Geometry of discrete quantum computing

2013 J. Phys. A: Math. Theor. 46 185301

(http://iopscience.iop.org/1751-8121/46/18/185301)

J. Phys. A: Math. Theor. **46** (2013) 185301 (21pp) doi:10.1088/1751-8113/46/18/185301

Geometry of discrete quantum computing

Andrew J Hanson[1], Gerardo Ortiz[2], Amr Sabry[1] and Yu-Tsung Tai[3]

[1] School of Informatics and Computing, Indiana University, Bloomington, IN 47405, USA
[2] Department of Physics, Indiana University, Bloomington, IN 47405, USA
[3] Department of Mathematics, Indiana University, Bloomington, IN 47405, USA

E-mail: ortizg@indiana.edu

Received 23 November 2012, in final form 4 March 2013
Published 17 April 2013
Online at stacks.iop.org/JPhysA/46/185301

Abstract
Conventional quantum computing entails a geometry based on the description of an n-qubit state using 2^n infinite precision complex numbers denoting a vector in a Hilbert space. Such numbers are in general uncomputable using any real-world resources, and, if we have the idea of physical law as some kind of computational algorithm of the universe, we would be compelled to alter our descriptions of physics to be consistent with computable numbers. Our purpose here is to examine the geometric implications of using finite fields $\mathbf{F}_p$ and finite complexified fields $\mathbf{F}_{p^2}$ (based on primes p congruent to 3 ($mod 4$)) as the basis for computations in a theory of discrete quantum computing, which would therefore become a computable theory. Because the states of a discrete n-qubit system are in principle enumerable, we are able to determine the proportions of entangled and unentangled states. In particular, we extend the Hopf fibration that defines the irreducible state space of conventional continuous n-qubit theories (which is the complex projective space $\mathbf{CP}^{2^n-1}$) to an analogous discrete geometry in which the Hopf circle for any n is found to be a discrete set of $p+1$ points. The tally of unit-length n-qubit states is given, and reduced via the generalized Hopf fibration to $\mathbf{DCP}^{2^n-1}$, the discrete analogue of the complex projective space, which has $p^{2^n-1}(p-1)\prod_{k=1}^{n-1}(p^{2^k}+1)$ irreducible states. Using a measure of entanglement, the *purity*, we explore the entanglement features of discrete quantum states and find that the n-qubit states based on the complexified field $\mathbf{F}_{p^2}$ have $p^n(p-1)^n$ unentangled states (the product of the tally for a single qubit) with purity 1, and they have $p^{n+1}(p-1)(p+1)^{n-1}$ maximally entangled states with purity zero.

PACS numbers: 03.67.−a, 03.67.Ac, 03.65.Ta, 02.10.De

(Some figures may appear in colour only in the online journal)

1. Introduction

Conventional quantum computing (CQC) is appealing because it expands our horizons on the concepts of computing in general. The fundamental principles of CQC broadly influence computer science, physics, mathematics, and logic. Not only would Turing have been fascinated by the implications of quantum computing for his own theory of computation, but he would also have been intrigued by the apparent absence of any further possible extensions. In this paper we go one step further, and study the beginnings of a fundamental consistent framework for *discrete quantum computing* (DQC). Our basic results in this paper include a detailed construction and analysis of the irreducible n-qubit states in DQC, a novel analysis of the structure of the discrete generalized Bloch sphere for n-qubits and a study of entanglement in the discrete domain.

Research on theoretical quantum computing focuses on two distinct aspects, algorithms and geometry. Since quantum computing contains features and components quite different from classical computational methods, the exploration of algorithms, computation, and the theory of computational methods is essential, and includes the study of topics such as the Deutsch–Jozsa algorithm whose task is to determine if a function is constant or balanced with preternatural speed, and Grover's algorithm for searching a database with the square root of the number of queries needed classically. But another essential branch of quantum computing research is the investigation of the nature of *states themselves*, the geometry of the spaces describing the n-qubit states upon which algorithms eventually act; the properties of such spaces are important in their own right, long before they are used in algorithms. Understanding these properties serves, for example, to explicate the nature of irreducible states (when all wave-function symmetries are eliminated), and exposes the nature of entangled states, a phenomenon completely absent from any non-quantum geometrical framework. The geometric aspects of conventional quantum theory and quantum computing are the subject of a vast literature, and entire books (see, e.g., [1]) have been devoted to quantum geometry and its relation to entanglement. An extensive picture of the geometry of CQC has emerged, showing that the complex projective spaces $\mathbf{CP}^{2^n-1}$ precisely embody the irreducible states of an n-qubit quantum circuit element, and, in addition, permit the explicit study of the actual paths in the irreducible state space that correspond to idealized quantum operations.

Our contribution, which involves issues possibly less familiar to readers of the algorithm-centered literature, is to extend the path of the corpus of 'conventional' geometry-based quantum computing research into the discrete domain. We start with a finite complexified Galois field $\mathbf{F}_{p^2}$ replacing the complex fields used in the existing literature for the geometry of quantum computing (e.g., [1, 2]) and examine the implications of calculating the geometric properties of n-qubit states with coefficients defined in discrete Galois fields. Our work for the first time explicates a rigorous approach to n-discrete-qubit complex geometry and the resulting discretized complex projective spaces. We rederive some of the basic results of discrete complex mathematics introduced by Arnold [3], and extend these to a discrete attack on the entire spectrum of geometric problems appearing in the CQC literature. Among the new insights that appear in our approach are explicit relative measures for counting the numbers of unentangled, partially entangled, and maximally entangled states, along with the dependence of these measures on the size of the chosen discrete fields. All of this structure is concealed by the infinite precision of real numbers in CQC, and thus the discrete methods provide ways of understanding the resources of quantum computing and isolating the relations between resources and problem size that cannot be studied in any other fashion. These are significant new results, whose ultimate implications cannot be trivially predicted.

This work is given impetus by the fact that the great majority of the laws of physics are formulated as equalities (more appropriately, as isomorphisms) between different physical observables. For instance, Newton's second law of classical mechanics equates the force acting on a system to its rate of change of momentum. Another type of law is the second law of thermodynamics, which asserts that the entropy of a system increases as the system evolves in time, with a corresponding mathematical formulation in terms of an inequality. It is certainly appealing to relate the laws of physics described in this way to computational algorithms. However, an important observation is that the laws of physics are in general implicitly formulated in terms of uncomputable numbers. We therefore concern ourselves with the issue of whether conventional quantum mechanics is physical, or whether perhaps extremely large discrete quantum theories that contain only computable numbers are at the heart of our physical universe. Imagining that physical laws might ultimately require computable numbers provides a compelling motivation for the research program in DQC to which this paper is devoted.

Of specific relevance to our topic is the fact that the title of Turing's seminal 1937 paper [4] was 'On Computable Numbers…'. The idea of computable numbers is of foundational significance in computer science and has had a significant impact on logic. However, despite arguments and challenges noted by prominent researchers [5–7], most mathematical models depend completely on uncomputable numbers, that is, the continuum of real (or complex) numbers; the mathematical framework of conventional quantum mechanics is based on Hilbert spaces, which have uncomputable numbers as their underlying field. In the words of Landauer [8],

> … the real world is unlikely to supply us with unlimited memory of unlimited Turing machine tapes. Therefore, continuum mathematics is not executable, and physical laws which invoke that cannot really be satisfactory …

Here we explore a further plausible principle of quantum computing—the hypothesis that, because of the finiteness of resources in the universe, the domain of physical computation (thus including quantum mechanics) could be restricted to computable numbers and finite fields.

When we began this research program some years ago, our starting point, like that of Schumacher and Westmoreland [9], was to investigate the properties of a version of quantum mechanics obtained by instantiating the mathematical framework of Hilbert spaces with the smallest finite field of Booleans instead of the field of complex numbers. That 'toy model' was called *modal quantum mechanics* by Schumacher and Westmoreland. Our first result [10] was to explicate the associated model of computing as a conventional classical model of relational programming with one twist that is responsible for all the 'quantum-ness'. More precisely, we isolated the 'quantum-ness' in the model in one operation: that of merging sets of answers computed by several alternative choices in the relational program. In the classical world, the answers are merged using a plain union; in modal quantum computing, the answers are merged using the *exclusive union*, which is responsible for creating quantum-like interference effects.

Despite the initial expectations that modal quantum computing would be a 'toy' version of CQC, we showed—in a surprising development—that modal quantum computing exhibited *supernatural* computational power. More precisely, we showed that the `UNIQUE-SAT` problem (the question of deciding whether a given Boolean formula has a satisfying assignment, assuming that it has at most one such assignment) can be solved *deterministically* and in a *constant number of black box evaluations* in modal quantum computing. We traced this supernatural power to the fact that general finite fields lack the geometrical structure necessary to define unitary transformations, and proposed instead the framework of *discrete quantum theory* [11]. This framework is based on complexified Galois fields (see, for example, [3]) with characteristic $p = 4\ell + 3$ for ℓ a non-negative integer (i.e., $p \equiv 3(mod 4)$)), which recover enough geometric structure to define orthogonality and hence allow the definition of Hermitian dot products and unitary transformations.

Discrete quantum theories eliminate the particular supernatural algorithm for `UNIQUE-SAT`. They however still allow subtle supernatural algorithms that depend on the precise relation of the characteristic of the field p and the number of qubits used in the calculation. In particular, we were able to show that supernatural behavior can happen in versions of `UNIQUE-SAT` for a database of size N if the characteristic p of the field divides $(2^N - 1)$ [11].

