

Algebraic Probability Foundations of Quantum Computing

Notes on the Mathematical Model of Universal Digital Quantum Computers

Antonio Falcó Montesinos

Universidad CEU Cardenal Herrera (CEU-UCH)

Department of Mathematics, Physics and Technological Sciences

afalco@uchceu.es

November 21, 2025

Abstract

These notes present a mathematical formulation of digital quantum computing grounded on the theory of algebraic probability spaces. Starting from the finite-dimensional matrix algebra $M_N(\mathbb{C})$, we describe the representation of quantum states, observables, and measurements within the probabilistic framework of density operators. The construction of quantum processors and circuits is then formalized in terms of unitary dynamics and elementary embeddings of $U(2)$ into $U(N)$. This algebraic approach naturally leads to a universal dictionary of quantum gates and provides a unified language bridging operator algebras, probability theory, and quantum computation.

Acknowledges: We gratefully acknowledge the support and collaboration of the Regional Ministry of Innovation, Industry, Trade and Tourism of the Generalitat Valenciana, which made the development and dissemination of this educational material possible.



Contents

1	Introduction	4
	Historical Background and Motivation	5
2	Basic Notions of Algebraic Probability	7
2.1	Finite-Dimensional Example: The Matrix Algebra $M_N(\mathbb{C})$	8
2.2	$M_N(\mathbb{C})$ as a Tensor Product Space	9
2.3	Hilbert–Schmidt Norm and the Spectral Theorem	9
2.4	States and Density Matrices	10
2.5	Random Variables, Events, and Probability Laws	10

2.6	Partial Measurements and Marginals on Tensor Factors	11
2.7	Distances and Contractivity from Quantum to Classical Laws	12
3	An Algebraic Probability Framework for Universal Digital Quantum Computers	13
3.1	The Qubit as an Algebraic Probability Space	14
3.2	Composite Systems and Tensor Product Structure	14
3.3	Unitary Dynamics and Quantum Gates	15
3.4	Computations with and without Ancillas: Marginalization and Reduced States . . .	15
3.5	Measurement and Probability Laws	16
3.6	Quantum Probability and Measurement	17
3.7	Summary and Perspective	17
4	Elementary Quantum Gates and Quantum Circuits	17
4.1	Elementary Quantum Gates and Quantum Circuits	17
5	Quantum Algorithms	19
5.1	Definition and General Structure	20
5.2	Algorithms Without Ancillas	21
5.3	Algorithms With Ancillas and Marginals	21
5.4	Composition and Oracle Representation	22
5.5	Algebraic Classification of Quantum Algorithms	22
5.6	From Circuits to Probabilistic Output Laws	22
6	Quantum Annealing and Adiabatic Computation	23
6.1	Adiabatic Evolution in the Algebraic Setting	23
6.2	Definition of Quantum Annealing	23
6.3	Algebraic Probability Interpretation	24
6.4	Relation to Optimization and QUBO Models	24
6.5	Discretization and Circuit Implementation	25
6.6	Summary and Physical Interpretation	25
7	Quantum Complexity	25
7.1	Complexity Measures in the Algebraic Framework	25
7.2	Continuous and Energy-Based Complexity	26
7.3	Quantum Complexity Classes	26
7.4	Approximation and Precision Complexity	27
7.5	Complexity of Quantum Annealing	27
7.6	Entropy and Information Complexity	27
7.7	Summary and Perspectives	28
8	Quantum Information Geometry	28
8.1	Differential Structure on the State Space	28
8.2	Monotone Riemannian Metrics	28
8.3	Geometric Interpretation of Complexity	29
8.4	Information Geometry and Statistical Distinguishability	29
8.5	Curvature and Quantum Speed Limits	29
8.6	Entropy, Divergences, and Dual Geometry	30
8.7	Summary and Outlook	30

9	Foundations and Open Problems	30
9.1	Summary of the Conceptual Structure	30
9.2	Foundational Questions	31
9.3	Mathematical and Physical Directions	32
9.4	Outlook	32
	Epilogue	33
	Bibliographical Note	33
A	Proofs of Results from Section 3.6	35

1 Introduction

Quantum computing can be understood as a principled extension of classical computation that emerges when *probability theory* is lifted from a commutative to a non-commutative (algebraic) setting. In the classical paradigm, a probability space (Ω, \mathcal{F}, P) encodes randomness on a set of outcomes, and random variables are real-valued measurable functions. By contrast, the quantum paradigm models observables as self-adjoint elements of a complex $*$ -algebra acting on a Hilbert space, and the probabilistic state of a system as a positive, normalized linear functional on that algebra. This perspective—formalized by *algebraic probability*—places quantum mechanics on the same conceptual footing as measure-theoretic probability while accommodating the essential feature of *non-commutativity*. We review the basic notions in Section 2.

In finite dimensions, the algebra of interest is the full matrix algebra $\mathbb{M}_N(\mathbb{C})$. A *state* is represented by a *density matrix* $\rho \in \mathbb{M}_N(\mathbb{C})$: a Hermitian, positive semidefinite operator with $\text{tr}(\rho) = 1$. Observables are Hermitian matrices $A \in \mathbb{M}_N(\mathbb{C})$, and their expected values in the state ρ are given by the linear functional

$$\mathbb{E}_\rho[A] = \varphi_\rho(A) = \text{tr}(\rho A).$$

Pure states correspond to rank-one projectors $\rho = |\Psi\rangle\langle\Psi|$, while mixed states describe convex combinations of pure states. This algebraic formalism already contains the two pillars needed for digital quantum computation: (i) reversible, norm- and trace-preserving evolution via unitary conjugation; and (ii) measurement as a projection that induces a classical probability law on a chosen basis.

Within this framework we model an n -qubit *quantum processing unit* (QPU) by the algebraic probability space $(\mathbb{M}_{2^n}(\mathbb{C}), \rho)$, where the computational Hilbert space is \mathbb{C}^{2^n} with orthonormal (computational) basis $\{|\mathbf{x}\rangle : \mathbf{x} \in \{0, 1\}^n\}$. Digital quantum dynamics are implemented by the unitary action

$$\rho \longmapsto U\rho U^*, \quad U \in \text{U}(2^n),$$

which preserves positivity, Hermiticity, and trace, and thus remains within the state manifold. A *quantum circuit* is a finite product of *elementary quantum gates* (local unitaries acting on one or a few qubits). As shown in Section 3, any $U \in \text{U}(2^n)$ may be realized as a finite sequence of such elementary operations, so that “algorithms” correspond precisely to unitary transformations generated by a gate dictionary.

Measurement turns quantum states into classical data. If ρ is a density matrix on \mathbb{C}^{2^n} , the probability of observing the computational basis outcome $\mathbf{w} \in \{0, 1\}^n$ is given by the Born rule

$$\mathbb{P}_\rho(\mathbf{w}) = \text{Tr}(\rho |\mathbf{w}\rangle\langle\mathbf{w}|),$$

which defines a probability distribution on $\{0, 1\}^n$. For pure states $\rho = |\psi\rangle\langle\psi|$, this reduces to $|\langle\mathbf{w}|\psi\rangle|^2$. When the Hilbert space decomposes as a tensor product $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$, partial measurements on a register are handled by the *partial trace*: the reduced state $\rho^{(1)} = \text{Tr}_{\mathcal{H}_2}(\rho)$ induces the marginal law on \mathcal{H}_1 . We formalize these constructions and their consequences in Section 3.6.

The algebraic viewpoint also yields a clean interface between quantum geometry and statistical distinguishability. At the level of states, the natural metric is the *trace distance* $D_{\text{tr}}(\rho, \sigma) = \frac{1}{2}\|\rho - \sigma\|_1$, which is unitarily invariant and contracts under completely positive trace-preserving

(CPTP) maps such as partial trace and pinching (diagonal projection). At the classical level, measurement outcomes are compared via the *statistical (total variation) distance* SD. A key hierarchy (Proposition 2.13) shows that partial measurement cannot increase distinguishability:

$$\text{SD}(\mathbb{P}_\rho^{(1)}, \mathbb{P}_\sigma^{(1)}) \leq D_{\text{tr}}(\rho, \sigma),$$

with a pure-state specialization $D_{\text{tr}}(|\psi\rangle\langle\psi|, |\phi\rangle\langle\phi|) = \sqrt{1 - |\langle\psi|\phi\rangle|^2}$. This bridge allows inner-product and operator-norm estimates to translate directly into statements about classical measurement statistics—an essential mechanism for algorithmic analysis and indistinguishability guarantees later in the paper.

Historical Background and Motivation

The theory of quantum computation stands at the intersection of physics, mathematics, and information theory. Its historical roots extend back to the early twentieth century, when the formal structure of quantum mechanics was itself being established. The mathematical architecture introduced by von Neumann between 1927 and 1932 provided the first unified language for quantum theory: states were represented by density operators on a Hilbert space, observables by self-adjoint operators, and physical expectations by the trace pairing

$$\varphi(A) = \text{Tr}(\rho A),$$

a formula that already exhibits the duality between algebra and probability at the heart of modern quantum information theory. The same structure underlies the concept of an *algebraic probability space* (\mathcal{A}, φ) , where \mathcal{A} is a C^* - or von Neumann algebra and φ a positive normalized linear functional. This noncommutative generalization of measure theory was developed through the works of Segal, Kadison, and others, and it would later become the cornerstone of the operator algebraic approach to quantum physics.

Parallel to these developments, Kolmogorov’s *Grundbegriffe der Wahrscheinlichkeitsrechnung* (1933) formalized classical probability as measure theory on σ -algebras. The analogy between the integration theory of Kolmogorov and the trace formalism of von Neumann has long suggested that quantum mechanics could be viewed as an extension of probability theory to noncommuting variables. This idea matured with the works of Accardi, Meyer, and Parthasarathy, who formulated the theory of *quantum probability* and *quantum stochastic calculus*. Their goal was not merely interpretational but structural: to treat quantum systems as genuine probabilistic objects within the framework of operator algebras.

The birth of quantum computation in the 1980s reopened this line of thought from a new perspective. In 1981, Richard Feynman observed that simulating quantum systems by classical computers appeared to require exponential resources, and he proposed using quantum mechanical systems themselves to perform computation. In 1985, David Deutsch formulated the notion of a *universal quantum Turing machine*, emphasizing the computational universality of unitary dynamics. The first concrete algorithms exhibiting quantum advantage—Shor’s integer factoring (1994) and Grover’s database search (1996)—demonstrated that quantum computation is not only a physical curiosity but a new computational paradigm.

In parallel, the work of Bennett, Schumacher, and Holevo established the foundations of *quantum information theory*. Concepts such as quantum entropy, mutual information, and channel capacity revealed that quantum mechanics admits a fully developed theory of information processing—one that extends and refines the Shannon–Kolmogorov framework. Within this context, the

unitary group $U(N)$ became the natural stage for quantum computation, and density operators in $\mathbb{M}_N(\mathbb{C})$ represented quantum probability distributions.

From a mathematical standpoint, the turn of the twenty-first century brought a synthesis between geometry, information, and computation. Nielsen’s *geometric approach to quantum circuit complexity* (2006) introduced a Riemannian viewpoint on the manifold of unitary operators, interpreting minimal quantum circuits as geodesics. Simultaneously, quantum information geometry—pioneered by Petz, Amari, and Nagaoka—provided a rich differential framework to measure distinguishability between states through monotone metrics such as the Bures or BKM metrics. These two perspectives, algorithmic and statistical, share a common structure: both define metrics on spaces of operators that encode informational or computational cost.

The present notes aim to integrate these strands into a single formal framework. The guiding principle is that the space of quantum states and operations should be viewed as an *algebraic probability space* endowed with natural geometric and metric structures. Within this setting:

- quantum gates are embeddings of $U(2)$ into $U(N)$, forming a dictionary of elementary transformations;
- quantum algorithms correspond to morphisms acting on states in $\mathbb{M}_N(\mathbb{C})$, possibly extended by ancillary systems;
- quantum annealing and adiabatic computation represent continuous flows generated by self-adjoint elements of \mathcal{A} ;
- and quantum complexity emerges as a metric property of $U(N)$, measured either discretely (through circuit length) or continuously (through geometric action and energy).

Thus, the algebraic approach unifies the discrete, continuous, and probabilistic aspects of quantum computation in a single mathematical language.

Historically, one may trace a conceptual trajectory:

Kolmogorov (1933) \longrightarrow von Neumann (1932) \longrightarrow Accardi–Meyer–Parthasarathy (1970–1990)
 \longrightarrow Deutsch–Feynman–Shor–Grover (1980–1996) \longrightarrow Nielsen–Petz–Amari (1996–2006).

