical (up): From the 23 problems of Hilbert, Turing laid the foundation of computation science. Shannon established the theory of communication, and von Neumann established the architecture of computers. The next breakthrough include PN junction and transistor, forming the building blocks of modern integrated circuits. Quantum (down): With the early study of EPR and Bell, the mathematical formalism of quantum channel, decoherence, and measurement were developed by Holevo, Kraus, etc. The BB84 secure protocol boosted the field. The theoretical achievement is the recent development of quantum resource theory as the theory of quantum information.

and particularly in the context of artificial intelligence algorithms—the realization of quantum algorithms and their advantages still faces significant hurdles.

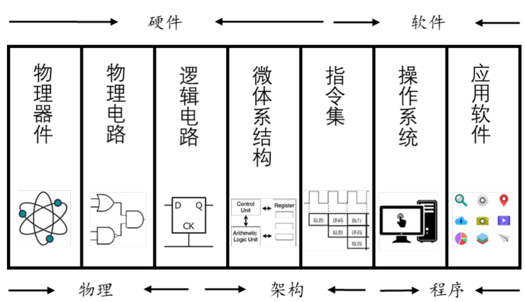

图 2: Hierarchy of computer system. There are layers of hardware and software, and also the layers of system architecture.

1.2 Information and Computation

Theoretically, characterizing the superposition of quantum information is a complex task, and our understanding of quantum information continues to deepen. This field has evolved simultaneously in terms of foundational research and practical applications, rather than following a linear progression from theory to application. Early explorations in quantum information can be found in the seminal work of M. Nielsen and I. Chuang [2]. However, this work does not cover many important topics that emerged later, such as many-body entangled states, universal computing models, and quantum Shannon theory, as these areas began to develop in subsequent years. Recent literature provides a more comprehensive view of these advancements [21–23].

Classical information is typically represented as a string of bits (i.e., digital signals), and its quantity can be measured using Shannon entropy. Shannon's three foundational theorems form the basis of classical information theory and coding [13]. In contrast, quantum information is represented by the quantum states of qubits, and its quantity is generally measured using von Neumann entropy. However, the von Neumann entropy of all pure states is zero, necessitating other quantities to distinguish between different pure states. Unlike classical bits, qubits exist in Hilbert space, and arbitrary quantum states cannot be copied (no-cloning theorem) or perfectly distinguished. The framework of quantum resource theory [24] has been developed to describe various aspects of quantum information, including coherence, entanglement, nonlocality, contextuality, complementarity, and uncertainty. Recently, this theoretical framework has also been applied as a foundation for quantum computing [25].

In quantum computing, the quantum circuit model is widely used, where a series of quantum gates are combined to form the desired process or algorithm [2]. This model parallels classical Boolean logic circuits. Classical models such as the Turing machine and cellular automata also have quantum counterparts. These models are considered universal computing models, meaning any classical or quantum algorithm can be effectively implemented within them. For both classical and quantum cases, these universal models are equivalent, as processes implementing the same algorithm can be mutually simulated. Researchers continue to discover new universal quantum computing models, such as adiabatic quantum computing [26] and topological quantum computing [27], which generally lack classical counterparts. These models have inspired numerous quantum algorithms and serve as the basis for quantum computing architectures developed by various companies. However, because these models were proposed at different times by experts from diverse backgrounds, they have not been systematically studied, and research focus varies widely. Unlike the unified description provided by quantum resource theory, there has been no unified framework to define and distinguish universal quantum computing models.

Recent studies have demonstrated that quantum resource theory and universal computing models can be integrated, offering multifaceted benefits. First, this integration provides a unified framework for defining and categorizing different universal quantum computing models, enabling systematic study. Second, it situates quantum resources within the context of universal quantum computing, offering a systematic perspective on how to distinguish and utilize these resources. Third, by describing computational models through resource theory, it becomes possible to identify the resources underlying quantum algorithms, resolving debates about the core resources quantum algorithms rely on. Finally, this approach has inspired the discovery and understanding of the quantum von Neumann architecture, which theoretically addresses the problem of quantum storage utilization and paves the way for the development of quantum computing from machine language to assembly language, ultimately enabling the construction of complete quantum computer systems.

It is important to note that this paper adopts a broad definition of quantum computing, encompassing the most general evolution of quantum information. In practice, narrower definitions may be used, such as distinguishing between quantum information (focusing on the fundamental properties of quantum states and processes) and quantum computing (focusing on quantum algorithms). Strict quantum information theory (i.e., quantum Shannon theory) [21] is a distinct focus for information theorists and differs significantly from the perspectives of physicists. Our research bridges resource theory and computational models, unifying the language of quantum information and quantum computing research. This approach could promote a holistic understanding of quantum information and its evolutionary properties.

This article is structured as follows: In Section 2, we review the fundamentals of quantum computing. In Sections 3 ∼ 5, we study the classification of universal quantum computing models and provide a brief analysis of each model. In Section 6, we explore the quantum von Neumann architecture and its applications. Finally, in Section 7, we discuss related issues, including the relationship between universal and dedicated architectures, potential challenges, and future directions. Since some quantum computing models, such as adiabatic quantum computation [26], topological quantum computing [27], quantum walks [28], quantum cellular automata [29], and cluster-state quantum computing (also known as measurement-based quantum computing) [30], have been extensively reviewed, this article focuses not on the details of these models but on their classification from the perspective of resource theory.

2 Basics for Quantum Computation

2.1 Circuit model and algorithm

The most commonly used quantum computing framework is the circuit model [2,8]. In this model, to implement a computational process or algorithm, a simple initial quantum state is first prepared, followed by an ordered execution of a series of unitary quantum gates, and finally the final state is measured. The measurement process generally requires multiple executions of this circuit, and the calculation results are obtained after statistical analysis. If the object being measured is the Hermitian operator E, the final result is expressed as the expected value on its final state ρ

$$\mathrm{tr}(E\rho) = \sum_i p_i e_i, \tag{1}$$

wherein e_i comes from the eigenvalue decomposition $E = \sum_i e_i |i\rangle\langle i|$, and the probability $p_i = \langle i|\rho|i\rangle$ need to be obtained through statistical analysis.

The process described above is similar to a typical quantum physics experiment. However, quantum computing has more requirements, which makes a computing system different from a physical experimental system [12]. Here we focus on three points, namely digitization, universality, and programmability. Digitization requires quantum states to be represented as multi-qubit states, quantum evolution processes to be represented as a combination of a series of fundamental quantum gates, and quantum measurements to be simple measurements of qubits. In fact, the digitization of information and its evolution is both a requirement for universality and fault-tolerance, that is, effective control of noise or errors.

An important fact is that there exists a so-called universal quantum gate set, such as {H, T, CNOT}, {H, CCNOT}, which allows any unitary operator to be precisely represented as a universal gate sequence [31]. This is the quantum correspondence of classical Boolean logic. Among them, H is the Hadamard gate that satisfies HXH=Z, HZH=X, X and Z are the Pauli operators, and T satisfies $\mathrm{T}^4 = \mathrm{Z}$. CNOT is a commonly used two-qubit control gate, while CCNOT stands for three-qubit control gate, also known as Toffoli gate. The existence of a universal gate set is a prerequisite for ensuring the universality of the circuit model. More generally, whether a computational model is universal often boils down to whether it can effectively simulate a set of universal gates. This also implies requirements for the preparation of initial states, measurement of final states, and coherence time. In the early days of quantum computing, these basic requirements for implementing quantum computing were generally referred to as DiVincenzo criteria [32].

Programmability is a relatively subtle but more advanced requirement. From a software perspective, different algorithms are represented as different circuits. In terms of hardware, achieving universality may require a large number of different circuits or chips. Therefore, people have developed programming methods that enable different algorithms to be implemented on the same chip. For the classical case, if the CPU's operation is G, for any input data bit string $\vec{b}$ and program A represented as $\vec{b}_A$, it needs to satisfy

$$G(\vec{b} \times \vec{b}_A) = A\vec{b} \times \vec{b}'_A, \quad (2)$$

where $A\vec{b}$ is the desired result, $\vec{b}_A$ can be used to restore the original program. However, for the quantum case, the unitary G acting on quantum data $|d\rangle$ and program state $|p_U\rangle$ with

$$G|d\rangle|p_U\rangle = U|d\rangle|p'_U\rangle \quad (3)$$

must satisfy $\langle p_V|p_U\rangle = 0, \forall U \neq V$ [33]. The storage states of different quantum algorithms or programs must be orthogonal, which is actually equivalent to classical storage. This so-called quantum no-programming theorem, also known as the quantum storage problem, was proven in 1997 by Nielsen and Chuang. Due to the continuity of unitary groups, the storage space grows rapidly. The limitation of this theorem allows people to only adopt a classical-quantum hybrid architecture, which uses quantum chips to execute quantum algorithms, and the storage of quantum algorithms is based on classical data. Recent studies have shown that this theorem is theoretically equivalent to the quantum no-cloning theorem [34,35]. The process of reading and downloading unknown programs is a metrological process, and if it can be implemented, the program can then be cloned. If only approximate implementation is required, the degree of approximation is limited by the uncertainty relation [34].

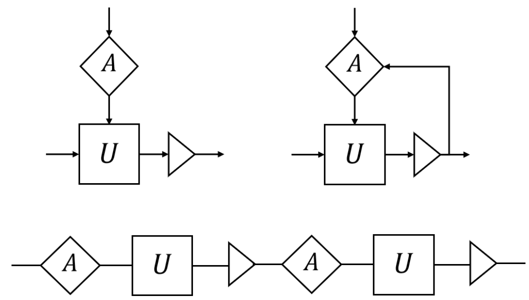

图 3: Structures of quantum circuit model and quantum algorithms. The basic structure (top-left) has a classical algorithm A that designs the quantum circuit U and measurement. It extends to the iterative classical-quantum algorithms (top-right), which can be "stretched" into a linear flow (bottom).

Within the framework of the circuit model, The design of quantum algorithms also requires a classical "mother" algorithm, see Fig. 3. For example, in Solovay-Kitaev's quantum compilation algorithm [36], For arbitrary unitary operator U and compilation precision ϵ, The classical algorithm $A(U,\epsilon)$ gives a classical representation of the quantum circuit U', denoted as $[U']$. The quantum circuit U' itself is implemented through a quantum gate. The effectiveness of the algorithm generally requires the complexity of the classical algorithm A and the quantum algorithm U', i.e. the time and storage space utilized, neither grows exponentially with $\frac{1}{\epsilon}$ and U, i.e. its cost

$$\text{cost} \in O\left(\text{poly}\left(\log\frac{1}{\epsilon}, |U|\right)\right), \quad (4)$$

and $|U|$ represents some measure of the size of U, such as a certain matrix norm. As the accuracy increases, $\log\frac{1}{\epsilon}$ may not necessarily reach, for example, the commonly used Trotter-Suzuki decomposition can only achieve the $\frac{1}{\epsilon}$ form [37]. To calculate the probability of the observed quantity in equation (1), A large amount of sampling is still required. By using the quantum amplitude amplification algorithm [38], probabilities can be converted into amplitudes, and the sampling cost is converted into computational cost. The requirement for accuracy actually implies fault-tolerance, which cannot be achieved yet currently. Therefore, most of the current experimental implementations of quantum algorithms are demonstration experiments.

2.2 Fault-tolerance and error correction

The literal meaning of fault-tolerance is the tolerance of errors, which requires the use of quantum error-correcting codes [39] to effectively overcome the effects of decoherence, noise, or errors. Strictly speaking, achieving universality also requires achieving fault-tolerance. In other words, it refers to the realization of arbitrarily long-lived qubits or the identity gate, which can connect other quantum gates, such as the previously mentioned H, T, and CNOT gates. In the proof of a model's universality, it is generally assumed that fault-tolerance can be guaranteed, meaning that error correction is a separate issue.

Quantum noise or errors are generally described as quantum channels [2]. The effect of a channel Φ on a state is represented as the superposition of a set of Kraus operators $\{E_i\}$

$$\Phi(\rho) = \sum_i E_i \rho E_i^\dagger, \tag{5}$$

with $\sum_i E_i^\dagger E_i = \mathbb{1}$ [5]. More generally, using quantum superchannel theory [40–42], quantum error correction is a quantum superchannel process $\hat{\mathcal{S}}$ that enables

$$F_E(\mathbb{1}^{\otimes k}, \hat{\mathcal{S}}(\Phi^{\otimes n})) \geq 1 - \epsilon. \tag{6}$$

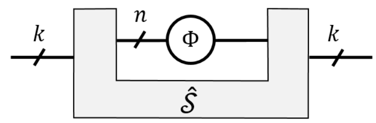

图 4: Structure of quantum error correction that converts $\Phi^{\otimes n}$ into $\mathbb{1}^{\otimes k}$ approximately by a superchannel $\hat{\mathcal{S}}$.

As shown in Figure 4, where $\epsilon \in [0, 1]$ is the accuracy or error of the error correction, and k, $n \geq k$ are positive integers, $r := k/n$ is the code rate. The specific form of the superchannel will be described later. The entanglement fidelity F_E is of the form $F_E(\Phi, \Psi) := F(\Phi \otimes \mathbb{1}(\omega), \Psi \otimes \mathbb{1}(\omega))$, and F is the usual fidelity of the state $F(\rho, \sigma) := \|\sqrt{\rho}\sqrt{\sigma}\|_1^2$, $\|\cdot\|_1$ is the trace norm, $\omega \propto \sum_i |ii\rangle$ is a Bell state, also known as an entangled bit (ebit). The state

$$\omega_\Phi := \Phi \otimes \mathbb{1}(\omega) \tag{7}$$

is also known as the Choi state of channel Φ. Its properties and Φ are equivalent, which is called the channel-state duality principle [43]. Like the uncertainty principle, it is a fundamental principle of quantum physics. These two principles will also be reflected in the quantum von Neumann architecture we will discuss later.

