Quantum theory from questions

Philipp Andres Höhn[1,*] and Christopher S. P. Wever[2,3,†]

[1]*Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Waterloo, Ontario, Canada N2L 2Y5*
[2]*Institute of Nuclear and Particle Physics, NCSR "Demokritos," Agia Paraskevi, 15310 Athens, Greece*
[3]*Institute for Theoretical Particle Physics (TTP), Karlsruhe Institute of Technology, Engesserstraße 7, D-76128 Karlsruhe and Institute for Nuclear Physics (IKP), Karlsruhe Institute of Technology, Hermann-von-Helmholtz-Platz 1, D-76344 Eggenstein-Leopoldshafen, Germany*

(Received 27 February 2016; published 3 January 2017)

We reconstruct the explicit formalism of qubit quantum theory from elementary rules on an observer's information acquisition. Our approach is purely operational: we consider an observer O interrogating a system S with binary questions and define S's state as O's "catalog of knowledge" about S. From the rules we derive the state spaces for N elementary systems and show that (a) they coincide with the set of density matrices over an N-qubit Hilbert space $\mathbb{C}^{2^N}$; (b) states evolve unitarily under the group $\mathrm{PSU}(2^N)$ according to the von Neumann evolution equation; and (c) O's binary questions correspond to projective Pauli operator measurements with outcome probabilities given by the Born rule. As a by-product, this results in a propositional formulation of quantum theory. Aside from offering an informational explanation for the theory's architecture, the reconstruction also unravels previously unnoticed structural insights. We show that, in a derived quadratic information measure, (d) qubits satisfy inequalities which bound the information content in any set of mutually complementary questions to 1 bit; and (e) maximal sets of mutually complementary questions for one and two qubits must carry precisely 1 bit of information in pure states. The latter relations constitute conserved informational charges which define the unitary groups and, together with their conservation conditions, the sets of pure quantum states. These results highlight information as a "charge of quantum theory" and the benefits of this informational approach. This work emphasizes the sufficiency of restricting to an observer's information to reconstruct the theory and completes the quantum reconstruction initiated in a companion paper (P. Höhn, arXiv:1412.8323).

DOI: 10.1103/PhysRevA.95.012102

I. INTRODUCTION

Quantum theory has enjoyed an outstanding success, allowing us to make precise predictions about the physical microcosm, leading to new information technologies and withstanding every experimental test to which it has been exposed thus far. Yet, in contrast to special and general relativity, quantum theory has evaded a commonly accepted apprehension and interpretation of its physical content, in part as a consequence of a lack of physical statements that fully characterize it. But, what makes quantum theory special? Quantum theory has perhaps become so successful that questioning its foundations and physical content have become peripheral matters in physics. However, with the ambition of developing more fundamental theories, involving or going beyond quantum theory, the question as regards its physical meaning and characterizing features returns. How could the world be different if we dropped some of the latter? The answer requires a better understanding of quantum theory within a larger landscape of alternative theories. Furthermore, a convincing conceptual scheme for a putative quantum theory of gravity presumably requires a deeper understanding of what quantum theory tells us about Nature, and of what we can say about it.

To be sure, within the simplified context of finite-dimensional Hilbert spaces, there have been considerable efforts to identify physical attributes special to quantum theory to remedy the flaw that quantum theory is still defined by operationally obscure textbook axioms rather than transparent physical statements. Among them are violation of the Bell [1,2] and more generally Clauser-Horne-Shimony-Holt inequalities [3], the "no-signaling" principle [4] and, its generalization, "information causality" [5], interference effects in mixtures [6], absence of third- and higher-order interference [7,8], a limit on the information content carried by systems [9–21], and others. However, all of these attributes yield incomplete characterizations, being shared by other probabilistic theories some of which admit unphysical correlation structures, as well as exotic information communication and processing tasks.

In fact, there actually exist a number of successful reconstructions of finite-dimensional quantum theory from operational axioms, most of which have been performed within the frameworks of generalized or operational probability theories [8,22–31] (see also [32] which is adapted to a spacetime language and the more mathematical reconstructions [33,34]). Despite the beauty and great technical achievements of some of these reconstructions, they arguably come short of providing a fully satisfactory physical and conceptual picture of quantum theory. First, the underlying axioms, while mathematically crisp, are operationally and intuitively less transparent than a statement of the type "all inertial observers agree on the speed of light" underlying special relativity. However, for clarity it would be desirable to have easily understandable, yet powerful postulates. Second, the ensuing

*Present address: Vienna Center for Quantum Science and Technology, and Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences, Boltzmanngasse 3, 1090 Vienna, Austria; hoephil@gmail.com
†christopher.wever@kit.edu

derivations of the quantum formalism are rather implicit than constructive, lacking, in particular, simple and intuitively comprehensible explanations for typical quantum phenomena such as entanglement or for the origin of the explicit structure of the formalism. By contrast, in special relativity, most of its characteristic traits, such as relativity of simultaneity, Lorentz contraction, etc., can be explained in simple thought experiments invoking essentially only the constancy of the speed of light. Third, apart from showing that an operational perspective is sufficient for deriving quantum theory, these reconstructions are interpretationally fairly neutral, focusing on characterizing the formalism rather than the physical and conceptual content of the theory.

The goal of this paper is to improve the situation; we shall show that, at least in the simple context of qubit systems, one can understand the physical content of quantum theory from an informational perspective. To this end, we shall exhibit, using the framework developed in Ref. [35], how the quantum formalism can be constructively and explicitly derived from simple operationally comprehensible rules which restrict an observer's acquisition of information about systems he is observing. The acquisition of information of the observer about the systems will proceed by interrogation with binary questions. This reconstruction yields the detailed (and not only general) structure of qubit quantum theory and is thereby much less abstract than previous reconstructions. However, it also involves many more steps.

In contrast to earlier works which aim at intrinsic properties and states of systems, here we shall solely focus on the relation of the observer with the systems, i.e., ultimately on the information which the observer has experimentally access too. In particular, we take the quantum state to represent the observer's "catalog of knowledge" about the observed system(s), rather than an intrinsic state of the latter. This is conceptually motivated by and in line with the relational interpretation of quantum mechanics [9,35–38], the informational interpretation in Refs. [10,11,13,15] and (at least elements of) QBism [39–41]. While this general philosophy goes back to Rovelli's seminal *relational quantum mechanics* [9], none of these earlier works provide a concrete framework from which to reconstruct the theory. This is a shortcoming which has been overcome in Ref. [35] and which will be exploited in the sequel. As such, this paper (together with [35]) can be viewed as a completion, in the context of qubit systems, of many of the ideas put forward in these earlier works and, in particular, of relational quantum theory [9].

Denoting the observer by O and the system by S, the rules on information acquisition from which we derive the quantum theory of N qubits can be schematically summarized as follows:

(1) O can maximally acquire N independent bits of information about S at any time.

(2) O can always get up to N new independent bits of information about S.

(3) O's total amount of information about S is preserved in-between interrogations.

(4) O's catalog of knowledge of S evolves continuously and every consistent such evolution is physically realizable.

(5) O can ask S any binary question that "makes sense."

In fact, these five rules cannot distinguish two-level systems over complex and real Hilbert spaces. Since the latter is both mathematically and physically a subcase of the former, these five rules are sufficient. However, if one also wishes to distinguish these two cases operationally, then an additional rule, imposed solely for this purpose, will do the job:

(6) O can determine his catalog of knowledge of a composite system S by interrogating only its constituents.

While here we shall focus less on conceptual matters than in Ref. [35], the successful reconstruction from this perspective underscores the sufficiency of taking a purely operational perspective, addressing only what an observer can say about the observed systems, in order to understand and derive the formalism of quantum theory. Ontic statements about a reality underlying the observer's interactions with the physical systems are unnecessary. This lends weight to Bohr's famous quote: "It is wrong to think that the task of physics is to find out how Nature *is*. Physics concerns what we can *say* about Nature" [42].

Apart from the fact that this reconstruction offers an instructive perspective on the physical content of quantum theory, it also leads to practically useful results. The tools of [35], while not geared for doing concrete physics with them, are simple and especially devised to expose the structure of qubit quantum theory. They not only admit intuitive graphical representations of the ensuing logical and informational structure of the theory, but they also permit to unravel structural insights into qubit quantum theory that have gone unnoticed in the literature. In particular, we shall show how finitely many *conserved informational charges*, resulting from complementarity relations, elucidate the origin of the unitary (time evolution) group and characterize pure state spaces. As clarified along the way, these observations emphasize information as a "charge of quantum theory"; the observer's information provides the conserved quantities of the unitary group which can be transferred among his questions in-between measurements.