Each stage added a layer: measure theory, operator algebra, probability in noncommutative spaces, algorithmic universality, and geometric structure. The present work continues this evolution by proposing that the algebraic probabilistic framework is not only adequate to describe quantum computation but also essential to understand its complexity and limits.

Finally, these notes are written in the spirit of constructive mathematics. They are motivated not solely by the abstract pursuit of generality but by the goal of building a bridge between rigorous algebraic foundations and practical realizations of quantum algorithms on real hardware. The formulation adopted here is designed to accommodate both finite-dimensional implementations—such as superconducting, photonic, or NMR-based quantum processors—and the theoretical extension to infinite-dimensional, continuous, or hybrid systems. In this sense, the algebraic probability model provides a conceptual continuum between the mathematical structure of quantum theory and the engineering of quantum devices.

*From measure to operator, from probability to geometry, from geometry to computation:
the history of quantum theory is also the history of its mathematization.*

It is within this long intellectual trajectory that the present notes are situated. They attempt to show that the language of algebraic probability—once regarded as a technical refinement of measure theory—may in fact contain the general grammar of quantum computation itself.

Contributions and roadmap. Section 2 develops the finite-dimensional algebraic probability formalism on $\mathbb{M}_N(\mathbb{C})$, including density matrices, spectral decomposition, and the interpretation of events and laws via projectors. Section 3 introduces a mathematical model of a universal digital quantum computer: n -qubit QPUs, unitary evolution as a discrete dynamical system on the state manifold, and a gate-based view of quantum circuits as products of elementary embeddings of $U(2)$ into $U(2^n)$. Section 3.6 provides the probabilistic toolkit: quantum probability distributions, partial measurement via partial trace, and a hierarchy linking trace distance to statistical distance under measurement. Together, these elements yield a unified, algebraically grounded introduction to quantum computing that connects operator-theoretic structure with computational practice.

2 Basic Notions of Algebraic Probability

This section introduces the fundamental notions and results in algebraic probability theory in a finite-dimensional setting, which will form the mathematical foundation of our quantum computational model developed in Section 3.

Classical probability theory is traditionally formulated in terms of measure spaces. A *classical probability space* is defined as a triple (Ω, \mathcal{F}, P) , where:

- Ω is the *sample space*, representing all possible outcomes of a stochastic experiment.
- $\mathcal{F} \subseteq 2^\Omega$ is a σ -algebra of measurable subsets (events).
- $P : \mathcal{F} \rightarrow [0, 1]$ is a *probability measure* assigning probabilities to events.

A random variable $X : (\Omega, \mathcal{F}, P) \rightarrow (\mathbb{R}, \mathcal{B}(\mathbb{R}))$ induces a probability measure P_X on \mathbb{R} , given by:

$$P_X(B) = P(X^{-1}(B)), \quad B \in \mathcal{B}(\mathbb{R}). \quad (2.1)$$

This measure is called the *distribution* (or *law*) of X . For random vectors (X_1, \dots, X_n) , the joint distribution is defined analogously.

However, in quantum mechanics, observables cannot generally be represented as commuting functions. Instead, they are modeled by self-adjoint operators on a complex Hilbert space. This non-commutativity implies that not all observables can be simultaneously measured with arbitrary precision, a structural feature that cannot be captured by classical measure theory. To address this limitation, one replaces measurable functions by algebraic observables and probability measures by *states* on algebras of operators. The result is the framework of *algebraic probability theory*, which unifies classical and quantum probability in a common algebraic setting.

Definition 2.1. An algebraic probability space (or quantum probability space) is a pair (\mathcal{A}, φ) , where:

- \mathcal{A} is a unital associative $*$ -algebra over \mathbb{C} ;
- $\varphi : \mathcal{A} \rightarrow \mathbb{C}$ is a state, i.e. a linear functional satisfying:
 1. Linearity: $\varphi(\lambda a + \mu b) = \lambda \varphi(a) + \mu \varphi(b)$ for all $a, b \in \mathcal{A}$ and $\lambda, \mu \in \mathbb{C}$;

2. Positivity: $\varphi(a^*a) \geq 0$ for all $a \in \mathcal{A}$;
3. Normalization: $\varphi(\mathbb{I}) = 1$, where \mathbb{I} is the unit of \mathcal{A} .

In this setting, a *quantum random variable* is any self-adjoint element $X \in \mathcal{A}$, and the state φ provides an expectation value

$$\mathbb{E}[X] = \varphi(X), \quad (2.2)$$

generalizing the classical notion of expectation.

A classical probability space (Ω, \mathcal{F}, P) can be embedded into this framework by taking:

- $\mathcal{A} = L^\infty(\Omega, \mathcal{F}, P)$, the algebra of bounded measurable functions;
- $f^*(\omega) = \overline{f(\omega)}$ (pointwise conjugation);
- $\varphi(f) = \int_\Omega f(\omega) dP(\omega)$.

Hence, classical probability corresponds to the commutative case of algebraic probability.

2.1 Finite-Dimensional Example: The Matrix Algebra $\mathbb{M}_N(\mathbb{C})$

Let $N \in \mathbb{N}$ and consider the finite-dimensional Hilbert space $\mathbb{H}_N := \mathbb{C}^N$. Vectors are expressed in Dirac notation:

$$|\Psi\rangle = \begin{bmatrix} \Psi_1 \\ \vdots \\ \Psi_N \end{bmatrix}, \quad \langle\Psi| = [\overline{\Psi_1} \quad \cdots \quad \overline{\Psi_N}].$$

The inner product is

$$\langle\Psi| \Phi\rangle = \sum_{i=1}^N \overline{\Psi_i} \Phi_i, \quad \|\Psi\| = \sqrt{\langle\Psi| \Psi\rangle}.$$

The outer product $|\Psi\rangle \langle\Phi|$ defines a matrix in $\mathbb{M}_N(\mathbb{C})$, and the algebra of all such matrices forms a non-commutative $*$ -algebra under the adjoint operation $A \mapsto A^*$.

The subsequent subsections develop:

- the tensor representation $\mathbb{M}_N(\mathbb{C}) \simeq \mathbb{H}_N \widehat{\otimes} \mathbb{H}_N^*$;
- the Hilbert–Schmidt norm and the spectral theorem;
- the characterization of *states* as density matrices;
- the definition of random variables, events, and probability laws in this algebraic context.

These constructions will allow us to reinterpret finite-dimensional quantum mechanics as a special case of algebraic probability and will provide the algebraic groundwork for the mathematical model of quantum computers developed in Section 3.

2.2 $\mathbb{M}_N(\mathbb{C})$ as a Tensor Product Space

In quantum mechanics, the algebra of complex $N \times N$ matrices $\mathbb{M}_N(\mathbb{C})$ can be realized as the tensor product of the Hilbert space \mathbb{H}_N with its dual:

$$\mathbb{M}_N(\mathbb{C}) \simeq \mathbb{H}_N \hat{\otimes} \mathbb{H}_N^*,$$

where $\hat{\otimes}$ denotes the algebraic tensor product. Given two vectors $|\Psi\rangle, |\Phi\rangle \in \mathbb{H}_N$, the rank-one matrix $|\Psi\rangle\langle\Phi|$ corresponds to the simple tensor $|\Psi\rangle \hat{\otimes} \langle\Phi|$. Explicitly,

$$|\Psi\rangle\langle\Phi| = \begin{bmatrix} \Psi_1 \\ \vdots \\ \Psi_N \end{bmatrix} \begin{bmatrix} \overline{\Phi_1} & \cdots & \overline{\Phi_N} \end{bmatrix} = (\Psi_i \overline{\Phi_j})_{i,j=1}^N.$$

The set of all rank-one matrices $\{|\Psi\rangle\langle\Phi|\}$ spans the entire algebra $\mathbb{M}_N(\mathbb{C})$. If $\{|e_1\rangle, \dots, |e_N\rangle\}$ is an orthonormal basis of \mathbb{H}_N , then $\{|e_i\rangle\langle e_j|\}_{i,j}$ forms an orthonormal basis of $\mathbb{M}_N(\mathbb{C})$ under the Hilbert–Schmidt inner product defined below.

The canonical trace functional $\text{tr} : \mathbb{M}_N(\mathbb{C}) \rightarrow \mathbb{C}$ is given by

$$\text{tr}(A) = \sum_{j=1}^N \langle e_j | A | e_j \rangle,$$

and satisfies the fundamental identity

$$\text{tr}(|\Psi\rangle\langle\Phi|) = \langle\Phi|\Psi\rangle. \quad (2.3)$$

Equation (2.3) establishes the link between inner products in \mathbb{H}_N and traces in the operator algebra $\mathbb{M}_N(\mathbb{C})$.

2.3 Hilbert–Schmidt Norm and the Spectral Theorem

Given $A, B \in \mathbb{M}_N(\mathbb{C})$, the *Hilbert–Schmidt inner product* is defined as

$$(A, B)_{HS} := \text{tr}(A^* B),$$

with associated norm

$$\|A\|_{HS} := \sqrt{\text{tr}(A^* A)}.$$

This makes $(\mathbb{M}_N(\mathbb{C}), \|\cdot\|_{HS})$ a finite-dimensional Hilbert space. The adjoint A^* is the conjugate transpose of A . A matrix A is *Hermitian* (or self-adjoint) if $A = A^*$.

By the *spectral theorem*, every Hermitian matrix $A \in \mathbb{M}_N(\mathbb{C})$ admits a decomposition

$$A = U D U^* = \sum_{i=1}^N \lambda_i |u_i\rangle\langle u_i|, \quad (2.4)$$

where $U \in \text{U}(N)$ is unitary, $\lambda_1, \dots, \lambda_N \in \mathbb{R}$ are the eigenvalues of A , and $\{|u_i\rangle\}$ is an orthonormal eigenbasis. The projectors $|u_i\rangle\langle u_i|$ are mutually orthogonal and satisfy $\sum_i |u_i\rangle\langle u_i| = \mathbb{I}_N$.

Equation (2.4) provides the foundation for defining events and probabilities associated with observables in the algebraic setting. Each eigenvalue corresponds to a measurable outcome, and its projector plays the role of an event indicator.

2.4 States and Density Matrices

A *state* on $\mathbb{M}_N(\mathbb{C})$ is a positive linear functional $\varphi : \mathbb{M}_N(\mathbb{C}) \rightarrow \mathbb{C}$ with $\varphi(\mathbb{I}_N) = 1$. Every such state can be represented uniquely by a density matrix ρ .

Theorem 2.2 (Density matrix representation). *For any state φ on $\mathbb{M}_N(\mathbb{C})$, there exists a unique $\rho \in \mathbb{M}_N(\mathbb{C})$ such that*

$$\varphi(A) = \text{tr}(\rho A), \quad A \in \mathbb{M}_N(\mathbb{C}), \quad (2.5)$$

and ρ satisfies:

1. $\rho = \rho^*$ (Hermitian),
2. $\rho \succeq 0$ (positive semidefinite),
3. $\text{tr}(\rho) = 1$.

The matrix ρ is called the *density matrix* of the state φ . The set of all density matrices forms a compact convex subset

$$\mathcal{S}(\mathbb{M}_N(\mathbb{C})) := \{\rho \in \mathbb{M}_N(\mathbb{C}) : \rho \succeq 0, \text{tr}(\rho) = 1\}.$$

Its extremal points correspond to *pure states*,

$$\mathcal{S}_1(\mathbb{M}_N(\mathbb{C})) = \{|\Psi\rangle \langle \Psi| : |\Psi\rangle \in \mathbb{H}_N, \|\Psi\| = 1\},$$

while convex combinations of pure states describe *mixed states*.

2.5 Random Variables, Events, and Probability Laws

In the algebraic framework, observables are Hermitian elements of the algebra, and their spectral decomposition defines the possible outcomes and their associated probabilities.

Definition 2.3 (Quantum random variable). *A random variable in the algebraic probability space $(\mathbb{M}_N(\mathbb{C}), \rho)$ is a Hermitian matrix $A = A^* \in \mathbb{M}_N(\mathbb{C})$.*

Let A admit the spectral decomposition (2.4). Each eigenvalue $\lambda \in \sigma(A)$ corresponds to the event $\{A = \lambda\}$ represented by the projector

$$P_{\{A=\lambda\}} = \sum_{|u_i\rangle \in \ker(A - \lambda \mathbb{I}_N)} |u_i\rangle \langle u_i|.$$

The collection of projectors $\{P_{\{A=\lambda\}}\}_{\lambda \in \sigma(A)}$ satisfies

$$P_{\{A=\lambda\}} P_{\{A=\mu\}} = \delta_{\lambda,\mu} P_{\{A=\lambda\}}, \quad \sum_{\lambda \in \sigma(A)} P_{\{A=\lambda\}} = \mathbb{I}_N,$$

analogous to the disjointness and completeness of classical events.