This paper explores the notions above in detail from first principles. We will focus our attention on the specific challenge that confronts any attempt to build an n-qubit quantum computing structure based on the classical mathematical domain of *finite fields*, and particularly on the shift in the concepts of geometry as one transitions from the continuous case (CQC) to the discrete case (DQC). The fundamental mathematical structure that we shall refer to throughout is the finite field $\mathbf{F}_{p^r}$, where p is a prime number, with some possible restrictions, and $r \geqslant 1$ is an integer. We shall see below that $\mathbf{F}_{p^2}$ in particular will give us a precise discrete analogue to the continuous complex probability amplitude coefficients of conventional n-qubit quantum states.

Our task is then to extract some minimal subset of the familiar geometric properties of CQC in the context of the unfamiliar geometric properties of DQC. It does not take long to discover a litany of issues such as the following.

- *CQC is based on continuous (typically uncomputable) complex state coefficients* in the complex number field $\mathbb{C}$, whose absolute squares are continuous (typically uncomputable) real probabilities in $\mathbb{R}$ that are *ordered*: one can always answer the question asking whether one probability is greater than another. In DQC, we still have (a discrete version of) complex numbers in $\mathbf{F}_{p^2}$, and their absolute squares still have real values in $\mathbf{F}_p$; however, in $\mathbf{F}_p$, there is no transitive *order*—all real values repeat modulo p, and, without additional structure, we cannot, *even in principle*, tell what the ordering should be (e.g., for $p = 3$, the label set $\{-1, 0, 1\}$ is just as good as $\{0, 1, 2\}$). There are ways to label 'positives' and 'negatives' in the finite field $\mathbf{F}_p$, and ways to assign ordered local neighborhoods under certain restrictive conditions, but we still have no consistent way to order the numbers in an entire field.
- *In CQC there is no distinction between geometric proximity of vectors and probability of closeness.* The calculation for the two concepts is the same. In DQC, there is no notion of closeness of vectors that can be computed by inner products or probabilities, although there are deep geometric structures on discrete lattices. One of our challenges is therefore to tease out some meaning from this geometry despite its failure to support the expected properties of such common operations as inner products that are compatible with our intuitions from real continuous geometry.
- *In ordinary real and complex geometry, we have continuous notions of trigonometry.* Additional notions implying continuous geometry for ordinary number fields include linear equations whose solutions are continuous lines, quadratic equations whose solutions are manifolds such as spheres, and continuous-valued measurable quantities such as lengths of line segments, areas of triangles, volumes of tetrahedra, etc. In a discrete real or complex lattice corresponding to $\mathbf{F}_p$ or $\mathbf{F}_{p^2}$, analogues of many of these familiar geometric structures exist, but they have unintuitive and unfamiliar properties. We will expand on these geometric structures in a future publication.

We proceed in our exposition first by reviewing the underlying geometry of continuous n-qubit states in CQC, including a discussion of the properties of entanglement. Our next step is to review the often non-trivial technology of real and complex discrete finite fields. Finally, we examine the features of discrete state geometry for n-qubits, including entanglement, as they appear in the context of states with discrete complex 'probability amplitude' coefficients. In particular, we extend the Hopf fibration of CQC (which is the complex projective space $\mathbf{CP}^{2^n-1}$) to a discrete geometry in which the Hopf circle contains $p + 1$ points. The resulting discrete complex projective space $\mathbf{DCP}^{2^n-1}$ has $p^{2^n-1}(p-1)\prod_{k=1}^{n-1}(p^{2^k}+1)$ irreducible states, $p^n(p-1)^n$ of which are unentangled and $p^{n+1}(p-1)(p+1)^{n-1}$ maximally entangled states.

2. Continuous quantum geometry

Conventional quantum computation is described by the following:

(i) $D = 2^n$ orthonormal basis vectors of an n-qubit state,
(ii) the normalized D complex probability amplitude coefficients describing the contribution of each basis vector,
(iii) a set of probability-conserving unitary matrix operators that suffice to describe all required state transformations of a quantum circuit,
(iv) and a measurement framework.

We remark that there are many things that are assumed in CQC, such as the absence of zero norm states for non-zero vectors, and the decomposition of complex amplitudes into a pair of ordinary real numbers. One also typically assumes the existence of a Hilbert space with an orthonormal basis, allowing us to write n-qubit *pure* states in general as Hilbert space vectors with an Hermitian inner product:

$$|\Psi\rangle = \sum_{i=0}^{D-1} \alpha_i |i\rangle. \tag{1}$$

Here $\alpha_i \in \mathbb{C}$ are complex probability amplitudes, $\vec{\alpha} \in \mathbb{C}^D$, and the $\{|i\rangle\}$ is an orthonormal basis of states obeying

$$\langle i|k\rangle = \delta_{ik}. \tag{2}$$

The meaning of this is that any state $|\Phi\rangle = \sum_{i=0}^{D-1} \beta_i |i\rangle$ can be projected onto another state $|\Psi\rangle$ by writing

$$\langle \Phi|\Psi\rangle = \sum_{i=0}^{D-1} \beta_i^* \alpha_i, \tag{3}$$

thus quantifying the proximity of the two states. (Here * denotes complex conjugation.) This is one of many properties we take for granted in continuum quantum mechanics that challenge us in defining a discrete quantum geometry.

In this paper, we focus on the discrete geometric issues raised by the properties (i) and (ii) given above for CQC, and leave for another time the important issues of (iii), (iv), and such conundrums as probabilities, zero norms, and dynamics in the theory of DQC.

To facilitate the transition to DQC carried out in later sections, we concern ourselves first with the properties of the simplest possible abstract state object in CQC, the single qubit state.

2.1. The single qubit problem

A single qubit already provides access to a wealth of geometric information and context. We write the single qubit state as

$$|\psi_1\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle \quad \alpha_0, \alpha_1 \in \mathbb{C}. \tag{4}$$

A convenience for probability calculations and a necessity for computing relative state properties is the normalization condition

$$\|\psi_1\|^2 = |\alpha_0|^2 + |\alpha_1|^2 = \alpha_0^*\alpha_0 + \alpha_1^*\alpha_1 = 1, \tag{5}$$

which identifies α_0 and α_1 as (complex) probability amplitudes and implies the conservation of probability in the closed world spanned by $\{|0\rangle, |1\rangle\}$. Note that we distinguish for future use the *norm* $\|\cdot\|$ of a vector from the *modulus* $|\cdot|$ of a complex number. Continuing, we see that if we want only the irreducible state descriptions, we must supplement the process of computing equation (5) by finding a way to remove the distinction between states that differ only by an overall phase transformation $e^{i\phi}$, that is,

$$(\alpha_0, \alpha_1) \sim (e^{i\phi}\alpha_0, e^{i\phi}\alpha_1). \tag{6}$$

This can be accomplished by the Hopf fibration, which we can write down as follows: let

$$\alpha_0 = x_0 + iy_0, \quad \alpha_1 = x_1 + iy_1. \tag{7}$$

Then equation (5) becomes the condition that the four real variables describing a qubit denote a point on the three-sphere $\mathbf{S}^3$ (a 3-manifold) embedded in $\mathbb{R}^4$:

$$x_0^2 + y_0^2 + x_1^2 + y_1^2 = 1. \tag{8}$$

There is a family of six equivalence classes of quadratic maps that take the remaining three degrees of freedom in equation (8) and reduce them to two degrees of freedom by effectively removing $e^{i\phi}$ ('fibering out by the circle $\mathbf{S}^1$'). The standard form of this class of maps ('the Hopf fibration') is

$$\begin{aligned} X &= 2\,\mathrm{Re}\, \alpha_0\alpha_1^* = 2x_0x_1 + 2y_0y_1 \\ Y &= 2\,\mathrm{Im}\, \alpha_0\alpha_1^* = 2x_1y_0 - 2x_0y_1 \\ Z &= |\alpha_0|^2 - |\alpha_1|^2 = x_0^2 + y_0^2 - x_1^2 - y_1^2. \end{aligned} \tag{9}$$

These transformed coordinates obey

$$\|\mathbf{X}\|^2 = X^2 + Y^2 + Z^2 = (|\alpha_0|^2 + |\alpha_1|^2)^2 = 1 \tag{10}$$

and therefore have only two remaining degrees of freedom describing all possible distinct one-qubit quantum states. In figure 1 we illustrate schematically the family of circles *each one of which is collapsed to a point* (θ, ϕ) on the surface $X^2 + Y^2 + Z^2 = 1$ by the Hopf map.

The resulting manifold is the 2-sphere $\mathbf{S}^2$ (a 2-manifold) embedded in $\mathbb{R}^3$. If we choose one of many possible coordinate systems describing $\mathbf{S}^3$ via equation (8) such as

$$(x_0, y_0, x_1, y_1) = \left(\cos\frac{\theta+\phi}{2}\cos\frac{\psi}{2},\ \sin\frac{\theta+\phi}{2}\cos\frac{\psi}{2},\ \cos\frac{\theta-\phi}{2}\sin\frac{\psi}{2},\ \sin\frac{\theta-\phi}{2}\sin\frac{\psi}{2}\right), \tag{11}$$

where $0 \leqslant \psi \leqslant \pi$, with $0 \leqslant \frac{\theta+\phi}{2} < 2\pi$ and $0 \leqslant \frac{\theta-\phi}{2} < 2\pi$, we see that

$$(X, Y, Z) = (\cos\phi\sin\psi,\ \sin\phi\sin\psi,\ \cos\psi). \tag{12}$$

Thus the one-qubit state is independent of θ, and we can choose $\theta = \phi$ without loss of generality, reducing the form of the unique one-qubit states to

$$|\psi_1\rangle = e^{i\phi}\cos\frac{\psi}{2}|0\rangle + \sin\frac{\psi}{2}|1\rangle, \tag{13}$$

and an irreducible state can be represented as a point on a sphere, as shown in figure 2(*a*).