The error correction form above (6) includes the earliest developed binary form, which first encodes with $\mathcal{V}$ and then decodes with $\mathcal{D}$ [39], as well as its approximate cases [44]. To achieve fault-tolerance, it is necessary to ensure that ϵ can arbitrarily approach 0. The case where the error $\epsilon = 0$ corresponds to strict or exact error correction, where the noise operators and encoding must satisfy the Knill-Laflamme condition

$$PK_i^\dagger K_j P = c_{ij} P, \tag{8}$$

where $P = VV^\dagger$, V is the isometric encoding, and $\{K_i\}$ is the set of Kraus operators for the noise [39]. A large class of exact error correction codes are the so-called stabilizer codes [2,45]. Typically, a stabilizer is composed of the direct product of Pauli operators, the encoding is formed by a set of commuting stabilizers, and decoding is achieved by measuring the stabilizers to determine if a bit flip X or phase flip Z error has occurred, and then correcting it.

Ensuring that ϵ can arbitrarily approach 0 is not straightforward. We recently proposed [46,47] that by introducing external parameters $\vec{\lambda}$, $\epsilon(\vec{\lambda})$ can approach 0 in the parameter space. Codes satisfying this condition are called quasi-exact codes, while those that do not are merely general approximate codes. These parameters include k, n, controllable parameters in the error correction process $\hat{\mathcal{S}}$, and some parameters of the noise Φ itself. Some well-known controllable parameters include the squeezing parameter in optics, photon number, external field frequency in Floquet control, chemical potential, temperature, and the number of steps in code concatenation. The fault-tolerance achievable using quasi-exact codes is termed "quasi fault-tolerance," which lies between non fault-tolerance and strict fault-tolerance. Accordingly, universality also needs to be reduced to quasi-universality.

Combining the general form of error correction (6), quasi-exact codes can also describe some generalized error correction mechanisms, such as entanglement distillation, dynamical decoupling, and schemes to increase the transmission distance in QKD. Specifically, quasi fault-tolerance can be divided into two types. 1) The first type is where $\epsilon(\vec{\lambda})$ cannot efficiently approach 0. For example, the recently developed covariant codes with continuous symmetries [46–49] have an error correction error that scales as $\text{poly}(\frac{1}{n})$ with system size n. This can be understood from the uncertainty relation, as covariant codes can be interpreted as a form of quantum metrology for unknown parameters [50]. Since no additional auxiliary qubits are used to reduce system noise, the error correction error from dynamical decoupling cannot decrease exponentially with the strength of decoupling [51]. 2) The second type is where $\epsilon(\vec{\lambda})$ can efficiently approach 0, but due to practical reasons, $\vec{\lambda}$ cannot be arbitrarily adjusted. This describes some noisy exact codes currently achievable in experiments, such as the surface code [52], as well as cases where error correction codes can be partially applied. This type, in principle, falls within the scope of fault-tolerance. Currently, the variety of quasi-exact codes known to us is limited, although they impose weaker structural requirements on codes compared to exact codes.

The development of classical error correction codes provides us with valuable insights [53]. Currently, commonly used classical codes include block codes, LDPC codes, convolutional codes, Turbo codes, and Polar codes, which play significant roles in computation and communication. Research on quantum codes has primarily focused on block codes and LDPC codes [54], while understanding of other types remains relatively limited [15]. More generally, how to theoretically classify error correction and encoding methods, and thereby systematically design error correction codes, is also an important research topic [55].

3 Universal Quantum Computing Models

In this section, we first introduce the classification methods for universal quantum computing models, and then discuss the main properties of these models separately. Due to historical reasons, some computational models actually start from fault-tolerance, such as topological quantum computing, which implements quantum logical gates in a special way. We find that both universality and fault-tolerance can be characterized from the perspective of quantum resource theory.

3.1 Quantum resource theory

For classification problems, the primary choice is group theory. However, computational processes generally do not involve specific symmetries. We find that the classification of universal quantum computing models requires the use of quantum resource theory. Mathematically, quantum resource theory can be described as a category theory [56], which can also be understood as a generalized symmetry theory.

A quantum resource theory is defined on a set $\mathcal{D}$, and includes three fundamental sets: $\mathcal{F} \subset \mathcal{D}$ as the free set, $\mathcal{O} : \mathcal{F} \to \mathcal{F}$ as the set of free operations, and $\mathcal{R} := \mathcal{D} \backslash \mathcal{F}$ as the resource set [24]. The relationship between $\mathcal{O}$ and $\mathcal{F}$ can be viewed as a generalized symmetry. To quantify the resource, a function f defined on $\mathcal{D}$ must satisfy specific conditions, which generally include:

i) Positivity: $f(\rho) = 0$, $\forall \rho \in \mathcal{F}$; $f(\rho) \geq 0$, $\forall \rho \in \mathcal{D}$;

ii) Continuity: $f(\rho) \to f(\sigma)$ if $\rho \to \sigma$, $\forall \rho, \sigma \in \mathcal{D}$;

iii) Additivity: $f(\rho \otimes \sigma) \leq f(\rho) + f(\sigma)$, $\forall \rho, \sigma \in \mathcal{D}$;

iv) Monotonicity: $f(\rho) \geq f(\Phi(\rho))$, $\forall \Phi \in \mathcal{O}$, $\forall \rho \in \mathcal{D}$.

The metric function f can adopt distance, entropy, Fisher information, etc. For example, a well-known example is bipartite entangled states, where the corresponding free set is separable states, the free operations are local operations and classical communication (LOCC), and the maximally entangled bipartite states are Bell states [57]. Later, it was also recognized that coherence is a resource [58]. By selecting a set of orthogonal bases, the states diagonal in this basis form the free set, which are all incoherent states, and incoherent operations can also be defined. In fact, von Neumann entropy itself defines the most basic resource theory of states: by choosing the maximally mixed state as the free set, and using negative entropy ($\log d - S(\rho)$) as a measure of the resource of a state ρ, all pure states have the maximum resource measure, while the free operations are processes that cannot decrease the entropy $S(\rho)$.

Additionally, the set can not only be the state space typically considered, but also other types of operator sets, such as Hamiltonians, measurements, channel evolutions, encodings, etc. Considering different types of operators can lead to different types of computational models.

Within the framework of resource theory, we define universality as using $\mathcal{O}(\mathcal{F} \otimes \mathcal{R})$ to implement any operation on $\mathcal{D}$. To classify universal computational models, we extend the form of resource theory in two ways [25]. First, we define the universal resource set $\mathcal{U}$, whose resource measure $f(\mathcal{U})$ reaches the maximum value. Then, using $\mathcal{O}(\mathcal{F} \otimes \mathcal{U})$ can effectively simulate other processes $\mathcal{O}(\mathcal{F} \otimes \mathcal{R})$. Second, we define resource sequences satisfying $\mathcal{F}_1 \subset \mathcal{F}_2 \subset \cdots$, $\mathcal{O}_1 \subset \mathcal{O}_2 \subset \cdots$. To achieve universality, the computational power of the universal resources needs to increase progressively, denoted as $\mathcal{U}_1 \succ \mathcal{U}_2 \succ \cdots$. Furthermore, for $u_{1,2} \in \mathcal{U}_{1,2}$, different universal resources must satisfy the following relation

$$(\mathcal{O}_2 \backslash \mathcal{O}_1)(u_2) = u_1, \ \mathcal{O}_1(u_1) = u_2. \tag{9}$$

This gives rise to a series of computational models, which we refer to as a "family." In principle, there is no upper limit to the number of members in a family, but here we consider only three members, which are already sufficient to generate a wide variety of computational models.

3.2 Table of UQCM

Based on the above analysis, we first abstract the computational process as $\mathcal{O}(\mathcal{F} \otimes \mathcal{U})$, along with the error correction process, which includes a series of logical and error correction steps, as shown in Fig. 5. We consider sets of quantum states, Hamiltonian, measurements, channel evolution, as well as logical gates and encoding operators. From the perspectives of information representation, evolution, and protection, we divide universal computational models into two major categories: Category I models, which depend on different forms of information representation, and Category II models, which depend on different forms of information evolution [59]. The protection of information involves the type of encoding itself, belonging to a third dimension, which is not discussed here [55]. The classification table of universal quantum computing models is shown in Fig. 6, where the definition and properties of each model are the main topics of this paper. Due to space limitations, a detailed analysis of each model cannot be provided, and readers are referred to additional literature for further details.

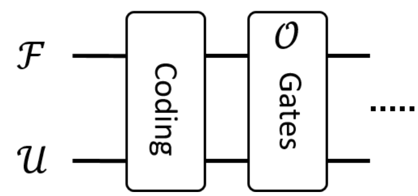

图 5: Structure of quantum computing model via quantum resource theory. The Category-I (-II) models are defined for different types of input (logical operations).

Category I models arise from different forms of information representation, where information is represented as certain properties of quantum states, Hamiltonian, measurements, and channels. They each define a family, with three generations within each family, resulting in a total of 12 models. Category II models stem from the classification of quantum logical gates, based on their implementation methods: time-independent unitary, time-dependent unitary, and non-unitary evolution. They each define a family, with three generations within each family, resulting in a total of 9 models. Further subdivision is possible but not discussed here. Combining information representation and logical evolution, there are a total of 108 basic models. Among these, some schemes have been thoroughly studied, while others have not. See [59] for an analysis of some of these schemes. Below, we explain the underlying

		Unitary			t-dependent			non-unitary		
State	Circuit									
	Turing									
	MBQC									
Hamilton ian	H-Sim									
	HQCA									
	AQC									
Measure ment	Context									
	Magic									
	Nonlocal									
Channel	von Neumann									

图 6: The classification table of universal quantum computing models. There are 12 (9) Category-I (-II) models, hence in total 108 complete models (grey boxes). The most well-studied are those based on circuit model. The channel-family models are all von Neumann architecture or models. Hybridization among models are also allowed.

logic of these models.

For example, in the state-family models, information is represented as the amplitudes ψ_i of quantum states, i.e., pure states $|\psi\rangle = \sum_i \psi_i |i\rangle$, in a given basis $\{|i\rangle\}$. Computation involves operations on these amplitudes, which is the well-known process of interference. Mixed states can be viewed as probabilistic mixtures of pure states. When considering multi-qubit computational processes, different restricted operation sets can be selected based on locality within the resource theory framework, defining a family. We find that the state family includes the well-known circuit model, as well as the local Turing machine model [60] and graph-state quantum computation, also known as measurement-based quantum computation [30,61,62]. Their universal computational resources correspond to coherence [58], entanglement [57], and specific forms of symmetry-protected entanglement [63–65]. Here, the local Turing machine is a simplification of the original quantum Turing machine model [9,10,66], highlighting the locality of interactions and the entanglement properties of quantum states.

Category II models primarily depend on different forms of logical gates. If an encoding is represented by an isometry V, then different types of logical gates $V^\dagger G V$ after encoding lead to different models. Note that this refers to the basic logical gates in a universal gate set, such as H and T, whose combinations can construct arbitrary logical gates. Unlike the usual considerations, the encoding here can be static (time-independent) or dynamic (time-dependent). For example, the time-dependent unitary class refers to $V(t)$ undergoing continuous unitary changes, with adiabatic quantum processes being an example [26]. The non-unitary class refers to cases where the encoding undergoes non-unitary changes, and here we mainly consider the case where the encoding is a set $\{V_i\}$, i.e., converting from one code to another, which is known as code switching [67].

A fundamental property of logical gates is their depth, which is relative to the size of the encoded system. As the name suggests, depth refers to the time or number of steps required to implement it, which is crucial for fault-tolerance during the logical gate implementation process. For example, a transversal unitary takes the form $\otimes_n U_n$, i.e., a global tensor product form, which does not spread local noise and thus has better fault-tolerance. Therefore, we distinguish three basic forms: transversal, local finite-depth, and high-depth, where local finite-depth refers to a finite number of local steps, and high-depth refers to steps that scale with the system size. For instance, the braiding operations of non-Abelian anyons in topological quantum computation have linear depth, belonging to the high-depth type model in the time-independent unitary family [27]. The other two models in this family have also been studied, where the transversal model can describe quantum metrology models [68], and the local finite-depth model can describe most encoding schemes, such as a multi-particle quantum walk model [59]. Additionally, resource theory can be used to characterize Category II models, i.e., classifying the set of logical gates $V^\dagger G V$ (e.g., based on depth), which requires further in-depth research.

A complete model that considers both universality and fault-tolerance needs to combine the above two categories. For example, the most commonly used approach combines the circuit model with a fixed encoding scheme, such as some stabilizer codes [2], but this is not necessarily the best approach. We see that, in principle, there are many equivalent universal quantum computing models, and when considering different physical experimental platforms, different physical implementations of quantum gates, and various hybrid combinations of models, even more computational schemes can emerge. In practice, specific choices are made. This illustrates the richness and complexity of quantum computing research. In summary, the classification table of models systematizes the study of theoretical schemes for achieving universal quantum computation, allowing for principled definitions and understanding of models, and the development of more computational schemes. Below, we focus on Category I models, introducing the properties of each family, as well as the specific forms and characteristics of each model.

4 Category I

4.1 State family

4.1.1 Resource-theoretic characterization

For the state family, according to resource theory, if the operations allowed on quantum states are very limited, such as single-qubit operations plus classical communication, then achieving universality requires some form of entangled state as a universal resource. This can be used to define graph-state quantum computation [30,61,62]. When the operation set is expanded to include local operations, this makes typical bipartite entangled states as the resource [57], and such a computational model is called the local Turing machine [60]. Further expanding the operation set to enable universal classical computation (e.g., using the Toffoli gate), the Hadamard gate becomes the universal resource, which can generate superposition, corresponding to quantum coherence [58], and is used to characterize the circuit model.