Definition 2.4 (Law of a random variable). *Let $(\mathbb{M}_N(\mathbb{C}), \rho)$ be an algebraic probability space and $A = A^*$ a random variable. The law of A is the probability distribution on $\sigma(A) \subset \mathbb{R}$ defined by*

$$\mathbb{P}_\rho(A = \lambda) := \text{tr}(\rho P_{\{A=\lambda\}}), \quad \lambda \in \sigma(A),$$

which satisfies $\sum_{\lambda \in \sigma(A)} \mathbb{P}_\rho(A = \lambda) = 1$.

In the special case of a pure state $\rho = |\Psi\rangle\langle\Psi|$, this becomes

$$\mathbb{P}_{|\Psi\rangle}(A = \lambda) = \langle\Psi| P_{\{A=\lambda\}} |\Psi\rangle = \sum_{|u_i\rangle \in \ker(A - \lambda I_N)} |\langle u_i | \Psi \rangle|^2.$$

Hence, the probability of observing the outcome λ is the total squared overlap between the state $|\Psi\rangle$ and the eigenspace corresponding to λ .

Example 2.5 (Bernoulli observable). *Let $\rho = |\Psi\rangle\langle\Psi|$ be a pure state in \mathbb{H}_N , and let $A = |u\rangle\langle u|$ be a rank-one Hermitian projector. Then $\sigma(A) = \{0, 1\}$ and*

$$\mathbb{P}_\rho(A = 1) = |\langle\Psi| u\rangle|^2, \quad \mathbb{P}_\rho(A = 0) = 1 - |\langle\Psi| u\rangle|^2.$$

Thus, a projective measurement corresponds to a Bernoulli random variable whose success probability is the squared inner product between the state and the measurement vector.

The above definitions complete the correspondence between classical and quantum probability. States (measures) are represented by density matrices, observables (random variables) by Hermitian matrices, and events by orthogonal project

2.6 Partial Measurements and Marginals on Tensor Factors

When the Hilbert space of a quantum system decomposes as a tensor product $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$, it is often necessary to compute probabilities associated with measurements on only one factor (say, \mathcal{H}_1). In this setting, the relevant probability law is obtained by taking the *marginal distribution* of the full state with respect to \mathcal{H}_1 . Mathematically, this corresponds to forming the reduced density operator on \mathcal{H}_1 via the partial trace over \mathcal{H}_2 , and then applying the general definition of quantum probability to this reduced state.

Definition 2.6 (Partial measurement on a register). *Let $|\psi\rangle \in \mathbb{C}^{2^{n+m}}$ be a pure state on two registers, with Hilbert space decomposition $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$, where $\mathcal{H}_1 \cong \mathbb{C}^{2^n}$ (first register) and $\mathcal{H}_2 \cong \mathbb{C}^{2^m}$ (second register). Writing*

$$|\psi\rangle = \sum_{\mathbf{x} \in \mathbb{Z}_2^n} \sum_{\mathbf{y} \in \mathbb{Z}_2^m} \alpha_{\mathbf{x}, \mathbf{y}} |\mathbf{x}\rangle \otimes |\mathbf{y}\rangle,$$

the associated density operator is $\rho = |\psi\rangle\langle\psi|$. The reduced density operator on the first register is obtained by tracing out \mathcal{H}_2 :

$$\rho^{(1)} := \text{Tr}_{\mathcal{H}_2}(\rho) = \sum_{\mathbf{x}, \mathbf{x}' \in \mathbb{Z}_2^n} \left(\sum_{\mathbf{y} \in \mathbb{Z}_2^m} \alpha_{\mathbf{x}, \mathbf{y}} \overline{\alpha_{\mathbf{x}', \mathbf{y}}} \right) |\mathbf{x}\rangle\langle\mathbf{x}'|.$$

For any $\mathbf{x} \in \mathbb{Z}_2^n$, the probability of observing \mathbf{x} when measuring only the first register in the computational basis is

$$\mathbb{P}_{|\psi\rangle}^{(1)}(\mathbf{x}) = \langle\mathbf{x}| \rho^{(1)} |\mathbf{x}\rangle = \sum_{\mathbf{y} \in \mathbb{Z}_2^m} |\alpha_{\mathbf{x}, \mathbf{y}}|^2.$$

Example 2.7 (Partial measurement on a two-qubit system). *Consider*

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \in \mathbb{C}^2 \otimes \mathbb{C}^2,$$

which is maximally entangled, with density $\rho = |\psi\rangle\langle\psi|$. Tracing out the second register yields

$$\rho^{(1)} = \text{Tr}_2(\rho) = \frac{1}{2} |0\rangle\langle 0| + \frac{1}{2} |1\rangle\langle 1|.$$

Hence, $\mathbb{P}_{|\psi\rangle}^{(1)}(0) = \mathbb{P}_{|\psi\rangle}^{(1)}(1) = \frac{1}{2}$. Although $|\psi\rangle$ is pure, the reduced state on the first register is mixed.

2.7 Distances and Contractivity from Quantum to Classical Laws

To compare quantum states quantitatively, we require a notion of distance on density operators that extends the overlap of pure states and behaves well under partial trace and measurement. The natural candidate is the *trace distance*, the quantum analogue of the L^1 metric. Measurement outcomes are classical distributions, compared via the *statistical (total variation) distance*.

Definition 2.8 (Trace distance between quantum states). *Let ρ, σ be density operators on a Hilbert space \mathcal{H} . The trace distance is*

$$D_{\text{tr}}(\rho, \sigma) := \frac{1}{2} \|\rho - \sigma\|_1,$$

where $\|A\|_1 = \text{Tr} \sqrt{A^\dagger A}$. For pure states $\rho = |\psi\rangle\langle\psi|$ and $\sigma = |\phi\rangle\langle\phi|$,

$$D_{\text{tr}}(|\psi\rangle\langle\psi|, |\phi\rangle\langle\phi|) = \sqrt{1 - |\langle\psi|\phi\rangle|^2}.$$

Definition 2.9 (Statistical distance). *For probability measures $\mathbb{P}_1, \mathbb{P}_2$ on a finite set Ω , the statistical (total variation) distance is*

$$\text{SD}(\mathbb{P}_1, \mathbb{P}_2) = \frac{1}{2} \sum_{\mathbf{w} \in \Omega} |\mathbb{P}_1(\mathbf{w}) - \mathbb{P}_2(\mathbf{w})|.$$

It obeys non-negativity, identity of indiscernibles, and the triangle inequality

$$\text{SD}(\mathbb{P}_1, \mathbb{P}_3) \leq \text{SD}(\mathbb{P}_1, \mathbb{P}_2) + \text{SD}(\mathbb{P}_2, \mathbb{P}_3). \quad (2.6)$$

Definition 2.10 (Negligible function). *A function $f : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}_{\geq 0}$ is negligible if for every $d > 0$ there exists λ_0 such that $f(\lambda) < \lambda^{-d}$ for all $\lambda \geq \lambda_0$. Two distributions are statistically indistinguishable if their SD is negligible.*

We record two basic contractivity properties for the trace norm that we will use to pass from quantum distances to distances between classical marginals. Detailed proofs are given in Appendix A.

Lemma 2.11 (Partial trace is contractive in trace norm). *Let $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ and $\text{Tr}_{\mathcal{H}_2} : \mathcal{B}(\mathcal{H}) \rightarrow \mathcal{B}(\mathcal{H}_1)$ be the partial trace. Then for every $X \in \mathcal{B}(\mathcal{H})$,*

$$\|\text{Tr}_{\mathcal{H}_2}(X)\|_1 \leq \|X\|_1.$$

Lemma 2.12 (Pinching/diagonal projection is contractive). *Let $\{\Pi_i\}_{i=1}^r$ be mutually orthogonal projections on \mathcal{H} with $\sum_{i=1}^r \Pi_i = I$. Define $\text{Diag}(Y) := \sum_{i=1}^r \Pi_i Y \Pi_i$. Then for all Y ,*

$$\|\text{Diag}(Y)\|_1 \leq \|Y\|_1.$$

These facts yield a hierarchy linking quantum distinguishability (trace distance) to classical distinguishability (statistical distance) after partial measurement.

Proposition 2.13 (Matrix-analytic hierarchy of distances). *Let $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ with $\mathcal{H}_1 \cong \mathbb{C}^{2^n}$, and let $\{\Pi_{\mathbf{x}}\}_{\mathbf{x} \in \mathbb{Z}_2^n}$ be the rank-one projectors onto the computational basis of \mathcal{H}_1 . For density operators ρ, σ on \mathcal{H} define the classical distributions on \mathbb{Z}_2^n by*

$$\mathbb{P}_{\rho}^{(1)}(\mathbf{x}) := \text{Tr}((\Pi_{\mathbf{x}} \otimes I) \rho) = \langle \mathbf{x} | \text{Tr}_{\mathcal{H}_2}(\rho) | \mathbf{x} \rangle, \quad \mathbb{P}_{\sigma}^{(1)}(\mathbf{x}) := \text{Tr}((\Pi_{\mathbf{x}} \otimes I) \sigma).$$

Then:

(i) **Unitary invariance:** $D_{\text{tr}}(U\rho U^\dagger, U\sigma U^\dagger) = D_{\text{tr}}(\rho, \sigma)$ for every unitary U on \mathcal{H} .

(ii) **Partial measurement is contractive:**

$$\text{SD}(\mathbb{P}_\rho^{(1)}, \mathbb{P}_\sigma^{(1)}) = \frac{1}{2} \|\text{Diag}(\text{Tr}_{\mathcal{H}_2}(\rho - \sigma))\|_1 \leq \frac{1}{2} \|\text{Tr}_{\mathcal{H}_2}(\rho - \sigma)\|_1 \leq D_{\text{tr}}(\rho, \sigma).$$

(iii) **Pure-state specialization:** If $\rho = |\psi\rangle\langle\psi|$ and $\sigma = |\phi\rangle\langle\phi|$, then

$$\text{SD}(\mathbb{P}_{|\psi\rangle}^{(1)}, \mathbb{P}_{|\phi\rangle}^{(1)}) \leq D_{\text{tr}}(|\psi\rangle, |\phi\rangle) = \sqrt{1 - |\langle\psi|\phi\rangle|^2}.$$

Remark 2.14 (Basis independence). *The same statement holds for any orthonormal basis on \mathcal{H}_1 , i.e., replacing $\{\Pi_{\mathbf{x}}\}$ by $\{U\Pi_{\mathbf{x}}U^\dagger\}$ for any unitary U on \mathcal{H}_1 , since Lemma 2.12 applies to any family of pairwise orthogonal projections.*

The hierarchy in Proposition 2.13 is a key bridge we will use throughout the paper: inner-product and operator-norm bounds at the quantum level translate directly into quantitative guarantees on the statistical indistinguishability of measurement outcomes. This will be crucial in the algorithmic analyses of Sections 3 and 3.6.

Transition to the computational model. The algebraic probability framework developed above provides a rigorous bridge between classical measure-theoretic probability and the operator formalism of quantum mechanics. In this setting, every finite-dimensional quantum system is described by an algebra of observables $\mathbb{M}_N(\mathbb{C})$ and a state ρ encoding the probabilistic structure of measurement outcomes. The dynamics of such systems arise from unitary transformations that preserve the algebraic and probabilistic structure of the pair $(\mathbb{M}_N(\mathbb{C}), \rho)$.

Section 3 builds upon this foundation to construct a formal mathematical model of a *universal digital quantum computer*. In that model, qubits are represented as elementary algebraic probability spaces of dimension two, and the global quantum processor is obtained as a tensor product of these elementary subsystems. Quantum logic gates are described as unitary operators acting on tensor factors, while measurement operations are represented by orthogonal projections. The resulting formulation connects the algebraic theory of states and observables with the algorithmic concepts of circuits, gates, and computational universality.

3 An Algebraic Probability Framework for Universal Digital Quantum Computers

In this section we formalize the structure of a digital quantum computer within the algebraic probability framework established in Section 2. The guiding principle is that computation can be viewed as a discrete dynamical process acting on the space of states $(\mathbb{M}_N(\mathbb{C}), \rho)$, where $N = 2^n$ for a system of n qubits. The elementary components of such a device are the qubit, the tensor-product structure of its composite state space, the unitary evolution (quantum gates), and the measurement mechanism that yields classical information.

