Arithmetic, mutually unbiased bases and complementary observables

M. D. Sheppeard
Oxford University Computing Laboratory, Wolfson Building, Parks Rd., Oxford OX1 3QD, United Kingdom

(Received 1 July 2009; accepted 10 November 2009; published online 1 February 2010)

Complementary observables in quantum mechanics may be viewed as Frobenius structures in a dagger monoidal category, such as the category of finite dimensional Hilbert spaces over the complex numbers. On the other hand, their properties crucially depend on the discrete Fourier transform and its associated quantum torus, requiring only the finite fields that underlie mutually unbiased bases. In axiomatic topos theory, the complex numbers are difficult to describe and should not be invoked unnecessarily. This paper surveys some fundamentals of quantum arithmetic using finite field complementary observables, with a view considering more general axiom systems. © 2010 American Institute of Physics. [doi:10.1063/1.3271045]

I. INTRODUCTION

The real or complex number field has no unique definition in a topos.¹ Moreover, all known categorical axiomatizations of these fields are nontrivial and it is not clear that such axiom systems should be applied directly to quantum physics, although quantum mechanics does traditionally rely on the complex numbers. A set of complementary observables is a small finite subset of a finite dimensional Hilbert space, and Hilbert spaces themselves may be replaced by the diagram calculus of dagger monoidal categories.²³ One would like therefore to consider categorical axioms for measurement structures without being restricted by the properties of the full field of complex numbers.

However, let us step back and consider first the collection of natural numbers \( \mathbb{N} \), or 1-ordinals. Arithmetic in \( \mathbb{N} \) is easy to define in a topos, and the topos \( \text{Set} \) has the special property of containing an object \( \mathbb{N} \). A given \( n \in \mathbb{N} \) measures the cardinality of an arbitrary finite set, or perhaps a basis set for a Hilbert space, in which case \( n \) is the dimension of the space. So one asks, in an axiom system for complementary observables which is not based on Hilbert spaces, what does \( n \) represent? Since sets categorify cardinality by one stage, and we assume that higher dimensional categories are required at a foundational level in quantum physics, a natural guess is that \( n \) should count not set elements, but perhaps categorical dimension. In each dimension, arithmetic itself would be categorified. We see a little of this idea in Batanin’s hierarchy of \( n \)-ordinals, described by \( n \) level trees.

There are several lines of evidence that categorified arithmetic describes physically significant structures, ranging from the works of Brannen⁴ and Pitkanen⁵ to applications of Batanin’s operads to particle physics. More concretely, as a Chu space, a Hilbert space requires a continuum of truth values to describe it, whereas the relations underlying Spekkens’ toy model⁶ for qubit systems can be described with a very small set of truth values. The difference between the toy model and the true quantum system is at the heart of nonlocality in quantum mechanics, as shown in Ref. 6, and is therefore indicative of intricate structures that are barely touched by the axioms of monoidal

---

¹Electronic mail: mdsheppeard@yahoo.com.
categories. On the other hand, the requirement of a complex $i$ in quantum mechanics follows from an elementary property of complementary observables for qubits, as shown in Sec. II.

This investigation is further inspired by the mathematical intuition that arithmetic in the integers, when viewed as a space, has a three dimensional structure, with primes being described by knots in this space. In particular, the Frobenius map $x \mapsto x^p$ for a finite field is viewed as a selection of a loop in the space $\text{Spec}(\mathbb{F}_p)$ associated with the prime field. Since complementary observables, in prime power dimensions, directly represent the finite field, we look at connections between them and braid mathematics.

Sections III–V introduce complementary observables, the arithmetic nature of their composite systems, and related elements of braid mathematics. Although the search for fundamental axioms is left for the future, certain axiomatic issues are discussed in Secs. VI and VII, where the finite projective geometry of composite systems is viewed from the perspective of groupoidification.

II. COMPLEMENTARY OBSERVABLES

The mathematics of ordinary quantum mechanics is required to account for the incompatibility of certain physical observables, such as the measurement of electron spin in orthogonal directions in space. For observables with only a finite number of possible outcomes, one conventionally works with finite dimensional Hilbert spaces over the complex number field.

In this section, special sets of operators and vectors in prime dimensional Hilbert spaces are introduced. Since these sets are strictly finite, their definition does not require the full set of complex numbers. In fact, for any prime power $d$, the structure of the finite field on $d$ elements is what really underlies maximal sets of complementary observables in dimension $d$. This suggests that we should consider a construction of quantum mechanics based on axiomatic arithmetic rather than complex number Hilbert spaces.

Definition 2.1: Given a complex Hilbert space $H$, a vector $|\psi\rangle$ in $H$ is unbiased with respect to a basis $\{|e_i\rangle\}$ if

$$|\langle e_i | \psi \rangle| = |\langle e_j | \psi \rangle|$$

for all $i$ and $j$. Two bases, $\{|f_i\rangle\}$, and $\{|e_j\rangle\}$, are complementary if every vector in one basis is unbiased with respect to the other basis. Two linear operators, acting on $H$, are complementary if their eigenvector sets form two complementary bases. Such a pair of operators corresponds to two mutually incompatible physical observables in that measurement of one observable destroys any information that we may have about the other.

