Modal quantum theory

Benjamin Schumacher* and Michael D. Westmoreland†

Kenyon College and Denison University

Abstract

We present a discrete model theory similar in structure to ordinary quantum mechanics, but based on a finite field instead of complex amplitudes. The interpretation of this theory involves only the "modal" concepts of possibility and necessity rather than quantitative probability measures. Despite its simplicity, our model theory includes entangled states and has versions of both Bell's theorem and the no cloning theorem.

Modal quantum theory

In quantum theory, the states of physical systems are represented by vectors in a complex Hilbert space. The complex scalars serve as probability amplitudes, quantities whose squared magnitudes are the probabilities of measurement outcomes. Other types of quantum theory have sometimes been considered, based on real or quaternionic amplitudes [1, 2]. Though the quantum mechanics of nature does not appear to be real or quaterionic, these alternate mathematical formalisms shed light on the structure of the actual quantum theory (which we will here abbreviate AQT).

Here we will explore the properties of another type of "toy model" of quantum theory using scalars drawn from a finite field $\mathcal{F}$. The simplest

*Department of Physics, Kenyon College. Email schumacherb@kenyon.edu

†Department of Mathematical Sciences, Denison University. Email westmoreland@denison.edu

example is based on the two-element field $\mathbb{Z}_2$, but many other choices are possible. Our toy model lacks much of the mathematical paraphernalia of complex Hilbert spaces. For instance, there is no natural inner product and thus no concept of "orthogonality" between vectors. Nevertheless, we will find that the theory is well-defined, that it has a sensible interpretational framework, and that entanglement and many other aspects of AQT have analogues in the theory.

The interpretation of AQT involves quantitative probabilities, but our interpretation of finite-field theories is more primitive, involving only the distinction between *possible* and *impossible* events. Suppose $\mathcal{E}$ is the set of outcomes of some experiment. In AQT, a given quantum state would yield a probability distribution over the elements of $\mathcal{E}$. But our new theory will only designate a non-empty subset $\mathcal{P} \subseteq \mathcal{E}$, the set of possible results, without distinguishing more or less likely elements of the set. Any outcome not in $\mathcal{P}$ is taken to be impossible, and if $\mathcal{P}$ only contains a single element r, then we may say that r is "certain" or "necessary".

This distinction between "possible", "impossible" and "necessary" events is exactly the distinction used in modal logic [3]. Thus, we will refer to our finite-field quantum theories as *modal quantum theory*, or MQT.

For a finite field $\mathcal{F}$, the MQT state of a system is a non-null vector $|\psi)$ in a finite-dimensional vector space $\mathcal{V}$, which is isomorphic to $\mathcal{F}^d$ for some dimension d. A measurement on the system corresponds to a basis set $A = \{|a)\}$ for $\mathcal{V}$, where each basis element $|a)$ is associated with an outcome a of the measurement procedure. (Note that, in the absence of an inner product, there is no requirement in MQT that the basis elements be orthogonal.) Every state vector $|\psi)$ can be written

$$|\psi) = \sum_a \psi_a \, |a) \, , \tag{1}$$

where the coefficients ψ_a are scalars in $\mathcal{F}$. The measurement outcome a is possible if and only if $\psi_a \neq 0$. For the basis A and state $|\psi)$, the set of possible measurement results is thus

$$\mathcal{P}(A|\psi) = \{a : \psi_a \neq 0\}. \tag{2}$$

The simplest type of MQT has $\mathcal{F} = \mathbb{Z}_2$, and the simplest MQT system has state space dimension $d = 2$. The resulting example may

be called a *mobit*. A mobit has three states: basis states $|0)$ and $|1)$, and a single superposition state $|\sigma) = |0)+|1)$. In fact, any one of these states is a superposition of the other two, and so any pair of the states is a basis for the vector space. We define three modal observables, which we will call X, Y and Z, associated with the three possible basis sets. For each measurement, we can conveniently label the two outcomes by $+$ and $-$. That is,

$$\begin{array}{lll} |+_z) = |0) & |+_x) = |1) & |+_y) = |\sigma) \\ |-_z) = |1) & |-_x) = |\sigma) & |-_y) = |0) \end{array} . \tag{3}$$

The question of whether a basis element corresponds to a possible outcome generally depends on the entire basis. For example, consider the mobit state $|\sigma)$. If we measure Z then the result $(+_z)$ corresponding to the basis vector $|0)$ is possible. However, if we measure Y then the result $(-_y)$ corresponding to the same basis vector $|0)$ is not possible.