Thus the geometry of a single qubit reduces to transformations among points on $\mathbf{S}^2$, which can be parametrized in an infinite one-parameter family of transformations, one of which is the geodesic or minimal-length transformation. Explicitly, given two one-qubit states denoted by points $\mathbf{a}$ and $\mathbf{b}$ on $\mathbf{S}^2$, the shortest rotation carrying the unit normal $\hat{\mathbf{a}}$ to the unit normal $\hat{\mathbf{b}}$ is the SLERP (spherical linear interpolation)

$$S(\hat{\mathbf{a}}, \hat{\mathbf{b}}, t) = \hat{\mathbf{a}}\,\frac{\sin((1-t)\theta)}{\sin\theta} + \hat{\mathbf{b}}\,\frac{\sin(t\theta)}{\sin\theta}, \tag{14}$$

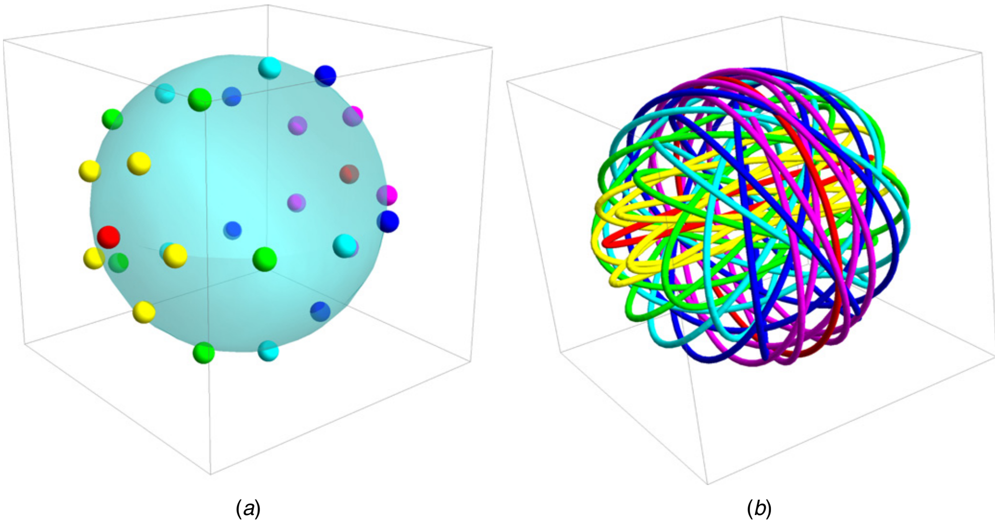

Figure 1. (*a*) The sphere represented by equation (10), which is the irreducible space of one-qubit states, along with a representative set of points on the sphere. (*b*) Representation of the Hopf fibration as a family of circles (the paths of $e^{i\phi}$), each corresponding to a single point on the sphere in (*a*). Points in (*a*) are color coded corresponding to circles in (*b*), e.g., one pole contains the red elliptical circle that would become an infinite-radius circle in a slightly different projection, and the opposite pole corresponds to the large perfectly round red circle at the equator.

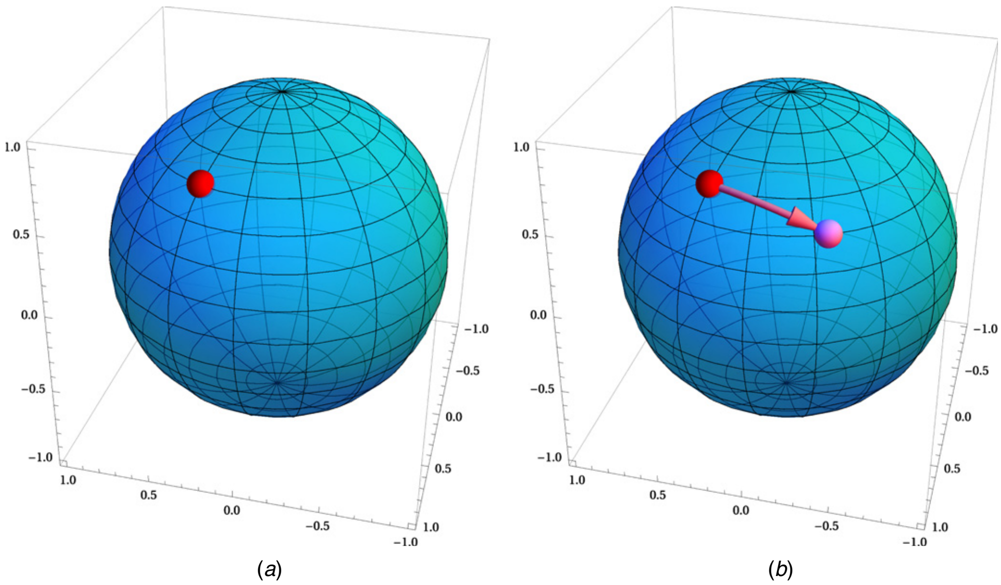

Figure 2. (*a*) The conventional Bloch sphere with a unique state represented by the point at the red sphere. (*b*) The geodesic shortest-distance arc connecting two one-qubit quantum states.

where $\hat{\mathbf{a}} \cdot \hat{\mathbf{b}} = \cos\theta$. Figure 2(*b*) illustrates the path traced by a SLERP between two irreducible one-qubit states on the Bloch sphere. Because states in CQC are defined by infinite precision real numbers, it is not possible, even in principle, to make an exact state transition as implied by figure 2(*b*). In practice, one has to be content with approximate, typically exponentially expensive, transitions from state to state.

2.2. The n-qubit problem

For n qubits, the irreducible states are encoded in a similar family of geometric structures known technically as the complex projective space $\mathbf{CP}^{D-1}$. We obtain these structures starting with the $D = 2^n$ initially unnormalized complex coefficients of the n-qubit state basis

$$|\Psi\rangle = \sum_{i=0}^{D-1} \alpha_i |i\rangle. \tag{15}$$

We then follow the analogue of the one-qubit procedure: conservation of probability requires that the norm of the vector $\vec{\alpha}$ be normalized to unity:

$$\langle\Psi|\Psi\rangle = \|\vec{\alpha}\|^2 = \sum_{i=0}^{D-1} |\alpha_i|^2 = 1. \tag{16}$$

Thus the initial equation for the geometry of a quantum state describes a *topological sphere* $\mathbf{S}^{2D-1}$ embedded in $\mathbb{R}^{2D}$. To see this, remember that we can write the real and imaginary parts of α_i as $\alpha_i = x_i + \mathrm{i}y_i$, so

$$\sum_{i=0}^{D-1} |\alpha_i|^2 = \sum_{i=0}^{D-1} \left({x_i}^2 + {y_i}^2\right) = 1 \tag{17}$$

describes the locus of a $2D$-dimensional real unit vector in $\mathbb{R}^{2D}$, which is by definition $\mathbf{S}^{2D-1}$, the $(2D - 1)$-sphere, with $D = 2^n$ for an n-qubit state.

This $\mathbf{S}^{2D-1}$ in turn is ambiguous up to the usual overall phase, inducing an $\mathbf{S}^1$ symmetry action, and identifying $\mathbf{S}^{2D-1}$ as an $\mathbf{S}^1$ bundle, whose base space is the $(D - 1)$-complex-dimensional projective space $\mathbf{CP}^{D-1}$. There are thus $2D - 2$ irreducible real degrees of freedom ($D - 1$ complex degrees of freedom) for a quantum state with a D-dimensional basis, $\{|i\rangle \mid i = 0, \ldots, D - 1\}$.

In summary, the full space of a $D = 2^n$-dimensional n-qubit quantum state, including its overall phase defining its relationship to other quantum states, is the topological space $\mathbf{S}^{2D-1}$. For an isolated system, the overall phase is not measurable, and eliminating the phase dependence in turn corresponds to identifying $\mathbf{S}^{2D-1}$ as a circle bundle over the base space $\mathbf{CP}^{D-1}$, and therefore $\mathbf{CP}^{D-1} = \mathbf{CP}^{2^n-1}$ defines the $2D - 2$ intrinsic, irreducible, degrees of freedom of the isolated n-qubit state's dynamics. In mathematical notation, this would be written

$$\mathbf{S}^1 \hookrightarrow \mathbf{S}^{2D-1} \to \mathbf{CP}^{D-1},$$

with $D = 2^n$ as usual. For $n = 1$, the single qubit, we have $2^n - 1 = 2 - 1 = 1$, and the base space of the circle bundle is $\mathbf{CP}^1 = \mathbf{S}^2$, the usual Bloch sphere. Note that only for $n = 1$ is this actually a sphere-like geometry due to an accident of low-dimensional topology.

2.3. Explicit n-qubit generalization of the Hopf fibration construction

For one qubit, we could easily solve the problem of reducing the full unit-norm space to its irreducible components $\mathbf{X} = (X, Y, Z)$ characterizing the Bloch sphere. We have just argued that essentially the same process is possible for n-qubits: in the abstract argument, we simply identify the family of coefficients $\{\alpha_i\}$ as being the same if they differ only by an overall phase $\mathrm{e}^{\mathrm{i}\phi}$. However, in practice this is not a construction that is easy to realize in a practical computation. We now outline an explicit algorithm for accomplishing the reduction to the irreducible n-qubit state space $\mathbf{CP}^{D-1}$; this construction will turn out to be useful for the validation of our discrete results to follow below.