Their universal resources satisfy the transformation relation (9). That is, the Bell state $|\omega\rangle$ can be generated from the maximal coherence state $|+\rangle = \frac{1}{\sqrt{d}}\sum_i |i\rangle$ according to

$$|\omega\rangle = \text{CNOT}|+\rangle|0\rangle, \tag{10}$$

where the CNOT gate is a given free operation in the circuit model, but is a resource in the local Turing machine. Similarly, using the local operations allowed in the Turing machine, the entangled states required for graph-state quantum computation can be generated from the Bell state. These special forms of states include two-dimensional cluster states [61] and AKLT states [69], among others. They take the form of matrix product states (MPS) [69–71]

$$|\psi\rangle = (\otimes_n \mathcal{P}_n)|\omega\rangle^{\otimes n}. \tag{11}$$

As shown in Fig. 7, MPS has three equivalent representation schemes. Since it can effectively represent arbitrary quantum states, it has broad applications, as will be evident from our subsequent discussion.

4.1.2 Model features

In Section 2.1, we have already introduced the basic content of the quantum circuit model. Here, we briefly discuss some of its features and limitations. Theoretically, whether classical or quantum, the circuit model is very fundamental and serves as the basis for designing both software and hardware. Other computational models can be understood from the perspective of the circuit model, although different models can inspire more novel ideas. Additionally, quantum circuits are easy to control classically (i.e., the spatiotemporal positions of each logical gate are controllable) and easy to represent classically (i.e., the type and spatiotemporal positions of logical gates can be represented as bit strings), making it the most popular model at present.

Compared to other models, the circuit model also has some more subtle requirements, such as the need for interactions between qubits, and the requirement that qubit coherence times be long enough to support deep circuits. This has practical implications. For example, in superconducting circuits, crosstalk between interacting qubits is a critical issue in current experiments [72].

Beyond universality, the circuit model does not adequately consider other requirements, including modularity, programmability, and security. For instance, if a quantum algorithm is represented as a circuit diagram, where the positions and types of gates are classical information, it can be freely used, including by adversaries, if not encrypted. Considerations of security are the starting point for many secure or privacy-preserving computational models, such as multi-party secure computation [73], blind quantum computation [74], and the quantum von Neumann architecture we discuss later [35].

From the perspective of computer design architecture (Fig. 2), the circuit model is primarily used for hardware circuit design at the machine language level, such as basic digital and analog circuits. To adapt to higher-level languages, the von Neumann model or architecture is required. Therefore, from a hardware perspective, current quantum computing research is still at the machine language level, and even stable qubits (i.e., fault-tolerance) have not been strictly achieved.

In classical computing, the Turing machine model is one of the earliest models, and it is of great significance for understanding computability, algorithms, and even computer architecture. In contrast, research on quantum Turing machines is relatively scarce. The main reason is that the original quantum Turing machine model is complex (e.g., using global interactions) and has some issues [66,75], which we will not elaborate on here. From the perspective of resource theory, i.e., transitioning from the coherence dependence of the circuit model to entanglement, we find that the model relying on entanglement as a resource is the local quantum Turing machine [60]. Mathematically, an appropriate form for characterizing entanglement is the matrix product state (11), which can also be expressed as

$$|\psi\rangle = \sum_{i_1,\ldots,i_N} \mathrm{tr}(BA^{i_N}\cdots A^{i_1})|i_1\ldots i_N\rangle. \qquad (12)$$

Here, the amplitude is represented as the trace of a product of a series of operators A and a boundary operator B. The space on which these operators act is the so-called "bond space," which can be referred to as the entanglement space [69–71].

It is important to note that any state can be written in the above form, and the dimension of the entanglement space can be a constant or scale with the system size N. The entanglement of a state corresponds to the properties of its entanglement space. This entanglement space can serve as the machine state space in the Turing machine model, where a computational process is completed through one-to-one interactions between this system and the data unit, with no direct interactions between data units (unlike the circuit model). However, exploration of this model in practice is still relatively limited.

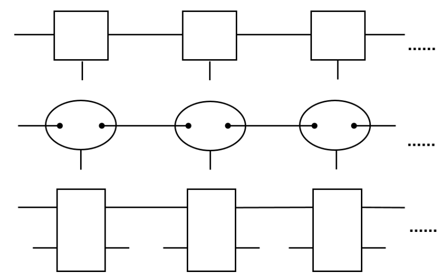

图 7: Representations of matrix-product states. (Top) Tensor form: the top register is the entanglement space, the vertical wires are physical sites, the boxes are the tensors or matrices. (Middle) VBS or AKLT form [69]: tensors are defined by local operators (circles) acting on Bell states (Eq.11). (Bottom) Circuit form: each tensor is realized by a unitary circuit (big boxes).

Historically, MPS and their derived tensor and neural networks have primarily been applied in many-body and statistical physics [76], with relatively few applications in quantum computing. From the perspective of entanglement, compared to pure computational tasks, its role in tasks such as storage and communication may be more pronounced, such as in distributed computing [77].

The graph-state quantum computation is also known as the "one-way" model or measurement-based quantum computation [30,61,62]. This model was discovered relatively early and, due to its novelty, garnered significant attention at the time. Unlike the circuit model, it does not require the design of various circuits or interactions between qubits, but instead involves a series of local measurements with feedback on a given resource state. These measurements induce quantum gate teleportation processes that can implement quantum gates [78]. Since measurements are destructive, a computational process consumes the resources contained in the resource state. This also explains the origin of the term "one-way" in its name. However, from the perspective of resource theory, it is more appropriate to refer to it as a computation model based on graph states or some equivalent resource states. To avoid confusion with the measurement family, in this paper, we generally refer to it as graph-state quantum computation. Additionally, it carries a hint of the stored-program concept, where multi-qubit entangling gates are potentially pre-stored in the initial resource state. These characteristics have inspired the development of the quantum von Neumann architecture, as both quantum gate teleportation and stored programs are core components of it [79].

At the same time, the research approach of studying universal models from the perspective of resources was also inspired by this model. This is because researchers have long been studying the universality and universal resource states in this model [80,81], such as determining which graph states are universal. Moreover, it has been found that if an arbitrary state is given, its entanglement is typically large, but it is not a universal resource in this model [82,83]. This once led to debates about whether the resource for quantum computation is entanglement or interference.

Recently, we first demonstrated [63–65] that the universal resource states need to be of a special type. Expressed in MPS form, they require a boundary form

$$|\psi(\ell)\rangle = \sum_{i_1,\dots,i_N} A^{i_N}\cdots A^{i_1}|\ell\rangle|i_1\dots i_N\rangle, \qquad (13)$$

and must satisfy the injectivity condition on the entanglement space, meaning that measurement operations on the physical space induce arbitrary unitary processes on the entanglement space, i.e., the state $|\ell\rangle$ can evolve into any desired state. An example is the case with symmetries, which are symmetry-protected states in many-body physics [84–86]. The previously mentioned cluster states possess one-dimensional $Z_2 \times Z_2$ [63] or two-dimensional Z_2 1-form symmetries [65], while the AKLT states have global SO(3) symmetry, among others [69]. See [25] for more characterizations based on resource theory.

In practice, this model has been more widely used in optical systems [87], because measuring multiple photons is easier to implement compared to interactions. The preparation of large-scale resource states is not necessarily easy, so they can also be generated in real-time. However, the ideal scenario is that the resource state is given, such as in a many-body quantum state, but the requirements for local measurements are currently difficult to achieve.

4.2 Hamiltonian family

4.2.1 Resource-theoretic characterization

The Hamiltonian family relies on the form of local Hamiltonian interactions and assumes that each interaction term can be turned on or off. For the algorithm, its input state can be regarded as an eigenvalue of a certain Hamiltonian, as shown in the equation

$$H|\psi\rangle = E|\psi\rangle, \qquad (14)$$

where the algorithm itself modifies the Hamiltonian, which in turn is equivalent to altering the state. Therefore, by considering the set of local Hamiltonian interactions and the operations on them, analogous to operations on quantum state amplitudes, the Hamiltonian family can be introduced. We find that it includes Hamiltonian quantum simulation, Hamiltonian quantum cellular automata, and adiabatic quantum computation models.

Hamiltonian quantum simulation refers to constructing other Hamiltonians using a finite set of interaction forms. Within its family, it allows the most general construction methods. If the way interaction terms are combined is restricted, such as allowing only parallel schemes, this leads to the Hamiltonian quantum cellular automata model. According to the transformation relations of universal resources, the interactions it relies on can be prepared using Hamiltonian simulation. If further restrictions are imposed, allowing only adiabatic schemes, this results in adiabatic quantum computation, whose universal interaction forms are more complex, such as the commonly used Feynman-Kitaev Hamiltonian form [88].

4.2.2 Model features

Hamiltonian quantum simulation has been considered for a long time [7,37,89,90], but it is generally framed within the context of the circuit model. The work on independently considering the universality of Hamiltonians themselves was completed in recent years [91–93], specifically studying what kinds of interactions can realize arbitrary interaction forms. The basic idea is to use the Trotter decomposition to express the desired Hamiltonian

$$H = \sum_n j_n h_n \tag{15}$$

and its evolution $U = \mathrm{e}^{\mathrm{i}Ht}$ as a product of a series of $\mathrm{e}^{\mathrm{i}t_n j_n h_n}$ [37]. Here, h_n can be just a limited number of interaction forms. It has been proven that almost any two-body interaction is universal [91–93]. In practice, compared to the circuit model, the control over interactions is not necessarily superior to quantum gates. This model may have a closer relationship to many-body quantum physics, such as in Hamiltonian complexity [93].

The more well-known Hamiltonian evolution simulation and analog simulation can be seen as simplified applications of this model. In quantum algorithms, Hamiltonian evolution simulation [94] mainly aims to decompose a certain evolution $U = \mathrm{e}^{iHt}$ (or its time-dependent form) into a series of smaller evolution, but without using a universal set of interactions. Another scenario is the so-called analog simulation (or emulation) [95], which requires even less control over local interactions. This situation is mainly suitable for certain specific physical systems, used for the study of particular specialized problems.

If the operations on Hamiltonian terms are restricted, new computational models can be introduced. A natural choice is to switch these interactions in parallel. To achieve universality, the required basic Hamiltonian forms become slightly more complex. This leads to the Hamiltonian cellular automata model [25]. It requires a one-dimensional system where each site contains two qubits (one data qubit and one auxiliary qubit) and a three-level system (qutrit). The basic interaction is given by

$$H = |0\rangle\langle 1| \otimes U + |1\rangle\langle 0| \otimes U^\dagger, \tag{16}$$

where the first part acts on the auxiliary qubit, and the unitary operator

$$U = P_0 \otimes \mathbb{1} + P_1 \otimes W + P_2 \otimes \Xi, \tag{17}$$

has its first part acting on the qutrit. Finally,

$$W = P_0 \otimes \mathbb{1} + P_1 \otimes \mathrm{HZ}, \tag{18}$$

acts on the two data qubits. Here, Ξ is the SWAP gate on the data qubits, which, together with W, forms a universal gate set $\{\Xi, W\}$ [96]. Thus, given any circuit composed of W and Ξ, it can be simulated by a cellular automata constructed from H (16). It is worth noting that the above complex forms are only necessary to prove universality and are not necessarily adopted in the study of specific problems.

This model is classically controllable, meaning its parallel interactions can be switched on or off. Although named an automaton, it is not a fully autonomous evolution form (i.e., e^{iHt}). Previous work has shown that models based on autonomous evolution cannot deterministically reach the desired final state, even if the requirement for parallelism is removed [28,97–100]. Additionally, there are gate-based cellular automata forms. Overall, research on such models is relatively limited [29]. An interesting observation is that one-dimensional quantum models can be universal, whereas classical models must be higher-dimensional [101]. Similar to the classical case, cellular automata models are less widely used than circuit models, but they are often employed in the simulation of dynamics [102].

In comparison, adiabatic quantum computation has received more extensive research [26], benefiting from studies on quantum adiabatic processes and quantum annealing. The universality of this model is typically proven using the Feynman-Kitaev history state method [88]. Specifically, given a circuit $U = U_L \cdots U_2 U_1$, it is transformed into a Hamiltonian H_{FK}, whose ground state is the history state

$$|\Phi\rangle = \frac{1}{\sqrt{L+1}} \sum_{\ell=0}^{L} |\gamma_\ell\rangle \tag{19}$$

where $|\gamma_\ell\rangle = |\psi_\ell\rangle|\ell\rangle$, $|\psi_\ell\rangle = U'_\ell|\psi_0\rangle$, $U'_\ell = U_\ell \cdots U_2 U_1$, $|\psi_0\rangle$ is the initial state, and $|\ell\rangle$ is the clock state. Adiabatic evolution is then employed to map the ground state $|\gamma_0\rangle \mapsto |\Phi\rangle$. The history state contains the true final state $|\gamma_L\rangle$, whose realization probability can be effectively increased, but at the cost of more clock qubits and interaction terms. We observe that, since the Hamiltonian terms can only be turned on or off adiabatically, the required Hamiltonian forms, or universal resources, become more complex. In the subspace $\{|\gamma_\ell\rangle\}$, it can be represented as a one-dimensional quantum walk form [25].

In practice, adiabatic quantum computation has been used to explore quantum advantages. However, due to the inability to guarantee computational precision, it is challenging to obtain deterministic results [103,104]. Since this model belongs to the Hamiltonian type, it is related to Hamiltonian computational complexity. For example, a class of Hamiltonians is quantum stochastic (stoquastic), and when the local parameter $k \geq 2$, it becomes a complete problem for the complexity class StoqMA [105]. Additionally, adiabatic processes have broader applications, such as in adiabatic geometric phases and quantum gates [106], primarily implemented within the framework of the circuit model for quantum gates. Due to their geometric nature, they exhibit a certain robustness to noise. This can be leveraged to enhance the fault-tolerance of adiabatic quantum computation.