Things are clearer if we associate a measurement with a basis of the dual space $\mathcal{V}^*$. Every basis $\{|a)\}$ for $\mathcal{V}$ is associated with a dual basis $\{(a|\}$ for $\mathcal{V}^*$ such that $(a\,|\psi\,) = \psi_a$, the component of $|\psi)$ in Equation 1. (In the absence of an inner product, the correspondence between $|a)$ and $(a|$ is basis-dependent.) We call the functionals in $\mathcal{V}^*$ *effects* and say that an effect $(a|$ is possible given the state $|\psi)$ provided $(a\,|\psi\,) \neq 0$. Thus, given a basis A for $\mathcal{V}^*$,

$$\mathcal{P}(A|\psi) = \{a : (a\,|\psi\,) \neq 0\}. \tag{4}$$

The question of whether a particular effect is possible does not depend on the dual basis to which it belongs.

We can express the X, Y and Z mobit measurements using dual bases. Let $\{(0|\,, (1|\}$ be the dual basis corresponding to the $\{|0)\,, |1)\}$ basis. Thus $(0\,|0\,) = (1\,|1\,) = 1$ and $(0\,|1\,) = (1\,|0\,) = 0$. The remaining dual vector is $(\sigma| = (0| + (1|$. Then we have

$$\begin{array}{lll} (+_z| = (0| & (+_x| = (\sigma| & (+_y| = (1| \\ (-_z| = (1| & (-_x| = (0| & (-_y| = (\sigma| \end{array} . \tag{5}$$

Compare Equation 3.

Finally, we can outline a framework for describing the time evolution of a system in MQT. Time must be regarded as a sequence of discrete intervals. Just as in AQT, the "coherent" time evolution of a system

over one of these intervals is represented by a linear transformation T of the state vector. Thus, if $|a) \to |a') = T\,|a)$ and $|b) \to |b') = T\,|b)$ then

$$|a) + |b) \to T\,(|a) + |b)) = T\,|a) + T\,|b) = |a') + |b')\,. \tag{6}$$

Since the zero vector is not a physical state, we require that $T\,|a) \neq 0$ for any state $|a)$. This means that the kernel of T is trivial, so that T is invertible.

No additional restriction (such as unitarity in AQT) on the time evolution operator T is motivated by the general framework of MQT. We will generally suppose that any invertible linear transformation of state vectors corresponds to a possible time evolution of the system.

Entangled states

In AQT, the Hilbert space describing a composite system is the tensor product of the Hilbert spaces describing the individual subsystems. The same rule applies to the vector spaces in MQT. In general, a composite system may have both product states and non-product (entangled) states. Since the state spaces in MQT are discrete, we can calculate the numbers of product and entangled states for a given pair of systems. We find that every composite system has both product and entangled states, and that as the subsystem state space dimensions become large, the entangled states greatly outnumber the product states.

Consider a pair of mobits, for which $\mathcal{F} = \mathbb{Z}_2$. There are 15 allowed state vectors for the pair, all representing distinct states of the system. Nine of these are product states and six are entangled.

One particular entangled state of two mobits has especially elegant properties: $|S) = |0, 1) + |1, 0)$. Any product effect $(a, a|$ is impossible for $|S)$ because

$$(a, a\,|S\,) = (a\,|0\,)\,(a\,|1\,) + (a\,|1\,)\,(a\,|0\,) = 0 \tag{7}$$

(recalling that $x + x = 0$ in $\mathbb{Z}_2$). From the dual basis forms of the X, Y and Z measurements given in Equation 5, we can draw the following conclusions:

- If the same measurement is made on each mobit, then the only possible joint results have opposite values for each mobit. For example, $(+_z, -_z)$ is possible; the result $(+_z, +_z)$ is impossible, since $(+_z, +_z| = (0, 0|$.