We begin by noting that a natural quantity characterizing an n-qubit system is its *density matrix*, $\rho = \left[\alpha_i \alpha_j^*\right]$, or

$$\rho = \begin{bmatrix} |\alpha_0|^2 & \alpha_0\alpha_1^* & \cdots & \alpha_0\alpha_{D-1}^* \\ \alpha_1\alpha_0^* & |\alpha_1|^2 & \cdots & \alpha_1\alpha_{D-1}^* \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{D-1}\alpha_0^* & \cdots & \alpha_{D-1}\alpha_{D-2}^* & |\alpha_{D-1}|^2 \end{bmatrix}. \tag{18}$$

We can now use the complex generalization of the classical Veronese coordinate system for projective geometry to remove the overall phase ambiguity $e^{i\phi}$ from the n-qubit states. If we take a particular weighting of the elements of the density matrix ρ, we can construct a *unit vector* of real dimension D^2 with the form:

$$\mathbf{X} = \left(|\alpha_i|^2, \ldots, \sqrt{2}\,\mathrm{Re}\,\alpha_i\alpha_j^*, \ldots, \sqrt{2}\,\mathrm{Im}\,\alpha_i\alpha_j^*, \ldots\right), \tag{19}$$

where

$$\mathbf{X}\cdot\mathbf{X} = \left(\sum_{i=0}^{D-1} |\alpha_i|^2\right)^2 = 1. \tag{20}$$

This construction gives an explicit embedding of the $(D-1)$-dimensional complex, or $(2D-2) = (2^{n+1}-2)$-dimensional real, object in a real space of dimension $D^2 = 2^{2n}$. However, this is somewhat subtle because the vector is of unit length, so technically the embedding space is a sphere of dimension $D^2 - 1 = 2^{2n} - 1$ embedded in $\mathbb{R}^{D^2}$; the one-qubit irreducible states could be represented in a 4D embedding, but the magnitude of every coordinate would be one; furthermore, the object embedded in the resulting $\mathbf{S}^3$ is indeed $\mathbf{S}^2$ because we can fix one complex coordinate to be unity, and let one vary, giving a total of two irreducible dimensions. In fact one must choose *two* coordinate patches, one covering one pole of $\mathbf{S}^2$ with coordinates

$$\begin{aligned} \alpha_0 &= 1 + 0\mathrm{i} \\ \alpha_1 &= x_1 + \mathrm{i}y_1 \end{aligned} \tag{21}$$

and the other patch covering the other pole of $\mathbf{S}^2$ with coordinates

$$\begin{aligned} \alpha_0 &= x_0 + \mathrm{i}y_0 \\ \alpha_1 &= 1 + 0\mathrm{i}. \end{aligned} \tag{22}$$

We finally see that the irreducible n-qubit state space $\mathbf{CP}^{D-1}$ is described by D projectively equivalent coordinates, one of which can always be scaled out to leave $(D-1)$ actual (complex) degrees of freedom. We must choose, in turn, D different local sets of complex variables defined by taking the value $\alpha_k = 1$, with $k = 0, \ldots, D-1$, and allowing the remaining $D-1$ complex (or $2D-2$ real) variables to run free. No single set of coordinates will work, since the submanifold including $\alpha_k = 0$ is undefined and another coordinate system must be chosen to cover that coordinate patch. This is a standard feature of the topology of non-trivial manifolds such as $\mathbf{CP}^{D-1}$ (see any textbook on geometry [12]).

2.4. The geometry of entanglement

Entanglement may be regarded as one of the main characteristics distinguishing quantum from classical mechanics. Entanglement involves quantum correlations such that the measurement outcomes in one subsystem are related to the measurement outcomes in another one. Within the standard framework, given a quantum system composed of n qubit subsystems, a pure state of the total system $|\Psi\rangle$ is said to be entangled if it cannot be written as a product of states of each subsystem. That is, a state $|\Psi\rangle$ is entangled if

$$|\Psi\rangle \neq |\psi_1\rangle \otimes \cdots \otimes |\psi_j\rangle \otimes \cdots \otimes |\psi_n\rangle, \tag{23}$$

where $|\psi_j\rangle$ refers to an arbitrary state of the jth qubit, and $\otimes$ represents the tensor product. This is equivalent to saying that if one calculates the reduced density operator ρ_j of the jth subsystem by tracing out all the other subsystems, $\rho_j = \mathrm{tr}_{\{1,\ldots,j-1,j+1,\ldots,n\}}(\rho)$, with $j = 1, \ldots, n$ and $\rho = |\Psi\rangle\langle\Psi|$, the normalized state $|\Psi\rangle$, $\langle\Psi|\Psi\rangle = 1$, is entangled if and only if at least one subsystem state is *mixed*; i.e., $\mathrm{tr}_j\big(\rho_j^2\big) < 1$. For example, consider

$$\rho_j = \frac{1}{2}\left(\mathbb{1} + \sum_{\mu=x,y,z} \langle\sigma_\mu^j\rangle\, \sigma_\mu^j\right), \tag{24}$$

where σ_μ^j, $\mu = x, y, z$, are the Pauli operators acting on the jth spin,

$$\sigma_\mu^j = \overbrace{\mathbb{1} \otimes \mathbb{1} \otimes \cdots \otimes \underbrace{\quad\sigma_\mu\quad}_{j\text{th factor}} \otimes \cdots \otimes \mathbb{1}}^{n\text{ factors}}, \tag{25}$$

with

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \sigma_y = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}, \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{26}$$

and $\langle\sigma_\mu^j\rangle = \langle\Psi|\sigma_\mu^j|\Psi\rangle$ denotes the corresponding expectation value. The vectors $\mathbf{X}_j = (\langle\sigma_x^j\rangle, \langle\sigma_y^j\rangle, \langle\sigma_y^j\rangle)$, $\mathbf{X}_j \in \mathbb{R}^3$, allow a geometric representation of each reduced state in $\mathbb{R}^3$, satisfying $0 \leqslant \|\mathbf{X}_j\| \leqslant 1$. Since $\mathrm{tr}_j\big(\rho_j^2\big) = \frac{1}{2}(1+\|\mathbf{X}_j\|^2)$, the state $|\Psi\rangle$ is entangled if $\|\mathbf{X}_j\| < 1$ for at least one j, represented by a point *inside* the corresponding local Bloch sphere. One may therefore consider $|\Psi\rangle$ to be maximally entangled if $\|\mathbf{X}_j\| = 0$ for all j. On the other hand, the state $|\Psi\rangle$ is unentangled (i.e., a product state) if $\|\mathbf{X}_j\| = 1$ for all j, corresponding to points lying on the surface of the Bloch sphere.

A natural geometric measure of multipartite entanglement is obtained by defining the *purity of a state relative to a set of observables* [15, 16]. If the set is chosen to be the set of *all local observables*, i.e., corresponding to each of the subsystems that compose the actual system, one recovers the standard notion of entanglement for multipartite systems. For example, if the system consists of n qubits, we obtain a measure of conventional entanglement by calculating the purity relative to the set $\mathfrak{h} = \{\sigma_x^1, \sigma_y^1, \sigma_z^1, \ldots, \sigma_x^n, \sigma_y^n, \sigma_z^n\}$,

$$P_{\mathfrak{h}} = \frac{1}{n}\sum_{j=1}^{n}\sum_{\mu=x,y,z} \langle\sigma_\mu^j\rangle^2, \quad 0 \leqslant P_{\mathfrak{h}} \leqslant 1. \tag{27}$$

Since $\mathfrak{h}$ is a semi-simple Lie algebra, its generalized unentangled states are the generalized coherent states obtained by applying any group operation to a reference state such as $|\mathsf{0}\rangle = |0\rangle \otimes \cdots \otimes |0\rangle$. For the algebra $\mathfrak{h}$ of local observables, such group operations are simply local rotations on each qubit. In other words, the group orbit describing the generalized coherent states of $\mathfrak{h}$ comprises all the product states of the form $|\Psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$, which have maximum purity (i.e., $P_{\mathfrak{h}} = 1$). Other states such as the Greenberger–Horne–Zeilinger state $|\Psi\rangle = |\mathsf{GHZ}_n\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes \cdots \otimes |0\rangle + |1\rangle \otimes \cdots \otimes |1\rangle)$ are (maximally) entangled relative to the set of local observables (i.e., $P_{\mathfrak{h}} = 0$).

Different entanglement measures are obtained when a set $\mathfrak{h}$ different from the local observables is chosen. An obvious example, in particular, is given by the set of all observables.

In this case, the purity takes its maximum value independently of the pure quantum state [15, 16], expressing the fact that any state is a generalized coherent state of the Lie algebra of all observables.

3. Vector spaces over complexified finite fields

In order to address the intrinsic problems induced by the notion of the continuum calculations of the previous section, one is led to replace the infinite fields of CQC by discrete computable fields. Accomplishing this while maintaining the essential elements of addition and multiplication requires a brief excursion into the theory of fields, and particularly the theory of finite fields.

3.1. Background

Abstract algebra deals with various kinds of algebraic structures, such as groups, rings, and fields, each defined by a different system of axioms. A field $\mathbf{F}$ is an algebraic structure consisting of a set of elements equipped with the operations of addition, subtraction, multiplication, and division [13]. Fields may contain an infinite or a finite number of elements. The rational $\mathbb{Q}$, real $\mathbb{R}$, and complex numbers $\mathbb{C}$ are examples of infinite fields, while the set $\mathbf{F}_3 = \{0, 1, 2\}$ under the usual multiplication and modular addition is an example of a finite field. Finite fields are also known as Galois fields [14].

There are two distinguished elements in a field, the addition identity 0, and the multiplication identity 1. Given the field $\mathbf{F}$, the closed operations of addition, '$+$', and multiplication, '$*$', satisfy the following set of axioms.