4.3 Measurement family

4.3.1 Resource-theoretic characterization

Next, we discuss the measurement family. Note that here, measurements are treated as resources, whereas in the previously discussed graph-state quantum computation, measurements are considered free operations. In fact, the measurement family can also be referred to as the (quasi)probability family, as it is based on the (quasi)probability representation or phase-space representation of quantum information. Specifically, a state is expanded as

$$\rho = \vec{r} \cdot \vec{\sigma}, \tag{20}$$

where $\vec{\sigma}$ forms a Hermitian operator basis, and ρ is reduced to a vector $\vec{r} = (r_i)$, satisfying $\text{sum}(\vec{r}) = \sum_i r_i = 1$ [107]. If $r_i \geq 0$ for all i, such states can be viewed as classical probability distributions. Correspondingly, the quantum nature of a state is characterized by the negativity of $\vec{r}$, i.e., the Wigner quasi-probability function. This formalism is widely used in quantum optics and phase-space representation theory. For computational models, an important conclusion is that pure states with positive $\vec{r}$ are stabilizer states [108], while mixed states are not. The free operations on stabilizer states are the so-called Clifford operations [2]. It has been discovered that universal quantum computation can be achieved by providing a sufficient number of "magic states" for the T gate, such as $|t\rangle := \text{T}|+\rangle$, leading to the magic-state computation model [109]. This can then be extended into a family of models, including contextuality-based computation models that directly rely on Wigner negativity and models that depend on Popescu-Rohrlich nonlocal correlations [110].

4.3.2 Model features

The mathematical description of measurement is POVM [2]. It is typically a collection $\{M_i\}$, where the positive operators $M_i \geq 0$ satisfy $\sum_i M_i = \mathbb{1}$. Given a state ρ, measuring it yields three pieces of information: the outcome i, its probability $p_i = \text{tr}(M_i \rho)$, and each final state ρ_i. Measurements can be implemented using channels, where the Kraus operators satisfy $K_i^\dagger K_i = M_i$ and retain the information about i. In practice, there are many types of measurements with different names, such as destructive measurements when ρ_i is destroyed, indirect measurements when auxiliary qubits are required, and weak measurements when one of the M_i is close to the identity operator $\mathbb{1}$.

The first model in the measurement family is the contextuality-based computation model we defined [25]. Contextuality is equivalent to the negativity of the Wigner function [111]. The core idea of this model is a class of contextual quantum circuits, which can be expressed as

$$\text{tr}_c(CV(U_2 \otimes \mathbb{1})CU(U_1 \otimes \mathbb{1})) \tag{21}$$

where U_1 and U_2 act on the auxiliary register, also called the control or context unit, while the other port is the data register. CV and CU are two control gates (also called multiplexer gates), taking the block-diagonal form

$$CU = \sum_i P_i \otimes U_i, \tag{22}$$

where $P_i = |i\rangle\langle i|$ is the projection operator on the control unit, and U_i acts on the data unit. The entire circuit can be viewed as using the ancilla to perform measurements on the data to enable evolution. We found that basic quantum gates such as H, T, and CNOT can all be expressed in this form, with the initial state of the ancilla being $|+\rangle$ and the measurement being the Pauli X measurement M_X. The gates used are all incoherent, meaning they cannot create superposition. This proves the universality of the model.

The universal resource in this model is the M_X measurement. If the initial state is replaced with $|0\rangle$, $|1\rangle$, or their probabilistic mixtures, and M_X is replaced with M_Z, then it can only prepare classical probability functions, i.e., Wigner functions with positive values. The role of the M_X measurement is similar to the H gate: M_X is equivalent to applying M_Z after an H gate. Given the $|0\rangle$ state, M_X can produce $|+\rangle$. In essence, its role is to create superposition of gates. More generally, we define quantum contextuality as the superposition of different contexts. A quantum context refers to a quantum operation, such as state preparation, evolution, or measurement (see [112]). When two operators commute, they are compatible and can coexist, reducing to classical numbers or functions. Quantum contextuality refers to the coexistence (i.e., superposition) of incompatible quantum contexts. Classical contextuality can then be defined as the mixture of quantum contexts. Similar to the quantum circuit model, its restricted set consists of classical circuits, so their universal resources (i.e., coherence and contextuality) are equivalent resources.

Since this is a new model, current understanding of it is still limited. Here, we briefly discuss a few points. First, contextual circuits can be seen as an extension of quantum teleportation and gates [113,114], with the latter being the origin of using measurements for computation or communication. It also highlights the importance of measurement outcomes, i.e., classical communication, which is a property that runs through the entire measurement family of models. The use of the control system to create superposition of gates originates from the so-called LCU algorithm [19,115–118], but it typically requires post-selection on the controller, making it probabilistic. The control unit is also a core component of the von Neumann architecture, so there may be some connections between these two types of models.

The magic-state quantum computation model uses a special class of Wigner-positive states as the restricted set, namely stabilizer states. This model has been studied earlier and is relatively mature, and its combination with stabilizer error-correcting codes is also natural [109]. Based on their action on Pauli operators, the k-th level of the Clifford hierarchy is defined as

$$\mathcal{C}^{(k)} := U|UPU^\dagger \in \mathcal{C}^{(k-1)}, \forall P \in \mathcal{P}_n, \tag{23}$$

where $\mathcal{P}_n$ is the Pauli group on n qubits [114]. Here $\mathcal{C}^{(2)}$ is the Clifford group, which consists of free operations on the set of stabilizer states. Therefore, to achieve universality, at least one higher-level gate is needed, such as the T gate or the CCNOT gate, which is equivalent to some non-Clifford measurement. Using stabilizer codes and teleportation, fault-tolerance and universality can be simultaneously achieved [119]. However, in practice, achieving fault-tolerance is not easy. One reason is that preparing stabilizer states and implementing error correction are significant experimental challenges, and another is that preparing the magic states required for teleportation (e.g., $|t\rangle = \mathrm{T}|+\rangle$) also requires purification or error correction processes.

In both of the above models, classical communication is a necessary part of deterministically implementing quantum gates. This actually highlights the role of correlations. A stronger form of correlation, known as Popescu-Rohrlich (PR) nonlocality [110], can replace classical communication to achieve the transmission of T gates [120]. For binary inputs x, y, the outputs a, b of a PR process satisfy

$$a \oplus b = x \cdot y, \tag{24}$$

which maximally violates the CHSH inequality [121], exceeding the value allowed by quantum theory. Based on this, we introduced the nonlocal magic-state (or "post-magical") computation model [25], which is briefly outlined here. It can be seen as a modification of graph-state quantum computation, where the measurement feedback process is replaced by PR correlations, enabling instantaneous nonlocal computation with one-way secrecy. Its restricted set of free operations is minimal, including only single-qubit Pauli measurements and the broadcasting (rather than two-way communication) of measurement results. Correspondingly, it requires PR correlations and some form of graph states to achieve universality.

This model makes PR correlations particularly special. Previous research has shown that if classical communication is not used in teleportation, an exponential amount of entanglement is required [122], which can be replaced by a small amount of PR correlations. Moreover, PR correlations do not need to be perfect; even a small amount of beyond-quantum correlation can replace classical communication [123]. Currently, the role of classical communication in quantum computation is not fully understood [124]. For example, in studies of error correction and channel capacity, the quantum channel capacity assisted by backward one-way classical communication differs from that assisted by two-way classical communication [125]. This is also related to interactive proof systems [126], and an open question worth exploring is whether there exists a finite interactive proof system that can replace PR correlations, leading to a new model in the measurement family.

4.4 Channel family

The core feature of the channel family model is the utilization of quantum channels to carry information, making them stored-program models, i.e., the quantum von Neumann architecture. According to the channel-state duality principle [43], a quantum channel is equivalent to its Choi state (7). In our model, quantum programs are represented as Choi states. The computation process consists of unitary operations and measurements on the Choi states. Since this type of model will be analyzed in detail later, we focus here on the characterization of its resource theory [127].

In the three types of models discussed earlier, we observe that their universal resources arise from different locality properties: if the set of free operations is larger, the universal resources are easier to prepare. For the set of channels, the three models we define depend on storage (i.e., the identity logical gate $\mathbb{1}$), bipartite storage (corresponding to entangled logical gates such as CNOT), and a non-local operation based on covariant quantum measurements [127]. The corresponding free sets are entanglement-breaking channels, bipartite local channels, and single-site channels, respectively. These three models are collectively referred to as the quantum von Neumann architecture, denoted as Model I, II, and III.

For Choi states, since they are derived from Bell states, their fundamental property is entanglement. A class of channels is the entanglement-breaking channels [128]

$$\mathcal{E}_{\mathrm{EB}}(\rho) = \sum_i \mathrm{tr}(M_i \rho)\sigma_i, \tag{25}$$

where $\{M_i\}$ is a POVM, and σ_i are states. The Choi states of such channels are separable and thus cannot be used for quantum information transmission. We know that classical computation can be described as a stochastic process, and any stochastic process $\vec{p} \mapsto \vec{q} = S\vec{p}$ can be implemented using some POVM $\{M_i\}$ as

$$S_{ij} = \langle j|M_i|j\rangle, \tag{26}$$

which is also a special type of entanglement-breaking channel. Therefore, we define the free set of Model I as entanglement-breaking channels, and all channels that do not break entanglement are resources. Clearly, the resource with the highest degree is unitary evolution, whose entanglement is equivalent to that of Bell states.

In fact, from the perspective of storage, Bell states are the fundamental units of storage [129, 130], enabling read and write functionalities, i.e., writing via measurement on one end and reading on the other. According to channel-state duality, Bell states serve as dynamical resources. This differs from the state family, where entangled states are static resources. The dynamical counterpart of entanglement is actually the bipartite entangled channel, which leads us to define Model II. Considering the locality of Choi states, for example, under the $A|B$ partition, a bipartite channel Φ^{AB} is separable if and only if $\omega_{\Phi^{AB}}$ is separable (note that the locality here differs from Model I). Thus, by analogy with entanglement, taking separable bipartite Choi states as the free set and local operations with classical communication as free operations, entangled bipartite channels become resources, with the maximal resource represented by the CNOT gate. This model can be used to design the structure of quantum chips, as will be discussed in detail in Section 6.

How, then, can we construct a Model III that relies on non-local storage? A natural consideration is to use non-local storage states, allowing the stored program to be directly recovered, i.e., Equation (3) can approximately hold. The previous two models cannot read out the program itself but only obtain certain observational results. This problem is equivalent to a metrological problem, where the process of reading the program is the process of measurement [34], and its precision is obviously limited by the uncertainty principle. If the size of the program state system is proportional to n, the computational precision is proportional to $\frac{1}{n^2}$. In a weaker sense, i.e., when the computational precision requirement is low, this can be considered as achieving quasi-universality [46]. Whether this model can be modified to achieve universality is a question worth further exploration. It is also straightforward to show that this scheme can be represented as operations on Choi states [127]. The quantum von Neumann architecture discussed later primarily relies on Models I and II.

5 Category II

We continue to discuss the type II models. As pointed out earlier, it is classified according to the depth of the basic logical gates. This type of model relies on the properties of error-correcting codes, especially the logical gates they support. Note that here we are mainly considering gates in the circuit model, because the operations in other type I models can also be reduced to the basic logical gates and measurements in the circuit model. Since our understanding is not yet mature, we will not analyze each model one by one. We will conduct a more detailed discussion of the case of fixed encoding.

In the (time-independent) unitary family, a coding method needs to be fixed, such as a certain isometry V. It basically also determines the optimal decoding method, although different decodings can be used in practice. In this family, the encoding of the single-step model is relatively simple. For a single fixed exact code, Eastin and Knill proved that the single-step (i.e. transversal) logical gates cannot achieve universality, because the number of transversal logical gates is finite [131]. In recent years, it has been found that this is related to symmetry. If continuous symmetries are allowed, such as U(1) or U(d), such so-called covariant codes can only be approximate codes [46–49], and their error-correcting accuracy is limited by the uncertainty relation. Since the transversal unitary operation does not change the entanglement of the system, the number of states that can be prepared by this model is finite, so it cannot achieve universality; on the contrary, since the covariant code is an approximate code, it can only achieve quasi-universality [46].

More generally, the SU(d) group is not necessarily a strict symmetry, and the quantum metrology task belongs to this case [68]. Covariant codes can also be used in metrology tasks, and their accuracy is limited by the uncertainty relation. Metrology does not assume symmetry, it generally refers to a process $O(\lambda)$ containing an unknown parameter λ acting on a certain resource state $|\psi\rangle$ in the form of single-step, and then estimating the value of λ by observing a certain quantity.

In addition, often in the field, quantum metrology and computing are listed as different research directions side by side [132], which is in a narrow sense. The former pays more attention to the processing of analog signals (such as λ) and has limited accuracy, while the latter pays more attention to digital information and has harsher requirements on accuracy. But in a broad sense, they both belong to the research scope of universal quantum computing or quantum information science.

The multi-step model can describe more situations of error-correcting codes. For example, for a general stabilizer code, the logical Pauli X and Z are generally single-step, and sometimes the H, S, CNOT, and even the T gates can also be single-step, but they cannot all be single-step at the same time [131]. There will be the problem of error correction in the implementation process of multi-step gates, because it will get away from the code space. This is an important problem, and one solution is to combine the idea of code conversion, forming other error-correcting codes during the implementation process, so that error correction can still be carried out [133].