- If different measurements are made on the mobits, then there is one joint result that is impossible. For example, $(+_z, -_x)$ is impossible, since $(+_z, -_x| = (0, 0|$.

Since corresponding measurements must lead to opposite results, the state $|S)$ is analogous to the "singlet" state $\frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle)$ of a pair of spins in AQT.

In AQT, Bell showed that the correlations between entangled quantum systems were incompatible with any local hidden variable theory [4]. He did this by devising a statistical inequality that must hold for local hidden variable theories but is violated by entangled quantum systems. Is there an analogous result for MQT? Unfortunately, in the absence of probabilities and expectation values the Bell approach will not work. However, Hardy [5] devised an alternate approach based only on possibility and impossibility.

Hardy constructs a non-maximally entangled state $|\Psi\rangle$ of a pair of qubits, together with binary observables A and B on each qubit. If we denote by $(x, y|X, Y)$ the outcome (x, y) of a joint measurement (X, Y), then Hardy's state has the following properties.

- $(0, 0|A, B)$ and $(0, 0|B, A)$ are both impossible—that is, they have quantum probability $p = 0$.

- $(0, 0|B, B)$ is possible $(p > 0)$.

- $(1, 1|A, A)$ is impossible $(p = 0)$.

How might a local hidden variable theory account for this situation? Since $(0, 0|B, B)$ is possible, we may restrict our attention to the set H of values of the hidden variables that lead to this result. The result of a measurement on one qubit is unaffected by a change in the choice of measurement on the other (locality). Furthermore, no allowed values of the hidden variables can lead to $(0, 0|A, B)$ or $(0, 0|B, A)$. Thus, for values in H, we would have to obtain the results $(1, 0|A, B)$ and $(0, 1|B, A)$. But these jointly imply that the result $(1, 1|A, A)$ would

be obtained for values in H, so that this result must be possible. This contradicts AQT.

In the same way, we can show that the structure of possible and impossible measurement results arising from the entangled mobit state $|S)$ above is incompatible with any local hidden variable theory.

In a hidden variable theory, we imagine that the MQT state $|S)$ corresponds to a set H of possible values of a hidden variable. We further imagine that the hidden variable controls the outcomes of the possible measurements on the mobits in a completely local way. That is, for any particular value $h \in H$, the set of possible results of Alice's measurement depends only on h and her own choice of measurement, not any measurement choices or results for Bob's mobit. Let $\mathcal{P}_h(E)$ be the set of possible results of a measurement of E for the hidden variable value h. Our locality assumption means that, given $V_{\rm A}$ and $W_{\rm B}$ measurements for Alice and Bob and a particular h value,

$$\mathcal{P}_h(V_{\rm A}, W_{\rm B}) = \mathcal{P}_h(V_{\rm A}) \times \mathcal{P}_h(W_{\rm B})\,, \tag{8}$$

the simple Cartesian product of separate sets $\mathcal{P}_h(V_{\rm A})$ and $\mathcal{P}_h(W_{\rm B})$.The MQT set of possible results arising from $|S)$ should therefore be

$$\mathcal{P}(V_{\rm A}, W_{\rm B}|S) = \bigcup_{h\in H} \mathcal{P}_h(V_{\rm A}) \times \mathcal{P}_h(W_{\rm A})\,. \tag{9}$$

The individual sets $\mathcal{P}_h(V_{\rm A})$, etc., are simultaneously defined for all of the measurements that can be made by Alice and Bob. Therefore, we may consider the set

$$\begin{aligned} \mathcal{J} \;=\; \bigcup_{h\in H} & \mathcal{P}_h(X_{\rm A}) \times \mathcal{P}_h(Y_{\rm A}) \times \mathcal{P}_h(Z_{\rm A}) \\ & \times \mathcal{P}_h(X_{\rm B}) \times \mathcal{P}_h(Y_{\rm B}) \times \mathcal{P}_h(Z_{\rm B})\,. \end{aligned} \tag{10}$$