It is known that in prime power dimensions $d$, there are always $d+1$ bases, which are complementary with respect to each other. In dimension 2, the eigenvector sets of the Pauli operators

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

form a set of three complementary bases, and, in general, we talk about the generalized Pauli operators. In what follows, simple normalization factors will be neglected.

There exists a second set of $d+1$ operators, which are unitary, that act by conjugation $CDC^\dagger$ on the diagonal element $D$ (the analog of $\sigma_2$) of the operator set to recover the other elements. A multiple of the identity always lies in this set in order to recover $D$ itself. In dimension 2, these operators may be chosen as

$$F_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad R_2 = \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}, \quad I = R_2^0.$$  

In odd prime dimensions, there is a circulant operator $R_d$ satisfying $R_d^d = I$, whose powers generate other elements of the cycle set. For example, in dimension 3 we have the two 1-circulants...
where \( \omega \) is the primitive cubed root of unity.

Observe that \( F_2 \), the Hadamard gate, is the qubit Fourier transform operator. One may well ask why the complex \( i \) is required here, given that \( i \sigma_y \) has basically the same eigenvectors. The reason is that the columns of \( F_2 \) and \( R_3 \) must recover the eigenvectors of the Pauli matrices. A similar thing happens in all prime power dimensions. In dimension 2, however, without the \( i \), the circulant nature of \( R_2 \) could at best multiply one column by \(-1\), returning the same eigenvector and failing to span the two dimensional space.

In general, for prime dimensions \( d \), the Fourier operator \( F_d \) is given by \( F_{ij} = \omega^{ij} \) for \( i,j \in 0,1,2,\ldots \) and \( \omega \) a primitive \( d \)th root of unity and is included in this set. By the nature of the transform, it always creates a circulant matrix when acting on \( D \), such as \( \sigma_X \). In odd prime dimensions, \( R_d \) is defined by

\[
(R_d)_{k+1} = \omega^{-k(k+1)/2}
\]

for \( k \in 0,1,\ldots,d-1 \). The column sets of matrices in this operator set recover the eigenvectors of the complementary basis sets. These operators are always unital Hadamard, meaning that the modulus of each entry is 1.

Like the diagonal matrix \( D \), the elements of the generalized Pauli set always have only one nonzero entry in each row or column, always a root of unity. It follows that products of such operators are defined over multiplication of the characters of a finite field rather than the full field of complex numbers. Moreover, the quantum Fourier operator \( F_d \) is technically built from entries, which are characters on the finite field which indexes the matrix. A Fourier series is a 1-circulant matrix, expressed as a sum

\[
a_1 V^1 + a_2 V^2 + \cdots + a_d V^d,
\]

where \( V \) is the cyclic permutation \((23\cdots d1)\) that generalizes \( \sigma_X \). The matrix \( F_d \) is the permutation \( W=(1d(d-1)\cdots2) \), a \( d-1 \)-circulant, which squares to the identity. Observe that multiplying a 1-circulant by a 2-circulant results in a 2-circulant, and so on, so a special set of 1-circulant matrices may be extended to equivalence classes of operators, with a representative in each circulant class. The matrix \( VW \) is always the codiagonal identity, which is a \( d-1 \)-circulant. It also squares to the identity.

Since for a prime \( p > 2 \), \( R_p = 1 \), and all powers of \( R_p \) are 1-circulants, these operators would themselves represent the cyclic multiplication of a field with \( p+1 \) elements except that \( p+1 \) is usually not prime. However, there is no reason for us to restrict our attention to fields since rings with zero divisors occur naturally in matrix algebras. As explained below, in general prime power dimensions \( d \), \( R_d \) is naturally defined in terms of prime factors.

The tensor composition of observables, for which dimensions are multiplied, is the vector space analog of Cartesian product for sets. Note also that the addition of basis sets, by disjoint union, corresponds to the multiplication of the number of vectors in a direct sum of vector spaces over a finite field. In this case, the adjunction between Set and Vect may be used to send all disjoint unions of sets, with \( m \) and \( n \) elements, respectively, to a set with \( d^m \times d^n \) elements, where \( d \) is the cardinality of the field (or ring, where modules replace vector spaces). This is naturally a Cartesian product of the \( d^m \), \( d^n \) element sets of the component spaces. Addition may thus be eliminated from the structure of quantum arithmetic, which relies instead on multiplication and power.
III. QUdITS AND ARITHMETIC

This section introduces further arithmetic elements underlying the structure of complementary observables. Here, we see the first hints of the need for richer categorical structures in the axioms of quantum mechanics, which we will finally discuss in Sec. VI.