Another noteworthy approach involves borrowing ideas from Hamiltonian simulation and space-time mapping. This entails viewing the direction of circuit evolution as space, treating logical gates as the evolution of Hamiltonians, and considering logical qubits as excited states of Hamiltonians. In this framework, each logical gate takes a multi-step form. This essentially represents a Hamiltonian-based multi-particle quantum walk model [28]. For instance, the Hubbard model has been proven to be a universal model. Alternatively, the spatial direction can be dispersed, meaning qubits are not arranged in a regular lattice structure. Instead, similar to circuit models, the time direction remains the actual evolution direction, with each logical qubit and gate stored in a small subsystem, akin to optical systems. This requires precise control over the system's excited states and their interactions [59].

From the perspective of entanglement, multi-step finite-depth operations can alter the system's short-range entanglement, while high-step operations can modify long-range topological entanglement [134]. Among high-step models, topological quantum computation is the most mature [27] and holds promise as the hardware foundation for future universal quantum computers. For Abelian anyons, such as surface codes [52], braiding operations are not high-step and cannot achieve universality. True universality is achieved through non-Abelian anyons (e.g., Fibonacci) via braiding operations, which must be implemented quasi-adiabatically, with the number of steps proportional to the system size [135]. However, topological systems cannot achieve self-correction [136], meaning topological information is disrupted at finite temperatures, and thermal excitations can lead to logical errors. During braiding, it is crucial to prevent anyons from interacting with thermally generated anyons. Although topological systems, such as fractional quantum Hall systems, have been experimentally realized, braiding anyons remains a significant challenge [137].

For dynamic codes, they are less well understood. Compared to static codes, dynamic codes offer the advantage of an additional controllable dimension, making error correction and universality easier to achieve. However, they impose higher demands on external controls (unitary or non-unitary). Several mature time-dependent control methods have been developed, including dynamical decoupling [51], Floquet control [138], adiabatic evolution [26], geometric phases [106], and measurement-based methods [67]. Among these, dynamical decoupling does not consume additional auxiliary qubits, offering approximate error correction capabilities [139]. Floquet control can be seen as an extension of this. For example, in many-body codes, Floquet many-body states can serve as error-correcting codes. Adiabatic evolution is primarily viewed as a type I model but can also be used to evolve code spaces. Currently, geometric phases are mainly used to construct quantum gates at the physical level, but this could be extended to the logical level, which remains an area for further research.

For non-unitary transformations in dynamic codes, they can be categorized into continuous and discontinuous types. The former is related to dissipative computing models [140], while the latter is associated with measurement-based quantum computation [61] and measurement-based code switching methods [67]. Currently, dissipative computing models are primarily used for quantum state preparation, with limited study on how to achieve transformations at the logical level. Measurement-based quantum computation is mainly viewed as a type I model but can also be seen as a single-step measurement-based code switching method, such as transitioning from one graph-state code to another. Measurement-based code switching can be seen as a generalization of it, leading to universal quantum computation schemes. For example, combining Reed-Muller codes with Steane codes can achieve a universal set of single-step logical gates [141], which is impossible with a single code. The transformations on dynamic codes can be viewed as costs for realizing logical gates, contributing to their depths. It is not hard to see it can also be classified into three types of models.

In all, compared to static codes, dynamic codes offer greater flexibility and impose different technical requirements. By combining multiple codes, they can outperform single codes, making them a promising direction for future development.

6 Quantum von Neumann architecture

6.1 Basic Structure

In this section, we focus on the quantum von Neumann architecture or model [35,79,127,142]. It includes quantum input, output, communication, control, storage, and computing units. In theory, it needs to overcome the impossibility theorems in the construction of quantum program storage units [33] and quantum control units [143]. Recent theoretical studies have shown that these difficulties can be overcome, thereby making a universal quantum von Neumann architecture possible. Its universality is also demonstrated by the simulation of quantum circuits, meaning that any given quantum circuit can be implemented by the basic operations in the von Neumann architecture, including measurement-driven read and write, i.e., input and output, and the combination of gates based on quantum gate teleportation. Compared to the circuit model and other models, the von Neumann architecture takes more into account the requirements of modularity, programmability, and security. Here, we focus on analyzing the processes related to storage and control. Additionally, our analysis is limited to theoretical aspects, not involving how to implement it on specific systems or more details, such as the type of storage.

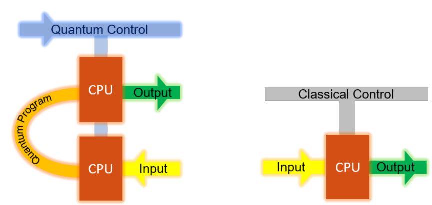

图 8: Schematics of the quantum von Neumann architecture (left) and the circuit model (right). For the later, there is no explicit quantum control unit and storage of quantum programs.

6.1.1 Read and write

As shown earlier, we use the Choi state to store the program. This can bypass Nielsen-Chuang's no-go theorem [33]. That is, unlike extracting the action of a program U on the state, We only ask for its observation on a certain quantity. According to the channel-state duality principle, the action of the channel or program $\mathcal{E}$ on the state ρ is implemented in the following way

$$\mathcal{E}(\rho) = d\, \text{tr}_\text{B}[\omega_\mathcal{E}(\mathbb{1} \otimes \rho^t)], \tag{27}$$

where ρ^t is a transpose of ρ, tr_B acts on the second part of $\omega_\mathcal{E}$, d is a dimension parameter. We often consider unitary case, that is $|\omega_U\rangle = (U \otimes \mathbb{1})|\omega\rangle$, or simply $|U\rangle$. In the above, ρ^t can be realized by the measurement process $\{\sqrt{\rho^t}, \sqrt{\mathbb{1} - \rho^t}\}$, which forms an initial-state injection, i.e. the writing process. The final result is a measurement of observable, i.e., $\mathrm{tr}(A\rho_f)$, which is weaker than the requirement of getting the entire state ρ_f.

For example, for the case of a pure state, suppose the initial state is $|0\rangle$, we need to calculate

$$p_i = |\langle\psi_i|U|0\rangle|^2. \tag{28}$$

The initial state is written by $\{P_0, P_{\bar{0}}\}$, $P_{\bar{0}} = \mathbb{1} - P_0$. The read operation is implemented by $\{|\psi_i\rangle\langle\psi_i|\}$. Here, the randomness of the measurement has been taken into account: P_0 will get p_i, $P_{\bar{0}}$ will get $p_i' = 1-p_i$, and they are equivalent [79]. When the initial dimension is large, it is also possible to effectively realize the initial-state injection with a binary measurement process. We see that the program states are all bipartite, with one end as the write side and the other as the read side.

In the model, the program state may be prepared by a dealer or someone else and sent over the network. Since it is a quantum state, it is secure from the outside world. We'll discuss this more later.

6.1.2 Universal quantum teleportation

The communication of quantum information (uploading, downloading, etc.) is an important part of this model. It can also be implemented in a variety of ways. Here we discuss the processes involving quantum state and gate teleportation. Quantum state teleportation can be expressed as

$$|\psi\rangle_\mathrm{B} = \sigma_{\mathrm{i,B}} M_\mathrm{AS}(i)|\omega\rangle_\mathrm{AB}|\psi\rangle_\mathrm{S}, \tag{29}$$

i.e., an unknown state $|\psi\rangle_\mathrm{S}$ measured by Bell measurement M_AS [2], and the result i is used to correct the Pauli byproduct σ_i. The state is transferred from system S to B.

Quantum state teleportation has an important symmetry, which is manifested in the fact that the probability of its Pauli correction is the same. The Pauli X and Z effects on the input S can be expressed as Pauli action on the final state. The symmetry is $Z_d \times Z_d$, which is also the global symmetry of a one-dimensional cluster state [78], whose application in computing is based on the quantum teleportation. Further, using the universal quantum gate teleportation mechanism [79], i.e. according to symmetry

$$U\sigma_i U^\dagger = \sum_j T_{ij}\sigma_j, \tag{30}$$

where $U \in \mathrm{SU}(d)$, $[T_{ij}] \in \mathrm{SU}(d^2)$ is an affine representation of U [144], the U at the input can be transferred to the output by the action of T at the measuring end, making

$$U|\psi\rangle_\mathrm{B} = \sigma_{\mathrm{i,B}} T M_\mathrm{AS}(i)|\omega_{U^t}\rangle_\mathrm{AB}|\psi\rangle_\mathrm{S}. \tag{31}$$

Note that here U is known and the measurement in the standard basis is made after the action of T. For $|\omega_{U^t}\rangle$, U needs to be transposed because $(U \otimes \mathbb{1})|\omega\rangle = (\mathbb{1} \otimes U^t)|\omega\rangle$. Then, using this mechanism and the read/write scheme, arbitrary algorithmic process (e.g., $\langle\psi_f|).U_n \cdots U_2U_1|\psi_i\rangle)$ can be simulated to prove the universality of the model. For hardware, this mechanism can be used in the construction of quantum chips. This is described later in the Section 6.3.

6.1.3 Program conversion

Given a quantum program, beyond measurements we can perform additional operations on it, which also forms the basis of algorithm design in the von Neumann architecture. Since the program is a Choi state, the general operation on it is a superchannel [40–42], which can be expressed as

$$\hat{\mathcal{S}}(\mathcal{E})(\rho) = \mathrm{tr}_a \mathcal{V}\,\mathcal{E}\,\mathcal{U}(\rho \otimes |0\rangle\langle 0|), \tag{32}$$

where ρ is the initial state, $\mathcal{U}$ and $\mathcal{V}$ are unitary operators, and a is the auxiliary system. The dimension of V can be larger than that of U [145]. The above equation can also be represented as an action on the Choi state

$$\hat{\mathcal{S}}(\mathcal{E})(\rho) = \mathrm{tr}_{\bar{\mathrm{S}}} \mathcal{V} \otimes \tilde{\mathcal{U}}(\omega_{\mathcal{E}} \otimes \omega)(\mathbb{1} \otimes \rho^t \otimes |0\rangle\langle 0|). \tag{33}$$

where $\tilde{\mathcal{U}}$ is equivalent to $\mathcal{U}$ [35]. $\mathrm{tr}_{\bar{\mathrm{S}}}$ does not act on the data end S. A series of superchannels cascaded together form what is known as a quantum comb, collectively referred to as superchannels in this work. By repeatedly utilizing the channel-state duality principle, higher-order superchannels can be obtained. We see that entangled bits (ebits) play a crucial role in the implementation of superchannels, which is also the basis for their resource theory characterization [127].

6.1.4 Quantum control unit

The quantum control unit refers to a quantum system capable of controlling the implementation of a quantum program. One of its fundamental roles is to transform a gate U into a controlled form $\wedge_U$. Initially, it was discovered that for any unknown quantum gate process, this is impossible to achieve, which is known as the uncontrollability theorem [143]. This is because it violates a fundamental principle of quantum mechanics, namely, it would convert the global phase of U into a physically significant relative phase. In fact, A. Kitaev was the first to discover that if one assumes knowledge of a certain eigenvalue and eigenstate of U, it can be utilized as an auxiliary to realize the control process [88]. That is,

$$f(U)|c\rangle|\psi\rangle|\lambda\rangle = \wedge_U |c\rangle|\psi\rangle|\lambda\rangle, \tag{34}$$

where $U|\lambda\rangle = |\lambda\rangle$, $f(U) = \wedge_\Xi(\mathbb{1}\ \mathbb{1}\ U)\wedge_\Xi$, $\wedge_\Xi$ is a controlled swap gate. This ancilla eliminates the factor of the global phase of U. Therefore, unlike quantum programs, the quantum control unit does not require measurements to be implemented, but can directly serve as a quantum input signal. The structure of the entire quantum von Neumann architecture is shown in Fig. 8. Unlike in the classical case, here the quantum control flow and information flow can become entangled. Quantum control can also be viewed as a type of superchannel process, where both the control unit and the data unit are equally important. The role of the quantum control unit warrants further in-depth research.

6.2 Features

Here, we analyze the fundamental characteristics of the quantum von Neumann architecture, including its modularity, security, programmability, and its overall matrix product state (MPS) structure. These characteristics can be better understood through comparisons with other models.

Modularity is a foundational principle in the construction of the von Neumann architecture. It plays a crucial role in the design of real computer hardware and is equally important in software development. Modules and the interfaces between them are essential components of modern computing devices [12]. Traditional circuit models often overlook modularity, as they primarily focus on the basic theoretical requirement of universality. Modularity, along with digitization (see Section 2.1), serves as an important metric to distinguish computing systems from physical systems. This is because natural physical systems, such as atoms and molecules, are not typically divided into replaceable functional parts.

Security is a key feature that distinguishes the quantum von Neumann architecture from classical computing and other quantum computing models. In this context, security is primarily based on quantum storage (as well as quantum communication) and extends the idea of secure communication to storage [146]. Since quantum programs are stored as Choi states, an external eavesdropper can only obtain information about the Choi state through measurement, which would disrupt the program. In communication, the program creator sends the Choi state to the user, who must be authenticated. Theoretical studies show that a certain number of Choi state copies can meet verification requirements [126,147] while ensuring that insufficient information about the Choi state is leaked to the user. This allows the program creator to maintain security against both the user and third parties.

This form of security differs from that of so-called blind quantum computing [74]. In blind quantum computing tasks, a user delegates a computational task to a computing center or provider without revealing the details of the computation (input, output, or process). In this scenario, the user knows the classical representation of the program $[U]$, but the provider has the capability to implement U or even prepare $|U\rangle$. In the von Neumann architecture, the provider typically knows both $[U]$ and U, while the user can utilize $|U\rangle$ without fully understanding its information $[U]$. Blind quantum computing may be suitable for specific stages or scenarios in quantum computing, such as when a limited number of quantum computing centers provide secure services to a broad user base.