Certainly, there are also some shortcomings of our approach. First, at present the language of [35] is only applicable to qubit systems, although a suitable generalization appears feasible. Second, while our background assumptions are operationally and conceptually transparent, they may be mathematically stronger than those underlying, e.g., [22–24,26,29], thus, in a strict sense, admitting a mathematically weaker reconstruction from within a smaller landscape of theories. Nevertheless, the derivation is a nontrivial proof of principle of the approach and can presumably be strengthened since the set of assumptions and postulates may be nonoptimal in the sense of containing partially redundant information. Third, the explicit framework restricts to projective measurements on a subset of qubit observables [although, once one has reconstructed the quantum formalism, one ultimately has access to all quantum operations and positive operator-valued measures (POVMs)].

The content of the paper is organized as follows. In Sec. II we give a review of the framework developed in Ref. [35], which provides the context for our reconstruction of qubit quantum theory. All relevant assumptions and postulates for the reconstruction are summarized in order to make the

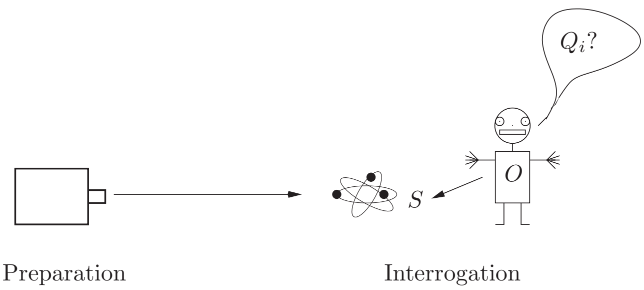


FIG. 1. An observer O interrogating a system S.

paper self-contained and we refer to [35] for a more detailed account. In Sec. III A we reconstruct the correct unitary time evolution group and state space of quantum theory for $N = 2$ qubits and in Sec. III B we extend their reconstruction to $N > 2$ qubits. The derivation of the set of binary questions which we permit an observer to ask a system of N qubits is performed in Sec. III C. This also involves a derivation of the Born rule for projective measurements. In Sec. III D we briefly discuss how the von Neumann evolution equation for the density matrix arises from our reconstruction and finally we present our conclusions in Sec. IV. In Appendix A we prove a statement of Sec. II G, while Appendixes B and C contain the detailed derivations of statements made in Secs. III A–III C, respectively.

II. BACKGROUND ASSUMPTIONS AND POSTULATES

The focus of this approach lies on the acquisition of information of an observer O about a set of systems and the relation this establishes between O and these systems. We shall follow the premise that we may only speak about the information which O has access to through interaction with the systems. This approach is thus purely operational, focusing on what an observer can say about a system rather than on the latter's intrinsic properties and states. This general philosophy has been inspired by Rovelli's *relational quantum mechanics* [9] and by the Brukner-Zeilinger informational interpretation of quantum theory [10,11,13,15], neither of which, however, offer a concrete framework for a reconstruction of quantum theory. The lack of a suitable mathematical framework for this endeavor has been overcome in Ref. [35] and this is what will be exploited in the remainder.

We shall begin by reviewing the landscape of theories within which the postulates for qubit quantum theory are formulated. This landscape is established by a set of operational background assumptions to which we expose O and the systems. The quantum postulates will constitute rules on O's acquisition of information about the systems. We refer to Ref. [35] for further details and more thorough explanations of the concepts employed below.

A. Basic setup: questions and answers

As in Fig. 1, the setup consists of a preparation device spitting out an ensemble of (identical) systems S_a, $a = 1,\dots,n$, which then are interrogated by O with *binary* questions. Every way of preparing the systems is assumed to yield a specific statistics over the answers to the binary questions which O may ask the S_a (for a sufficiently large ensemble). More precisely, we shall employ two basic ingredients:

(i) $\mathcal{Q}$ denotes the set of those binary questions Q_i which in this approach we permit O to ask a system S. We shall subject $\mathcal{Q}$ to a number of restrictions such that $\mathcal{Q}$ will ultimately be a strict subset of all possible binary questions which O could, in principle, ask S. For instance, whenever O asks S any $Q_i \in \mathcal{Q}$ he shall always get an answer[1] and any $Q_i \in \mathcal{Q}$ shall be nontrivial such that S's answer to it is not independent of its preparation. Furthermore, any $Q_i \in \mathcal{Q}$ shall be *repeatable*, i.e., if O asks the same Q_i m times in immediate succession on the same S he shall receive m times the same answer.

(ii) Σ denotes the set of all possible answer statistics for all $Q_i \in \mathcal{Q}$ for all possible ways of preparing the S_a.

In this work, we therefore do *not* address the measurement problem: we simply assume a division between the system S and a "classical" observer O and shall neither explain the origin and nature of this "classical" O, nor why S gives definite answers (i.e., yields definite measurement outcomes) upon being asked some $Q_i \in \mathcal{Q}$ by O. This will nevertheless allow us to derive the quantum formalism for qubits relative to this O.

Just like any experimenter in a real laboratory, we assume O to have developed a theoretical model by means of which he interprets the outcomes to his interrogations (and which, up to his experimental accuracy, is consistent with his observations). In particular, we shall assume O to have a model for both $\mathcal{Q}$ and Σ and thereby to be able to decide whether a given question is contained in (his model for) $\mathcal{Q}$ or not. In this work, it is not our ambition to clarify how O has arrived at this model. Instead, it will be our task to determine what this model is, subject to the background assumptions and postulates below.

B. Probabilities and notions of independence and compatibility

For any specific system S to be interrogated next, O assigns a probability y_i that the answer to any $Q_i \in \mathcal{Q}$ will be "yes" in a Bayesian manner. O will estimate y_i according to his model of Σ and to any *prior* information about S, which consists of frequencies of "yes" and "no" answers recorded in a previous interrogation of an ensemble of systems prepared identically to S. In the sequel, O is only permitted to acquire information about the systems through the binary questions in $\mathcal{Q}$. Hence, the y_i encode O's entire information about a system S. We thus identify *the state of S relative to O* as O's catalog of knowledge about S, namely, as the collection of $\{y_i\}_{\forall\, Q_i\in\mathcal{Q}}$. It thus is a state of information associated to the relation of O with S and not an intrinsic state of S. The state is an element of Σ which therefore constitutes the *state space* of S and any state in Σ assigns a probability y_i for all $Q_i \in \mathcal{Q}$.

For operational reasons, Σ is assumed to be convex. This will permit O to build convex combinations of states; thereby

[1] In this work, we tacitly assume the probability for S being present to be 1.

O is able to assign a single prior state to a collection of identical systems [i.e., systems with identical $(\mathcal{Q},\Sigma)$, but not necessarily in the same state] when he uses a (possibly biased) coin toss cascade to decide which of the systems to interrogate (see [35] for more details).

We require that a special method of preparation exists which produces entirely random question outcomes. More precisely, we assume that there exists a special state in Σ, defined by $y_i = \frac{1}{2}, \forall\ Q_i \in \mathcal{Q}$ and referred to as the *state of no information*. Note that the existence of this state is a restriction on the pair $(\mathcal{Q},\Sigma)$.[2] This state of no information serves two purposes: (1) it is the prior state O will start with in a Bayesian updating once he has "no prior information" about a system other than what the corresponding model $(\mathcal{Q},\Sigma)$ is (including also the set of possible time evolutions $\mathcal{T}$, see below); and (2) it permits us to define a notion of *independence* of questions. Indeed, the notion of independence of questions is state dependent[3] such that we need a distinguished state relative to which we can unambiguously define it.

More precisely, consider $Q_i \in \mathcal{Q}$ and assume O receives S in the state of no information. On account of repeatability, upon asking S the question Q_i and receiving the answer "yes" or "no", O will assign a probability of $y_i = 1$ or 0, respectively, that he will receive a "yes" answer from S if asking Q_i again. This is part of a *state update rule* which permits O to update his information about the specific S which he is interrogating according to the answers he receives. Clearly, the probability y_j for any other $Q_j \in \mathcal{Q}$ will depend on this update rule. We shall not specify the update rule much further, but just assume that there is a consistent one. Given such an update rule, we shall call $Q_i, Q_j \in \mathcal{Q}$ as follows:

Independent if, after having asked Q_i to S in the state of no information, the probability $y_j = 1/2$. That is, if the answer to Q_i relative to the state of no information tells O "nothing" about the answer to Q_j.