The initial question is this: if special matrix sets represent something utterly different from linear operators, then what do the matrix entries represent? Our matrices contain a limited set of possible values, but in what sense are these numbers? The categorical motivation suggests that the most fundamental finite sets of numbers are sets of truth values. For example, in the category Set, there are two Boolean truth values. By analogy, complex number Hilbert spaces require a continuum of truth values; but such a continuum seems absurd. The physics of quantum mechanical observables with a finite number of outcomes ought to be described by a logic based on a finite number of truths.

Let us begin with dimension 2. The algebra of qubits requires at least the field $F = \mathbb{F}_5$, but for now we view $i$ merely as a symbol, representing some new kind of truth value beyond the $\mathbb{F}_2$ of set theory. That it must satisfy $i^2 = 1$ follows directly from the eigenvector equation for $\sigma_y$,

$$
\begin{pmatrix}
 0 & -i \\
 1 & i
\end{pmatrix} \begin{pmatrix}
 1 & i \\
 i & 1
\end{pmatrix} = \begin{pmatrix}
 1 & -i \\
 i & 1
\end{pmatrix}.
$$

(6)

Eigenectors are always collected into the operator set, a first step in removing Hilbert spaces from the axioms. Note also that due to the zeroes in $\sigma_y$, only a multiplication operation is used. This happens in all prime dimensions.

Let the dimension $d = p^n$. In general, a system of $n$ qudits has $p^n + 1$ associated complementary observables. When $n = 2$, the Fourier operator $F_p \otimes F_p$ diagonalizes block circulant matrices of the form $(A_0, A_1, \ldots, A_{p-1})$, where $A_i$ is itself a circulant matrix. An example of such a matrix, using the identity and $i\sigma_y$, is the operator

$$
R = \begin{pmatrix}
 1 & 0 & 0 & 1 \\
 0 & 1 & -1 & 0 \\
 0 & 1 & 1 & 0 \\
 -1 & 0 & 0 & 1
\end{pmatrix},
$$

(7)

which may be used to define a representation of braids, and hence a link invariant. This process of building circulants may be iterated $n$ times to create operators on a space of dimension $p^n$. It is shown in Ref. 10 that the Fourier operator $F_p^{\otimes n}$ diagonalizes these operators by acting locally on circulants. The Galois field $\mathbb{F}_p^n$ indexes the analog of the $R_p$ operators, which are defined as follows. An additive character $\chi$ for the field $\mathbb{F}_p^n$ is given on an element $x$ by

$$
\chi(x) = \exp \left( \frac{2\pi i \operatorname{tr}(x)}{p} \right),
$$

(8)

which generalizes roots of unity in the case $n = 1$. Here, the trace map is defined by

$$
\operatorname{tr}(x) = x + x^p + x^{p^2} + \cdots + x^{p^{n-1}}.
$$

(9)

The generalized permutation, or shift, operator $V_x$ takes $y \in \mathbb{F}_p^n$ to $x + y$. Choose the basis for $\mathbb{F}_p^{\otimes 2}$ in the order

$$
0, t, 2t, \ldots, 1 + t, 1 + 2t, \ldots, p - 1, (p - 1) + (p - 1)t.
$$

Then,
\[ R_x = \sum_{y \in \mathbb{F}_p} c_x(y)V_y, \]  
where, for \( y \neq 0 \), the coefficients are given by

\[ c_x(y) = \frac{1}{p} \chi \left( \frac{y^2}{2x} \right). \]

For example, when \( p = 3 \), the \( 9 \times 9 \) operator for \( x = 2t \) is given by

\[ R_{2t} = I \otimes I + V \otimes I + I \otimes V + V^2 \otimes I + I \otimes V^2 + \omega V \otimes V + \omega V^2 \otimes V^2 + \omega^2 V^2 \otimes V + \omega^2 V \otimes V^2. \]

Observe that the basis here consists entirely of \( 9 \times 9 \) permutation matrices, and \( R_{2t} \) has idempotent circulant blocks. The off diagonal blocks are zero divisors in dimension 3. Note that we could define analogs of these operators in any dimension. For example, in dimension 6, the permutation tensor products \( V_2^3 \otimes V_3^2 \) may be considered a basis for a generalized Fourier series.

These new block circulants, for \( d \geq 3 \), satisfy the group law \( R_{xy} = R_x R_y \). From our categorical point of view, the group law expresses the functorial nature of the whole collection of operators \( \{R_x\} \) on the category \( \mathbb{F}_p \). But how is the field a category? First, as an additive group, it is a one object category with addition as arrow composition, and \( R \) is a \( d \) dimensional representation of the group. However, the existence of a second product, namely, multiplication, suggests considering some combination of fields as a collection of two dimensional arrows, where elements of a field might be represented in different categories and perhaps more than once. This is a simple minded, but nonetheless compelling, way to see that the collection of primes should form a three dimensional space!