3.1 The Qubit as an Algebraic Probability Space

A single qubit is the simplest non-trivial quantum system, modeled by the algebraic probability space

$$(\mathbb{M}_2(\mathbb{C}), \rho),$$

where ρ is a density matrix acting on the Hilbert space $\mathbb{H}_2 = \mathbb{C}^2$ with orthonormal (computational) basis $\{|0\rangle, |1\rangle\}$. Pure qubit states are vectors of the form

$$|\Psi\rangle = \alpha |0\rangle + \beta |1\rangle, \quad \alpha, \beta \in \mathbb{C}, \quad |\alpha|^2 + |\beta|^2 = 1,$$

and their density matrices are $\rho = |\Psi\rangle\langle\Psi|$. Mixed qubit states are convex combinations of pure ones,

$$\rho = p |\Psi_1\rangle\langle\Psi_1| + (1-p) |\Psi_2\rangle\langle\Psi_2|, \quad 0 \leq p \leq 1.$$

Every Hermitian matrix $A \in \mathbb{M}_2(\mathbb{C})$ can be written as a linear combination of the Pauli matrices

$$\sigma_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

so that

$$A = a_0 \sigma_0 + a_x \sigma_x + a_y \sigma_y + a_z \sigma_z, \quad a_\mu \in \mathbb{R}.$$

Consequently, any state ρ admits the Bloch representation

$$\rho = \frac{1}{2}(\sigma_0 + \mathbf{r} \cdot \boldsymbol{\sigma}), \quad \mathbf{r} \in \mathbb{R}^3, \quad \|\mathbf{r}\| \leq 1, \quad (3.1)$$

where $\boldsymbol{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$. The vector \mathbf{r} is the *Bloch vector* of the state: $|\mathbf{r}| = 1$ corresponds to pure states (points on the Bloch sphere), while $|\mathbf{r}| < 1$ corresponds to mixed states.

3.2 Composite Systems and Tensor Product Structure

A register of n qubits is described by the tensor-product Hilbert space

$$\mathbb{H}_{2^n} = \underbrace{\mathbb{H}_2 \otimes \cdots \otimes \mathbb{H}_2}_{n \text{ times}},$$

of dimension 2^n . The algebra of observables is $\mathbb{M}_{2^n}(\mathbb{C}) \simeq \mathbb{M}_2(\mathbb{C})^{\otimes n}$. States on the composite system are density matrices $\rho \in \mathbb{M}_{2^n}(\mathbb{C})$ satisfying $\rho \succeq 0$ and $\text{tr}(\rho) = 1$.

Given subsystems A and B , the reduced state of A is obtained by the *partial trace*:

$$\rho_A = \text{Tr}_B(\rho_{AB}),$$

which preserves positivity and normalization. Entangled states are precisely those ρ_{AB} that cannot be written as convex combinations of tensor products of local states.

Example 3.1 (Bell state). *For two qubits,*

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad \rho_{\Phi^+} = |\Phi^+\rangle\langle\Phi^+|.$$

The reduced state on either qubit is maximally mixed: $\text{Tr}_2(\rho_{\Phi^+}) = \frac{1}{2}\mathbb{I}_2$.

3.3 Unitary Dynamics and Quantum Gates

Time evolution in quantum mechanics is implemented by unitary conjugation, which preserves positivity, Hermiticity, and trace. In the algebraic probability space $(\mathbb{M}_{2^n}(\mathbb{C}), \rho)$, a computation step is represented by

$$\rho \mapsto U\rho U^*, \quad U \in \mathcal{U}(2^n). \quad (3.2)$$

The map (3.2) is a $*$ -automorphism of the algebra $\mathbb{M}_{2^n}(\mathbb{C})$ that leaves the state space invariant.

In the circuit model, unitaries are generated by a finite set of elementary gates acting on one or two qubits. Typical one-qubit gates include:

$$X = \sigma_x, \quad Y = \sigma_y, \quad Z = \sigma_z, \quad H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

and the phase and rotation gates

$$R_z(\theta) = e^{-i\theta\sigma_z/2}, \quad R_x(\theta) = e^{-i\theta\sigma_x/2}.$$

A standard two-qubit gate is the controlled-NOT (CNOT) gate:

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

Definition 3.2 (Quantum circuit). *A quantum circuit on n qubits is a finite ordered product*

$$U = U_m U_{m-1} \cdots U_1,$$

where each U_j acts as a unitary transformation on one or two tensor factors of \mathbb{H}_{2^n} .

By the *Solovay–Kitaev theorem*, any unitary $U \in \text{SU}(2^n)$ can be approximated to arbitrary precision by a product of such elementary gates from a finite universal set. Hence, the circuit model is computationally universal.

3.4 Computations with and without Ancillas: Marginalization and Reduced States

In practice, quantum computations may be carried out either on a *closed system* using only the computational qubits, or on an *extended system* in which additional auxiliary qubits (ancillas) are temporarily introduced to simplify or reversibly implement transformations.

Closed computation. If the computation acts solely on the n computational qubits, the evolution follows (3.2) with $U \in \mathcal{U}(2^n)$. The input and output states are both in $\mathcal{S}(\mathbb{M}_{2^n}(\mathbb{C}))$, and the mapping $\rho \mapsto U\rho U^*$ is bijective and trace-preserving. Such computations are *reversible* and correspond to unitary dynamics on a closed system.

Computation with ancillas. To represent intermediate workspace or to implement non-unitary operations reversibly, one may introduce an ancillary register \mathcal{H}_A of k qubits initialized in a fixed pure state $|0_A\rangle$. The combined state space is $\mathcal{H}_{2^{n+k}} = \mathcal{H}_C \otimes \mathcal{H}_A$, and the joint initial state is $\rho_C \otimes |0_A\rangle\langle 0_A|$. A global unitary U_{CA} acts on both registers, after which the ancilla is traced out:

$$\rho'_C = \text{Tr}_A(U_{CA}(\rho_C \otimes |0_A\rangle\langle 0_A|)U_{CA}^*).$$

The resulting map

$$\Phi(\rho_C) := \text{Tr}_A(U_{CA}(\rho_C \otimes |0_A\rangle\langle 0_A|)U_{CA}^*) \quad (3.3)$$

is a *completely positive trace-preserving* (CPTP) transformation. It represents the most general physically admissible quantum evolution, and reduces to a unitary conjugation when no ancillas are present.

Marginalization and reduced dynamics. Equation (3.3) shows that marginalization (partial trace over the ancillas) plays the same role in quantum computation as integration (marginalization) in classical probability: it yields the effective dynamics on the subsystem of interest. Hence, the two paradigms of quantum computation can be distinguished as:

$$\text{Closed computation: } \rho' = U\rho U^*, \quad \text{Open computation: } \rho' = \Phi(\rho) = \text{Tr}_A(U_{CA}(\rho \otimes \rho_A)U_{CA}^*).$$

The first corresponds to reversible evolution on a closed algebraic system, while the second corresponds to a marginal of a reversible evolution on an extended algebraic system.

3.5 Measurement and Probability Laws

Measurement transforms quantum information into classical data. Formally, a measurement is defined by a family of orthogonal projectors $\{P_i\} \subset \mathbb{M}_{2^n}(\mathbb{C})$ satisfying

$$P_i P_j = \delta_{ij} P_i, \quad \sum_i P_i = \mathbb{I}_{2^n}.$$

Given a state ρ , the outcome i occurs with probability

$$\mathbb{P}_\rho(i) = \text{tr}(\rho P_i), \quad (3.4)$$

and the post-measurement state (assuming projection postulate) is

$$\rho_i = \frac{P_i \rho P_i}{\text{tr}(\rho P_i)}.$$

Equation (3.4) generalizes the Born rule introduced in Section 2, expressing the measurement statistics of a quantum observable in the algebraic framework.

Example 3.3 (Measurement in the computational basis). *Let $\rho = |\Psi\rangle\langle\Psi|$ on \mathbb{C}^{2^n} , and let $P_{\mathbf{w}} = |\mathbf{w}\rangle\langle\mathbf{w}|$ for each basis vector $|\mathbf{w}\rangle \in \{|0\rangle, |1\rangle\}^{\otimes n}$. Then*

$$\mathbb{P}_\rho(\mathbf{w}) = |\langle\mathbf{w}|\Psi\rangle|^2,$$

which defines a classical probability distribution on $\{0, 1\}^n$.

3.6 Quantum Probability and Measurement

The measurement process links quantum states to classical probability distributions. For any observable with spectral decomposition into projectors $\{P_i\}$, the Born rule provides the bridge between the quantum and classical domains through Equation (3.4). This establishes quantum probability distributions on classical outcome spaces.

The partial trace operation enables the treatment of composite quantum systems and partial measurements. For a bipartite system with state ρ_{AB} on $\mathcal{H}_A \otimes \mathcal{H}_B$, measuring subsystem A yields marginal probabilities governed by the reduced state $\rho_A = \text{Tr}_B(\rho_{AB})$.

The trace distance hierarchy connecting quantum states to classical measurement statistics provides the foundation for algorithmic analysis and error bounds in quantum computation. As established in Proposition 2.13, measurement cannot increase distinguishability, ensuring that quantum indistinguishability implies classical indistinguishability.

3.7 Summary and Perspective

We have formulated the mathematical model of a digital quantum computer within the framework of algebraic probability:

- a qubit corresponds to the space $(\mathbb{M}_2(\mathbb{C}), \rho)$;
- a register of n qubits corresponds to $(\mathbb{M}_{2^n}(\mathbb{C}), \rho)$;
- computation corresponds to unitary conjugation preserving the probabilistic structure;
- computation with ancillas induces CPTP maps via partial trace;
- measurement corresponds to a family of orthogonal projectors inducing the probability law (3.4).

This algebraic formulation unifies the operator-theoretic and probabilistic aspects of quantum mechanics, and provides a mathematically transparent model for quantum information processing. In the next section, we will apply this formalism to define the embedding of finite arithmetic lattices into quantum registers and to analyze the accuracy of finite-dimensional approximations of continuous variables in the context of quantum algorithms.

4 Elementary Quantum Gates and Quantum Circuits

In this section we formalize the notion of *elementary quantum gates* as the fundamental building blocks of quantum computation and use them to define *quantum circuits*, which represent oracles or quantum algorithms within $U(N)$, where $N = 2^n$ for an n -qubit device.

4.1 Elementary Quantum Gates and Quantum Circuits

We begin by recalling that a function $f : U(2) \rightarrow U(N)$ is a group homomorphism if it satisfies

$$f(UV) = f(U)f(V) \quad \text{for all } U, V \in U(2).$$

A homomorphism is a *monomorphism* if it is injective. We denote by $\text{Emb}(U(2), U(N))$ the set of such group monomorphisms and define

$$\text{Emb}^*(U(2), U(N)) = \{ f \in \text{Emb}(U(2), U(N)) \mid f(U)^* = f(U^*) \text{ for all } U \in U(2) \}.$$

Definition 4.1 (Elementary quantum gate). *A matrix $U \in U(N)$ is called an elementary quantum gate if there exists a pair $(V, i) \in U(2) \times \text{Emb}^*(U(2), U(N))$ such that $U = i(V)$. The set of all elementary quantum gates in $U(N)$ is denoted by $\text{QG}(N)$.*

From the definition, $\text{QG}(2) = U(2)$. The set of elementary gates can be viewed as a *dictionary*. More generally, a subset $\mathcal{D} \subset U(N)$ is a dictionary if it is nonempty and satisfies the involutive symmetry

$$\mathcal{D}^* := \{U^* : U \in \mathcal{D}\} = \mathcal{D}.$$

Remark 4.2. *If $U \in \text{QG}(N)$, then $U^* \in \text{QG}(N)$; hence $\text{QG}(N)$ is a dictionary in $U(N)$.*

For a dictionary \mathcal{D} , write

$$\langle \mathcal{D} \rangle = \bigcup_{k \geq 0} \mathcal{D}^{(k)}, \quad \mathcal{D}^{(0)} = \{I_N\}, \quad \mathcal{D}^{(k)} = \{U_1 U_2 \cdots U_k : U_i \in \mathcal{D}\}.$$

We call \mathcal{D} *universal* if $\langle \mathcal{D} \rangle = U(N)$.