Dependent if, after having asked Q_i to S in the state of no information, the probability $y_j = 0,1$. That is, if the answer to Q_i relative to the state of no information implies also the answer to Q_j.

Partially dependent if, after having asked Q_i to S in the state of no information, the probability $y_j \neq 0,\frac{1}{2},1$. That is, if the answer to Q_i relative to the state of no information gives O partial information about the answer to Q_j.

We shall require that these (in)dependence relations be symmetric such that, e.g., Q_i is independent of Q_j iff Q_j is independent of Q_i,[4] etc. We emphasize that these notions of (in)dependence are *a priori* update rule dependent.

We also need a notion of compatibility and complementarity; $Q_i, Q_j \in \mathcal{Q}$ are called as follows:

(*Maximally*) *compatible* if O may know the answers to both Q_i, Q_j simultaneously, i.e., if there exists a state in Σ such that y_i, y_j can be simultaneously 0 or 1.

(*Maximally*) *complementary* if every state in Σ which features $y_i = 0,1$ necessarily implies $y_j = \frac{1}{2}$ (and vice versa).

One can also define notions of partial compatibility [35].

This brings us to our last constraint on the update rule: if Q_i, Q_j are maximally compatible and independent, then asking Q_i shall not change y_j, and vice versa, regardless of S's state. That is, by asking a question Q, O shall not gain or lose information about questions which are compatible with but independent of Q.

For clarification, we emphasize that the assumption is as follows: $\mathcal{Q}$ is sufficient to describe the properties of S and, in particular, any of its states. From the perspective of information acquisition it is also natural to assume that there exists a state corresponding to O having "no information" about the measurement outcomes of those properties that he uses to characterize S; $\mathcal{Q}$ contains questions that are "natural" in this sense. The assumption, however, is *not* that $\mathcal{Q}$ encodes a complete description of *all* the binary measurements O can physically carry out on S. We say nothing about whether O cannot, in principle, also physically perform other measurements. While these would not be contained in $\mathcal{Q}$, they would also not be necessary to do tomography on S and thus to describe its state. For our purposes, it is therefore sufficient to restrict O to the "natural" set $\mathcal{Q}$. Ultimately, upon imposing the quantum principles, this will result in projective binary measurements as the "natural" questions, while nonprojective POVMs would not be encompassed by $\mathcal{Q}$.

C. Informational completeness

We shall call a set of pairwise-independent questions $\mathcal{Q}_M := \{Q_1,\dots,Q_D\}$ *maximal* if no further question from $\mathcal{Q}\setminus\mathcal{Q}_M$ can be added to it that is also pairwise independent of all other members of $\mathcal{Q}_M$ too. Pairwise-independent questions shall constitute the fundamental building blocks of the theories we consider. As such, we shall assume that any maximal set of pairwise-independent questions $\mathcal{Q}_M$ also constitutes an *informationally complete set of questions* in the sense that, for S in *any* state from Σ, the probabilities $\{y_i\}_{i=1}^D$ are sufficient to compute all $y_j\ \forall\ Q_j \in \mathcal{Q}$. This is a nontrivial restriction; if it was not satisfied, O would require additional questions that are at least partially dependent on some elements in $\mathcal{Q}_M$ in order to parametrize Σ. This would complicate the discussion and conflict with our premise that pairwise-independent questions form the fundamental building blocks of system descriptions.

[2]Clearly, not all pairs $(\mathcal{Q},\Sigma)$ will satisfy this. For example, ({binary POVMs},{density matrices}) would not satisfy this restriction since there does not exist a quantum state which yields probability 1/2 for *all* binary POVMs. Namely, there exist binary POVMs with an inherent bias, such as $(E_1 = \frac{2}{3}\cdot\mathbb{1}, E_2 = \frac{1}{3}\cdot\mathbb{1})$.

[3]For example, in quantum theory, the questions $Q_{x_1} =$ "is the spin of qubit 1 up in x direction?" and $Q_{x_2} =$ "is the spin of qubit 2 up in x direction?" are independent relative to the completely mixed state, however, not relative to an entangled state (with correlation in x direction).

[4]This means that Q_i, Q_j are stochastically independent with respect to the state of no information, i.e., the joint probabilities factorize relative to the latter, $p(Q_i,Q_j) = y_i\cdot y_j = \frac{1}{2}\cdot\frac{1}{2} = \frac{1}{4}$, where $p(Q_i,Q_j) = p(Q_j,Q_i)$ denotes the probability that Q_i and Q_j give "yes" answers if asked in *sequence* on the same S.

We thus simply preclude this complication by making the assumption of informational completeness[5] which, however, still leaves open a large landscape of theories compatible with it. Then, one can show that any such $\mathcal{Q}_M$ contains the same number D of elements [35]. In consequence, we may represent Σ as a D-dimensional convex set, with states as vectors

$$\vec{y} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_D \end{pmatrix}.$$

Any convex set is defined by its extremal points [43]. The extremal states in Σ are special because they cannot be written as convex mixtures of other states, but all other states are convex mixtures of these. Since (finite) convex mixtures can be operationally understood in terms of (cascades of biased) coin flips, O may prepare nonextremal states by applying cascades of coin flips to ensembles of extremal states. But, since the extremal states themselves cannot be prepared via coin-flip cascades from other states, their preparation must have an unambiguous operational meaning. For this purpose, we wish any extremal state to be achievable by O as the posterior state of an individual system in an interrogation. More specifically, we shall require that O can prepare *any* extremal state from the state of no information in a *single shot interrogation*[6] by only asking questions from an informationally complete set $\mathcal{Q}_M$ and possibly letting the resulting state evolve in time.

It will become crucial to appropriately quantify O's information about any system. To this end, we quantify O's information about the outcome to any $Q_i \in \mathcal{Q}$ implicitly by a function $\alpha(y_i)$ with $0 \leqslant \alpha(y_i) \leqslant 1$ bit and $\alpha(y) = 0 \Leftrightarrow y = \frac{1}{2}$ and $\alpha(0) = \alpha(1) = 1$ bit. O's total information about S must be a function of the state $\vec{y}$; we define it to be

$$I(\vec{y}) := \sum_{i=1}^{D} \alpha(y_i).$$

The specific form of α is derived from the principles.

D. Complementarity properties

For practical purposes, we shall also sharpen the notion of complementarity of questions. First, we shall permit O to use classical rules of inference (in the form of Boolean logic) exclusively on sets of *mutually compatible* questions. Classical rules of inference assume propositions to have truth values simultaneously which, in O's description of the world, is only true for mutually compatible questions because any truth value must be operational. This is to prevent him from making statements about logical connectives of complementary questions whose truthfulness he could never test by interrogations (see [35]).

Second, we shall require that any set of $n \in \mathbb{N}$ mutually (maximally) complementary questions $\{Q_1, \ldots, Q_n\}$ (not to be confused with $\mathcal{Q}_M$ above) cannot support more than 1 bit of information:

$$\alpha(y_1) + \cdots + \alpha(y_n) \leqslant 1 \text{ bit}. \tag{2.1}$$

This statement follows trivially from the definition of complementarity and the basic requirements on α whenever O has maximal information $\alpha(y_i) = 1$ bit about any question in this set. However, we require (2.1) for *all* states for otherwise it would be possible for O to *reduce* his total information about this set by asking another question from it. Namely, suppose (2.1) was violated. Then, upon asking *any* question from this set, he will have maximal information about this question and none about the others such that (2.1) would be saturated again and O has experienced a net loss of information about the set. Such peculiar situations will be ruled out in O's world. We shall call the informational relations defined by (2.1) *complementarity inequalities*. They can be viewed as informational uncertainty relations, describing how the information gain about one question enforces an information loss about questions complementary to it.