In line with category theory conventions, on the representation side, we will view tensor products as horizontal compositions and matrix multiplication as vertical composition. The functorial group law for \( R \) suggests letting vertical composition in the field correspond to addition. The \( R \) operators show that multiplication for \( \mathbb{F}_{d+1} \) is basically the same thing as addition for \( \mathbb{F}_d \), forgetting that this usually only makes sense for Mersenne primes. In other words, a combination of the additive rings \( \mathbb{F}_d \) and \( \mathbb{F}_{d-1} \) captures all the arithmetic of \( \mathbb{F}_d \). So a quantum successor map \( d \mapsto d+1 \) would involve substituting multiplication for addition and vice versa. More abstractly, this is the categorical domain of a distribution law \( \lambda : + \Rightarrow \times \) for the monads of addition and multiplication, which are associated with a whole square of adjunctions between the category Set and the category of rings, \( \text{Rng} \). Note that a possible advantage of this point of view is that the failure of the \( p = 2 \) operators to satisfy an exact group law may be attributed to a two dimensional weakening of functors to pseudofunctors.

Now we would like the Fourier operator \( F_d \) to represent a resolution of the zero element, which is missing in the representation of the multiplicative group by the \( R_d \) operators and the identity. Since \( R_i \) is always unitary, under ordinary matrix multiplication \( R_i \) represents the multiplicative inverse of \( R_i \). Happily, the ordinary product \( F_d R_i \) returns another (permuted) form of \( F_d \) in analogy to the statement \( 0 \cdot x = 0 \), and the trace of the Fourier operator \( F_p \) is zero.

Observe that the Frobenius map \( x \mapsto x^p \) on a finite field is represented by a power of the matrix \( R \), which means that it operates as a natural transformation 2-arrow between the functors \( R \) and \( \mathbb{F} \). This arrow is supposed to be a knotty representation of the prime \( p \) since \( \text{Spec} \mathbb{F}_p \) behaves like a circle from a homotopic point of view. In quantum mechanics, this circle comes from a set of coordinates for the quantum torus of the Fourier transform except that all powers \( p^n \) of a prime contribute to the space.

IV. QUANTUM DIAGRAMS

Connections between knot theory and number theory have been developed in fruitful directions in recent years. In particular, there is the sophisticated notion of a field with one element. Roughly speaking, this is the field that underlies the category Set of sets, considered as vector
spaces over a field. The braid groups are general linear groups associated with Set.

The unification of sets and vector spaces also occurs in categorical quantum theory, where both classical and quantum information must be considered, so perhaps it would not be surprising to find that the mathematics of both knots and numbers is relevant to searches for deeper axioms.

One does not expect that complementary observables will be directly associated with a full invariant for knots and links because there would be severe truncations due to the canonical choice of deformation parameter as a root of unity. For example, the Jones invariant of a trefoil knot at a cubed root of unity is simply 1, the same value as for the unknot, and this may be considered a normalization for all torus knots.

This example is an analogy to the zero entropy of the W state for three qubits, which may be labeled by the trefoil knot in the sense that the symmetric matrix of projectivized amplitudes for the W state is the incidence matrix for the dual trivalent graph of the trefoil knot. Similarly, there is an entangled state of two qubits corresponding to the Hopf link, which has two crossings in its braid diagram.

Entanglement in qubit systems helps clarify the relation between quantum mechanics and ordinary sets. The entanglement measure for three spin 1/2 particles is known to be a hyperdeterminant, which has also appeared as a measure of black hole entropy. For the three qubit state

$$\Psi = a_{000}|000\rangle + a_{100}|100\rangle + a_{010}|010\rangle + a_{001}|001\rangle + a_{110}|110\rangle + a_{101}|101\rangle + a_{011}|011\rangle + a_{111}|111\rangle,$$

(13)

the hyperdeterminant is given explicitly by

$$\Delta(\Psi) = a_{000}a_{111}^2 + a_{100}a_{011}^2 + a_{010}a_{101}^2 + a_{001}a_{110}^2 + 4(a_{000}a_{101}a_{110}a_{011} + a_{111}a_{100}a_{010}a_{001})$$

$$- 2(a_{000}a_{010}a_{110}a_{101} + a_{001}a_{010}a_{111}a_{101} + a_{000}a_{110}a_{101}a_{011} + a_{110}a_{100}a_{010}a_{001})$$

(14)

Usually a state $\Psi$ is normalized so that the sum of squares of the amplitudes is 1, namely $\langle \Psi | \Psi \rangle = 1$. However, the physical states are projective analogs of the Hilbert space states, so we may consider the amplitudes as projective coordinates. A reduction to (most of) the projective space is achieved by setting one coordinate to 1, say $a_{000} = 1$. Then we have

$$\Delta(\Psi) = a_{111}^2 + a_{100}a_{011}^2 + a_{010}a_{101}^2 + a_{001}a_{110}^2 + 4(a_{011}a_{110}a_{101} + a_{111}a_{100}a_{010}a_{001}) - 2(a_{100}a_{011}a_{110})$$

$$+ a_{010}a_{111}a_{101} + a_{010}a_{110}a_{111} + a_{100}a_{010}a_{101}a_{011} + a_{010}a_{001}a_{110}a_{101} + a_{100}a_{001}a_{110}a_{011}.$$ 