(i) $\mathbf{F}$ is an Abelian group under the addition operation $+$ (additive group).
(ii) The multiplication operation $*$ is associative and commutative. The field has a multiplicative identity and the property that every nonzero element has a multiplicative inverse.
(iii) Distributive laws: for all $a, b, c \in \mathbf{F}$

$$a * (b + c) = a * b + a * c \tag{28}$$

$$(b + c) * a = b * a + c * a. \tag{29}$$

From now on, unless specified, we will omit the symbol $*$ whenever we multiply two elements of a field.

Finite fields of q elements, $\mathbf{F}_q = \{0, \ldots, q-1\}$, will play a special role in this work. A simple explicit example is the following addition and multiplication tables for $\mathbf{F}_3$:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$*$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

3.2. Cyclic properties of finite fields

Finite fields are classified by size. The characteristic of a field is the least positive integer m such that $m = 1 + 1 + 1 + \cdots + 1 \equiv 0$, and if no such m exists we say that the field has characteristic zero (which is the case for infinite fields such as $\mathbb{R}$). It turns out that if the characteristic is non-zero it must be a prime p. For every prime p and positive integer r there is a finite field $\mathbf{F}_{p^r}$ of cardinality $q = p^r$ and characteristic p (Lagrange's theorem), which is unique up to field isomorphisms. For every $a \in \mathbf{F}_q$, $a \neq 0$, then $a^{q-1} = 1$, implying the Frobenius endomorphism (also a consequence of Fermat's little theorem) $a^q = a$, which in turn permits us to write the multiplicative inverse of any non-zero element in the field as $a^{-1} = a^{q-2}$, since $a^{q-2}a = a^{q-1} = 1$. Every subfield of the field $\mathbf{F}_q$, of cardinality $q = p^r$, has $p^{r'}$ elements with some r' dividing r, and for a given r' it is unique. Notice that a fundamental difference between finite and infinite fields is one of topology: finite fields induce a compact structure because of their modular arithmetic, permitting *wrapping around*, while that is not the case for fields of characteristic zero. This feature may lead to fundamental physical consequences.

3.3. Complexified finite fields

Consider the polynomial $x^2 + 1 = 0$ over a finite field $\mathbf{F}_p$. It is known that this polynomial does not have solutions in the field precisely when the prime p is congruent to $3(mod 4)$ (see, e.g., [13]).

For such primes, it is therefore possible to construct an extended field $\mathbf{F}_{p^2}$ whose elements are of the form $\alpha = a + \mathrm{i}b$ with $a \in \mathbf{F}_p$, $b \in \mathbf{F}_p$, and i the root of the polynomial $x^2 + 1 = 0$. Since the field elements $a + \mathrm{i}b$ behave like discrete versions of the complex numbers, we will refer to fields $\mathbf{F}_p$ with prime p congruent to $3(mod 4)$ as *complexifiable finite fields*, and i-extended fields $\mathbf{F}_{p^2}$ with p congruent to $3(mod 4)$ as *complexified finite fields*.

In a complexified finite field $\mathbf{F}_{p^2}$, the Frobenius automorphism that maps $\alpha \in \mathbf{F}_{p^2}$ to $\alpha^p \in \mathbf{F}_{p^2}$ acts like complex conjugation. For example, in $\mathbf{F}_{3^2}$, we have $(2 + \mathrm{i})^3 = 8 + 12\mathrm{i} - 6 - \mathrm{i} = 2 + 11\mathrm{i}$ which, in the field, is equal to $2 - \mathrm{i}$ since $11 \equiv -1(mod 3)$.

We define the *field norm* $\mathsf{N}(\cdot)$ as the map from $(a + \mathrm{i}b) \in \mathbf{F}_{p^2}$ to $a^2 + b^2 \in \mathbf{F}_p$,

$$\mathsf{N}(\alpha = a + \mathrm{i}b) = a^2 + b^2. \tag{30}$$

We avoid the square root in the discrete field framework because, unlike the continuous case, the square root does not always exist.

3.4. Vector spaces

In this section we want to build a theory of discrete vector spaces that approximates as closely as possible the features of conventional quantum theory. Such a structure would ideally consist of the following: (i) a vector space over the field of complex numbers, and (ii) an inner product $\langle\Phi|\Psi\rangle$ associating to each pair of vectors a complex number, and satisfying the following properties:

(A) $\langle\Phi|\Psi\rangle$ is the complex conjugate of $\langle\Psi|\Phi\rangle$;
(B) $\langle\Phi|\Psi\rangle$ is conjugate linear in its first argument and linear in its second argument;
(C) $\langle\Psi|\Psi\rangle$ is always non-negative and is equal to 0 only if $|\Psi\rangle$ is the zero vector.

It turns out that a vector space defined over a finite field cannot have an inner product satisfying the properties above. However, we will introduce an Hermitian 'dot product' satisfying some of those properties.

We are interested in the n-qubit vector space $\mathcal{H}$ of dimension $D = 2^n$ defined over the complexified field $\mathbf{F}_{p^2}$. Let $|\Psi\rangle = (\alpha_0\alpha_1 \ldots \alpha_{D-1})^T$ and $|\Phi\rangle = (\beta_0\beta_1 \ldots \beta_{D-1})^T$ represent vectors in $\mathcal{H}$, with numbers α_i and β_i drawn from $\mathbf{F}_{p^2}$, and where $(\cdot)^T$ is the transpose.

Definition 3.1 (Hermitian dot product)**.** *Given vectors $|\Phi\rangle$ and $|\Psi\rangle \in \mathcal{H}$, the Hermitian dot product of these vectors is:*

$$\langle\Phi|\Psi\rangle = \sum_{i=0}^{D-1} \beta_i^p \alpha_i. \tag{31}$$

Two vectors $|\Phi\rangle$ and $|\Psi\rangle \in \mathcal{H}$ are said to be orthogonal if $\langle\Phi|\Psi\rangle = 0$. This product satisfies conditions A and B for inner products but violates condition C since in every finite field there always exists a non-zero vector $|\Psi\rangle$ such that $\langle\Psi|\Psi\rangle = 0$. The reason is that addition in finite fields eventually 'wraps around' (because of their cyclic or modular structure), allowing the sum of non-zero elements to be zero. The fraction of non-zero vectors satisfying $\langle\Psi|\Psi\rangle = 0$ decreases with the order p.

For any vector $|\Psi\rangle = (\alpha_0\alpha_1 \ldots \alpha_{D-1})^T$, the Hermitian dot product $\langle\Psi|\Psi\rangle$ is equal to $\sum_{i=0}^{D-1} \mathsf{N}(\alpha_i)$, which is the sum of the field norms for the complex coefficients. For convenience, we now extend the field norm to include vector arguments by defining

$$\mathsf{N}(|\Psi\rangle) = \langle\Psi|\Psi\rangle = \sum_{i=0}^{D-1} \mathsf{N}(\alpha_i). \tag{32}$$

The field norm of a vector can vanish for non-vanishing vectors.

For vectors $|\Psi\rangle$ such that $\langle\Psi|\Psi\rangle = \sum_{i=0}^{D-1} \alpha_i^p \alpha_i = \sum_{i=0}^{D-1} \alpha_i^{p+1} = \sum_{i=0}^{D-1} |\alpha_i|^2$ has a square root in the field, one can define the following 'norm':

$$||\Psi|| = \sqrt{\langle\Psi|\Psi\rangle}, \tag{33}$$

which is valid only on a subspace of the field norm for finite fields.

4. Irreducible discrete *n*-qubit states: generalized discrete Bloch sphere

In the one-qubit state with coefficients in $\mathbf{F}_{p^2}$, the discrete analogue of the Bloch sphere is constructed by exact analogy to the continuous case: we first require that the coefficients of the single qubit basis obey

$$\|\psi_1\|^2 = |\alpha_0|^2 + |\alpha_1|^2 = 1 \tag{34}$$

in the discrete field. In section A.2 in the appendix, we show that there are $p(p^2 - 1)$ such values. Given this requirement, which is similar in form to the conservation of probability, but not as useful due to the lack of orderable probability values, we can immediately conclude that the discrete analogue of the Hopf fibration is again

$$\begin{aligned} X &= 2\,\mathrm{Re}\,\alpha_0\alpha_1^* = 2x_0x_1 + 2y_0y_1 \\ Y &= 2\,\mathrm{Im}\,\alpha_0\alpha_1^* = 2x_1y_0 - 2x_0y_1 \\ Z &= |\alpha_0|^2 - |\alpha_1|^2 = x_0^2 + y_0^2 - x_1^2 - y_1^2, \end{aligned} \tag{35}$$

but now with all computations in $(mod\, p)$. At this point one simply writes down all possible discrete values for the complex numbers $\{\alpha_0, \alpha_1\}$ satisfying equation (34) and enumerates those that project to the same value of $\{X, Y, Z\}$. This equivalence class is the discrete analogue of the circle in the complex plane that was eliminated in the continuous case. In section A.1 in the appendix, we show that $p + 1$ discrete values of $\{\alpha_0, \alpha_1\}$ with unit norm map to the same point under the Hopf map equation (35); we may think of these as discrete circles or projective lines of equivalent, physically indistinguishable, complex phase. The surviving $p(p - 1)$ values of $\{\alpha_0, \alpha_1\}$ correspond to irreducible physical states of the discrete single qubit system. Thus, for example, choosing the underlying field to be $\mathbf{F}_{3^2}$, there are exactly six single-qubit state vectors to populate the Bloch sphere; the four equivalent phase-multiples mapping to each of the six points on the $\mathbf{F}_{3^2}$ Bloch sphere are collapsed and regarded as physically indistinguishable. In figure 3, we plot the irreducible states on the Bloch sphere for $p = 3$, 7, and 11. Note that the Cartesian lengths of the real vectors corresponding to the points on the Bloch sphere vary considerably due to the nature of discrete fields; we have artificially normalized them to a 'continuous world' unit radius sphere for conceptual clarity.