E. Composite systems

Since we will be dealing with systems composed of N qubits below, we must clarify what kind of composite systems we shall consider in this language. Let $\mathcal{Q}_{A,B}$ be the question sets associated to systems $S_{A,B}$. We shall say that they form the composite system S_{AB} if all questions in $\mathcal{Q}_A$ are maximally compatible with questions in $\mathcal{Q}_B$ and if

$$\mathcal{Q}_{AB} = \mathcal{Q}_A \cup \mathcal{Q}_B \cup \tilde{\mathcal{Q}}_{AB}, \tag{2.2}$$

where $\tilde{\mathcal{Q}}_{AB}$ contains only composite questions that are iterative compositions $Q_a *_1 Q_b, Q_a *_2 (Q_{a'} *_3 Q_b), (Q_a *_4 Q_b) *_5 Q_{b'}, (Q_a *_6 Q_b) *_7 (Q_{a'} *_8 Q_{b'}), \ldots$ via some logical connectives $*_1, *_2, *_3, \ldots$ of questions $Q_a, Q_{a'}, \ldots \in \mathcal{Q}_A$ and $Q_b, Q_{b'}, \ldots \in \mathcal{Q}_B$. Given the assumption about rules of inference above, note that O can only logically connect two (possibly composite) questions *directly* with some $*$ if they are compatible [35]. The logical connective $*$ which can be used to build informationally complete sets for composite systems will be determined later. We use this definition of composite systems recursively for more than two systems.

F. Time evolution

The state that O assigns to the system S is allowed to evolve in time. We shall assume temporal translation invariance, such that any time evolution defines a map $T_{\Delta t}[\vec{y}(t_0)] = \vec{y}(t_0 + \Delta t)$ from Σ to itself which only depends on the time interval Δt and not, however, on the instant of time itself. The set of all possible time evolutions T will be denoted by $\mathcal{T}$ and constitutes another ingredient of O's model for describing S. O's theoretical model for S is thus encoded in the triple $(\mathcal{Q}, \Sigma, \mathcal{T})$.

[5]We do not rule out the possibility that this property of informational completeness of maximal sets could also be proven using the principles below. In fact, for certain subcases the authors were able to prove it. However, the general case remains open.

[6]In a single shot interrogation, a single system S is prepared in some state and subsequently exposed to questions (see [35] for more details).

G. How to compute probabilities

The assumption of informational completeness asserts that the probabilities for "yes" outcomes to the questions in an informationally complete set are sufficient to compute the outcome probabilities for *all* questions in the set $\mathcal{Q}$ in *any* given state. Hence, by assumption, the probability function $Y(Q|\vec{y})$ that $Q =$ "yes", given the state $\vec{y}$, exists and is meaningful for all $Q \in \mathcal{Q}$. But, how do we compute it?

Suppose O has access to two identical (but not necessarily identically prepared) systems[7] S_1, S_2 such that O may ask the same questions to both. O may perform a biased coin flip which yields "heads" with probability $\lambda \in [0,1]$, in which case he will interrogate S_1, and "tails" with probability $(1-\lambda)$ in which case he will interrogate S_2. This implies that the state of the combined system (before tossing the coin) reads as $\vec{y}_{12} = \lambda\,\vec{y}_1 + (1-\lambda)\,\vec{y}_2$ since this holds for each component y_i (see also [35]). We recall from Sec. II B that O determines the probabilities by recording the frequencies of question outcomes in repeated interrogations of identically prepared systems. Hence, $Y(Q|\vec{y})$ is determined from the frequency of "yes" outcomes of Q when asked to a very large (ideally infinite) ensemble of systems identically prepared in the state $\vec{y}$. But, then

$$Y[Q|\lambda\,\vec{y}_1 + (1-\lambda)\,\vec{y}_2] = \lambda\,Y(Q|\vec{y}_1) + (1-\lambda)\,Y(Q|\vec{y}_2)$$

since O may repeat this interrogation of S_1, S_2 a very large number of times. In that case, the heads and tails ensembles constitute subensembles of the total ensemble of systems being interrogated and O could just record the frequencies of the $Q =$ "yes" outcomes relative to (1) the total ensemble, (2), the heads ensemble, and (3) the tails ensemble. Taking the relative frequency λ of the heads and tails ensembles into account, it is clear that the total frequency of $Q =$ "yes" outcomes must be of the form above (see also [22]).

Using that in the state of no information $\vec{y} = \frac{1}{2}\,\vec{1}$ we must have $Y(Q|\frac{1}{2}\,\vec{1}) = \frac{1}{2}$ for all $Q \in \mathcal{Q}$, where $\vec{1}$ is a vector with each coefficient equal to 1 (in the basis corresponding to the informationally complete set), we show in Appendix A that this implies affine linearity in the state $\vec{y}$:

$$Y(Q|\vec{y}) = Y(\vec{q}|\vec{y}) = \tfrac{1}{2}[\vec{q}\cdot(2\vec{y} - \vec{1}) + 1]. \tag{2.3}$$

Here, $\vec{q} \in \mathbb{R}^D$ is a vector which depends on $Q \in \mathcal{Q}$. This formula will ultimately give rise to the Born rule (for projective measurements).

We thus see that every question $Q \in \mathcal{Q}$ can be parametrized by a *question vector* $\vec{q} \in \mathbb{R}^D$ such that $Y(Q|\vec{y}) \in [0,1]\ \forall\ \vec{y} \in \Sigma$. O can chose to remove any redundancy from his description of $\mathcal{Q}$. Clearly, if $Q, Q' \in \mathcal{Q}$ were both represented by the same $\vec{q}$, then they would give rise to exactly the same "yes" probabilities in every state. But, if Q, Q' are probabilistically not distinguishable, O must regard them as being logically equivalent in his world. O is free to restrict his description of $\mathcal{Q}$ by erasing any questions from it that are redundant through equivalence.[8] As a result, every question vector $\vec{q}$, if physically permitted at all, will correspond to a unique $Q \in \mathcal{Q}$.

Given the assumption that S always gives an answer to any $Q \in \mathcal{Q}$ if asked by O, it is clear that for *every* $Q \in \mathcal{Q}$ there exists a state $\vec{y}_Q$ of S encoding the situation that O has asked *only* the single question Q to S in the state of no information $\vec{y} = \frac{1}{2}\vec{1}$ and received a "yes" answer (i.e., $\vec{y}_Q$ is the updated state after receiving $Q =$ "yes" relative to $\vec{y} = \frac{1}{2}\vec{1}$). We shall make one natural (but nontrivial) requirement: since O had precisely 0 bits of information prior to asking Q and $\vec{y}_Q$ corresponds to only having received the answer to this question, $\vec{y}_Q$ shall encode precisely 1 independent bit of information. We thus demand that for every $Q \in \mathcal{Q}$ there exists $\vec{y}_Q \in \Sigma$ with $I(\vec{y}_Q) = 1$ bit such that $Y(Q|\vec{y}_Q) = 1$.

This concludes our review of the landscape of inference theories.

H. Quantum principles as rules on information acquisition

Within this landscape, we shall impose five rules on the acquisition of information of O about a composite system S of $N \in \mathbb{N}$ generalized bits (or gbits) from Ref. [35] to which we refer for motivation. The rules are given both in colloquial and mathematical form. For clarification, we shall attach the number N henceforth to $\mathcal{Q}_N, \Sigma_N, \mathcal{T}_N$. The first two principles assert a limit on the information available to O and the existence of complementarity.

Principle 1: (*Limited information*). "The observer O can acquire maximally $N \in \mathbb{N}$ independent bits of information about the system S at any moment of time."

There exists a maximal set $Q_i, i = 1, \ldots, N$, of N mutually maximally independent and compatible questions in $\mathcal{Q}_N$.

Principle 2: (*Complementarity*). "The observer O can always get up to N new independent bits of information about the system S. But, whenever O asks S a new question, he experiences no net loss in his total amount of information about S."

There exists another maximal set Q'_i, $i = 1, \ldots, N$, of N mutually maximally independent and compatible questions in $\mathcal{Q}_N$ such that Q'_i, Q_i are maximally complementary and $Q'_i, Q_{j\neq i}$ are maximally compatible.

The systems are thus characterized by the number N. Principles 1 and 2 are conceptually motivated by earlier proposals by Rovelli [9] and Brukner and Zeilinger [10–14]. However, they do not suffice. We also require O not to gain or lose information without asking questions.

Principle 3: (*Information preservation*). "The total amount of information O has about (an otherwise noninteracting) S is preserved in-between interrogations."

$I(\vec{y})$ is *constant* in time in-between interrogations for (an otherwise noninteracting) S.

In fact, this principle can also be used to define the notion of "noninteracting."

[7] By identical systems we mean systems featuring the same triple $(\mathcal{Q}, \Sigma, \mathcal{T})$ (see [35] for further details on identical systems and a definition of "identically prepared").