(15)

As pointed out in Ref. 15, when $\Delta(\Psi) = 0$, Eq. (15) exactly expresses the determinant $D = a_{111}$ of the symmetric $3 \times 3$ matrix,

$$M(\Psi) = \begin{pmatrix}
    a_{100} & \sqrt{a_{100}a_{010} - a_{110}^2} & \sqrt{a_{100}a_{001} - a_{111}^2} \\
    \sqrt{a_{100}a_{010} - a_{110}^2} & a_{010} & \sqrt{a_{010}a_{001} - a_{011}^2} \\
    \sqrt{a_{100}a_{001} - a_{111}^2} & \sqrt{a_{010}a_{001} - a_{011}^2} & a_{001}
\end{pmatrix}$$

(16)

indexed by the three qubits. The entry sets of six $a_{ijk}$ are the principal minors. That is, there is a set of eight determinants associated with $M$, including $D$ for the full matrix and $a_{000} = 1$ for the empty matrix. When $\Delta(\Psi) \neq 0$, the determinant $D(M)$ differs from the amplitude $a_{111}$, and this difference characterizes the entanglement.

Recall the three Reidemeister moves for braid diagrams.
There is one obvious connection between groups of complementary observables and knots. Any group may be considered a *rack* under the conjugation action. A group rack labels the three pieces of a crossing diagram by group elements \( g, h, \) and \( ghg^{-1} \), where the latter labels the outgoing strand of the undercrossing. These gadgets generally fail to satisfy the first Reidemeister rule, but the other moves follow easily from conjugation. Note that the Pauli matrices also form a proper quandle for the trefoil knot under ordinary composition, up to \( \pm I \).

Here we are more interested in seeing how braid rules are related to the \( R_x \) operators and the Fourier transform. First note that the diagonal \( D \) in dimension \( d \) may always be used to represent the product \( d = d - 1 \), where \( d \) is the braid group generator for \( B_d \). Since the generalized Pauli set is always recovered from the conjugation action of the complementary observables on \( D \), any new braid representation for \( F_d \) and \( R_d \) may be carried over to link diagrams for the Pauli set. However, things will not work out quite so easily exactly because of the higher dimensional structure lurking behind these operators.

To begin with, let \( J \) be the democratic \( d \times d \) matrix whose entries are all 1. A Schur inverse for a \( d \times d \) matrix \( M \), under the multiplication \( (AB)_{ij} = A_{ij}B_{ij} \), satisfies \( M^{-1}M = I \). A matrix is of type II (Ref. 16) if (a) its Schur inverse exists and (b) it satisfies \( M(M^{-1})^T = dI \) for ordinary matrix multiplication. Type II matrices are interesting since under one further condition they define spin models, which give rise to link invariants. However, of the \( R_d \) operators, only \( R_2 \) is a spin model.

**Lemma 4.1:** In any prime dimension \( p \), the matrices \( R_p \) and \( F_p \) are type II.

**Proof:** The Fourier operator \( F_p \) is always symmetric and unitary, so the Schur inverse is given by either complex conjugation or dagger, and \( FF^\dagger = nI \). The Schur inverse, \( R_p \), of \( R_p \) is given by the complex conjugate. Since this is also a circulant matrix, and its transpose is circulant, \( R = R_p(R_p)^T \) must be circulant. Thus, we only need check the first row of \( R \). \( R_{11} \) is given by

\[
1 + \omega^{-1} \cdot \omega + \omega^{-3} \cdot \omega^3 + \cdots + 1,
\]

which equals \( d \) as required. Then,

\[
R_{12} = \sum_{k=0}^{d-1} \omega^{-k} = 0,
\]

and for \( j > 2 \), \( R_{ij} \) cycles through the prime number of roots in a different order. Note that \( R_{1,k+1} \) being zero relies crucially on the form (4) for matrix entries so that \( (k+1)(k+2) - (k+1)k = 2(k + 1) \). It turns out that all the \( R_p \) are unitary. In general, we can ask: which unitary, unital circulants are of type II? Observe that any shift of \( R_p \) by a power of the cyclic permutation \( V \) also results in a type II matrix.

**Lemma 4.2:** In any prime power dimension \( d \), all the matrices \( R_p \) and \( F_d \) are of type II.

**Proof:** The Schur inverse of \( R_p \) is always the conjugate matrix, and since \( R_p \) is unitary, type II condition is satisfied. Similarly for \( F_d \).

An operator obeys the third Reidemeister rule if it satisfies a *spin matrix* condition. Given a type II matrix \( A \), first construct the set of all vectors of the form \( v_{ij} = Ae_iA^{-1}e_j \) for the standard basis vectors \( e_i \). If all these vectors are eigenvectors for \( A \), then \( A \) is a spin matrix.