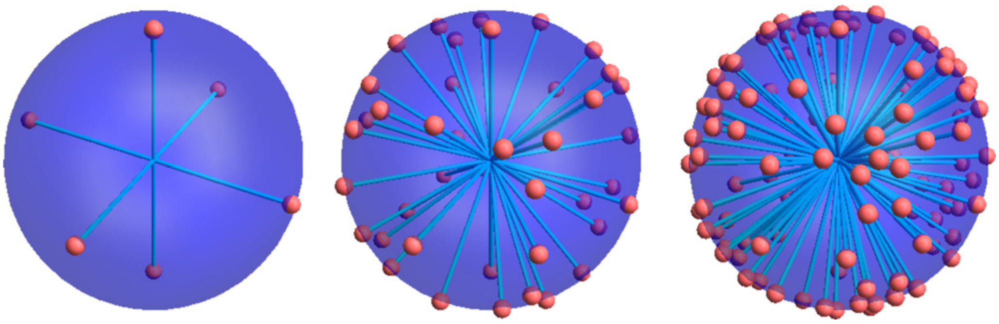

Figure 3. Schematically normalized plots of the elements of the discrete Bloch sphere, the irreducible single-qubit (two-dimensional) state vectors with unit norm over the field $\mathbf{F}_{p^2}$. We show the results for $p = 3$, 7, and 11. For example, in $\mathbf{F}_{3^2}$, there are 24 vectors of unit norm, but only the 6 inequivalent classes appear in the plot. The $p + 1 = 4$ equivalent vectors in each class differ only by a complex discrete phase.

4.1. Counting states on the n-qubit Bloch sphere

We have the unique opportunity in the finite-field approach to quantum computing to precisely identify and enumerate the physical states. In the conventional theory, as we have seen, we employ a generalized Hopf fibration on the normalized states to project out a circle of phase-equivalent states, yielding the generalized Bloch sphere.

In the introduction to this section, we sketched the counting of the irreducible single-qubit discrete states. To count the number of inequivalent discrete states for the general n-qubit case with coefficients in $\mathbf{F}_{p^2}$, we first must find the set of unit-norm states, and then determine the equivalence classes of unit-norm states under discrete phase transformations; we can then enumerate the list of states on the discrete generalized Bloch sphere. By executing computer searches of these spaces, we discovered an hypothesis for a closed-form solution for the counting of the states, and were then able to find a rigorous inductive proof of the enumeration, which is presented in the appendix.

This process of describing the discrete n-qubit irreducible states can again be understood geometrically by following the discrete analogue of the Hopf fibration. First, we construct the discrete version of the quadratic unit-length form that automatically annihilates the distinction among states differing only by a discrete phase,

$$\mathbf{X} = \left(|\alpha_i|^2, \ldots, \sqrt{2}\,\mathrm{Re}\,\alpha_i\alpha_j^*, \ldots, \sqrt{2}\,\mathrm{Im}\,\alpha_i\alpha_j^*, \ldots\right), \tag{36}$$

where

$$\mathbf{X}\cdot\mathbf{X} = \left(\sum_{i=0}^{D-1}|\alpha_i|^2\right)^2 = 1. \tag{37}$$

From section A.1 in the appendix, we know that $p + 1$ elements of this discrete $\mathbf{S}^{2\times 2^n-1}$ structure map to the *same point* in $\mathbf{X}$. Each set of $(p + 1)$ redundant points is, geometrically speaking, the *discrete Hopf fibration circle* living above each *irreducible* point of the n-qubit state description. These $p+1$ points are interpretable as the p finite points plus the single point at infinity of the projective discrete line (see, e.g., [3]).

The next part of this argument is the determination of the unit-norm states, effectively the space of allowed discrete partitions of unity; we cannot exactly call these ‘probability-conserving’ sectors of the state coefficients since we do not have a well defined notion of probability, but we do have a well-defined notion of partition of unity. The tally of unit-norm states is $p^{2^n-1}(p^{2^n}-1)$ (see section A.2 in the appendix) compared to the total number $p^{2\times 2^n}$ of possible complex integer state vectors that could be chosen. This unit-norm state structure is the discrete analogue of $\mathbf{S}^{2\times 2^n-1}$.

Finally, we repeat the last step of the n-qubit continuous Hopf fibration process for discrete n-qubit states, eliminating the discrete set of $p+1$ equivalent points that map to the same point $\mathbf{X}$ on the generalized n-qubit Bloch sphere. Dividing the tally $p^{2^n-1}(p^{2^n}-1)$ of unit norm states by the $p+1$ elements of each phase-equivalent discrete circle, we find

$$\frac{p^{2^n-1}(p^{2^n}-1)}{p+1} = p^{2^n-1}(p-1)\prod_{k=1}^{n-1}(p^{2^k}+1)$$

as the total count of unique irreducible states in a discrete n-qubit configuration (see section A.3 in the appendix). The resulting object is precisely the discrete version of $\mathbf{CP}^{D-1}$, which we might call a *discrete complex projective space* or $\mathbf{DCP}^{D-1}$, where $D=2^n$ as usual.

5. Geometry of entangled states

Without regard to uniqueness, an n-qubit state with discrete complex coefficients in $\mathbf{F}_{p^2}$ will have the total possible space of coefficients with dimension $p^{2\times 2^n}$ (including the null state). Imposing the condition of a length-one norm in $\mathbf{F}_p$, this number is reduced to $p^{2^n-1}(p^{2^n}-1)$. The ratio of all the states to the unit-norm states is asymptotically p:

$$\frac{p^{2^n+1}}{p^{2^n}-1} \to p, \tag{38}$$

so there are roughly p sets of coefficients, for any number of qubits n, that are discarded for each retained unit-length state vector. A factor of $p+1$ more states are discarded in forming the discrete Bloch sphere of irreducible states. Selected plots of the full space compared to both the unit-norm space and the irreducible space for a selection of complexified finite fields are shown in figure 4 for one, two, three, and four qubits.

5.1. Unentangled versus entangled discrete states

For a given p and the corresponding complexified field $\mathbf{F}_{p^2}$, the n-qubit discrete quantum states with coefficients in $\mathbf{F}_{p^2}$ can be classified by their degree of entanglement to a level of precision that is unavailable in the continuous theory. We look first at the unentangled n-qubit states, which are direct product states of the form

$$|\Psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_j\rangle \otimes \cdots \otimes |\psi_n\rangle. \tag{39}$$

Without regard to normalization, there are $(p^4)^n$ possible unentangled states out of the total of $p^{2\times 2^n}$ states noted above. When we normalize the individual product states to unit norm, the norm of the entire n-qubit state becomes the product of those unit norms, and is automatically normalized to one. We have already seen that each single-qubit normalized state in the tensor product equation (39) has precisely $p(p-1)$ irreducible components.

5.2. Completely unentangled states and the discrete Bloch sphere

In effect, the irreducible states for unentangled n-qubit configurations reduce to a single Bloch sphere for each one-qubit component $|\psi_j\rangle$, and thus the whole set of states is defined by an n-tuple of discrete Bloch sphere coordinates. Since each Bloch sphere in $\mathbf{F}_{p^2}$ has $p(p-1)$ distinct irreducible components, we have

$$\textbf{Count of unentangled states} = p^n(p-1)^n.$$

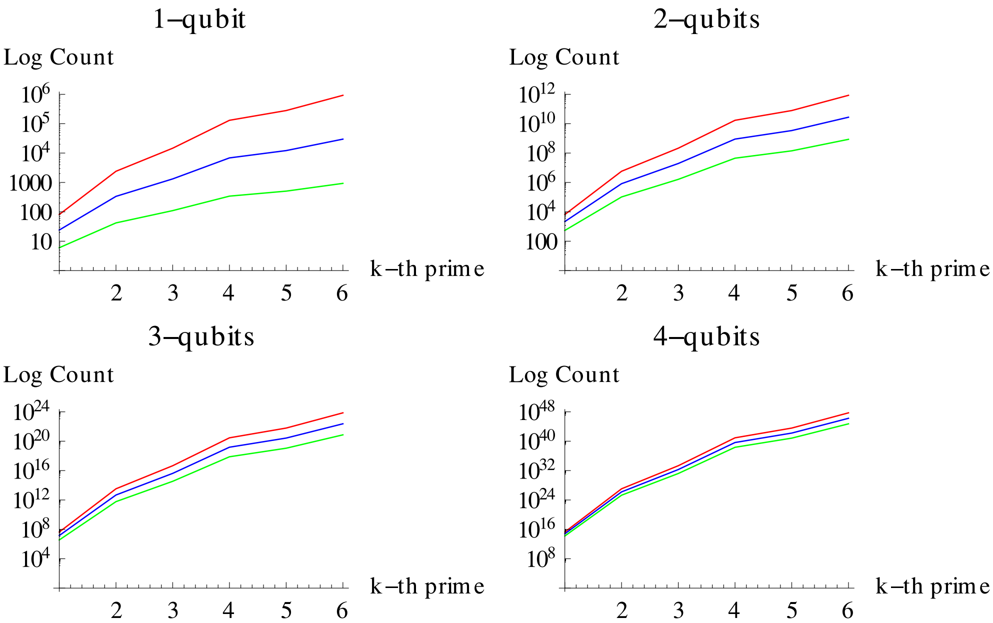

Figure 4. Logarithmic plot of the number of discrete unnormalized states (top, in red), versus the number of normalized discrete states (middle, in blue), versus the irreducible states (bottom, in green) for the first six $\mathbf{F}_{p^2}$-compatible primes, (3, 7, 11, 19, 23, 31), for the number of qubits 1, 2, 3 and 4.