[8] For example, if $Q \in \mathcal{Q}$ then clearly $Q \wedge Q$ and $Q \vee Q$ can be safely omitted by O from a nonredundant description of $\mathcal{Q}$.

In order to render O's world interesting for him, it should be as dynamical and interactive as possible. We shall thus require that it "maximizes" the number of ways in which any given state of S can change in time rather than the number of states in which it can be relative to O.

Principle 4: (*Time evolution*). "O's catalog of knowledge about S changes continuously in time in-between interrogations and every consistent such evolution is physically realizable."

$\mathcal{T}_N$ is the maximal set of transformations $T_{\Delta t}$ on states such that, for any *fixed* state $\vec{y}$, $T_{\Delta t}(\vec{y})$ is *continuous* in Δt and compatible with Principles 1–3 (and the structure of the theory landscape).

These four rules on O's acquisition of information about S will determine $(\Sigma_N, \mathcal{T}_N)$ and informationally complete sets $\mathcal{Q}_{M_N}$, however, not the *full* $\mathcal{Q}_N$. We thus add another rule: we shall allow O to ask S *any* question which "makes sense."

Principle 5: (*Question unrestrictedness*). "Every question which yields legitimate probabilities for every way of preparing S is physically realizable by O."

Every question vector $\vec{q} \in \mathbb{R}^{D_N}$ which satisfies $Y(\vec{q}|\vec{y}) \in [0,1]\ \forall\ \vec{y} \in \Sigma_N$ and for which there exists $\vec{y}_Q \in \Sigma_N$ with $I(\vec{y}_Q) = 1$ bit such that $Y(\vec{q}|\vec{y}_Q) = 1$ corresponds to a $Q \in \mathcal{Q}_N$.

It is our task to derive what the triple $(\mathcal{Q}_N, \Sigma_N, \mathcal{T}_N)$ compatible with the rules is. As shown in Ref. [35], there are only two solutions to these five principles within the established landscape of theories: In this paper we shall complete the proof that one solution is standard qubit quantum theory and, as exhibited in a companion paper [44], the second solution is rebit quantum theory, i.e., two-level systems over real Hilbert spaces. The second solution is mathematically a subcase of the former and also experimentally realizable in a laboratory. Therefore, the above five rules are physically sufficient. If, however, one wishes to discriminate between the two solutions, one may invoke the following additional rule adapted from [23–26,28,45,46]:

Principle 6: (*Tomographic locality*). "If S is a composite system, O can determine its state by interrogating only its subsystems."

It follows from [35] that this last rule eliminates rebits in favor of qubits. We shall appeal to tomographic locality in this paper *solely* for this purpose.[9]

More precisely, we shall prove that Principles 1–6 are equivalent to (part of) the textbook axioms:

Claim. The only solution to Principles 1–6 is qubit quantum theory where

(i) $\Sigma_N \simeq$ convex hull of $\mathbb{CP}^{2^N-1}$ is the space of $2^N \times 2^N$ density matrices over $\mathbb{C}^{2^N}$;

(ii) states evolve unitarily according to $\mathcal{T}_N \simeq \mathrm{PSU}(2^N)$ and the equation describing the state dynamics is (equivalent to) the von Neumann evolution equation;

[9]In fact, this rule is quite possibly a partially redundant addition. At least in the context of generalized probability theories [23–26,28,45,46], tomographic locality implies some of the properties that already follow from the other rules.

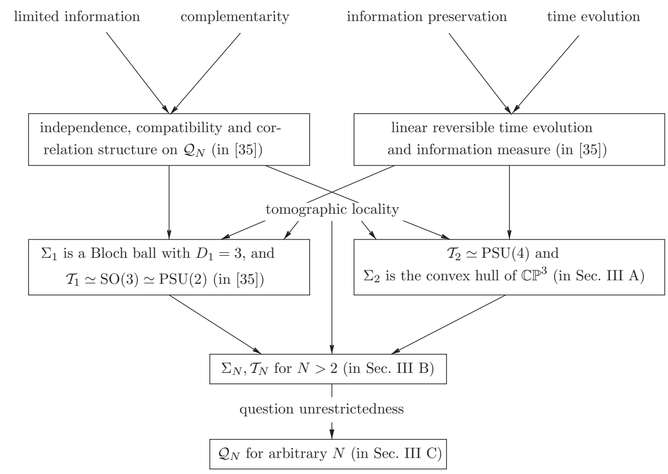


FIG. 2. Strategy and main steps of the reconstruction.

(iii) $\mathcal{Q}_N \simeq \mathbb{CP}^{2^N-1}$ is (isomorphic to) the set of projective measurements onto the $+1$ eigenspaces of N-qubit Pauli operators[10] and the probability for $Q \in \mathcal{Q}_N$ to be answered with "yes" in some state is given by the Born rule for projective measurements.

I. Summary of previous results and strategy

The essential steps of the proof and derivation of qubit quantum theory, involving results from [35], can be summarized diagrammatically (see Fig. 2). In particular, in Ref. [35] the entire compatibility, complementarity, and independence structure of any informationally complete set $\mathcal{Q}_{M_N}$ for arbitrary N is derived, showing that the logical connective $*$ in Eq. (2.2) which can be used to build $\mathcal{Q}_{M_N}$ from subsystem questions must either be the XNOR or the (up to an overall negation) equivalent XOR. As a by-product, it is demonstrated how entanglement, monogamy, and the correlation structure for arbitrarily many qubits follow from Principles 1 and 2 alone. Furthermore, Principles 3 and 4, together with elementary operational conditions, can be shown to entail (a) a linear *reversible* time evolution of the Bloch vector $\vec{r} = 2\,\vec{y} - \vec{1}$ under a continuous one-parameter matrix group, and (b) a quadratic information measure

$$\alpha(y_i) = (2\,y_i - 1)^2. \tag{2.4}$$

The total information $I_N(\vec{y}) = |\vec{r}|^2$, quantifying O's information about S, is thus the square norm of the Bloch vector [35]. This quadratic information measure was earlier proposed by Brukner and Zeilinger from a different perspective [11,12,14,47,48]. Finally, it is demonstrated in Ref. [35] how the conjunction of these results correctly yields the three-dimensional Bloch ball together with its isometry group $\mathrm{SO}(3) \simeq \mathrm{PSU}(2)$ as the state space Σ_1 and time evolution group $\mathcal{T}_1$, respectively, for a single qubit (i.e., the $N = 1$ case). It was also argued that $\mathcal{Q}_1 = \mathbb{CP}^1$. But, the reconstruction of $(\mathcal{Q}_N, \Sigma_N, \mathcal{T}_N)$ was left open for $N > 1$.

[10]The set of Pauli operators is given by all Hermitian operators on $\mathbb{C}^{2^N}$ with two eigenvalues ± 1 of equal eigenspace dimensions.

J. Pure states

With Principle 1 at our disposal, we can define a notion of *pure state*: a pure state of S_N (a composite system of N gbits) is a state of maximal information (and thus of maximal length) in which O knows the maximal amount of N independent bits of information.[11]

III. RECONSTRUCTION

These results will be exploited in the sequel to extend the reconstruction to arbitrary $N > 1$ and thus to prove the claim given in the previous section. This will complete the work started in Ref. [35].

A. $N = 2$ qubits

Principles 1, 2, and 6 imply that an informationally complete question set for two qubits is given by six individual questions $\{Q_{x_1}, Q_{y_1}, Q_{z_1}, Q_{x_2}, Q_{y_2}, Q_{z_2}\}$ about qubits 1 and 2 and by nine "correlation questions" $\{Q_{xx}, Q_{xy}, Q_{xz}, Q_{yx}, Q_{yy}, Q_{yz}, Q_{zx}, Q_{zy}, Q_{zz}\}$, where, e.g., $Q_{xx} := Q_{x_1} \leftrightarrow Q_{x_2}$ represents the question, "are the answers to Q_{x_1} and Q_{x_2} the same?," and $\leftrightarrow$ denotes the XNOR connective.[12] Proving this statement is quite nontrivial and takes a number of steps which, for reasons of space, we shall not summarize here. Instead, we shall simply use this result and refer the interested reader to Ref. [35] for a constructive proof of it.

For example, for two spin-$\frac{1}{2}$ particles Q_{x_1}, Q_{xx} could represent the questions "is the spin of qubit 1 up in the x direction?" and "are the spins of qubits 1 and 2 correlated in the x direction?," respectively. The compatibility, complementarity, and correlation structure of these questions, ensuing from Principles 1 and 2, is derived in Ref. [35], and is represented in terms of correlation triangles in Fig. 3.