Programmability is a critical requirement for hardware, enabling the same hardware structure to achieve different functions. This capability played a pivotal role in the development of general-purpose computers and facilitated the transition from analog to digital signals in many technologies. In this context, programmability requires that a process or function can be stored as data, effectively converting hardware into software for further use. In the circuit model, programs are represented as classical circuit "diagrams," i.e., $[U]$. For example, in a superconducting platform, programmability refers to the ability to execute different programs $[U]$ on the same platform, representing classical programmability. In our model, quantum programs are represented as Choi states, and quantum programmability refers to the ability to execute different programs $|U\rangle$ on the same platform. Additionally, the combination of Choi states is controllable. For instance, based on control signals, one can choose whether to incorporate a specific Choi state [127,142], corresponding to the activation or deactivation of a gate. If quantum control signals are used, they become part of the overall quantum algorithm, enhancing quantum programmability.

At a higher level, the combination of Choi states is related to the matrix product state (MPS) form, which also plays a significant role in local Turing machines and measurement-based quantum computing (see Section 4.1). MPS are represented as a series of tensors (see Fig. 7), where each tensor has both physical and virtual (entangled) indices. In the von Neumann architecture, the Choi state can be viewed as living in the entanglement space, and operations in the CPU involve constructing tensors and measuring their indices. A local Turing machine assumes the availability of ebits, from which MPS states are prepared by constructing tensors. Measurement-based quantum computing typically assumes the availability of an MPS, with computation performed by measuring the physical indices. From this perspective, the von Neumann architecture can be seen as an extension of these two models.

In summary, the quantum von Neumann architecture integrates modularity, security, programmability, and an MPS-based structure, offering a versatile framework that extends and enhances existing quantum computing models.

6.3 Chip design

Existing classical electronic chips are generally designed based on the von Neumann architecture, with their hardware foundation consisting of circuits composed of semiconductor diodes, transistors, and other components. From a hardware perspective, a single piece of hardware can perform multiple functions, such as storing data, executing programs, and serving as part of logical gates or even analog circuits. As mentioned earlier, its structure is modular and hierarchical, incorporating numerous programmable logic modules. This serves as an excellent example for the development of quantum chips.

To illustrate some structural characteristics of current quantum chips, let us consider a few examples. In superconducting chips, qubits serve as the hardware, while quantum gates are generated in real time based on the interaction between qubits and control systems. As previously mentioned, their programmability is classical in nature. In quantum optical chips [148], quantum gates are the hardware, and qubits are generated in real time using lasers. Of course, photons can also be stored in hardware such as optical fibers or optical cavities. Currently, these systems employ a classical-quantum hybrid architecture, where the quantum chip acts as the computing unit, and the remaining data processing is handled by classical computers.

The structure of quantum chips can be further extended using the quantum von Neumann architecture. This involves integrating quantum program and control modules. For instance, in a superconducting platform, program storage modules and control modules can both be composed of superconducting qubits. This approach breaks the traditional correspondence between gates and qubits in space and time, meaning quantum gates can exist both in space (as hardware) and in time (generated in real time), and the same applies to qubits. In fact, classical chips have already implemented this concept. The program module can contain a large system of programs or some basic gate programs. By leveraging the quantum gate mechanism and the superchannel process, programmable gate arrays can be formed using H, T, and CNOT gate programs, with FPGA serving as the basic structure of quantum chips. Additionally, various systems can be mixed and matched in hardware, combining the properties of different physical systems, which is also a direction currently being explored [149].

Similar to classical systems, quantum systems can incorporate various types of storage, such as internal memory, external memory, and flash memory, utilizing physical methods like electricity, magnetism, and optics. External memory typically uses disks or optical discs, but due to their slower speeds, modern chips rely on internal memory. When running a program, data is usually imported from external memory into internal memory, and the final results are stored back in external memory. For fast calculations, the lifetime of a qubit in memory or on a chip does not need to be arbitrarily long. However, if stable quantum memory is required, decoherence must be fundamentally overcome. Unlike the magnetic states used in classical disks, no self-correcting quantum system has been discovered [136]. If active quantum error correction is employed, it incurs significant overhead. Therefore, the development of suitable quantum memory devices remains an important experimental direction [150].

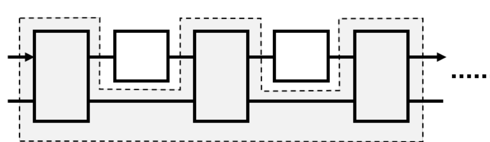

图 9: Schemetics of quantum super-algorithm. The ‘mother’ algorithm (shaded) maps the input data (boxes) into the desired ‘child’ algorithm, which acts on the data system (top register). The classical-quantum hybrid algorithm (Fig.3) is a special case, and the MPS formula (Fig.7) is also a special case of it. There can also be quantum correlation or memory (unshown) between the input (boxes).

6.4 Algorithm design

In the above discussion, we have not strictly distinguished between the concepts of program, algorithm, or process, because mathematically they can all be represented as unitary evolution or channels. In computers, an algorithm and a program are not the same. Programming or the implementation of a program depends on programming languages, such as machine language, assembly language, and high-level languages, whereas an algorithm is mathematical in nature, and the same algorithm can be implemented by different programs. Generally speaking, both are aspects of computer software.

The impact of the quantum von Neumann architecture on software can also be divided into two points. In terms of programs, it makes quantum assembly language possible, while currently, we are still in the stage of quantum machine language. The development of languages mainly depends on computer scientists. In terms of algorithms, analogous to the significance of super-channels to channels, it makes the design of quantum super-algorithms possible. The structure of a quantum super-algorithm is shown in Fig. 9, where a quantum “parent” algorithm is used to design a quantum “child” algorithm. The algorithm structure in the circuit model we mentioned (Fig. 3) is a special case of it: the parent algorithm is classical or classical-quantum hybrid. It should be noted that although a super-algorithm can also be treated as an ordinary algorithm, just as any computational model can be simulated by the circuit model, considering it as a super-algorithm provides new perspectives. From the perspective of resource theory, it utilizes quantum storage or memory as a resource [127]. In classical algorithms, super-algorithms have already been widely applied, such as the well-known machine learning algorithms.

Some quantum algorithms or schemes that have been discovered can be viewed as quantum super-algorithms. For example, the quantum channel discrimination scheme is one of the earliest applications of quantum superchannel theory, using superchannels instead of simple channels can improve the success rate of certain channel discriminations [151]. The recently proposed quantum singular value transformation (QSVT) [20] can uniformly describe several quantum algorithms, it is also a quantum super-algorithm [59]. Other examples include quantum game theory [152], metrology schemes [153], quantum optimization [154], and especially quantum machine learning [155–158]. Machine learning forms an algorithm to solve problems after learning from a large number of samples. Compared to classical machine learning, quantum machine learning algorithms offer exponential speedups in certain high-precision computational problems [158,159].

7 Discussion and Conclusion

In this paper, we investigate the classification of universal quantum computing models from the perspective of quantum resource theory, and specifically analyze certain models, such as the quantum von Neumann architecture. Among these, the development of some models is relatively mature, while the development of others has only just begun.

Since DiVincenzo [32] proposed the fundamental requirements for realizing universal quantum computing at the beginning of the century, numerous universal quantum computing models or architectures have been developed to explore the implementation of quantum computers. These models have demonstrated a richer landscape than the conventional circuit model in terms of quantum algorithm design, physical implementation, and application scenarios. This paper attempts to systematically understand universal quantum computing models from the perspective of quantum resource theory, although our research remains insufficient so far. In the main text, we have raised several questions. For example, the nonlocal computing model utilizes PR correlations, which go beyond the scope of quantum theory, and whether they can be modified is a question worth investigating. We have also overlooked the issue of resource quantification. The most mature development lies in the quantification of quantum state resources, such as coherence and entanglement. Although other types of resources can also be converted into state resources for quantification, this still requires specific research. Additionally, due to space limitations, we were unable to analyze in detail the specific schemes for combining two types of models in the classification table, which are closely related to the error-correcting codes employed.

Before concluding, we further discuss topics such as quantum resources and quantum advantage, universal versus dedicated models, with the aim of fostering a broader understanding of universal quantum computing.

7.1 Quantum resources and quantum advantages

In the early stages of quantum computing development, the understanding of the core characteristics of quantum computing was not clear. For example, based on Shor's algorithm, Grover's algorithm, and others, some computer scientists believed that the cause of quantum speedup lay in quantum interference [160]. However, in quantum teleportation, quantum encryption communication, and even quantum computing, quantum entanglement also plays a crucial role [113,161,162]. Later, on one hand, it was shown in the measurement-based quantum computing model that a large amount of entanglement does not necessarily lead to universality [82,83], while on the other hand, it was demonstrated in the circuit model that a small amount of entanglement is sufficient to ensure universality [163]. At the same time, some studies suggested that the foundation of quantum speedup is quantum contextuality [164]. Our systematic research indicates that quantum resources need to be understood within the framework of a universal quantum computing model, and they cannot be simply compared or substituted. Instead, they are all quantum resources that can be utilized, and studying their mutual transformations is also beneficial.

Quantum advantage stems from the rational utilization of quantum resources. People generally equate quantum advantage with quantum speedup, but it can also manifest in other aspects such as storage, security, energy consumption, and metrology [142]. For example, security was one of the earliest recognized aspects [146], and the confidentiality and security of quantum communication, as well as its integration with quantum computing, remain important research directions in the field [73,74,165]. This could potentially avoid some security issues present in existing non-quantum networks. In terms of storage, A. Holevo was the first to study the communication capacity (and also storage capacity) of qubits and channels from an information theory perspective [166]. Recently, it has been discovered that utilizing quantum storage (or memory) makes quantum machine learning algorithms significantly superior to classical algorithms in certain problems [158,159]. People have also begun to focus on studying quantum advantages in areas such as energy consumption [167,168] and metrology precision [68,132]. However, it is currently not possible to control the required quantum systems with arbitrarily high precision, which poses a challenge to the realization of near-term quantum advantage.

7.2 Universal and non-universal

Beyond the research paradigm of universal quantum computing, there exists the direction of dedicated non-universal quantum computing. Dedicated or specialized, as the name suggests, is aimed at specific types of problems, and it does not need to simultaneously meet the requirements of digitization, universality, and programmability. However, it is also difficult to define the scope of dedicated quantum computing, with examples of research directions including quantum emulation [95] and continuous-variable quantum information processing [169]. This is also the case in classical computing, and specialized computing models are increasingly gaining attention. As shown in Fig. 10, GPUs, optical chips, memristors, and others have demonstrated advantages over existing CPU architectures in certain computational tasks. These specialized computing models can be seen as a reasonable transition from classical computing to universal quantum computing.

Since achieving fault-tolerance is currently challenging, developing specialized quantum computing is also important. For example, in quantum emulation or simulation, the reliable emulation of certain quantum many-body physical phenomena will aid scientific research, as these phenomena or models (such as superconductivity and the Hubbard model) are mostly difficult to solve on existing computers [170]. To improve the reliability of emulation, it is also necessary to develop error control techniques, which can include dynamical decoupling [51], error mitigation and estimation methods [171,172]. Additionally, research on continuous variables (photons, phonons, etc.) is essential. It should be noted that in the classical domain, analog (i.e., continuous-variable) circuits have always accompanied digital circuits, playing a significant role in various electronic devices.

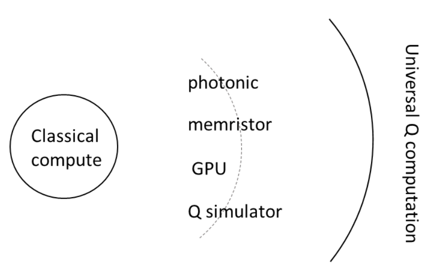

图 10: In between the current classical computers and the universal quantum computers in the future, there are other research paradigm, such as optical chips, memristors, GPU for AI, and quantum simulators etc.

7.3 Challenges

Although the field of quantum computing has developed for over 30 years, it still faces many core challenges. These challenges broadly fall into three aspects: fundamental theory, hardware, and software. On the theoretical side, some properties of quantum channels are not yet fully understood. For example, the capacity of quantum channels is extremely difficult to calculate, due to certain peculiar properties (such as non-additivity) [173], which means that the quantum version of Shannon's information theory has not yet been fully established. Channel capacity is the supremum of communication rates (bandwidth), and it has significant guiding implications for the design of high-efficiency error-correcting codes. Additionally, using the matrix product state formalism, the properties of quantum states can be reduced to the properties of channels, yet the classification problem of few-body quantum entangled states remains unresolved [174], an issue closely related to distributed quantum computing. On the hardware side, there is still a fundamental need to overcome decoherence and achieve large-scale quantum error correction [175]. While on the software side, there is a need to discover more quantum algorithms and develop quantum programming and application software. In summary, our research on universal quantum computing models indicates that there are still many fundamental properties and applications of quantum information remaining to be explored.

Acknowledgement

Thanks to Yongjian Han, Jiang Zhang, Lin Li, Dianmin Tong, Xiaodong Yu, Yunjiang Wang, Shunlong Luo, and Heng Fan for their valuable suggestions, Yuandong Liu, Kai Wang and other students participated in the discussion. Thanks to the reviewers for their suggestions.

Reference

[1] J. Preskill, Quantum computing in the nisq era and beyond, Quantum 2 (2018) 79.

[2] M. A. Nielsen, I. L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, Cambridge U.K., 2000.

[3] J.-W. Pan, Quantum information technology: Current status and prospects, Acta Phys. Sin. 73 (2024) 010301.

[4] J. S. Bell, On the problem of hidden variables in quantum mechanics, Rev. Mod. Phys. 38 (1966) 447–452.

[5] K. Kraus, States, Effects, and Operations: Fundamental Notions of Quantum Theory, Vol. 190 of Lecture Notes in Physics, Springer-Verlag, Berlin, 1983.

[6] A. S. Holevo, Probabilistic and Statistical Aspect of Quantum Theory, North-Holland, Amsterdam, 1982.