We know that the total number of irreducible states (points in the generalized $\mathbf{DCP}^{2^n-1}$ Bloch sphere) for an n-qubit state is $p^{2^n-1}(p^{2^n}-1)/(p+1)$, and so the number of states containing some measure of entanglement is

$$\textbf{Count of entangled states} = \frac{p^{2^n-1}(p^{2^n}-1)}{p+1} - p^n(p-1)^n.$$

Therefore a very small fraction of the unit norm states are unentangled.

5.3. Partial entanglement

A partially entangled state can be constructed by taking individual component states to enter as direct products, starting by picking n distinct single qubits to be unentangled ($n = 2$ exhausts its freedom with one pick). Then we can choose $n(n-1)/2$ pairs of distinct qubits as product states ($n = 3$ exhausts its freedom with one pick), and so on. Then, starting with $n = 3$, we can pick fully entangled 2-qubit subspaces as product spaces, combining them with single-qubit product components ($n = 3$ has no single-qubit freedom left after picking any of its three 2-qubit subspaces), and so on. Precise measures of entanglement such as that given in equation (27) can then be applied just as in the continuous case.

5.4. Maximal entanglement

Numerical and analytic calculations of the entanglement measure equation (27), taken (mod$p$), extend to the best of our knowledge to the discrete case, so that the unentangled states constructed above have $P_{\mathfrak{h}} = 1$. This leads us to study one final aspect of the discrete n-qubit states, namely the *maximally* entangled states with $P_{\mathfrak{h}} = 0$.

Computing some examples for various n and small values of p, one can verify explicitly that unit-norm unentangled states for $n = 2$, $p = \{3, 7, 11, 19, \ldots\}$ occur with frequency

$$(p+1)p^2(p-1)^2 = \{144, 14\,112, 145\,200, 2339\,280, \ldots\},$$

and for general n, $(p+1)p^n(p-1)^n$.

The irreducible state counts are reduced by $(p+1)$, giving

$$p^2(p-1)^2 = \{36, 1764, 12\,100, 116\,964, \ldots\},$$

and in general for n-qubits, $p^n(p-1)^n$ instances of pure states with $P_\mathfrak{h} = 1$.

Repeating the computation to discover the frequency of maximally entangled (purity $P_\mathfrak{h} = 0$ states), we find $p^{n+1}(p-1)(p+1)^n$ maximally entangled states, with example frequencies for two qubits of

$$p^3(p-1)(p+1)^2 = \{864, 131\,712, 1916\,640, 49\,384\,800, \ldots\}.$$

The irreducible state counts for maximal entanglement are reduced by $(p+1)$, giving for $n = 2$

$$p^3(p^2-1) = \{216, 16\,464, 159\,720, 2469\,240, \ldots\},$$

and in general for n-qubits, $p^{n+1}(p-1)(p+1)^{n-1}$ instances of pure states with $P_\mathfrak{h} = 0$.

Therefore, the ratio of maximally entangled to unentangled states is

$$\textbf{Max entangled/unentangled} = p\left(\frac{p+1}{p-1}\right)^{n-1}.$$

6. Summary

Given a discrete basis for the complex coefficients of an n-qubit quantum state, DQC permits us in principle to explicitly determine the relative frequencies of phases and to determine exactly the generalized Bloch sphere coordinates of the irreducible states. The size of the set of states that must be taken as equivalent to get irreducibility is the size of the ‘circle’ or phase group, and this is $p+1$ for any p and for any n (related to the size of the finite projective line, see [3]). Exploring the discrete manifestation of the purity measure equation (27), our DQC approach can determine not only the size of the irreducible space of states, but also the relative sizes of the unentangled and entangled states for n discrete qubits.

Appendix. Proofs

In this appendix, we prove the state-counting formulas for discrete n-qubit states labeled by a prime p satisfying $p = 4\ell + 3$ for integer $\ell \geqslant 0$. We show that: (1) the number of points on a discrete complex unit circle, (the discrete complex phase equivalence) is $p+1$; (2) the number of unit-length D-dimensional vectors with coefficients in $\mathbf{F}_{p^2}$ is $p^{D-1}(p^D - (-1)^D)$; for n-qubit states, $D = 2^n$ and the result becomes $p^{2^n-1}\left(p^{2^n} - 1\right)$; and (3) the number of irreducible n-qubit states is $p^{2^n-1}(p-1)\prod_{k=1}^{n-1}(p^{2^k}+1)$.

We will carry out an inductive proof starting with an hypothesis for the number of zero-norm D-dimensional vectors suggested by computing representative examples. We will accomplish this by exploring the properties of finite fields using the one-dimensional and n-dimensional field norms over $\mathbf{F}_{p^2}$ defined in equations (30) and (32), that is,

$$\mathsf{N}(\alpha = a + \mathrm{i}b) = a^2 + b^2$$

and

$$\mathsf{N}(\alpha_0, \ldots, \alpha_{D-1}) \equiv \mathsf{N}(D) = \sum_{k=0}^{D-1} \mathsf{N}(\alpha_k),$$

where we will specify real discrete values using roman letters such as (a, b, c) and complex discrete values using Greek letters such as α, which stands for $\alpha = a + \mathrm{i}b$. We carry out the calculations for arbitrary D, and then specialize at the end to the even-D, n-qubit case $D = 2^n$. For additional general background, see, e.g., chapter 6 in [13] and section 18.4 in [14].

A.1. Counting of the quadratic map

Proposition A.1. *The discrete analogue of phase-equivalence under* $z \to \mathrm{e}^{\mathrm{i}\phi}z$ *is a set of* $(p + 1)$ *discrete points* $\alpha \in \mathbf{F}_{p^2}$ *that map to unity in* $\mathbf{F}_p$ *under the action of* $\mathsf{N}(\alpha)$.

Method. *To prove proposition 1, we start by defining a special case of the field norm* $\mathsf{N}(.)$, *namely the real quadratic map* $Q(e) = e^2$ *taking an arbitrary element* $e \in \mathbf{F}_p$ *to its square in the field. We exploit the fact that the image of* $Q(e)$ *has* $(p + 1)/2$ *unique elements in* $\mathbf{F}_p$, *including the zero element; the map* $Q^*(e)$ *excluding the zero element produces* $(p - 1)/2$ *elements (the quadratic residues); the* $(p - 1)/2$ *remaining elements of* $\mathbf{F}_p$ *(the quadratic non-residues) are analogous to negative numbers, having no square roots in the field* $\mathbf{F}_p$.

Proof. We let A be the image of the map $Q(e)$ in $\mathbf{F}_p$, and note that the set A_c resulting from displacing an element $x = b^2$ of A to $c - x = c - b^2$ with $c \in \mathbf{F}_p$ also has $(p + 1)/2$ unique elements because the result is simply a cyclic shift of element labels. We now observe that for any non-zero $c \in \mathbf{F}_p$, the join of the two sets A and A_c has size $p + 1$, which is greater than the size p of $\mathbf{F}_p$, and so there must be at least one common element such that

$$a^2 = c - b^2.$$

Thus some element $c \in \mathbf{F}_p$ is the field norm of some element $\alpha = a + \mathrm{i}b \in \mathbf{F}_{p^2}$,

$$\mathsf{N}(\alpha) = a^2 + b^2 = c.$$

Since we required c to be non-zero, and $\mathsf{N}(\alpha = a + \mathrm{i}b) = 0$ only for $a = b = 0$, the corresponding element $\alpha \in \mathbf{F}_{p^2}$ must be non-vanishing.

This shows that for any non-zero element $c \in \mathbf{F}_p$, there exists a non-vanishing element $\alpha \in \mathbf{F}_{p^2}$ with $\mathsf{N}(\alpha) = c$, and thus we find that the map $\mathsf{N}(\alpha) : \alpha \in \mathbf{F}_{p^2} \to c \in \mathbf{F}_p$ is onto; in addition, since we could displace c to any element of $\mathbf{F}_p$, each non-zero element in the range $\mathbf{F}_p$ of the map $\mathsf{N}(\alpha)$ must correspond to the same number of non-zero domain elements $\alpha \in \mathbf{F}_{p^2}$. Restoring the zero-element case, we see also that no elements of the full set of $\mathbf{F}_p$ are missed in the range of $\mathsf{N}(\alpha)$.

We can now compute the size of the equivalence class of complex unit-modulus phases corresponding to the Hopf fibration circle. Since $\mathbf{F}_{p^2}$ has $p^2 - 1$ non-zero values, and the map $\mathsf{N}(\alpha)$ distributes these equally across the domain of $p - 1$ non-zero elements $c \in \mathbf{F}_p$, there are $(p^2 - 1)/(p - 1) = p + 1$ (non-zero) domain elements in $\mathbf{F}_{p^2}$ for each (non-zero) image element in $\mathbf{F}_p$. We illustrate this graphically in figure A1. Thus the Hopf circle always has size $p + 1$, corresponding essentially to a discrete projective line, and that is the size of each equivalence class of the map $\mathsf{N}(\alpha)$ for non-vanishing α, including in particular the map to the unit norm value $c = 1 \in \mathbf{F}_p$. □

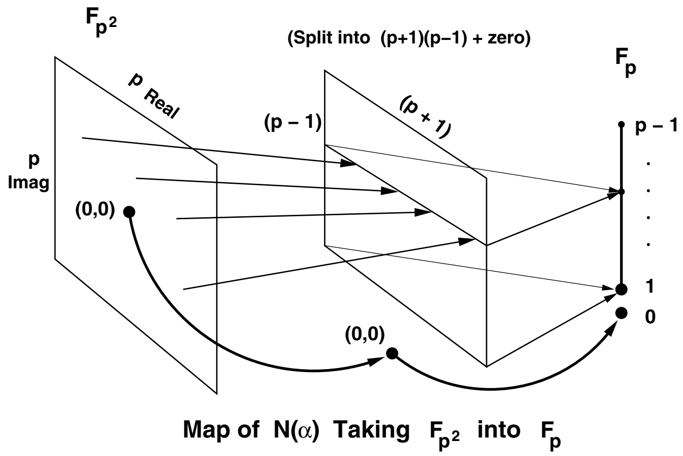

Figure A1. Sketch of the map from $\mathbf{F}_{p^2}$ to $\mathbf{F}_p$ using $\mathsf{N}(\alpha)$, showing the decomposition of $\mathbf{F}_{p^2}$ into the zero element $(0, 0)$ and the $p^2 - 1 = (p + 1)(p - 1)$ non-zero elements that map onto the $(p - 1)$ non-zero elements of $\mathbf{F}_p$ with multiplicity $(p + 1)$.