In an n -qubit device, a *wire* represents the action of $U(2)$ on the j -th qubit (QPU) and is modeled by elements of $\text{Emb}^*(U(2), U(2^n))$. For $1 \leq j \leq n$, define

$$w_j^{(n)} : U(2) \longrightarrow U(2^n), \quad U \longmapsto w_j^{(n)}(U) := I_2^{\otimes(j-1)} \otimes U \otimes I_2^{\otimes(n-j)}.$$

The action of $w_j^{(n)}(U)$ on the standard initial state $|b_n(0)\rangle \langle b_n(0)|$ of a universal digital quantum computer (UDQC) is

$$\begin{aligned} \mathcal{N}_{|b_n(0)\rangle \langle b_n(0)|}(w_j^{(n)}(U)) &= |b_{j-1}(0)\rangle \langle b_{j-1}(0)| \otimes U |0\rangle \langle 0| U^* \otimes |b_{n-j}(0)\rangle \langle b_{n-j}(0)| \\ &= |b_{j-1}(0)\rangle \langle b_{j-1}(0)| \otimes \mathcal{N}_{|0\rangle \langle 0|}(U) \otimes |b_{n-j}(0)\rangle \langle b_{n-j}(0)|. \end{aligned}$$

Hence $w_j^{(n)}(U)$ implements the one-qubit action of U on wire j . Moreover, the wires satisfy the composition property

$$w_1^{(n)}(U_1) w_2^{(n)}(U_2) \cdots w_n^{(n)}(U_n) = U_1 \otimes U_2 \otimes \cdots \otimes U_n.$$

Given indices $1 \leq i_1 < i_2 < \cdots < i_k \leq n$ with $1 \leq k \leq n$, define

$$(w_{i_1}^{(n)} \wedge \cdots \wedge w_{i_k}^{(n)}) : U(2) \longrightarrow U(2^n), \quad (w_{i_1}^{(n)} \wedge \cdots \wedge w_{i_k}^{(n)})(U) := \prod_{t=1}^k w_{i_t}^{(n)}(U).$$

Then $(w_{i_1}^{(n)} \wedge \cdots \wedge w_{i_k}^{(n)}) \in \text{Emb}^*(U(2), U(2^n))$. In particular, for any $U \in U(2)$, the unitary $U^{\otimes n} \in U(2^n)$ is an elementary quantum gate.

Define the set of one-wire embeddings

$$\mathcal{W}_N := \{w_j^{(n)}(V) : V \in U(2), 1 \leq j \leq n\} \subset \text{QG}(N),$$

which forms a dictionary generating the subgroup

$$\langle \mathcal{W}_N \rangle = U(2)^{\otimes n} \subset U(N).$$

Although $U(2)^{\otimes n}$ is a proper subgroup of $U(N)$, it is contained in the group generated by all elementary gates:

$$U(2)^{\otimes n} \subset \langle \text{QG}(N) \rangle.$$

A natural question arises: is $\text{QG}(N)$ itself universal in $U(N)$? The next result gives an affirmative answer.

Theorem 4.3. *The set $\text{QG}(N)$ is a universal dictionary for $\text{U}(N)$; that is, for every $\text{U} \in \text{U}(N)$ there exists an integer $m = \frac{N(N-1)}{2}$ such that U can be expressed as a product of m elementary quantum gates.*

Proof. See Appendix A. □

An immediate consequence is that every unitary in $\text{U}(N)$ can be represented as a finite sequence of elementary gates. This motivates the following.

Definition 4.4 (Quantum circuit). *Let $\text{U} \in \text{U}(N)$. A quantum circuit of length $\ell \geq 0$ for U is defined as follows: $\ell = 0$ iff $\text{U} = \text{I}_N$; otherwise, it is a finite sequence $\{\text{U}_1, \dots, \text{U}_\ell\} \subset \text{QG}(N) \setminus \{\text{I}_N\}$ such that*

$$\text{U} = \text{U}_\ell \text{U}_{\ell-1} \cdots \text{U}_1,$$

with the additional condition $\text{U}_{i+1}\text{U}_i \neq \text{I}_N$ for all $1 \leq i < \ell$.

Thus, if $\text{U} \in \text{QG}(N)$ has circuit length $\ell \geq 1$, then for each $1 \leq k \leq \ell$ there exist $(\text{V}_k, \text{i}_k) \in \text{U}(2) \times \text{Emb}^*(\text{U}(2), \text{U}(N))$ with $\text{U}_k = \text{i}_k(\text{V}_k)$, and

$$\text{U} = \text{i}_\ell(\text{V}_\ell) \text{i}_{\ell-1}(\text{V}_{\ell-1}) \cdots \text{i}_1(\text{V}_1).$$

Note that circuit realizations are generally non-unique. The identity $\text{I}_N = \text{I}_2^{\otimes n}$ is itself an elementary gate (e.g. $w_1^{(n)}(\text{I}_2) = \text{I}_N$) and plays the role of the empty word; consequently, ℓ can be interpreted as the number of elementary one-qubit operations required to implement a circuit.

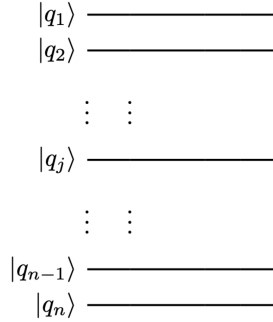


Figure 4.1: Wire diagram for an n -qubit universal digital quantum computer.

A circuit is typically depicted via wire diagrams comprised of:

- (a) *Wires*: horizontal lines representing qubits (Figure 4.1);
- (b) *Elementary gates*: symbols along wires acting on single qubits (Figure 4.2);
- (c) *Directionality*: left-to-right temporal ordering (Figure 4.3).

5 Quantum Algorithms

Quantum algorithms are finite sequences of unitary and measurement operations acting within the algebraic probability space $(\mathbb{M}_N(\mathbb{C}), \rho)$ that represents a universal digital quantum computer (UDQC). In this setting, a quantum algorithm can be understood as a transformation of states, or equivalently, as a morphism of algebraic probability spaces that maps input states to output distributions according to a prescribed computational goal.

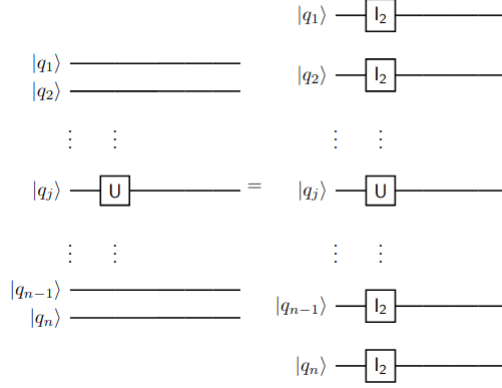


Figure 4.2: Elementary one-wire gate $w_j^{(n)}(U) = I_2^{\otimes(j-1)} \otimes U \otimes I_2^{\otimes(n-j)}$.

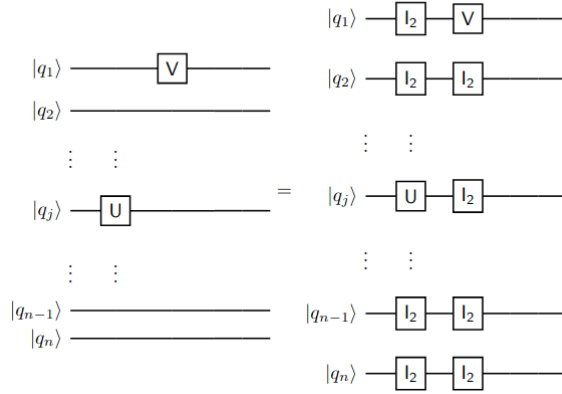


Figure 4.3: Product of elementary gates: $w_1^{(n)}(V) w_j^{(n)}(U) = V \otimes I_2^{\otimes(j-2)} \otimes U \otimes I_2^{\otimes(n-j)}$.

5.1 Definition and General Structure

Let $\mathcal{H}_n \cong \mathbb{C}^{2^n}$ be the Hilbert space of n qubits and $\rho_{\text{in}} \in \mathbb{M}_{2^n}(\mathbb{C})$ a density operator representing the input state. A *quantum algorithm* is defined by a tuple

$$\mathcal{A} = (n, U, \mathcal{M}),$$

where:

1. n is the number of qubits used by the algorithm,
2. $U \in \mathcal{U}(2^n)$ is the unitary transformation representing the coherent evolution of the system, and
3. \mathcal{M} is a measurement scheme mapping the final quantum state to a classical probability distribution.

The algorithm acts as

$$\rho_{\text{out}} = U \rho_{\text{in}} U^\star, \quad \mathbb{P}_{\mathcal{A}}(x) = \text{Tr}(\rho_{\text{out}} \Pi_x),$$

where $\{\Pi_x\}$ denotes the orthogonal projectors of the measurement \mathcal{M} .

This definition naturally generalizes classical algorithms: the unitary U plays the role of the deterministic update rule, while \mathcal{M} corresponds to the extraction of observable information from the probabilistic output of the quantum system.

5.2 Algorithms Without Ancillas

A *pure quantum algorithm without ancillas* acts directly on the n -qubit register, transforming $\rho_{\text{in}} \in \mathbb{M}_{2^n}(\mathbb{C})$ into an output state ρ_{out} . The computation is therefore described by a sequence of elementary gates

$$U = U_\ell U_{\ell-1} \cdots U_1, \quad U_i \in \text{QG}(2^n),$$

as introduced in Section 4. The length ℓ represents the circuit depth of the algorithm. The overall mapping

$$\Phi_U : \rho_{\text{in}} \mapsto U \rho_{\text{in}} U^\star$$

is a trace-preserving, completely positive map—that is, a morphism of algebraic probability spaces preserving normalization and positivity.

Example: the Hadamard transform. For a single qubit ($n = 1$), the Hadamard gate

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \in \text{U}(2)$$

maps the computational basis $\{|0\rangle, |1\rangle\}$ into the superposition basis $\{\frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)\}$. As a one-step algorithm, $\mathcal{A}_H = (1, H, \mathcal{M}_Z)$, it transforms the input state $|0\rangle$ into a uniform distribution upon measurement in the Z -basis.

5.3 Algorithms With Ancillas and Marginals

In many quantum algorithms, additional qubits are used as *ancillas* to facilitate intermediate computations or to encode auxiliary information. Mathematically, the presence of ancillas corresponds to an extension of the algebraic probability space by a tensor factor:

$$\mathcal{H}_{n+m} = \mathcal{H}_n \otimes \mathcal{H}_m, \quad \rho_{\text{in}}^{(n+m)} = \rho_{\text{in}}^{(n)} \otimes \rho_{\text{anc}}^{(m)}.$$

The algorithm acts as

$$\rho_{\text{out}}^{(n+m)} = U \rho_{\text{in}}^{(n+m)} U^\star,$$

followed by measurement on a subsystem of interest, typically the first n qubits. The corresponding output distribution is the marginal obtained by tracing out the ancilla register:

$$\rho_{\text{out}}^{(n)} = \text{Tr}_{\text{anc}}(\rho_{\text{out}}^{(n+m)}), \quad \mathbb{P}_{\mathcal{A}}^{(n)}(x) = \langle x | \rho_{\text{out}}^{(n)} | x \rangle.$$

This formulation unifies the notion of quantum algorithms *with* and *without* ancillas: in the latter case $m = 0$, and the partial trace is the identity.

5.4 Composition and Oracle Representation

A crucial feature of the algebraic framework is that quantum algorithms compose by operator multiplication. If $\mathcal{A}_1 = (n, U_1, \mathcal{M})$ and $\mathcal{A}_2 = (n, U_2, \mathcal{M})$ act on the same space, their composition is

$$\mathcal{A}_2 \circ \mathcal{A}_1 = (n, U_2 U_1, \mathcal{M}),$$

and corresponds to concatenating the respective circuits. This operatorial structure allows quantum algorithms to be viewed as elements of a noncommutative semigroup under matrix multiplication.

In particular, a quantum algorithm may encode a *black-box* or *oracle* operation through a unitary map

$$U_f : |x\rangle \otimes |y\rangle \mapsto |x\rangle \otimes |y \oplus f(x)\rangle,$$

where $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$ is a classical Boolean function and \oplus denotes bitwise addition modulo 2. This definition extends naturally to general group-valued homomorphisms $h : \mathbb{Z}^d \rightarrow G$, as introduced in Section 3, yielding the unitary U_h used in oracle-based quantum algorithms such as Grover's search or Shor's factoring routine.

5.5 Algebraic Classification of Quantum Algorithms

Within the algebraic probability setting, quantum algorithms can be classified according to the structure of the unitary transformations they employ:

- (i) **Abelian algorithms**, based on commuting unitaries such as phase estimation, quantum Fourier transform (QFT), or adiabatic evolutions over diagonal Hamiltonians;
- (ii) **Non-Abelian algorithms**, involving non-commuting generators, including amplitude amplification, Grover search, or quantum walk algorithms;
- (iii) **Hybrid algorithms**, where unitary evolution is interleaved with measurement and classical control, as in variational or measurement-based protocols.

Each class admits an algebraic characterization in terms of the underlying subalgebra of $\mathbb{M}_N(\mathbb{C})$ that remains invariant under the action of the circuit group $\langle \text{QG}(N) \rangle$.