[7] R. P. Feynman, Simulating physics with computers, Int. J. Theor. Phys. 21 (6/7) (1982) 467–488.

[8] D. Deutsch, Quantum theory, the Church-Turing principle and the universal quantum computer, in: Proc. R. Soc. (London), Ser. A, Vol. 400, The Royal Society, 1985, pp. 97–117.

[9] A. C.-C. Yao, Quantum circuit complexity, in: Foundations of Computer Science, 1993. Proceedings., 34th Annual Symposium on, IEEE, 1993, pp. 352–361.

[10] E. Bernstein, U. Vazirani, Quantum complexity theory, SIAM J. Comput. 26 (5) (1997) 1411–1473.

[11] P. W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, in: Proceedings 35th annual symposium on foundations of computer science, IEEE, 1994, pp. 124–134.

[12] D. M. Harris, S. L. Harris, Digital design and computer architecture, Elsevier, 2013.

[13] C. Shannon, A mathematical theory of communication, The Bell System Technical Journal 27 (1948) 379.

[14] J. von Neumann, First draft of a report on the edvac, IEEE Annals of the History of Computing 15 (1993) 27–75.

[15] D. Lidar, T. A. Brun (Eds.), Quantum error correction, Cambridge University Press, 2013.

[16] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, J. L. O' Brien, Quantum computers, Nature 464 (7285) (2010) 45–53.

[17] L. K. Grover, A fast quantum mechanical algorithm for database search, in: Proceedings of the twenty-eighth annual ACM Symposium on Theory of Computing, 1996.

[18] A. W. Harrow, A. Hassidim, S. Lloyd, Quantum algorithm for linear systems of equations, Phys. Rev. Lett. 103 (2009) 150502.

[19] G. L. Long, Duality quantum computing and duality quantum information processing, Int. J. Theor. Phys. 50 (2011) 1305.

[20] J. M. Martyn, Z. M. Rossi, A. K. Tan, I. L. Chuang, Grand unification of quantum algorithms, PRX Quantum 2 (2021) 040203.

[21] J. Watrous, The Theory of Quantum Information, Cambridge University Press, 2018.

[22] M. Hayashi, Quantum Information Theory: Mathematical Foundation, 2nd edition, Springer, 2017.

[23] M. Wilde, Quantum Information Theory, Cambridge University Press, 2017.

[24] E. Chitambar, G. Gour, Quantum resource theories, Rev. Mod. Phys. 91 (2019) 025001.

[25] D.-S. Wang, Universal resources for quantum computing, Commun. Theor. Phys. 75 (2023) 125101.

[26] T. Albash, D. A. Lidar, Adiabatic quantum computation, Rev. Mod. Phys. 90 (2018) 015002.

[27] C. Nayak, S. H. Simon, A. Stern, M. Freedman, S. D. Sarma, Non-abelian anyons and topological quantum computation, Rev. Mod. Phys. 80 (3) (2008) 1083.

[28] A. M. Childs, D. Gosset, Z. Webb, Universal computation by multiparticle quantum walk, Science 339 (2013) 791.

[29] P. Arrighi, An overview of quantum cellular automata, Natural Computing 18 (2019) 885–899.

[30] H. J. Briegel, D. E. Browne, W. Dür, R. Raussendorf, M. Van den Nest, Measurement-based quantum computation, Nat. Phys. 5 (1) (2009) 19–26.

[31] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, H. Weinfurter, Elementary gates for quantum computation, Phys. Rev. A 52 (5) (1995) 3457.

[32] D. P. DiVincenzo, The Physical Implementation of Quantum Computation, arXiv:quant-ph/0002077 (2000).

[33] M. A. Nielsen, I. L. Chuang, Programmable quantum gate arrays, Phys. Rev. Lett. 79 (1997) 321–324.

[34] Y. Yang, R. Renner, G. Chiribella, Optimal universal programming of unitary gates, Phys. Rev. Lett. 125 (2020) 210501.

[35] D.-S. Wang, A prototype of quantum von Neumann architecture, Commun. Theor. Phys. 74 (2022) 095103.

[36] C. M. Dawson, M. A. Nielsen, The solovay-kitaev algorithm, Quantum Inf. Comput. 6 (1) (2006) 81–95.

[37] S. Lloyd, Universal quantum simulators, Science 273 (5278) (1996) 1073–1078.

[38] G. Brassard, P. Høyer, M. Mosca, A. Tapp, Quantum amplitude amplification and estimation, Contem. Mathemat. 305 (2002) 53–74.

[39] E. Knill, R. Laflamme, Theory of quantum error-correcting codes, Phys. Rev. A 55 (1997) 900–911.

[40] G. Chiribella, G. M. D'Ariano, P. Perinotti, Transforming quantum operations: Quantum supermaps, Europhys. Lett. 83 (2008) 30004.

[41] G. Chiribella, G. M. D'Ariano, P. Perinotti, Quantum circuit architecture, Phys. Rev. Lett. 101 (2008) 060401.

[42] G. Chiribella, G. M. D'Ariano, P. Perinotti, Theoretical framework for quantum networks, Phys. Rev. A 80 (2009) 022339.

[43] M.-D. Choi, Completely positive linear maps on complex matrices, Linear Algebra Appl. 10 (1975) 285–290.

[44] C. Bény, O. Oreshkov, General conditions for approximate quantum error correction and near-optimal recovery channels, Phys. Rev. Lett. 104 (2010) 120501.

[45] D. Gottesman, Theory of fault-tolerant quantum computation, Phys. Rev. A 57 (1998) 127–137.

[46] D.-S. Wang, G. Zhu, C. Okay, R. Laflamme, Quasi-exact quantum computation, Phys. Rev. Res. 2 (2020) 033116.

[47] D.-S. Wang, Y.-J. Wang, N. Cao, B. Zeng, R. Laflamme, Theory of quasi-exact fault-tolerant quantum computing and valence-bond-solid codes, New J. Phys. 24 (2022) 023019.

[48] S. Zhou, Z.-W. Liu, L. Jiang, New perspectives on covariant quantum error correction, Quantum 5 (2021) 521.

[49] Y. Yang, Y. Mo, J. M. Renes, G. Chiribella, M. P. Woods, Optimal universal quantum error correction via bounded reference frames, Phys. Rev. Res. 4 (2022) 023107.

[50] A. Kubica, R. Demkowicz-Dobrzański, Using quantum metrological bounds in quantum error correction: A simple proof of the approximate eastin-knill theorem, Phys. Rev. Lett. 126 (2021) 150503.

[51] L. Viola, E. Knill, S. Lloyd, Dynamical decoupling of open quantum systems, Phys. Rev. Lett. 82 (1999) 2417–2421.

[52] A. Y. Kitaev, Fault-tolerant quantum computation by anyons, Ann. Phys. 303 (1) (2003) 2–30.

[53] W. E. Ryan, S. Lin, Channel Codes: Classical and Modern, Cambridge University Press, 2009.

[54] N. P. Breuckmann, J. N. Eberhardt, Quantum low-density parity-check codes, PRX Quantum 2 (2021) 040101.

[55] D.-S. Wang, Y.-D. Liu, Y.-J. Wang, S. Luo, Quantum resource theory of coding for error correction, Phys. Rev. A 110 (2024) 032413.

[56] B. Coecke, T. Fritz, R. W. Spekkens, A mathematical theory of resources, Information and Computation 250 (2016) 59–86.

[57] R. Horodecki, P. Horodecki, M. Horodecki, K. Horodecki, Quantum entanglement, Rev. Mod. Phys. 81 (2009) 865–942.

[58] A. Streltsov, G. Adesso, M. B. Plenio, Colloquium: Quantum coherence as a resource, Rev. Mod. Phys. 89 (2017) 041003.

[59] D.-S. Wang, A comparative study of universal quantum computing models: towards a physical unification, Quantum Engineering 2 (2021) e85.

[60] D.-S. Wang, A local model of quantum Turing machines, Quant. Infor. Comput. 20 (3) (2020) 0213–0229.

[61] R. Raussendorf, H. J. Briegel, A one-way quantum computer, Phys. Rev. Lett. 86 (2001) 5188–5191.

[62] M. A. Nielsen, Cluster-state quantum computation, Reports on Math. Phys. 57 (1) (2006) 147–161.

[63] D.-S. Wang, D. T. Stephen, R. Raussendorf, Qudit quantum computation on matrix product states with global symmetry, Phys. Rev. A 95 (2017) 032312.

[64] D. T. Stephen, D.-S. Wang, A. Prakash, T.-C. Wei, R. Raussendorf, Computational power of symmetry-protected topological phases, Phys. Rev. Lett. 119 (2017) 010504.

[65] R. Raussendorf, C. Okay, D.-S. Wang, D. T. Stephen, H. P. Nautrup, Computationally universal phase of quantum matter, Phys. Rev. Lett. 122 (2019) 090501.

[66] A. Molina, J. Watrous, Revisiting the simulation of quantum Turing machines by quantum circuits, Proc. Royal Soc. A 475 (2226) (2019) 20180767.

[67] A. Paetznick, B. W. Reichardt, Universal fault-tolerant quantum computation with only transversal gates and error correction, Phys. Rev. Lett. 111 (2013) 090505.

[68] G. Tóth, I. Apellaniz, Quantum metrology from a quantum information science perspective, J. Phys. A: Math. Theor. 47 (2014) 424006.

[69] I. Affleck, T. Kennedy, E. H. Lieb, H. Tasaki, Rigorous results on valence-bond ground states in antiferromagnets, Phys. Rev. Lett. 59 (1987) 799–802.

[70] M. Fannes, B. Nachtergaele, R. F. Werner, Finitely correlated states on quantum spin chains, Commun. Math. Phys. 144 (3) (1992) 443–490.

[71] D. Perez-Garcia, F. Verstraete, M. Wolf, J. Cirac, Matrix product state representations, Quantum Inf. Comput. 7 (5) (2007) 401–430.

[72] M. Sarovar, T. Proctor, K. Rudinger, K. Young, E. Nielsen, R. Blume-Kohout, Detecting crosstalk errors in quantum information processors, Quantum 4 (2020) 321.

[73] C. Crépeau, D. Gottesman, A. Smith, Secure multi-party quantum computation, in: STOC ' 02: Proc. 34rd Annual ACM Symp. Theory of Computing, 2002, p. 643.

[74] A. Broadbent, J. Fitzsimons, E. Kashefi, Universal blind quantum computation, in: Proceedings of the 50th Annual Symposium on Foundations of Computer Science (IEEE Computer Society, Los Alamitos, CA, 2009), 2009, pp. 517–527.

[75] J. M. Myers, Can a universal quantum computer be fully quantum?, Phys. Rev. Lett. 78 (1997) 1823–1824.

[76] J. I. Cirac, D. Pérez-García, N. Schuch, F. Verstraete, Matrix product states and projected entangled pair states: Concepts, symmetries, theorems, Rev. Mod. Phys. 93 (2021) 045003.

[77] S. Wehner, D. Elkouss, R. Hanson, Quantum internet: A vision for the road ahead, Science 362 (2018) 303.

[78] D.-S. Wang, Quantum computation by teleportation and symmetry, Int. J. Mod. Phys. B 33 (15) (2019) 1930004.

[79] D.-S. Wang, Choi states, symmetry-based quantum gate teleportation, and stored-program quantum computing, Phys. Rev. A 101 (2020) 052311.

[80] M. Van den Nest, W. Dür, G. Vidal, H. J. Briegel, Classical simulation versus universality in measurement-based quantum computation, Phys. Rev. A 75 (2007) 012337.

[81] M. Van den Nest, W. Dür, A. Miyake, H. J. Briegel, Fundamentals of universality in one-way quantum computation, New J. Phys. 9 (2007) 204.

[82] D. Gross, S. T. Flammia, J. Eisert, Most quantum states are too entangled to be useful as computational resources, Phys. Rev. Lett. 102 (2009) 190501.

[83] M. J. Bremner, C. Mora, A. Winter, Are random pure states useful for quantum computation?, Phys. Rev. Lett. 102 (2009) 190502.

[84] Z.-C. Gu, X.-G. Wen, Tensor-entanglement-filtering renormalization approach and symmetry-protected topological order, Phys. Rev. B 80 (2009) 155131.

[85] X. Chen, Z.-C. Gu, X.-G. Wen, Classification of gapped symmetric phases in one-dimensional spin systems, Phys. Rev. B 83 (2011) 035107.

[86] N. Schuch, D. Pérez-García, I. Cirac, Classifying quantum phases using matrix product states and projected entangled pair states, Phys. Rev. B 84 (2011) 165139.

[87] S. Bartolucci, P. Birchall, H. Bombin, H. Cable, C. Dawson, M. Gimeno-Segovia, E. Johnston, K. Kieling, N. Nickerson, M. Pant, F. Pastawski, T. Rudolph, C. Sparrow, Fusion-based quantum computation, Nat. Commun. 14 (2023) 912.

[88] A. Kitaev, A. H. Shen, M. N. Vyalyi, Classical and Quantum Computation, Vol. 47 of Graduate Studies in Mathematics, American Mathematical Society, Providence, 2002.

[89] P. Wocjan, M. Roetteler, D. Janzing, T. Beth, Universal simulation of hamiltonians using a finite set of control operations, Quant. Infor. Comput. 2 (2) (2002) 133.

[90] J. L. Dodd, M. A. Nielsen, M. J. Bremner, R. T. Thew, Universal quantum computation and simulation using any entangling hamiltonian and local unitaries, Phys. Rev. A 65 (2002) 040301.

[91] T. S. Cubitt, A. Montanaro, S. Piddock, Universal quantum hamiltonians, Proceedings of the National Academy of Sciences 115 (38) (2018) 9497–9502.

[92] T. Kohler, S. Piddock, J. Bausch, T. Cubitt, Translationally-invariant universal quantum hamiltonians in 1d, Ann. Henri Poincaré 23 (2021) 223–254.