A.2. Counting of unit-norm states

Proposition A.2. *The number of unit-norm states described by a D-dimensional vector* $(\alpha_0, \ldots, \alpha_{D-1})$ *with coefficients* $\alpha_i \in \mathbf{F}_{p^2}$ *is* $\omega(D, p) = p^{D-1}(p^D - (-1)^D)$.

Method. *We generalize proposition 2 to also provide the count of the zero-norm states* $\zeta(D, p) = p^{D-1}(p^D + (-1)^D(p - 1))$ *and prove both formulas simultaneously by induction on D.*

Proof. The field-norm map $\mathsf{N}(\alpha_0, \ldots, \alpha_{D-1}) = \mathsf{N}(D) : (\mathbf{F}_{p^2})^D \to \mathbf{F}_p$ takes the domain of D-dimensional vectors, with total number of possible cases $(p^2)^D = p^{2D}$, to an image of discrete size p in $\mathbf{F}_p$, which we can think of either as a zero-origin set $\{0, 1, \ldots, p - 1\}$ or as a zero-centered set $\{(-(p - 1)/2, \ldots, -1, 0, 1, \ldots, (p - 1)/2\}$. The latter is useful for considering pairings of numbers that sum to zero in the field $\mathbf{F}_p$.

Zero-norm case. We begin with our experimentally generated hypothesis for the *number of zero-norm vectors* with no restriction on the parity of D, allowing $D + 1$ to be odd as well as even:

$$\zeta(D, p) = p^{D-1}(p^D + (-1)^D(p - 1)). \tag{A.1}$$

This is the proposed number of values of $(\alpha_0, \ldots, \alpha_{D-1}) \in (\mathbf{F}_{p^2})^D$ for which $\mathsf{N}(D) = 0$.

Unit-norm case. Next, we observe that, since there are p^2 elements $\alpha \in \mathbf{F}_{p^2}$, we must have $(p^2)^D = p^{2D}$ possible values of a D-dimensional vector $(\alpha_0, \ldots, \alpha_{D-1})$. There are $p^2 - 1$ non-zero values of $\alpha \in \mathbf{F}_{p^2}$, and we showed in proposition 1 that $\mathsf{N}(\alpha)$ maps exactly $p + 1$ values in that set to each of the $p - 1$ non-zero values in $\mathbf{F}_p$. Therefore, we can propose that the *unit-norm case* has a count of domain elements that is $1/(p - 1)$ of the total number of non-zero-norm cases. The proposed number of unit-norm cases following from the hypothesis equation (A.1) would then be

$$\omega(D, p) = \frac{p^{2D} - \zeta(D, p)}{p - 1}. \tag{A.2}$$

Proof by induction on D. Since, by equation (A.2), the proposed unit-norm counting formula $\omega(D, p)$ for a given D follows immediately from the proposed zero-norm counting formula $\zeta(D, p)$ for the same D, it is sufficient to perform our inductive proof on the zero-norm counting formula implicitly using the statement for the one-norm counting formula. We thus assume that we are given $\zeta(D, p)$, and proceed to examine the relation between the vanishing domains of $\mathsf{N}(D)$ and $\mathsf{N}(D+1)$, which can be written for generic $\alpha = \alpha_D$ as

$$\mathsf{N}(D+1) = \mathsf{N}(D) + \mathsf{N}(\alpha). \tag{A.3}$$

The counting of elements in the domain of the $\mathsf{N}(D+1)$ map whose image in $\mathbf{F}_p$ is zero consists of two parts.

- *Simple zeros*. If $\alpha = 0$, the only possible zeros of $\mathsf{N}(D+1)$ are the zeros of $\mathsf{N}(D)$, counted by one instance of $\zeta(D, p)$.
- *Compound zeros*. If $\alpha \neq 0$, then $\mathsf{N}(\alpha) = c$ for non-zero $c \in \mathbf{F}_p$. As we noted, the values of c can be written as $(p-1)/2$ pairs of matched positive and negative numbers that sum pairwise to zero in the field $\mathbf{F}_p$. However, we know that $\mathsf{N}(D)$ maps its domain to *each* value of non-zero $c \in \mathbf{F}_p$ exactly $p+1$ times. Assuming that $\zeta(D, p)$ is true, we may use the resulting hypothesis for the formula of equation (A.2) expressing $\omega(D, p)$, the unit-norm counting hypothesis, directly in terms of $\zeta(D, p)$. The compound zero counts then follow from using $\omega(D, p)$ as the number of times that the *negated* value, that is $-c$, is encountered to match each non-zero value of $\mathsf{N}(\alpha) = c$. Therefore we find that $p^2 - 1$ instances of the count $\omega(D, p)$ would contribute to the final hypothesized tally of zeros of $\mathsf{N}(D+1)$.

The inductive proof of equation (A.1) then proceeds by verifying the validity of the base case

$$\zeta(1, p) = 1$$

combined with the following verification of the counting of the zeros $\zeta(D+1, p)$ of $\mathsf{N}(D+1)$ in terms of $\zeta(D, p)$:

$$\begin{aligned}
\zeta(D+1, p) &= \zeta(D, p) + (p^2 - 1)\,\omega(D, p) \\
&\overset{(A.2)}{=} \zeta(D, p) + (p^2 - 1)\,\frac{p^{2D} - \zeta(D, p)}{p - 1} \\
&= p^{2D+1} + p^{2D} - p\,\zeta(D, p) \\
&\overset{(A.1)}{=} p^D(p^{D+1} + (-1)^{D+1}(p - 1)).
\end{aligned} \tag{A.4}$$

The result follows from observing that this is the required form of equation (A.1) for $D \to D+1$. Since equation (A.1) is the zero-norm count for all (D, p), a corollary is that equation (A.2) is the count of unit-norm discrete states for all (D, p). □

A.3. n-qubit formulas

Moving to the case of interest where $D = 2^n$ is the (even) state-vector length for an n-qubit state, we have proven that the number of unit-norm states of an n-qubit vector $|\Psi\rangle$ is

$$\omega(2^n, p) = p^{2^n - 1}(p^{2^n} - 1).$$

Since the multiplicity of points $\alpha \in \mathbf{F}_{p^2}$ mapping to the same point, in particular the unit value, under the action of $\mathsf{N}(\alpha)$ is $p+1$, the number of irreducible discrete n-qubit states on the generalized discrete Bloch sphere is simply the quotient

$$\text{Irreducible } n\text{-qubit states} = \frac{p^{2^n-1}(p^{2^n} - 1)}{p+1} = p^{2^n-1}(p-1)\prod_{k=1}^{n-1}(p^{2^k} + 1).$$

References

[1] Bengtsson I and Zyczkowski K 2008 *Geometry of Quantum States: An Introduction to Quantum Entanglement* (Cambridge: Cambridge University Press)
[2] Mosseri R and Dandoloff R 2001 *J. Phys. A: Math. Gen.* **34** 10243
[3] Arnold V I 2011 *Dynamics, Statistics and Projective Geometry of Galois Fields* (Cambridge: Cambridge University Press)
[4] Turing A M 1937 *Proc. Lond. Math. Soc.* **42** 230
Turing A M 1937 *Proc. Lond. Math. Soc.* **43** 544 (erratum)
[5] Minsky M 1967 The computable real numbers *Computation: Finite and Infinite Machines* (Englewood Cliffs, NJ: Prentice-Hall) chapter 9
[6] Chaitin G J 2007 *Thinking about Gödel and Turing* (Singapore: World Scientific)
[7] Feynman R P 1982 *Int. J. Theor. Phys.* **21** 467
[8] Landauer R 1996 *Phys. Lett.* A **217** 188
[9] Schumacher B and Westmoreland M D 2012 *Found. Phys.* **42** 918
[10] James R P, Ortiz G and Sabry A 2011 arXiv:1101.3764
[11] Hanson A J, Ortiz G, Sabry A and Willcock J 2011 arXiv:1104.1630
[12] Berger M and Gostiaux B 1988 *Differential Geometry: Manifolds, Curves, and Surfaces* (New York: Springer)
[13] Hardy G H and Wright E M 2006 *An Introduction to the Theory of Numbers* (Oxford: Oxford University Press)
[14] Stewart I 2004 *Galois Theory* (Boca Raton, FL: Chapman and Hall)
[15] Barnum H, Knill E, Ortiz G and Viola L 2003 *Phys. Rev.* A **68** 032308
[16] Barnum H, Knill E, Ortiz G, Somma R and Viola L 2004 *Phys. Rev. Lett.* **92** 107902