**Lemma 4.3:** For \( p = 2, R_2 \) is a spin matrix.
The higher dimensional $R_p$ is not a spin operator. However, observe that $(1, 1, \ldots, 1)$ is always the diagonal spin vector $v_\mu$. This is always an eigenvector for the $R_p$ matrices since they are circulant. Type III Reidemeister move is associated with a Yang–Baxter equation of the form

$$ABA = BAB,$$

where usually one takes $A=C \otimes I$ and $B=I \otimes C$ with $C$ acting on two copies $V \otimes V$ of a space, and $I$ the identity. The 2-categorical interchange rule

$$(1 \otimes C)(C \otimes 1) = (C \otimes 1)(1 \otimes C)$$

for $I$ acting on the same space $V \otimes V$ as an operator $C$ has the usual diagrammatic representation


in a monoidal category, where we choose to draw double strands to represent the object $V \otimes V$. This rule is a condition on the two kinds of composition: tensor product and matrix multiplication. Now the failure of the four strand Yang–Baxter rule takes the form

$$(I \otimes C)(C \otimes I)(I \otimes C) = C \otimes C^2,$$

$$(C \otimes I)(I \otimes C)(C \otimes I) = C^2 \otimes C.$$  

Here, the swapping of $C$ and $C^2$ merely says that boxes can be dragged through a crossing of the two ribbons in order to get the right number of boxes (1 or 2) on each pair of strands. This rule is always satisfied. Let us try to use circulant matrices to define the operators $A$ and $B$ of the type III rule. Consider a matrix $C$ acting on a $p^2$ dimensional space $V \otimes V$. To begin with, let $C$ be the block matrix built from $p^2$ blocks, with each block being equal to a $p \times p$ matrix $K$. In other words, $C = J \otimes K$, where $J$ is the Schur identity. Now compare $(C \otimes I)(I \otimes C)(C \otimes I)$ and $(I \otimes C)(C \otimes I)(I \otimes C)$. These expressions are equal provided that (i) $K$ is idempotent and (ii) $pKJ = JK$. The normalization in (ii) is due to the different number of factors of $J$ on each side. For circulants, or any magic matrix with row and column sums all equal, this rule is satisfied since the democracy of $J$ ensures that $JK = \alpha I$, where $\alpha$ is the row sum of $K$. Unfortunately, the only nontrivial idempotent circulant, with row sum not equal to zero, is the matrix $J$ itself, which is not even type II.

Now let $F_3 = R_3^{-1} PR_3^{-1}$ for a matrix $P$ with only three nonzero phase entries. Then, one may verify that

$$R_3^{-1} P^{-1} R_3^{-1} = PR_3 P$$

since $F_3 = 1$. In general, let $P = R_p F_p R_p$. Then (20) holds. This rule expresses symmetry in terms of the type III move, although $P$ is not of type II, and both $P$ and $F_p$ truncate to the identity at some point. If the Yang–Baxter rule holds, this symmetry rule reduces $B_3$ (by its center) to the modular group. Truncations of $B_3$ would result in finite subgroups of the modular group. However, the Yang–Baxter rule cannot hold for $R_p$ and $P$ due to the following. It is easy to see that the Yang–Baxter rule holds only if

$$PR_p^2 PPR_p^2 = 1,$$

but the left hand side evaluates to $F_p^2$ in all dimensions. This is only the identity for dimension 2. That is, the fact that $R_2$ may be associated with a (truncated) braid group representation is entirely due to the Fourier transform property $F_2^2 = 1$. For odd primes this rule is only slightly weakened, to $F_p^2 = 1$, suggesting an odd prime analog of spin structures based on the almost braid rule.
Since $F_3^2$ is always a simple permutation matrix, we could consider $P$ and $PF_3^2$ to be equivalent under a permutation of certain indices. The same operation turns any 1-circulant $R_p$ into an equivalent circulant. A labeling of braid diagrams by equivalence classes of operators might then satisfy the strict Yang–Baxter rule. However, in Sec. V, we will see that the weak Yang–Baxter rule is interesting in its own right.

V. QUDITS AND QUANTUM GROUPS

Matrix quantum groups often appear in applications of knot theory to physics since they are dual to the deformations of universal enveloping algebras, the representations of which naturally form braided monoidal categories. Here we verify that there is a relation between rules for mutually unbiased bases and rules for matrix quantum groups.