5.6 From Circuits to Probabilistic Output Laws

Finally, the algebraic formulation provides a direct link between circuit synthesis and output statistics. For any quantum algorithm $\mathcal{A} = (n, U, \mathcal{M})$, the probability law of measurement outcomes in a basis $\{|x\rangle\}$ is

$$\mathbb{P}_{\mathcal{A}}(x) = \text{Tr}(U \rho_{\text{in}} U^* \Pi_x) = \langle x | U \rho_{\text{in}} U^* | x \rangle.$$

Consequently, two algorithms \mathcal{A}_1 and \mathcal{A}_2 are statistically indistinguishable if

$$\text{SD}(\mathbb{P}_{\mathcal{A}_1}, \mathbb{P}_{\mathcal{A}_2}) \text{ is negligible,}$$

linking the analytic distance on unitary operators with the statistical distance of their observable outcomes, as developed in Section 2.7.

Summary. In the algebraic probability framework, a quantum algorithm is thus a morphism between state spaces induced by unitary conjugation, possibly extended by ancillas and followed by partial measurement. This unified perspective allows the general theory of quantum algorithms to be formulated entirely in operator-algebraic terms, setting the stage for explicit constructions such as Grover–Rudolph amplitude amplification, Regev’s lattice- based algorithms, and adiabatic optimization methods developed in the next sections.

6 Quantum Annealing and Adiabatic Computation

The unitary circuit model developed in the previous sections describes quantum computation as a sequence of discrete transformations in the algebraic probability space $(\mathbb{M}_N(\mathbb{C}), \rho)$. An alternative but equivalent approach is provided by *quantum annealing* or, more generally, by *adiabatic quantum computation* (AQC), in which the evolution of the quantum state is continuous in time and driven by a time-dependent Hamiltonian. In the algebraic framework, the evolution is represented by a continuous one-parameter family of unitaries acting on $\mathbb{M}_N(\mathbb{C})$ and preserving the probabilistic structure of the state.

6.1 Adiabatic Evolution in the Algebraic Setting

Let $\mathcal{H}_n \cong \mathbb{C}^{2^n}$ be the Hilbert space of n qubits and ρ_t the state of the system at time $t \in [0, T]$. The dynamics are generated by a self-adjoint Hamiltonian $H(t) \in \mathbb{M}_{2^n}(\mathbb{C})$, according to the *Liouville–von Neumann equation*

$$\frac{d\rho_t}{dt} = -i [H(t), \rho_t], \quad \rho_0 = \rho_{\text{in}}. \quad (6.1)$$

The solution can be written as

$$\rho_t = U_t \rho_{\text{in}} U_t^*, \quad U_t = \mathcal{T} \exp\left(-i \int_0^t H(s) ds\right),$$

where \mathcal{T} denotes the time-ordering operator. Hence, the time evolution $\{U_t\}_{t \in [0, T]}$ forms a continuous one-parameter group in $U(2^n)$ acting by conjugation on the algebraic probability space.

When $H(t)$ varies slowly with respect to the spectral gap between the ground and excited eigenstates, the *adiabatic theorem* guarantees that the system remains close to its instantaneous ground state throughout the evolution. This property provides the foundation for quantum annealing as a computational paradigm.

6.2 Definition of Quantum Annealing

Quantum annealing aims to find the minimum of a cost function $E : \mathbb{Z}_2^n \rightarrow \mathbb{R}$ by encoding E in the diagonal elements of a *problem Hamiltonian* H_P :

$$H_P = \sum_{x \in \mathbb{Z}_2^n} E(x) |x\rangle \langle x|.$$

The computation starts from an initial Hamiltonian H_I whose ground state is easy to prepare, typically a uniform superposition, and proceeds by slowly interpolating between H_I and H_P :

$$H(t) = (1 - s(t)) H_I + s(t) H_P, \quad s : [0, T] \rightarrow [0, 1], \quad s(0) = 0, \quad s(T) = 1. \quad (6.2)$$

The function $s(t)$ is the *annealing schedule*, and its regularity determines the adiabaticity of the evolution. The final state at time T is

$$\rho_T = U_T \rho_{\text{in}} U_T^*, \quad U_T = \mathcal{T} \exp\left(-i \int_0^T H(t) dt\right),$$

and a projective measurement in the computational basis yields a random variable $X \in \mathbb{Z}_2^n$ distributed according to

$$\mathbb{P}_{\mathcal{A}_{\text{QA}}}(x) = \langle x | \rho_T | x \rangle.$$

The optimal solution corresponds to the most probable outcome, ideally the ground state of H_P .

6.3 Algebraic Probability Interpretation

Within the algebraic probability formalism, the pair $(\mathbb{M}_{2^n}(\mathbb{C}), \rho_t)$ defines a time-dependent probability space whose state evolves under the derivation $\delta_t(A) = i[H(t), A]$. The annealing process is therefore an instance of a *noncommutative diffusion* governed by a slowly varying generator. The expected energy at time t is

$$\mathbb{E}_t[H_P] = \text{Tr}(\rho_t H_P),$$

which decreases monotonically in the adiabatic regime, guiding the system toward the ground-state manifold.

Definition 6.1 (Quantum annealing algorithm). *A quantum annealing algorithm is a triple*

$$\mathcal{A}_{\text{QA}} = (H_I, H_P, s(t)),$$

where $H_I, H_P \in \mathbb{M}_{2^n}(\mathbb{C})$ are self-adjoint and $s(t)$ is a smooth, monotonically increasing schedule on $[0, T]$. The output law is the measurement distribution $\mathbb{P}_{\mathcal{A}_{\text{QA}}}(x) = \langle x | \rho_T | x \rangle$ associated with the final state ρ_T obtained by solving (6.1)–(6.2).

6.4 Relation to Optimization and QUBO Models

Many optimization problems can be reformulated as minimizing a quadratic function over binary variables, leading to the *Quadratic Unconstrained Binary Optimization* (QUBO) model:

$$E(x) = x^\top Q x, \quad x \in \{0, 1\}^n, \quad Q \in \mathbb{R}^{n \times n}.$$

The corresponding problem Hamiltonian is

$$H_P = \sum_{x \in \mathbb{Z}_2^n} x^\top Q x |x\rangle \langle x|,$$

and the initial Hamiltonian is often chosen as

$$H_I = - \sum_{j=1}^n \sigma_x^{(j)},$$

where σ_x is the Pauli- X operator acting on qubit j . The total annealing Hamiltonian thus takes the standard transverse-field Ising form

$$H(t) = (1 - s(t)) \left(- \sum_{j=1}^n \sigma_x^{(j)} \right) + s(t) \left(\sum_{x \in \mathbb{Z}_2^n} x^\top Q x |x\rangle \langle x| \right).$$

This formulation shows that the adiabatic model and the discrete QUBO energy landscape are connected by the algebraic identification of diagonal observables in $\mathbb{M}_{2^n}(\mathbb{C})$ with classical cost functions on \mathbb{Z}_2^n .

6.5 Discretization and Circuit Implementation

Although the annealing model is continuous in time, it can be approximated by a sequence of small unitary steps, leading to a Trotter discretization

$$U_T \approx \prod_{k=1}^K \exp(-i \Delta t H(t_k)), \quad \Delta t = T/K.$$

Each exponential factor can be implemented as a quantum circuit composed of elementary gates from $\text{QG}(2^n)$, as described in Section 4. Hence, adiabatic evolution can be simulated on a universal digital quantum computer, demonstrating the computational equivalence between the circuit and annealing models.

6.6 Summary and Physical Interpretation

Quantum annealing provides a physically motivated realization of quantum computation in which the algebraic probability space evolves smoothly under a family of self-adjoint generators. In the adiabatic limit, the system remains close to its instantaneous ground state, and the final measurement reveals the minimum of the encoded cost function. This model unifies continuous and discrete formulations of quantum computation within the same operator-algebraic framework:

$$\text{Circuit Model: } U = U_\ell \cdots U_1 \quad \Longleftrightarrow \quad \text{Annealing Model: } U_T = \mathcal{T} \exp\left(-i \int_0^T H(t) dt\right).$$

Both correspond to norm-preserving automorphisms of $\mathbb{M}_N(\mathbb{C})$ and define computational processes consistent with the algebraic probability formalism introduced in Section 2.

7 Quantum Complexity

The algebraic formulation of quantum computation developed in the previous sections provides a natural foundation for analyzing computational resources and complexity. In this section, we formalize the concept of *quantum complexity* as a measure of the resources required to realize a unitary transformation, prepare a quantum state, or approximate a probability law within the algebraic probability space $(\mathbb{M}_N(\mathbb{C}), \rho)$.

7.1 Complexity Measures in the Algebraic Framework

Let $U \in \text{U}(N)$ be a unitary matrix representing a quantum transformation on n qubits ($N = 2^n$). In the circuit model, U is implemented as a finite product of elementary gates $U_k \in \text{QG}(N)$,

$$U = U_\ell U_{\ell-1} \cdots U_1, \quad U_k = \mathbf{i}_k(V_k), \quad V_k \in \text{U}(2).$$

The integer ℓ represents the *circuit length* or *gate complexity* of U , denoted $C_{\text{gate}}(U)$.

Definition 7.1 (Gate complexity). *For a universal dictionary $\mathcal{D} \subset \text{U}(N)$, the gate complexity of $U \in \text{U}(N)$ is*

$$C_{\text{gate}}(U) = \min\{\ell \geq 0 : U = U_\ell U_{\ell-1} \cdots U_1, U_i \in \mathcal{D}\}.$$

Analogously, we define the *state preparation complexity* as the minimum circuit length needed to generate a target state $|\psi\rangle$ from the reference state $|b_n(0)\rangle = |0\rangle^{\otimes n}$.

Definition 7.2 (State preparation complexity). *The complexity of preparing $|\psi\rangle \in \mathbb{C}^{2^n}$ is*

$$C_{\text{prep}}(|\psi\rangle) = \min\{\ell \geq 0 : |\psi\rangle = U_\ell U_{\ell-1} \cdots U_1 |b_n(0)\rangle, U_i \in \text{QG}(2^n)\}.$$

These quantities define norms on the unitary group viewed as a word metric with respect to the generating set $\text{QG}(N)$, endowing $U(N)$ with a discrete *complexity geometry*.

7.2 Continuous and Energy-Based Complexity

In the adiabatic or annealing model (Section 6), complexity can also be expressed in terms of the total action or energy required to perform a continuous evolution. Let U_t satisfy the Schrödinger equation

$$\dot{U}_t = -i H(t) U_t, \quad U_0 = \mathbb{I}_N.$$

The *Hamiltonian energy cost* of the evolution is defined as

$$\mathcal{C}_{\text{energy}}(U_T) = \int_0^T \|H(t)\|_{\text{HS}} dt,$$

where $\|\cdot\|_{\text{HS}}$ denotes the Hilbert–Schmidt norm on $\mathbb{M}_N(\mathbb{C})$. This integral quantifies the geometric length of the path $t \mapsto U_t$ in $U(N)$ with respect to the right-invariant Riemannian metric

$$g_U(X, Y) = \text{Tr}(X^* Y), \quad X, Y \in T_U U(N) \simeq i \mathfrak{u}(N).$$

Thus, the adiabatic and circuit complexity notions are unified: the gate length corresponds to the discrete geodesic length, while the energy integral represents its continuous limit.

7.3 Quantum Complexity Classes

Quantum complexity theory categorizes computational problems according to the resources required by a quantum Turing machine or, equivalently, by a uniform family of quantum circuits.

Definition 7.3 (BQP). *A decision problem belongs to the class BQP (Bounded-Error Quantum Polynomial Time) if there exists a uniform family of quantum circuits $\{U_n\}$ acting on $\text{poly}(n)$ qubits, with circuit depth $\text{poly}(n)$, such that for every input $x \in \{0, 1\}^n$,*

$$\Pr[U_n(x) \text{ accepts}] \geq \frac{2}{3} \quad \text{if } x \text{ is a yes-instance}, \quad \Pr[U_n(x) \text{ accepts}] \leq \frac{1}{3} \quad \text{otherwise}.$$

Other fundamental classes include:

- QMA (Quantum Merlin–Arthur), the quantum analogue of NP, where the witness is a quantum state verified by a polynomial-time quantum circuit.
- QIP (Quantum Interactive Polynomial time), representing interactive quantum proof systems.
- BPP, the classical bounded-error probabilistic class, which satisfies $\text{BPP} \subseteq \text{BQP}$.