For the sequel, it is important to note that we could have equally chosen to use the XOR instead of the XNOR connective to build up composite questions from individual questions (the XOR is up to an overall negation equivalent to the XNOR) [35]. For example, in that case and instead of Q_{xx} as defined above, we would have $\tilde{Q}_{xx} := \neg(Q_{x_1} \leftrightarrow Q_{x_2})$ as an "anti-correlation question", corresponding to "are the answers to Q_{x_1} and Q_{x_2} different?." This would yield a logically equivalent representation of O's experiences in his world, however, with flipped correlation structure (e.g., with odd correlation triangles in Fig. 3 replaced by even ones, and vice versa). For $N > 2$ gbits, different conventions of how to build up composite questions from the individual ones using the allowed XNOR or XOR can lead to many equivalent representations that will also arise in the reconstruction below. Therefore, to fix the representation, we shall henceforth make the convention that we build up composite questions from the individual ones for $N \geqslant 2$ solely by the XNOR connective.

[11] We emphasize the difference to reconstructions within the context of generalized probability theories [23–26,28,45,46] where pure states are simply defined to be the extremal states of the convex state space.

[12] We recall that $Q \leftrightarrow Q' = 1$ if $Q = Q'$ and $Q \leftrightarrow Q' = 0$ otherwise.

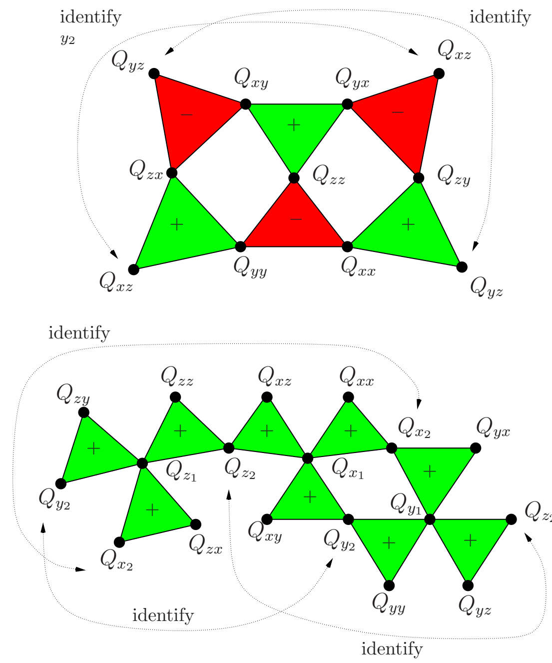


FIG. 3. The compatibility, complementarity, and correlation structure of an informationally complete set for two qubits. If two questions are connected by an edge, they are compatible. If two questions are *not* connected by an edge, they are complementary. Red triangles denote *odd* (or anti)correlation; for instance, $Q_{zz} = \neg(Q_{xx} \leftrightarrow Q_{yy})$. Green triangles symbolize *even* correlation; for example, $Q_{zz} = Q_{xy} \leftrightarrow Q_{yx}$. Every question resides in exactly three triangles and is thereby compatible with six and complementary to eight other questions. (See [35] for further details.)

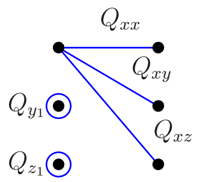
We note that a *pure state* as a state of maximal information will have length

$$I_{N=2}(\vec{r}_{\text{pure}}) = |\vec{r}_{\text{pure}}|^2 = 3 \text{ bits},$$

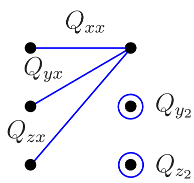
corresponding to O knowing the answers to two independent and compatible questions with certainty (Principle 1)—this yields two *independent* bits—and, on account of the XNOR properties, also knowing the correlation of these questions—this yields a third *dependent* bit [35]. For instance, if O knows the answers to Q_{x_1}, Q_{x_2}, he evidently knows the answer to Q_{xx} too. By Principle 3, the time evolution image of any such state will feature the same length and thus constitutes a pure state too.

1. *Maximal mutually complementary sets of questions*

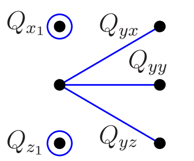
The three questions $\{Q_x, Q_y, Q_z\}$ form a single maximal mutually complementary set of questions for a single qubit. It is also useful to group the 15 questions for two qubits into *maximal mutually complementary sets* such that no further question can be added to such a set which would be complementary to all others in the same set too. This results in six complementarity sets, each containing five questions, which can be understood and represented conveniently in terms of question graphs



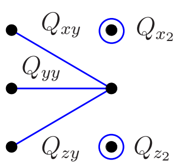
$$\mathrm{Pent}_1 = \{Q_{xx}, Q_{xy}, Q_{xz}, Q_{y_1}, Q_{z_1}\},$$



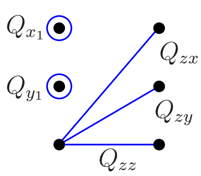
$$\mathrm{Pent}_2 = \{Q_{xx}, Q_{yx}, Q_{zx}, Q_{y_2}, Q_{z_2}\},$$



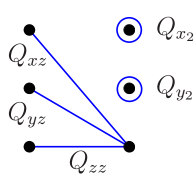
$$\mathrm{Pent}_3 = \{Q_{yx}, Q_{yy}, Q_{yz}, Q_{x_1}, Q_{z_1}\},$$



$$\mathrm{Pent}_4 = \{Q_{xy}, Q_{yy}, Q_{zy}, Q_{x_2}, Q_{z_2}\},$$



$$\mathrm{Pent}_5 = \{Q_{zx}, Q_{zy}, Q_{zz}, Q_{x_1}, Q_{y_1}\},$$



$$\mathrm{Pent}_6 = \{Q_{xz}, Q_{yz}, Q_{zz}, Q_{x_2}, Q_{y_2}\}. \tag{3.1}$$

The vertices correspond to individual questions while the edges connecting them represent the corresponding correlation questions. Vertices on the left correspond to qubit 1 and are compatible with the vertices on the right, corresponding to qubit 2, but not with each other. Vertices are compatible with edges if and only if they are vertices of the latter and edges are compatible if and only if they do not intersect in a vertex [35]. These complementarity relations are conveniently represented in Fig. 4 in terms of a lattice of pentagons, where each pentagon corresponds to one of the six sets in Eq. (3.1). It can be easily checked, using such question graphs, that no other maximal complementarity sets of five or more questions exist. However, there also exist 20 maximal sets of three elements, 4 of which are shown as green triangles in Fig. 4. Since these 20 sets will only be employed for consistency checks of the complementarity inequalities (2.1) but not for the main flow of the arguments, we choose to display and explain them using the question graphs in Appendix B 1. There are no other maximal complementarity sets for two qubits.

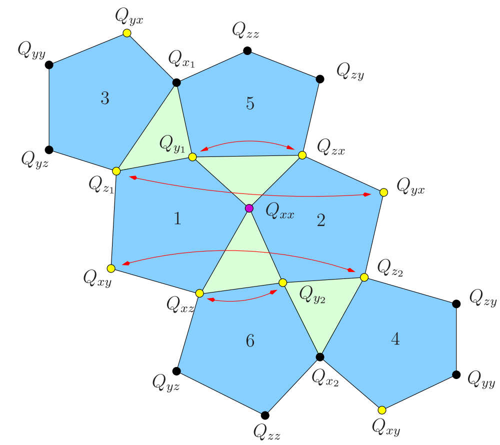


FIG. 4. The six maximal mutually complementary question sets (3.1) represented as pentagons. In contrast to Fig. 3, if two questions lie in the same pentagon or are connected by an edge it means they are complementary (in all other cases they are compatible). Every question appears in precisely two pentagons such that every pentagon is connected to all other five. The green triangles are 4 of 20 maximal complementarity triangles (see Appendix B 1). The red arrows denote the information swap between pentagons 1 and 2 in Eq. (3.9) which leaves all pentagon equalities (3.3) invariant and defines the time evolution generator (3.11).

2. *Constraints on the information distribution over the questions*

For pure states of a single qubit, the single maximal complementarity set carries precisely 1 bit of information $I_{N=1} = \alpha_x + \alpha_y + \alpha_z = r_x^2 + r_y^2 + r_z^2 = 1$ `bit` (r_i are the Bloch vector components) which, according to Principle 3, is a conserved "charge" of time evolution. This *defines* the unitary time evolution group PSU(2) and the Bloch sphere of pure states for a single qubit [35]. We shall now show the analog for two qubits.