The three dimensional qutrit analog of the Pauli matrix antisymmetry $\sigma_i \sigma_j = -\sigma_j \sigma_i$ is the quantum plane relation

$$M_i M_j = \omega^i M_j M_i,$$

which is satisfied by all pairs of operators in the set

$$M_1 = V = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad M_2 = D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix},$$

$$M_3 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & \omega \\ \omega^2 & 0 & 0 \end{pmatrix}, \quad M_4 = \begin{pmatrix} 0 & 0 & 1 \\ \omega & 0 & 0 \\ 0 & \omega^2 & 0 \end{pmatrix}.$$ (23)

We also have

$$F_3 M_2 F_3^\dagger = M_1,$$

$$R_3 M_2 R_3^\dagger = M_3,$$

$$R_3^2 M_2 (R_3^2)^\dagger = M_4.$$ (24)

Conjugates and cycled forms $VM_i$ also form complementary sets. Products in the $M_i$ nominally use $F_3$ addition via characters or, equivalently, $F_4$ multiplication. Addition in $F_4$ is characterized by the cyclic relations

$$a + b = 1, \quad a + 1 = b, \quad b + 1 = a.$$ (25)

Observe that these relations are modeled by multiplication of the Pauli matrices, modulo $-I$, where we choose $\sigma_z$ to represent the unit. Then the identity matrix $I$ acts as a zero for $F_4$ addition. The finite field is completely characterized by multiplication of the qubit Bell states and multiplication of the truth value entries of the qutrit observables, so long as we can identify the roots of unity $\omega$ and $\omega^2$ with the Pauli operators $\sigma_x$ and $\sigma_y$.

The matrix quantum group$^{18} GL_q(2)$ has four generators $a, b, c,$ and $d$ subject to the relations

$$ba = qab, \quad ca = qac, \quad bc = cb,$$

$$dc = qcd, \quad db = qbd,$$
\[ da = ad + (q - q^{-1})bc. \] (26)

Set \( q = \omega \) and consider the qutrit complementary observables

\[ a = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix}, \]
\[ c = \begin{pmatrix} \omega^2 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad d = \begin{pmatrix} 0 & 0 & \omega \\ \omega^2 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}. \] (27)

One easily verifies that these matrices satisfy the purely multiplicative relations. Under complex number addition, they do not obey the final relation, but under addition in \( \mathbb{F}_3 \) they do. In other words, certain sets of qutrit complementary observables may be used to form quantum matrices

\[ M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \] (28)

although the quantum group thus described is truncated due to the deformation being a root of unity.

In higher dimensions there are even more complementary observables obeying quantum plane relations. These generalized Pauli observables replaced quantum states in the original Hilbert space. Now \( 2 \times 2 \) blocks containing \( R_p \) and Fourier operators act via conjugation on the quantum group \( GL_\omega(2) \). There is a tower of these structures for all prime power dimensions \( p \) and deformation parameters \( \omega = \exp(2\pi i/p) \). As \( p \) grows, the truncation of \( GL_\omega(2) \) becomes less severe. The quantum group relations are expressed via an \( R \)-matrix,

\[ R = \begin{pmatrix} \omega & 0 & 0 & 0 \\ 0 & \omega - 1 & \omega & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & \omega \end{pmatrix}. \] (29)

which defines a representation of the braid groups \( B_n \) up to truncation. Since \( R \) defines a braiding element on \( V \otimes V \), we may view the two dimensional space \( V \) as a quantum space object in a braided monoidal category. The coordinates for objects in this category are specified by the complementary observables. So perhaps complementary observables are best seen as quantum points and not as operators acting on classical Hilbert spaces.

VI. PLANAR GROUPOIDIFICATION

We have observed that complementary observables, and mutually unbiased bases, obey rules that arise from finite field arithmetic, and that knot diagrams may be useful in considering alternative formalisms for quantum mechanics based on this arithmetic.

In this section it is observed that the weak Yang–Baxter rule of Sec. IV naturally arises in the categorified geometry of groupoidification, which also involves the structure of finite fields in a way reminiscent of the geometry of entanglement. In other words, groupoidification is very relevant to quantum physics.

Consider the case of three qubits. In Ref. 7, Lédavay et al. showed that the 63 nonidentity elements of the local Pauli group \( G = \{ I, \sigma_X, \sigma_Y, \sigma_Z \}^{\otimes 3} \) (defined up to \( \pm I \)) correspond exactly to the 7 points, 7 lines, 21 flags, and 28 antiflags of the Fano plane. An antiflag is a line with a point off the line in the Fano plane, which is a finite projective geometry with 7 points. The Fano lines are the group elements that use only \( I \) and \( \sigma_X \), such as \( \sigma_X \otimes \sigma_Y \otimes I \), and the points are the elements
constructed from $I$ and $\sigma_Z$. The Fourier transform $F_2$ exchanges points and lines, expressing geometric duality.

By swapping $\sigma_Z$ and $\sigma_Y$, the operator $R_2$ has a more complicated action on Fano flags. A full flag is any element of $G$ that involves $\sigma_Y$. It is a real flag if there are two factors of $\sigma_Y$ (the symmetric case) and an antiflag if there are an odd number of $\sigma_Y$. $R_2$ fixes the point of a flag, but swaps other objects in the group. For example, for the point $\sigma_Z \otimes I \otimes \sigma_Z$, $R_2$ swaps the antiflag $\sigma_Y \otimes I \otimes \sigma_Y$ for the point itself.