Remark 7.4. *The algebraic-probability framework provides a unifying interpretation of these classes: each class corresponds to a family of morphisms $\Phi : \rho \mapsto U \rho U^*$ in $\mathbb{M}_{2^n}(\mathbb{C})$, constrained by resource bounds on $C_{\text{gate}}(U)$ or $\mathcal{C}_{\text{energy}}(U_T)$.*

7.4 Approximation and Precision Complexity

Since real physical implementations can only approximate ideal unitaries, it is necessary to introduce a precision parameter $\varepsilon > 0$. We say that $U' \in U(N)$ approximates U with precision ε if

$$\|U' - U\|_{\text{op}} \leq \varepsilon.$$

The corresponding ε -approximation complexity is

$$C_{\text{gate}}^\varepsilon(U) = \min\{\ell \geq 0 : \exists U' \text{ such that } U' = U_\ell \cdots U_1, U_i \in \text{QG}(N), \|U' - U\|_{\text{op}} \leq \varepsilon\}.$$

By the Solovay–Kitaev theorem, for any universal gate set \mathcal{D} and any $\varepsilon > 0$, there exists a constant c such that

$$C_{\text{gate}}^\varepsilon(U) = O\left(\log^c \frac{1}{\varepsilon}\right) C_{\text{gate}}(U),$$

showing that efficient ε -approximation is always achievable with polylogarithmic overhead.

7.5 Complexity of Quantum Annealing

In the adiabatic framework, the computational cost is governed by the minimum spectral gap Δ_{\min} of the Hamiltonian (6.2). The runtime required to ensure an adiabatic evolution with bounded error satisfies the scaling

$$T \gtrsim \frac{\|\dot{H}(t)\|}{\Delta_{\min}^2}.$$

Thus, problems with exponentially small spectral gaps require exponentially long annealing times, paralleling the exponential circuit depth of hard quantum algorithms. From the algebraic perspective, this corresponds to the norm constraint on the generator $\delta_t(A) = i[H(t), A]$, which controls the rate of change of the quantum state in the probability space $(\mathbb{M}_N(\mathbb{C}), \rho_t)$.

7.6 Entropy and Information Complexity

The information content of a quantum state can be quantified by the von Neumann entropy

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

For pure states $S(\rho) = 0$, while mixed states encode classical uncertainty. The entropy production during a computation provides an alternative measure of complexity, capturing the amount of information generated or lost under unitary evolution and measurement. In particular, for an algorithm $\mathcal{A} = (n, U, \mathcal{M})$ with output distribution $\mathbb{P}_{\mathcal{A}}$, the Shannon entropy

$$H(\mathbb{P}_{\mathcal{A}}) = -\sum_x \mathbb{P}_{\mathcal{A}}(x) \log \mathbb{P}_{\mathcal{A}}(x)$$

measures the classical randomness induced by the quantum process. This quantity connects the operator-algebraic and probabilistic aspects of complexity.

7.7 Summary and Perspectives

Quantum complexity bridges the discrete circuit model, the continuous annealing model, and the probabilistic interpretation of quantum computation. Within the algebraic probability framework, all these perspectives correspond to geometric or metric notions on $U(N)$:

Gate complexity \leftrightarrow discrete word length, Energy complexity \leftrightarrow continuous path length, Information

This unified viewpoint reveals that the essential computational content of quantum mechanics resides in the geometry and algebraic structure of unitary transformations, linking operator theory, probability, and algorithmic complexity within a single formal framework.

8 Quantum Information Geometry

The algebraic probability formulation of quantum mechanics provides a natural geometric structure on the space of quantum states and unitary transformations. Quantum information geometry studies this structure in terms of Riemannian or Finsler metrics that quantify the distinguishability of states, the infinitesimal cost of transformations, and the geodesic paths representing optimal computations. This section unifies the statistical and geometric viewpoints introduced in Sections 5–7.

8.1 Differential Structure on the State Space

Let $\mathcal{S}_N = \{\rho \in \mathbb{M}_N(\mathbb{C}) : \rho \geq 0, \text{Tr } \rho = 1\}$ be the convex manifold of density operators. The tangent space at ρ is given by

$$T_\rho \mathcal{S}_N = \{X \in \mathbb{M}_N(\mathbb{C})_{\text{Herm}} : \text{Tr}(X) = 0\}.$$

A differentiable path $\rho_t \in \mathcal{S}_N$ satisfies $\dot{\rho}_t \in T_{\rho_t} \mathcal{S}_N$. Under unitary evolution $\rho_t = U_t \rho_0 U_t^\star$, the tangent vector is $\dot{\rho}_t = -i[H(t), \rho_t]$.

8.2 Monotone Riemannian Metrics

A Riemannian metric $g_\rho(X, Y)$ on \mathcal{S}_N is *monotone* if it contracts under completely positive trace-preserving (CPTP) maps Φ :

$$g_{\Phi(\rho)}(\Phi(X), \Phi(Y)) \leq g_\rho(X, Y).$$

Petz's classification theorem states that all monotone metrics arise from operator means. Two fundamental examples are:

- (i) The **Bures–Helstrom (quantum Fisher) metric**

$$g_\rho^{\text{B}}(X, Y) = \frac{1}{2} \text{Tr}(X \Omega_\rho^{-1}(Y)), \quad \Omega_\rho^{-1}(Y) = \int_0^\infty (\rho + sI)^{-1} Y (\rho + sI)^{-1} ds,$$

which induces the Bures distance $d_{\text{B}}(\rho, \sigma) = \sqrt{2(1 - F(\rho, \sigma))}$, where $F(\rho, \sigma) = \text{Tr} \sqrt{\rho^{1/2} \sigma \rho^{1/2}}$ is the quantum fidelity.

- (ii) The **Bogoliubov–Kubo–Mori (BKM) metric**

$$g_\rho^{\text{BKM}}(X, Y) = \int_0^1 \text{Tr}(\rho^s X \rho^{1-s} Y) ds,$$

which plays a key role in quantum statistical mechanics and relative entropy.

Remark 8.1. For pure states $\rho = |\psi\rangle\langle\psi|$, all monotone metrics coincide and reduce to the Fubini–Study metric on projective Hilbert space,

$$ds^2 = \langle d\psi|d\psi\rangle - |\langle\psi|d\psi\rangle|^2,$$

which represents the infinitesimal angle between rays.

8.3 Geometric Interpretation of Complexity

Let $U_t \in U(N)$ denote a differentiable path connecting I_N and a target U . The tangent vector \dot{U}_t belongs to the Lie algebra $\mathfrak{u}(N) = \{X \in \mathbb{M}_N(\mathbb{C}) : X^\star = -X\}$, and the infinitesimal cost of motion can be quantified by a right-invariant Riemannian or Finsler metric

$$\mathcal{F}_{U_t}(\dot{U}_t) = \sqrt{\text{Tr}(G(\dot{U}_t^\star \dot{U}_t))},$$

where G is a positive definite operator acting as a weight on different directions of $\mathfrak{u}(N)$. The associated *geodesic length*

$$\mathcal{L}(U_T) = \int_0^T \mathcal{F}_{U_t}(\dot{U}_t) dt$$

defines the continuous analogue of gate complexity introduced in Section 7. Minimal-length paths correspond to optimal implementations of unitaries, linking quantum complexity to geodesic geometry on $U(N)$.

Definition 8.2 (Geometric quantum complexity). For a right-invariant metric \mathcal{F} on $U(N)$, the geometric complexity of $U \in U(N)$ is

$$\mathcal{C}_{\mathcal{F}}(U) = \inf_{U_t: U_0=I, U_T=U} \int_0^T \mathcal{F}_{U_t}(\dot{U}_t) dt.$$

8.4 Information Geometry and Statistical Distinguishability

In the probabilistic picture, distinguishability between quantum states can be quantified by statistical distances derived from the Fisher information. For infinitesimal variations $\rho_\theta = \rho + \theta X$, the quantum Fisher information metric is

$$I_\rho(X) = g_\rho^B(X, X) = \text{Tr}(X \Omega_\rho^{-1}(X)).$$

This metric governs the Cramér–Rao bound for quantum estimation:

$$\text{Var}(\hat{\theta}) \geq \frac{1}{I_\rho(X)}.$$

Thus, the geometry of the state manifold encodes both computational and informational constraints, unifying statistical inference and algorithmic evolution.

8.5 Curvature and Quantum Speed Limits

The geometry of \mathcal{S}_N and $U(N)$ imposes intrinsic bounds on the rate of state evolution. For a pure-state trajectory $|\psi_t\rangle$ governed by Hamiltonian $H(t)$, the Fubini–Study metric leads to the *Mandelstam–Tamm bound*

$$T \geq \frac{\arccos |\langle\psi_0|\psi_T\rangle|}{\Delta E}, \quad \Delta E = \sqrt{\langle\psi_t|H(t)^2|\psi_t\rangle - \langle\psi_t|H(t)|\psi_t\rangle^2}.$$

In the mixed-state setting, the same principle follows from the Bures metric, producing the generalized quantum speed limit

$$\|\dot{\rho}_t\|_{g^B} \leq 2 \Delta E_t.$$

These inequalities express fundamental geometric limits on computational speed and energy cost within the algebraic probability space.

8.6 Entropy, Divergences, and Dual Geometry

The BKM metric is intimately related to the relative entropy $S(\rho\|\sigma) = \text{Tr}(\rho(\log \rho - \log \sigma))$, which defines a non-symmetric divergence function. Its second-order expansion around $\rho = \sigma$ recovers g_ρ^{BKM} . This dual structure induces two affine connections: the *mixture* and *exponential* connections, leading to the Amari–Nagaoka α -geometry on quantum state space. In this framework, the pair $(\mathcal{S}_N, g^{\text{BKM}}, \nabla^{(\pm 1)})$ forms a dually flat manifold, bridging quantum statistical inference and algorithmic optimization.

8.7 Summary and Outlook

Quantum information geometry provides a unified description of computational cost, statistical distinguishability, and dynamical evolution. The discrete gate complexity of Section 7, the continuous energy complexity of Section 6, and the statistical distances of Section 2.7 are all manifestations of the same underlying geometric structure:

Quantum computation \equiv geodesic motion on the manifold of quantum states and unitaries.

This viewpoint links operator algebras, probability theory, and differential geometry, suggesting that the fundamental limits of computation are geometric in nature—arising from curvature, metric constraints, and the topology of $U(N)$ itself.

9 Foundations and Open Problems

The framework developed throughout these notes establishes a unified algebraic and geometric foundation for quantum computation. Beginning from the theory of algebraic probability spaces, we have constructed a mathematical model in which quantum states, observables, and algorithms appear as morphisms and transformations of the algebra $\mathbb{M}_N(\mathbb{C})$, endowed with a noncommutative probabilistic structure. Within this setting, the discrete circuit model, the continuous adiabatic model, and their associated notions of complexity emerge as complementary manifestations of a single underlying principle: computation as the controlled evolution of quantum probability.

9.1 Summary of the Conceptual Structure

The main conceptual steps developed in this work can be summarized as follows:

- (i) **Algebraic Probability.** Quantum mechanics is formulated as a noncommutative extension of measure theory, where the pair $(\mathcal{A}, \varphi) = (\mathbb{M}_N(\mathbb{C}), \rho)$ defines a probability space over observables. States are density operators, and measurements correspond to positive operator-valued measures.
- (ii) **Digital Quantum Computation.** The universal digital quantum computer (UDQC) is represented as a finite-dimensional algebraic probability space acted upon by unitary automorphisms. Quantum gates are embeddings of $U(2)$ into $U(N)$, and quantum circuits are finite sequences of such embeddings forming a universal dictionary.

- (iii) **Quantum Algorithms.** Algorithms correspond to morphisms of state spaces, possibly extended by ancillary registers and followed by partial measurement. This abstraction unifies discrete oracles, reversible logic, and probabilistic post-processing.
- (iv) **Quantum Annealing.** The continuous-time limit of quantum computation is obtained through adiabatic evolution under time-dependent Hamiltonians. The Liouville–von Neumann equation describes the flow of states within the algebraic probability space, linking the quantum dynamics to optimization and variational principles.
- (v) **Quantum Complexity.** Computational cost can be quantified discretely (gate count), continuously (energy or path length), or informationally (entropy or statistical distinguishability). All these measures are geometrically consistent and obey the same algebraic constraints.
- (vi) **Quantum Information Geometry.** The manifold of density operators and unitaries carries natural monotone Riemannian metrics—Bures, BKM, Fubini–Study—whose geodesics represent optimal quantum evolutions. Complexity thus becomes a geometric length functional on $U(N)$ or on the state manifold \mathcal{S}_N .

These elements reveal that the essence of quantum computation lies in the geometry and algebra of transformations preserving positivity, trace, and inner product structure.

9.2 Foundational Questions

Despite its coherence, several mathematical and conceptual aspects remain open for further investigation:

(1) Infinite-Dimensional Extensions. While our framework has been developed for $M_N(\mathbb{C})$, it should extend to von Neumann algebras acting on separable Hilbert spaces. This raises deep questions about the spectral and measure-theoretic structure of unbounded Hamiltonians, the adiabatic theorem in infinite dimensions, and the convergence of discrete-to-continuous approximations.