Since every question is contained in precisely two pentagons, the sum of the information contained in each pentagon yields twice the total information of O about the two qubits

$$\sum_{a=1}^{6} I(\mathrm{Pent}_a) = 2\left[\sum_{i=x,y,z}(\alpha_{i_1}+\alpha_{i_2}) + \sum_{i,j=x,y,z}\alpha_{ij}\right] = 2\, I_{N=2}(\vec{r}), \tag{3.2}$$

where, thanks to (2.1), 0 bits $\leqslant I(\mathrm{Pent}_a) = \sum_{i\in\mathrm{Pent}_a}\alpha_i \leqslant$ 1 bit is the sum of the information carried by the five questions in pentagon a. Since for pure states $I_{N=2}(\vec{r}_{\mathrm{pure}}) = 3$ bits, it follows that every pure state must satisfy what we shall call the *pentagon equalities*:

$$\text{pure states:}\quad I(\mathrm{Pent}_a) \equiv 1 \text{ bit}, \quad a = 1,\ldots,6. \tag{3.3}$$

In analogy to the single-qubit case, every pentagon therefore carries precisely one bit of information for every pure state. Hence, the pentagon equalities must also be conserved "informational charges" of time evolution. We shall see shortly in Sec. III A 3 that these relations single out the unitary group for two qubits. There are no such conserved informational charges for the maximal complementarity sets consisting of only three elements (see Appendix B 1).

These identities are remarkable because the underlying probabilities y_i in $\alpha_i = (2\,y_i - 1)^2$ of the 15 questions are

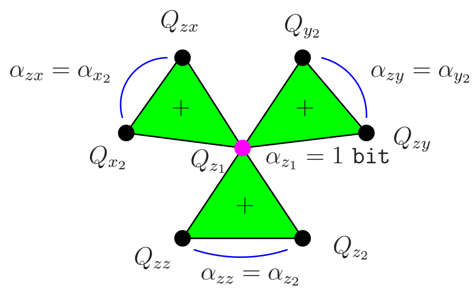


FIG. 5. If any question carries precisely 1 bit, the adjacent correlation triangles carry all remaining information, also for states of nonmaximal information. Moreover, within any correlation triangle, the information contained in the two other questions must be equal.

independent coordinates on Σ_2 and thus do not satisfy any linear identities for all pure states. This observation emphasizes the strength of considering the information content in the questions in addition to their probabilities in quantum theory. In fact, writing $|\psi\rangle = \alpha|x_+x_+\rangle + \beta|x_-x_-\rangle + \gamma|x_+x_-\rangle + \delta|x_-x_+\rangle$ for an arbitrary two-qubit pure state, where $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$ and $x_\pm$ stands for "up and down" in the x direction, one can easily verify (using a computer program) that quantum theory actually satisfies the pentagon equalities (3.3) for the quadratic measure $\alpha_i = (2\,y_i - 1)^2$ (where, e.g., y_{x_1} is the probability that the spin of qubit 1 is up, y_{xx} is the probability that the spins of qubits 1 and 2 are correlated in the x direction, etc.). For example, to put the pentagon identities (3.3) in the case of quantum theory into a more familiar language, the identity for Pent_1 reads for pure states

$$I(\text{Pent}_1) = \langle\sigma_y \otimes \mathbb{1}\rangle^2 + \langle\sigma_z \otimes \mathbb{1}\rangle^2 + \langle\sigma_x \otimes \sigma_x\rangle^2 + \langle\sigma_x \otimes \sigma_y\rangle^2 + \langle\sigma_x \otimes \sigma_z\rangle^2 = 1,$$

and similarly for the other pentagon identities. These informational pentagon identities (3.3) seem to have previously gone unnoticed in quantum theory.

The pentagon equalities have two interesting consequences for pure states. First, $I(\text{Pent}_1) + I(\text{Pent}_3) + I(\text{Pent}_5) - I(\text{Pent}_2) - I(\text{Pent}_4) - I(\text{Pent}_6) = 0$ implies that O knows as much individual information about qubit 1 as about qubit 2:

$$\text{pure states:} \quad \alpha_{x_1} + \alpha_{y_1} + \alpha_{z_1} = \alpha_{x_2} + \alpha_{y_2} + \alpha_{z_2}.$$

(Clearly, this identity cannot hold for all states of nonmaximal information.) We exhibit further such identities in Appendix B 1. Second, the pentagon equalities entail that the amount of information carried by any question is determined by the amount of information carried by the six questions compatible with it, and vice versa. In terms of the correlation triangles in Fig. 3, this results in a "bulk and boundary" relation. For instance, for the three correlation triangles in Fig. 5, excised from Fig. 3, (3.2) and (3.3) yield

$$\begin{aligned} \text{pure states:} \quad \alpha_{z_1} &= \text{boundary}_{z_1} - 1 \text{ bit}, \quad \text{where} \\ 1 \text{ bit} \leqslant \text{boundary}_{z_1} &:= \alpha_{x_2} + \alpha_{zx} + \alpha_{y_2} \\ &\quad + \alpha_{zy} + \alpha_{zz} + \alpha_{z_2} \leqslant 2 \text{ bits}. \end{aligned} \tag{3.4}$$

The special case $\alpha_{z_1} = 1$ bit arises if and only if $\text{boundary}_{z_1} = 2$ bits and the three triangles adjacent to Q_{z_1} thus carry all 3 bits of information. Analogous relations hold for any other question in Fig. 3.

It is easy to convince oneself, using that any question in a correlation triangle of Fig. 3 is either the correlation or anticorrelation of the other two questions in the triangle, that whenever one question carries 1 bit of information, the other two questions in the correlation triangle must carry equal amounts. For example, if the central vertex Q_{z_1} in Fig. 5 carries $\alpha_{z_1} = 1$ bit, then $\alpha_{zz} = \alpha_{z_2}$, etc. as indicated.[13] While this must hold for states of nonmaximal information too, for pure states it also follows directly from the pentagon identities (3.3): e.g., inserting $\alpha_{z_1} = 1$ bit, and thus $\alpha_i = 0$ for any Q_i complementary to Q_{z_1}, into $I(\text{Pent}_5) + I(\text{Pent}_6) - I(\text{Pent}_2) - I(\text{Pent}_4) = 0$ implies directly $\alpha_{zz} = \alpha_{z_2}$. The analogous results can be similarly derived for all triangle neighbors of any $\alpha_i = 1$ bit.

These observations will become valuable shortly.

3. Derivation of the unitary group

Any given time evolution acts linearly and continuously on the states (in-between interrogations) $r_i(t) = T_{ij}(t)\,r_j(0)$, where $\vec{r} = 2\,\vec{y} - \vec{1} \in \mathbb{R}^{15}$ is the generalized Bloch vector and constitutes a one-parameter subgroup of $\mathcal{T}_2$ which itself is a group [35]. Principle 3 asserts that the total information is a "conserved charge" of time evolution $I_{N=2}[T(t)\cdot\vec{r}] = I_{N=2}(\vec{r})$. Since the total information is given by the square norm of the Bloch vector (2.4), this implies that $\mathcal{T}_2 \subset \text{SO}(15)$ (time evolution must be connected to the identity). In fact, $\mathcal{T}_2$ must be a proper subgroup of SO(15) because the latter contains transformations that map all 3 bits of information contained in any pure state into a single question, e.g., $\vec{r} = (1,1,1,0,\dots,0)$ to $\vec{r} = (\sqrt{3},0,0,0,\dots,0)$, which is illegal.

In particular, every pure state evolves to a pure state. Therefore, the pentagon equalities (3.3) are likewise conserved charges, such that we must have $I[\text{Pent}_a(T(t)\cdot\vec{r})] = I[\text{Pent}_a(\vec{r})]$, $a = 1,\dots,6$. Given that $\mathcal{T}_2 \subset \text{SO}(15)$ and $T(t_1+t_2) = T(t_1)\cdot T(t_2) = T(t_2)\cdot T(t_1)$, we may write $T(t) = \exp(t\,G)$ for some generator $G \in \text{so}(15)$ which yields (to linear order in t)

$$\sum_{i\in\text{Pent}_a,\,1\leqslant j\leqslant 15} r_i\,G_{ij}\,r_j = 0, \quad a = 1,\dots 6 \tag{3.5}$$

where $G_{ij} = -G_{ji}$ since $G \in \text{so}(15)$. This implies, in particular, conservation of the total information $I_{N=2}$.