There might be up to $2^6 = 64$ elements in $\mathcal{J}$. However, since $\mathcal{J}$ can only contain elements that agree with the properties of $|S)$, we can eliminate many elements. For instance, the fact that corresponding measurements on the two mobits must give opposite results tells us that $(+,+,+,+,+,+)$ cannot be in $\mathcal{J}$, though $(+,+,+,-,-,-)$ might be. However, when all the properties of $|S)$ are applied, we find the surprising result that *all* of the elements of $\mathcal{J}$ are eliminated. *No* assignment of

definite results to all six possible measurements can possibly agree with the correspondences obtained from the entangled MQT state $|S)$. We therefore conclude that these correspondences are incompatible with any local hidden variable theory.

Mixed states and cloning

In both actual quantum theory and modal quantum theory, a *mixed state* arises when we cannot ascribe a definite quantum state vector to a system. This may happen because several state vectors are possible, or because the system is only a part of a larger system in an entangled state.

Suppose that a system in MQT might be in any one of several possible states $|\psi_1)$, $|\psi_2)$, etc. We collect these together into a set M, which characterizes the mixture of states. An effect is possible for the mixture M if it is possible for at least one of the state vectors in M. Equivalently, we say that $(a|$ is *impossible* for M provided $(a\,|\psi\,) = 0$ for all $|\psi) \in M$.

Two mixtures M_1 and M_2 are equivalent when they lead to exactly the same possible effects. Because the effect functionals are linear, it follows that any mixture M is equivalent to the subspace $\langle M\rangle$ spanned by M. Therefore, two mixtures M_1 and M_2 will be equivalent if $\langle M_1\rangle = \langle M_2\rangle$. If the two mixtures span different subspaces, then we can always find an effect (a linear functional) which is possible for one but not the other. Therefore, we identify the mixed state $\mathcal{M}$ as the subspace $\langle M\rangle$ spanned by the mixture M. In MQT, mixed states are subspaces of $\mathcal{V}$.

How can we arrive at a mixed state for a subsystem of an entangled system in MQT? Suppose systems #1 and #2 have a joint state vector $|\psi_{12})$. Given a basis $\{|a)\}$ for system #1, we can write this as

$$|\psi_{12}) = \sum_a |a, \psi_a)\,. \tag{11}$$

We can take the non-zero states $|\psi_a)$ that appear in this to define a mixture M for system #2, which defines in turn a mixed state $\mathcal{M} = \langle M\rangle$. It is straightforward to show that this mixed state for system #2 is independent of the choice of basis $\{|a)\}$ for system #1.

Finally, we note that a no-cloning theorem holds in MQT, and that its proof is virtually identical to that of Wootters and Zurek for AQT [6]. We imagine a cloning machine that successfully copies distinct input states $|a)$ and $|b)$, a process that can be represented by the evolution of the input, output and machine systems:

$$|a, 0, M_0) \to |a, a, M_a) \quad \text{and} \quad |b, 0, M_0) \to |b, b, M_b)\,. \tag{12}$$

If we now consider the superposition input state $|c) = |a) + |b)$, linearity of the overall evolution means that the final state of input and output is instead either a superposition or mixture of $|a, a)$ and $|b, b)$ (depending on the relation of the final machine states $|M_a)$ and $|M_b)$). In neither case do we obtain the cloned state $|c, c) = |a, a) + |a, b) + |b, a) + |b, b)$. Therefore, any cloning machine in MQT must fail for some input states.