(2) Algebraic Topology of Quantum Computation. The unitary group $U(N)$ has nontrivial topology (with $\pi_1(U(N)) \cong \mathbb{Z}$), suggesting that quantum algorithms may possess topological invariants related to winding numbers, Berry phases, or holonomy classes. A rigorous topological classification of computational paths could lead to a homotopy-theoretic approach to algorithmic equivalence.

(3) Quantum Thermodynamics and Entropy Production. The probabilistic interpretation of quantum computation invites an explicit connection with thermodynamic entropy and energy dissipation. Understanding computation as an entropy-preserving (or entropy-constrained) process may bridge quantum information theory and non-equilibrium statistical mechanics.

(4) Complexity Geometry and Curvature. The Riemannian geometry of $U(N)$ induced by right-invariant metrics can exhibit nontrivial curvature, affecting the stability and optimality of computational paths. A full geometric characterization of curvature, geodesic deviation, and sectional bounds in relation to algorithmic complexity remains to be developed.

(5) Quantum Probability on Tensor Banach Spaces. The formulation of quantum probability in Banach or tensor product spaces opens the door to studying infinite-dimensional or approximate quantum processors. The definition of tensor norms compatible with positivity and trace preservation poses a nontrivial challenge for functional analysis.

(6) Quantum Algorithmic Universality Beyond $U(N)$. More general computational models—based on Lie semigroups, Lindbladian dynamics, or completely positive maps—might extend universality to open quantum systems and non-unitary evolutions. Establishing universality criteria in this broader setting requires a synthesis of algebraic and geometric techniques.

9.3 Mathematical and Physical Directions

From a mathematical perspective, the following research lines appear particularly promising:

- Developing a full *category of algebraic probability spaces*, where objects are pairs (\mathcal{A}, φ) and morphisms are completely positive unital maps, unifying states, channels, and algorithms under the same algebraic structure.
- Extending the *adiabatic theorem* to infinite-dimensional Banach and tensor spaces, with explicit conditions on the generator spectrum and the rate of convergence to the instantaneous ground state.
- Establishing a *metric equivalence theorem* connecting the discrete gate metric, the continuous energy metric, and the Bures–Helstrom information metric on $U(N)$.
- Characterizing *quantum computational curvature* as the obstruction to integrability of optimal control flows on $U(N)$, linking complexity geometry with Riemannian submersion theory.
- Investigating *entropy–complexity relations* in non-unitary channels, particularly the connection between entropy production, trace-distance contraction, and algorithmic irreversibility.

9.4 Outlook

The algebraic probability model of quantum computation presented here unifies discrete and continuous formulations, measurement theory, and geometric complexity into a single mathematical language. It reveals that the act of computing is fundamentally a process of evolving probability within noncommutative algebras under symmetry and positivity constraints.

This viewpoint provides a rigorous bridge between several domains:

$$\text{Algebraic probability} \longleftrightarrow \text{Operator algebras} \longleftrightarrow \text{Quantum computation} \longleftrightarrow \text{Information geometry}.$$

In this sense, quantum computation can be regarded as a physical realization of noncommutative probability geometry, where information processing is governed by the structure of $U(N)$ and the statistical laws encoded in its algebra. The mathematical and physical open problems outlined above suggest that the theory of algebraic probability may become not only a descriptive but also a constructive foundation for the next generation of quantum algorithms, complexity theory, and computational physics.

Epilogue

The development presented in these notes has traced a continuous line from *algebraic probability* to *quantum computation*, and from there to *complexity* and *geometry*. At its core lies a simple but powerful principle: quantum computation is the dynamics of probability within noncommutative algebras.

By identifying the algebra $\mathbb{M}_N(\mathbb{C})$ as the basic stage of finite quantum information, we have reinterpreted computation as the controlled evolution of states under unitary automorphisms. Every quantum algorithm, whether implemented by discrete gates or by continuous Hamiltonian flows, is thus a trajectory in the geometric manifold of states—an ordered path in a space where information, probability, and symmetry intertwine.

This perspective blurs the traditional boundary between physics and computation. The quantum computer becomes not merely a machine but a geometric object whose motion is governed by algebraic laws. Complexity acquires a metric meaning; information flow is described by curvature; and the limits of computation appear as constraints on energy, entropy, and geometry.

Beyond its mathematical consistency, the framework also points toward a synthesis of disciplines: operator algebras, quantum information, optimal control, and differential geometry converge to describe a single phenomenon—the propagation of structure through noncommutative probability. Whether realized in discrete circuits, adiabatic annealers, or hybrid analog-digital architectures, every quantum process unfolds along the same algebraic manifold.

*Computation, in this sense, is not an algorithmic accident of physics,
but a geometric expression of the laws that govern transformation and measure.*

The open problems outlined in Section 9 suggest that this perspective is still far from complete. Extending it to infinite-dimensional settings, understanding the topology of quantum evolutions, and uncovering the full interplay between entropy, curvature, and complexity remain major theoretical challenges. Yet they all share the same conceptual nucleus: the realization that *to compute is to evolve within the geometry of probability*.

Acknowledgment. These notes have been written as part of the ongoing effort to establish a unified mathematical theory of quantum computation grounded in algebraic probability and information geometry. They are dedicated to the many colleagues and students whose questions and insights continue to shape this evolving landscape.

Bibliographical Note

The theoretical background of these notes lies at the intersection of operator algebras, quantum probability, and computational complexity. The algebraic foundations originate from the works of Meyer [8] and Parthasarathy [11], which formalize quantum probability as a noncommutative extension of classical measure theory. The study of quantum information geometry, monotone metrics, and Fisher information traces back to Petz [12] and the seminal monograph of Amari and Nagaoka [1].

The geometric and algorithmic theory of quantum computation has been shaped by the comprehensive treatment of Nielsen and Chuang [9], together with Nielsen’s geometric approach to circuit complexity [10]. The adiabatic and annealing perspectives follow the works of Farhi and collaborators [5, 4], while the Solovay–Kitaev theorem and universality results are drawn from Dawson and Nielsen [3].

The geometric and statistical interpretations of quantum mechanics and information processing, including the Bures and BKM metrics, are treated in detail in the works of Helstrom [6], Uhlmann [13], and the review of Bengtsson and Życzkowski [2]. Connections between quantum probability, operator algebras, and information theory may be further explored in Holevo’s foundational text [7].

These references together provide the mathematical and conceptual context in which the algebraic-probabilistic model of quantum computation developed here finds its natural place.

References

- [1] Shun-ichi Amari and Hiroshi Nagaoka. *Methods of Information Geometry*, volume 191 of *Translations of Mathematical Monographs*. American Mathematical Society, Providence, RI, 2000.
- [2] Ingemar Bengtsson and Karol Życzkowski. *Geometry of Quantum States: An Introduction to Quantum Entanglement*. Cambridge University Press, Cambridge, 2017.
- [3] Christopher M. Dawson and Michael A. Nielsen. The solovay–kitaev algorithm. *Quantum Information & Computation*, 6(1):81–95, 2005.
- [4] Edward Farhi, Jeffrey Goldstone, Sam Gutmann, Joshua Lapan, Andrew Lundgren, and Daniel Preda. Quantum computation by adiabatic evolution. *arXiv preprint quant-ph/0001106*, 2001.
- [5] Edward Farhi, Jeffrey Goldstone, Sam Gutmann, and Michael Sipser. A quantum adiabatic evolution algorithm applied to random instances of an np-complete problem. *Science*, 292(5516):472–475, 2001.
- [6] Carl W. Helstrom. *Quantum Detection and Estimation Theory*. Academic Press, New York, 1976.
- [7] Alexander S. Holevo. *Quantum Systems, Channels, Information: A Mathematical Introduction*. De Gruyter, Berlin, 2019.
- [8] Paul-André Meyer. *Quantum Probability for Probabilists*, volume 1538 of *Lecture Notes in Mathematics*. Springer, Berlin, 1993.
- [9] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 2000.
- [10] Michael A. Nielsen, Mark R. Dowling, Mile Gu, and Andrew C. Doherty. A geometric approach to quantum circuit lower bounds. *Science*, 311(5764):1133–1135, 2006.
- [11] Kalyanapuram R. Parthasarathy. *An Introduction to Quantum Stochastic Calculus*. Birkhäuser, Basel, 1992.
- [12] Dénes Petz. Monotone metrics on matrix spaces. *Linear Algebra and its Applications*, 244:81–96, 1996.
- [13] Armin Uhlmann. The “transition probability” in the state space of a $*$ -algebra. *Reports on Mathematical Physics*, 9(2):273–279, 1976.

Appendix A Proofs of Results from Section 3.6

This appendix collects the technical proofs omitted from Section 3 for readability.

Proof of Lemma 2.11. We use the variational (dual) characterization of the trace norm:

$$\|Y\|_1 = \sup_{\|K\|_\infty \leq 1} |\text{Tr}(KY)|, \quad Y \in \mathcal{B}(\mathcal{H}_1),$$

where $\|\cdot\|_\infty$ is the operator norm. For any $K \in \mathcal{B}(\mathcal{H}_1)$ with $\|K\|_\infty \leq 1$, the definition of partial trace gives

$$\text{Tr}(K \text{Tr}_{\mathcal{H}_2}(X)) = \text{Tr}((K \otimes I_{\mathcal{H}_2})X).$$

Hence, by Hölder's inequality for Schatten norms,

$$|\text{Tr}(K \text{Tr}_{\mathcal{H}_2}(X))| = |\text{Tr}((K \otimes I)X)| \leq \|K \otimes I\|_\infty \|X\|_1 = \|K\|_\infty \|X\|_1 \leq \|X\|_1.$$

Taking the supremum over all $\|K\|_\infty \leq 1$ yields $\|\text{Tr}_{\mathcal{H}_2}(X)\|_1 \leq \|X\|_1$, as claimed. \square

Proof of Lemma 2.12. For each sign vector $s = (s_1, \dots, s_r) \in \{\pm 1\}^r$, set $U_s := \sum_{i=1}^r s_i \Pi_i$. Then U_s is unitary, since $U_s U_s^\dagger = \sum_i \Pi_i = I_{\mathcal{H}}$ and $U_s^\dagger = U_s$. Averaging over all sign patterns gives the pinching identity

$$\frac{1}{2^r} \sum_{s \in \{\pm 1\}^r} U_s Y U_s^\dagger = \sum_{i=1}^r \Pi_i Y \Pi_i = \text{Diag}(Y),$$

because mixed terms $\Pi_i Y \Pi_j$ with $i \neq j$ cancel by symmetry. Using unitary invariance and convexity of the trace norm,

$$\|\text{Diag}(Y)\|_1 = \left\| \frac{1}{2^r} \sum_s U_s Y U_s^\dagger \right\|_1 \leq \frac{1}{2^r} \sum_s \|U_s Y U_s^\dagger\|_1 = \frac{1}{2^r} \sum_s \|Y\|_1 = \|Y\|_1.$$

\square

Proof of Proposition 2.13. (i) Unitary invariance of the trace norm gives $\|U(\rho - \sigma)U^\dagger\|_1 = \|\rho - \sigma\|_1$, hence the claim.

(ii) By definition of total variation and of the diagonal map,

$$\text{SD}(\mathbb{P}_\rho^{(1)}, \mathbb{P}_\sigma^{(1)}) = \frac{1}{2} \sum_{\mathbf{x}} |\mathbb{P}_\rho^{(1)}(\mathbf{x}) - \mathbb{P}_\sigma^{(1)}(\mathbf{x})| = \frac{1}{2} \left\| \sum_{\mathbf{x}} \Pi_{\mathbf{x}} (\text{Tr}_{\mathcal{H}_2}(\rho - \sigma)) \Pi_{\mathbf{x}} \right\|_1.$$

Apply Lemma 2.12 (pinching is contractive) to get

$$\frac{1}{2} \left\| \text{Diag}(\text{Tr}_{\mathcal{H}_2}(\rho - \sigma)) \right\|_1 \leq \frac{1}{2} \|\text{Tr}_{\mathcal{H}_2}(\rho - \sigma)\|_1,$$

and then Lemma 2.11 (partial trace is contractive) to conclude

$$\frac{1}{2} \|\text{Tr}_{\mathcal{H}_2}(\rho - \sigma)\|_1 \leq \frac{1}{2} \|\rho - \sigma\|_1 = D_{\text{tr}}(\rho, \sigma).$$

(iii) Use the pure-state identity for trace distance: $D_{\text{tr}}(|\psi\rangle, |\phi\rangle) = \sqrt{1 - |\langle\psi|\phi\rangle|^2}$, which is an immediate consequence of the Helstrom bound in the 2-dimensional span of $\{|\psi\rangle, |\phi\rangle\}$. \square