In the program of groupoidification, Baez et al. explained how flags for vector spaces over finite fields characterize a categorified Hecke algebra. For (real) qubits, this Hecke algebra has two generators, $P$ for points and $L$ for lines, so one considers a planar projective geometry. Over $F_2$, this is the Fano plane. Since groupoidification involves higher dimensional categories, the Yang–Baxter rule

$$PLP = LPL$$

is only a weak equivalence, requiring geometric duality to transform one side into the other. Objects are actually spans of groupoids, but here we will simply consider them as operations on flags. $P$ is the operation of altering a point, given an initial flag with its marked point. Over $F_p$, there are $q+1$ points on a line. Having selected one of $q$ available points on the flag, to select yet another point one must either (i) choose the same point again or (ii) choose one of the remaining $q-1$ points. This logic is expressed by the Hecke relation on flag operations,

$$P^2 = (q - 1) \times P + q \times 1_G,$$

where we have categorical operations, namely, Cartesian product and coproduct, for the logical connectives. The identity map $1_G$ is really an identity span on flags.

Under degroupoidification, a span of groupoids becomes a linear map for a vector space. Real numbers can arise as cardinalities for groupoids, generalizing the natural number cardinalities of sets. In this setting, it is better to think of a set as a vector space over the field with one element, a partly mythical but powerful mathematical concept, which unifies sets and vector spaces. From this point of view, complementary basis sets and their associated observables are all linear maps, albeit possibly over different number fields. This is just what we have seen above. Allowing for a magical field $F_q^3$, one may construct a field rather than a ring, with $p+1$ elements from the object $F_q^p \cup \mathbf{F}_1$. Although for complex Hilbert spaces we use the number zero for the required additional matrix element, in a more abstract setting it makes sense to think of the zeroes as simply keeping track of the permutations of bases, which is exactly what linear maps on $F_q$ are supposed to do.

The next simplest projective plane, which is of the order of 3, has 13 points and 13 lines. With four points per line, there are 52 flags and 117 antiflags, bringing the total number of geometric elements to 195. We would like these 195 objects to arise from a complementary observable group of the order of 196. The factorization $196 = 4^2 \cdot 7^2$ suggests a component that arises from the two qudit system for qudits of dimension 5, which has six complementary observables plus the identity, along with a two qubit system. This is already a complicated system to analyze.

Since $(F_p^\otimes n)^2$ is involved in exchanging points, lines, and other geometric elements by definition, the rule (21) is the same as the weak Yang–Baxter rule from groupoidification. In the qutrit case, this rule is

$$PR_3P = R_3PR_3(VW),$$

where $VW$ is the 2-circulant permutation matrix for (13). If qutrits describe abstract surfaces of points, lines, and faces, $VW$ swaps points and lines while fixing faces. There is a similar relation for $R_3$. Complementary observables in all prime power dimensions represent groupoidified Hecke operations in this manner.
VII. CONCLUSIONS

Complementary observables may be defined in terms of diagram rules for dagger categories. Here, we have seen that complementary observables in all prime power dimensions have properties that are closely related to the arithmetic of finite fields. It is therefore possible that the slow progress in understanding non prime power dimensions is due to the need to consider composite natural numbers in a higher dimensional categorical setting.

Having committed ourselves to higher dimensional categories, we would like a simple set of axioms that capture modular arithmetic, but without the axiom of infinity that is usually attached to sets. These objects would be the building blocks for an arithmetic geometry.

We have shown that restriction to the stabilizer formalism for qudits in dimension $d$ may be carried out using only finite field arithmetic. In this case, the direct limit of all fields on $d^n$ elements is the $d$-adic integers. That is, much of quantum mechanics can be discussed without resorting to the complex number field. Note also that the projective geometry that arises here is closely related to descriptions of entanglement measures, in particular, those known for three qubit systems.

Planar geometries of points and lines define a groupoidified Hecke algebra for the braid group $B_3$. This group is the fundamental group for the trefoil knot complement, and a covering of the modular group $PSL(2,\mathbb{Z})$. The covering relation is $(xy)(yx)=1$, which always holds for the equivalence classes of operators, which satisfy the weak Yang–Baxter rule. In other words, complementary observables actually provide representations of interesting subgroups of the modular group rather than true braids. However, their possible connection to the theory of the field on one element allows us to reinterpret the forced symmetry as a homomorphism from braid groups, which are considered as general linear groups for the field on one element. In other words, classical structures in quantum mechanics concretely manifest the symmetrization of tensor product for the natural braiding associated with the absolute point of $\mathbb{F}_1$, which, in some sense, represents the classical concept of a certain measurement outcome.

ACKNOWLEDGMENTS

I am grateful to Bob Coecke, Samson Abramsky, and the whole Foundations group at the Computing Laboratory for bringing me to Oxford and giving me the opportunity to do research. This work is funded by the QICS project.

18. C. Kassel, Quantum Groups (Springer-Verlag, Berlin, 1995).