Superdense coding and teleportation

One remarkable feature of entangled states in AQT is superdense coding [7], whereby entanglement can double the information capacity of a quantum system. There is a straightforward analogue of this in MQT. Consider the following set of states for two mobits:

$$\begin{array}{ll} |R) = |0,0) + |1,1) & |U) = |0,0) + |1,0) + |1,1) \\ |S) = |0,1) + |1,0) & |V) = |0,0) + |0,1) + |1,0) \end{array}\,. \tag{13}$$

These four entangled states form a basis, and so may be identified with the outcome of some measurement. We also note that any of the four states can be transformed into any other one by invertible linear evolution on one of the mobits. Given operators G and K such that

$$\begin{array}{ll} G\,|0) = |1) & K\,|0) = |0) \\ G\,|1) = |0) & K\,|1) = |0) + |1) \end{array} \tag{14}$$

we find that

$$|S) = G_1\,|R) \qquad |U) = K_1\,|R) \qquad |V) = K_1 G_1\,|R)\,. \tag{15}$$

Suppose that Alice wishes to send Bob a message by transferring a single mobit to him. She can reliably transmit one bit (two possible

messages), since she can encode the message by two basis states $|0)$ and $|1)$, which Bob can distinguish by a Z measurement. She cannot send more without the possibility of error; and in any case, there are only three distinct mobit states available for her to use.

But now suppose instead that Alice and Bob initially share a pair of mobits in the joint state $|R)$. Alice can encode two bits (four possible messages) by choosing to apply the operators 1, G, K or KG to her mobit, resulting in one of the four states $|R)$, $|S)$, $|U)$ or $|V)$. If she then delivers her transformed mobit to Bob, he can perform a joint measurement on both mobits to reliably distinguish these possibilities. This is the MQT analogue of superdense coding.

The same set of entangled mobit states and single-mobit transformations can also be used to accomplish the MQT analogue of quantum teleportation [8].

Remarks

The mathematical structure of MQT is considerably simpler than the Hilbert space of AQT. Without an inner product, MQT lacks probability amplitudes (and thus probabilities), orthogonal bases, and unitary (inner-product-preserving) evolution. Without an outer product, MQT cannot represent mixed states by density operators, or numerical observables by Hermitian operators. There is no Hermitian conjugate (†) operation. Furthermore, when $\mathcal{F}$ is finite, systems only have a finite number of available states, and time evolution must be discrete rather than continuous.

Nevertheless, modal quantum theory exemplifies many of the basic ideas of actual quantum theory, and has analogues for many of the most striking quantum phenomena. There is a distinction between "classical" and "quantum" modal variables. Modal quantum systems exhibit superposition and interference effects, and the time evolution of an isolated system can be described by a linear operator. These systems display complementarity between incompatible observables. The properties of entangled states can be used to exclude local hidden variable theories and cloning; they also support information protocols such as superdense coding and teleportation. Finally, mixed states of modal quantum systems can be naturally identified with the subspaces of the

modal state space.

Thus, despite its extreme simplicity, MQT is a remarkably rich "toy model" for quantum physics.

References

[1] D. Finkelstein, J. M. Jauch, S. Schiminovich and D. Speiser, "Foundations of quaternion quantum mechanics", *Journal of Mathematical Physics* **3**, 207 (1962).

[2] S. Aaronson, "Is Quantum Mechanics an Island In Theoryspace?", *Proceedings of the Växjö Conference "Quantum Theory: Reconsideration of Foundations"*, A. Khrennikov, ed. (Växjö University Press, 2004).

[3] G. Hughes and M. Cresswell, *A New Introduction to Modal Logic* (Routledge, London, 1996).

[4] J. S. Bell, "On the Einstein-Podolsky-Rosen paradox", *Physics* **1**, 195 (1964).

[5] L. Hardy, "Non-locality for two particles without inequalities for almost all entangled states", *Physical Review Letters* **71**, 1665 (1993).

[6] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned", *Nature* **299**, 802 (1982).

[7] C. H. Bennett and S. J. Wiesner, "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states", *Physical Review Letters* **69**, 2881 (1992).

[8] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres and W. Wootters, "Teleporting an unknown quantum state via dual classical and EPR channels", *Physical Review Letters* **70**, 1895 (1993).