[93] T. Kohler, S. Piddock, J. Bausch, T. Cubitt, General conditions for universality of quantum hamiltonians, PRX Quantum 3 (2022) 010308.

[94] D. W. Berry, G. Ahokas, R. Cleve, B. C. Sanders, Efficient quantum algorithms for simulating sparse hamiltonians, Commun. Math. Phys. 270 (2) (2007) 359–371.

[95] J. I. Cirac, P. Zoller, Goals and opportunities in quantum simulation, Nat. Phys. 8 (4) (2012) 264–266.

[96] D. J. Shepherd, T. Franz, R. F. Werner, Universally programmable quantum cellular automaton, Phys. Rev. Lett. 97 (2006) 020502.

[97] D. Janzing, Spin-1/2 particles moving on a two-dimensional lattice with nearest-neighbor interactions can realize an autonomous quantum computer, Phys. Rev. A 75 (2007) 012307.

[98] D. Nagaj, P. Wocjan, Hamiltonian quantum cellular automata in one dimension, Phys. Rev. A 78 (2008) 032311.

[99] D. Nagaj, Universal two-body-hamiltonian quantum computing, Phys. Rev. A 85 (2012) 032330.

[100] S. Lloyd, B. Terhal, Adiabatic and Hamiltonian computing on a 2d lattice with simple two-qubit interactions, New J. Phys. 18 (2) (2016) 023042.

[101] T. Toffoli, N. Margolus, Cellular Automata Machines: A new environment for modeling, MIT Press, 1987.

[102] A. Bisio, G. M. D' Ariano, A. Tosini, Quantum field as a quantum cellular automaton: The dirac free evolution in one dimension, Ann. Phys. 354 (2015) 244.

[103] B. Heim, T. F. Rønnow, S. V. Isakov, M. Troyer, Quantum versus classical annealing of ising spin glasses, Science 348 (6231) (2015) 215–217.

[104] A. Villanueva, P. Najafi, H. J. Kappen, Why adiabatic quantum annealing is unlikely to yield speed-up, J. Phys. A: Math. Theor. 56 (46) (2023) 465304.

[105] S. Bravyi, D. P. DiVincenzo, R. I. Oliveira, B. M. Terhal, The complexity of stoquastic local hamiltonian problems, Quantum Infor. Comput. 8 (5) (2008) 0361.

[106] J. Zhang, T. H. Kyaw, S. Filipp, L.-C. Kwek, E. Sjöqvist, D. Tong, Geometric and holonomic quantum computation, Phys. Reports 1027 (2023) 1–53.

[107] W. K. Wootters, A Wigner-function formulation of finite-state quantum mechanics, Ann. Phys. 176 (1987) 1.

[108] D. Gross, Hudson's theorem for finite-dimensional quantum systems, J. Math. Phys. 47 (2006) 122107.

[109] S. Bravyi, A. Kitaev, Universal quantum computation with ideal clifford gates and noisy ancillas, Phys. Rev. A 71 (2005) 022316.

[110] S. Popescu, D. Rohrlich, Quantum nonlocality as an axiom, Found. Phys. 24 (1994) 379.

[111] R. W. Spekkens, Negativity and contextuality are equivalent notions of nonclassicality, Phys. Rev. Lett. 101 (2008) 020401.

[112] R. W. Spekkens, Contextuality for preparations, transformations, and unsharp measurements, Phys. Rev. A 71 (2005) 052108.

[113] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, W. K. Wootters, Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels, Phys. Rev. Lett. 70 (1993) 1895–1899.

[114] D. Gottesman, I. L. Chuang, Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations, Nature 402 (6760) (1999) 390–393.

[115] G. L. Long, General quantum interference principle and duality computer, Commun. Theor. Phys. 45 (2006) 825–844.

[116] A. M. Childs, N. Wiebe, Hamiltonian simulation using linear combinations of unitary operations, Quant. Infor. Comput. 12 (2012) 901.

[117] D. W. Berry, A. M. Childs, R. Cleve, R. Kothari, R. D. Somma, Simulating hamiltonian dynamics with a truncated taylor series, Phys. Rev. Lett. 114 (2015) 090502.

[118] S. Wei, G. L. Long, Duality quantum computer and the efficient quantum simulations, Quantum Infor. Processing 15 (2016) 1189–1212.

[119] X. Zhou, D. W. Leung, I. L. Chuang, Methodology for quantum logic gate construction, Phys. Rev. A 62 (2000) 052316.

[120] A. Broadbent, Popescu-Rohrlich correlations imply efficient instantaneous nonlocal quantum computation, Phys. Rev. A 94 (2016) 022318.

[121] J. F. Clauser, M. A. Horne, A. Shimony, R. A. Holt, Proposed experiment to test local hidden-variable theories, Phys. Rev. Lett. 23 (1969) 880–884.

[122] L. Vaidman, Instantaneous measurement of nonlocal variables, Phys. Rev. Lett. 90 (2003) 010402.

[123] G. Brassard, H. Buhrman, N. Linden, A. A. Méthot, A. Tapp, F. Unger, Limit on nonlocality in any world in which communication complexity is not trivial, Phys. Rev. Lett. 96 (2006) 250401.

[124] E. Chitambar, D. Leung, L. Mančinska, M. Ozols, A. Winter, Everything you always wanted to know about locc (but were afraid to ask), Commun. Math. Phys. 328 (1) (2014) 303–326.

[125] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, Capacities of quantum erasure channels, Phys. Rev. Lett. 78 (1997) 3217–3220.

[126] A. Gheorghiu, T. Kapourniotis, E. Kashefi, Verification of quantum computation: An overview of existing approaches, Theory of Computing Systems 63 (2019) 715–808.

[127] D.-S. Wang, A family of quantum von Neumann architecture, Chin. Phys. B 33 (2024) 080302.

[128] M. Horodecki, P. Shor, M. B. Ruskai, Entanglement breaking channels, Rev. Math. Phys. 15 (2003) 629–641.

[129] D. Rosset, F. Buscemi, Y.-C. Liang, Resource theory of quantum memories and their faithful verification with minimal assumptions, Phys. Rev. X 8 (2018) 021033.

[130] L. Li, M. J. W. Hall, H. M. Wiseman, Concepts of quantum non-markovianity: a hierarchy, Phys. Reports 759 (2018) 1–51.

[131] B. Eastin, E. Knill, Restrictions on transversal encoded quantum gate sets, Phys. Rev. Lett. 102 (2009) 110502.

[132] C. L. Degen, F. Reinhard, P. Cappellaro, Quantum sensing, Rev. Mod. Phys. 89 (2017) 035002.

[133] T. J. Yoder, R. Takagi, I. L. Chuang, Universal fault-tolerant gates on concatenated stabilizer codes, Phys. Rev. X 6 (2016) 031039.

[134] B. Zeng, X. Chen, D.-L. Zhou, X.-G. Wen, Quantum Information Meets Quantum Matter, Springer-Verlag New York, 2019.

[135] R. Koenig, G. Kuperberg, B. W. Reichardt, Quantum computation with Turaev–Viro codes, Ann. Phys. 325 (12) (2010) 2707–2749.

[136] B. J. Brown, D. Loss, J. K. Pachos, C. N. Self, J. R. Wootton, Quantum memories at finite temperature, Rev. Mod. Phys. 88 (2016) 045005.

[137] S. D. Sarma, M. Freedman, C. Nayak, Majorana zero modes and topological quantum computation, npj Quantum Information 1 (2015) 15001.

[138] F. Harper, R. Roy, M. S. Rudner, S. L. Sondhi, Topology and broken symmetry in floquet systems, Ann. Rev. Condensed Matter Phys. 11 (2020) 345.

[139] K. Khodjasteh, D. A. Lidar, Rigorous bounds on the performance of a hybrid dynamical-decoupling quantum-computing scheme, Phys. Rev. A 78 (2008) 012355.

[140] F. Verstraete, M. M. Wolf, J. I. Cirac, Quantum computation and quantum-state engineering driven by dissipation, Nat. Phys. 5 (9) (2009) 633–636.

[141] J. T. Anderson, G. Duclos-Cianci, D. Poulin, Fault-tolerant conversion between the steane and reed-muller quantum codes, Phys. Rev. Lett. 113 (2014) 080501.

[142] Y.-T. Liu, K. Wang, Y.-D. Liu, D.-S. Wang, A Survey of Universal Quantum von Neumann Architecture, Entropy 25 (8) (2023) 1187.

[143] M. Araujo, A. Feix, F. Costa, C. Brukner, Quantum circuits cannot control unknown operations, New J. Phys. 16 (2014) 093026.

[144] I. Bengtsson, K. Życzkowski, Geometry of Quantum States, Cambridge University Press, Cambridge U.K., 2006.

[145] K. Wang, D.-S. Wang, Quantum circuit simulation of superchannels, New J. Phys. 25 (4) (2023) 043013.

[146] C. H. Bennett, G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, (IEEE, New York), 1984, p. 175–179.

[147] J. Morris, V. Saggio, A. Gocanin, B. Dakic, Quantum verification and estimation with few copies, Adv. Quantum Technol. 5 (2022) 2100118.

[148] J. Wang, F. Sciarrino, A. Laing, M. G. Thompson, Integrated photonic quantum technologies, Nat. Photonics 14 (2020) 273–284.

[149] Editorial, 40 years of quantum computing, Nat. Rev. Phys. 4 (2022) 1.

[150] Y. Ma, Y. Z. Ma, Z. Q. Zhou, C.-F. Li, G.-C. Guo, One-hour coherent optical storage in an atomic frequency comb memory, Nat. Commun. 12 (2021) 2381.

[151] G. Chiribella, G. M. D'Ariano, P. Perinotti, Memory effects in quantum channel discrimination, Phys. Rev. Lett. 101 (2008) 180501.

[152] G. Gutoski, J. Watrous, Toward a general theory of quantum games, in: Proceedings of the 39th ACM Symposium on Theory of Computing, 2007, p. 565574.

[153] P. Mehta, M. Bukov, C.-H. Wang, A. G. R. Day, C. Richardson, C. K. Fisher, D. J. Schwab, A high-bias, low-variance introduction to machine learning for physicists, Phys. Reports 810 (2019) 1–124.

[154] D. Lim, J. F. Doriguello, P. Rebentrost, Quantum algorithm for robust optimization via stochastic-gradient online learning, arXiv:quant-ph/2304.02262 (2023).

[155] V. Dunjko, H. J. Briegel, Machine learning & artificial intelligence in the quantum domain: a review of recent progress, Rep. Prog. Phys. 81 (7) (2018) 074001.

[156] G. Verdon, J. Pye, M. Broughton, A universal training algorithm for quantum deep learning, arXiv:quant-ph/1806.09729 (2018).

[157] M. Benedetti, E. Lloyd, S. Sack, M. Fiorentini, Parameterized quantum circuits as machine learning models, Quantum Science and Technology 4 (4) (2019) 043001.

[158] H.-Y. Huang, R. Kueng, J. Preskill, Information-theoretic bounds on quantum advantage in machine learning, Phys. Rev. Lett. 126 (2021) 190505.

[159] M. C. Caro, Learning quantum processes and hamiltonians via the pauli transfer matrix, ACM Trans. Quantum Comput. 5 (2024) 2.

[160] R. Cleve, A. Ekert, C. Macchiavello, M. Mosca, Quantum algorithms revisited, Proc. R. Soc. (London), Ser. A 454 (1998) 339.

[161] R. Jozsa, N. Linden, On the Role of Entanglement in Quantum-Computational Speed-Up, Proc. R. Soc. (London), Ser. A 459 (2003) 2011.

[162] A. M. Steane, A quantum computer only needs one universe, Studies in History and Philosophy of Modern Physics 34 (3) (2003) 469–478.

[163] M. Van den Nest, Universal quantum computation with little entanglement, Phys. Rev. Lett. 110 (2013) 060504.

[164] M. Howard, J. Wallman, V. Veitch, J. Emerson, Contextuality supplies the 'magic' for quantum computation, Nature 510 (2014) 351.

[165] V. Giovannetti, L. Maccone, T. Morimae, T. G. Rudolph, Efficient universal blind quantum computation, Phys. Rev. Lett. 111 (2013) 230501.

[166] A. S. Holevo, Problems in the mathematical theory of quantum communication channels, Rep. Math. Phys. 12 (1977) 273.

[167] H. Tajima, N. Shiraishi, K. Saito, Uncertainty relations in implementation of unitary operations, Phys. Rev. Lett. 121 (2018) 110403.

[168] G. Chiribella, Y. Yang, R. Renner, Fundamental energy requirement of reversible quantum operations, Phys. Rev. X 11 (2021) 021014.

[169] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, S. Lloyd, Gaussian quantum information, Rev. Mod. Phys. 84 (2012) 621–669.

[170] K. Xu, H. Fan, Quantum simulation and quantum computation of noisy-intermediate scale, Chin. Phys. B 31 (10) (2022) 100304.

[171] J. Emerson, Y. S. Weinstein, M. Saraceno, S. Lloyd, D. G. Cory, Pseudo-random unitary operators for quantum information processing, Science 302 (2003) 2098–2100.

[172] D. Qin, X. Xu, Y. Li, An overview of quantum error mitigation formulas, Chin. Phys. B 31 (2022) 090306.

[173] G. Smith, J. Yard, Quantum communication with zero-capacity channels, Science 321 (2008) 1812.

[174] D. Sauerwein, N. R. Wallach, G. Gour, B. Kraus, Transformations among pure multipartite entangled states via local operations are almost never possible, Phys. Rev. X 8 (2018) 031020.

[175] Google Quantum AI and Collaborators, Quantum error correction below the surface code threshold, Naturehttps://doi.org/10.1038/s41586-024-08449-y (2024).