Equation (3.5) constitutes restrictions on both the set of pure states and time evolution generators; *any* legal pure state must satisfy (3.5) for every legal time evolution generator G and, vice versa, *any* legal time evolution generator must satisfy (3.5) for every legal pure state. Of course, at this stage, we neither know what the set of legal pure states nor what the time evolution group $\mathcal{T}_2$ is. As we shall see shortly, however, the pentagon equalities (3.3) and the conditions (3.5) are sufficient, together with the principles and background assumptions, to single out $\mathcal{T}_2 = \text{PSU}(4)$ and the two-qubit

[13] For example, if O knew with certainty that $Q_{z_1} =$ "yes", he would know that the answers to Q_{zz}, Q_{z_2} are correlated, such that $y_{zz} = y_{z_2}$ and hence $\alpha_{zz} = \alpha_{z_2}$. (Note that $y_{zz} = y_{z_2} = \frac{1}{2}$ is possible too, of course.)

quantum state space. This is subject to the already employed convention to use only the XNOR connective $\leftrightarrow$ (rather than the XOR) for building multipartite questions from the individuals, e.g., $Q_{xx} = Q_{x_1} \leftrightarrow Q_{x_2}$.

To this end, we recall Principle 4 which declares that for *any* state, the set of legal time evolutions is the maximal one compatible with the other principles. Given that the set of all time evolutions forms a group (which acts linearly and state independently on states) [35], the principle thus requires the latter somehow to be "maximal." In particular, we can check maximality for specific states that we know must be in Σ_N. Namely, for any set of mutually compatible questions, there must, by definition, exist a state in which these questions are simultaneously answered. Furthermore, for every set of N mutually compatible and independent questions (as in Principle 1) there must exist a state for every "yes" or "no" answer configuration. For $N = 2$, every such state must also respect the correlation structure of Fig. 3. This entails that the set of legal pure states must contain

$$\begin{aligned} \vec{r} &= \vec{\delta}_{z_1} + \vec{\delta}_{z_2} + \vec{\delta}_{z_1 z_2}, \\ \vec{r} &= \vec{\delta}_{z_1} - \vec{\delta}_{z_2} - \vec{\delta}_{z_1 z_2}, \\ \vec{r} &= \vec{\delta}_{z_1} + \vec{\delta}_{z_2} - \vec{\delta}_{z_1 z_2}, \end{aligned} \tag{3.6}$$

where $\vec{\delta}_i$ denotes a vector in $\mathbb{R}^{15}$ with the ith component equal to 1 and all others 0. But (3.5) must, in particular, be satisfied for these three pure states which result in

$$\begin{aligned} G_{z1z1} + G_{z1z2} + G_{z1(z1z2)} &= 0, \\ G_{z1z1} - G_{z1z2} - G_{z1(z1z2)} &= 0, \\ G_{z1z1} + G_{z1z2} - G_{z1(z1z2)} &= 0, \end{aligned} \tag{3.7}$$

and thus

$$G_{z1z1} = G_{z1z2} = G_{z1(z1z2)} = 0.$$

It is easy to convince oneself, by repeating the same argument with every correlation or anticorrelation triangle in Fig. 3, that *any* legal time evolution generator G must feature

$$G_{ij} = 0, \quad \text{whenever } Q_i, Q_j \text{ are compatible.} \tag{3.8}$$

That is, *any* legal time evolution generator can only have nonzero components for pairs of indices corresponding to complementary questions. It follows from Fig. 3 that every question is complementary to precisely eight questions from the informationally complete set. Since there are 15 questions, there are precisely $15 \times 8/2 = 60$ pairs of complementary questions. Thus, given the antisymmetry $G_{ij} = -G_{ji}$, there could at most be 60 linearly independent generators satisfying conditions (3.5) for every pure state.

We shall now construct such a set of 60 linearly independent generators which satisfy (3.8) and have a clear operational meaning. However, as we shall see shortly, only 15 of such generators can be consistent with the principles at once.

Since any two pentagons overlap in precisely one question, there is no transformation which redistributes the information only within a single pentagon and leaves all pentagon equalities invariant. However, for any pair of pentagons there exists a *unique* transformation which swaps the information from one pentagon to the other and leaves all other pentagons and all pentagon equalities (3.3) invariant. Consider, e.g., pentagons Pent_1 and Pent_2 in Fig. 4. The red arrows denote the complete information swap ($\longleftrightarrow$ is not to be confused with the XNOR)

$$\begin{aligned} &\alpha_{y_1} \longleftrightarrow \alpha_{zx}\ (\text{Pent}_5), \quad \alpha_{z_1} \longleftrightarrow \alpha_{yx}\ (\text{Pent}_3), \\ &\alpha_{xy} \longleftrightarrow \alpha_{z_2}\ (\text{Pent}_4), \quad \alpha_{xz} \longleftrightarrow \alpha_{y_2}\ (\text{Pent}_6) \end{aligned} \tag{3.9}$$

between the two pentagons which leaves the composite α_{xx} and all other questions invariant. Since each of the swaps in Eq. (3.9) occurs within precisely one of the remaining four pentagons, all pentagon equalities (3.3) are preserved. Such a full swap of information between two pentagon sets is thus a good candidate for a legal time evolution. W.l.o.g., this swap transformation can be written as $T = \exp[(\pi/2)\, G^{\text{Pent}_1,\text{Pent}_2}]$ acting on $\vec{r}$ with

$$\begin{aligned} G_{ij}^{\text{Pent}_1,\text{Pent}_2} &= \delta_{iy_1}\delta_{jzx} + s_1\,\delta_{iz_1}\delta_{jyx} + s_2\,\delta_{ixy}\delta_{jz_2} \\ &\quad + s_3\,\delta_{ixz}\delta_{jy_2} - (i \longleftrightarrow j), \end{aligned} \tag{3.10}$$

where s_1,s_2,s_3 are three signs to be determined. Given that there are four linearly independent terms in the generator, one can produce precisely four linearly independent generators from (3.10) by changing the signs s_1,s_2,s_3. However, a legal time evolution generator must be consistent with the correlation structure in Fig. 3 and the constraints on information distribution of Sec. III A 2. In Appendix B 2 a, it is shown that these constraints uniquely determine the generator candidate (up to an unimportant overall sign) to

$$\begin{aligned} G_{ij}^{\text{Pent}_1,\text{Pent}_2} &= \delta_{iy_1}\delta_{jzx} - \delta_{iz_1}\delta_{jyx} + \delta_{ixy}\delta_{jz_2} \\ &\quad - \delta_{ixz}\delta_{jy_2} - (i \longleftrightarrow j). \end{aligned} \tag{3.11}$$

For every pair of pentagons there exists such a unique information swap, resulting in $\binom{6}{2} = 15$ transformations which are consistent with the correlation structure and the constraints on the information distribution. The form of their generators can be found similarly [see (B5) and (B7) in Appendix B 2 a]. There are nine swaps leaving a composite and six swaps leaving an individual question as the overlap of the pentagons invariant. As an example for the latter, the information swap between Pent_3 and Pent_5 leaves the individual α_{x_1} invariant and is generated by

$$\begin{aligned} G_{ij}^{\text{Pent}_3,\text{Pent}_5} &= \delta_{iy_1}\delta_{jz_1} - \delta_{iyx}\delta_{jzx} - \delta_{iyy}\delta_{jzy} \\ &\quad - \delta_{iyz}\delta_{jzz} - (i \longleftrightarrow j). \end{aligned} \tag{3.12}$$

In Appendix B 2 a, it is shown that the various sign distributions over these 15 generators, as in Eq. (3.10), produce precisely 60 linearly independent generators satisfying (3.8). Regardless of the sign structure, each of these 60 linearly independent generators thus corresponds precisely to a complete information swap between two pentagon sets and for each pair of pentagon sets there are four linearly independent such swap generators. That is, whatever the resulting time evolution group consistent with (3.5) may be, it must be fully generated by complete information swaps between pentagons. Clearly, it cannot be generated by all 60 such generators as the only state which would satisfy (3.5) for all 60 generators is the state of no information $\vec{r} = 0$. Indeed, requiring consistency with the correlation structure of Fig. 3, and thus consistency with the convention of only using the XNOR connective for building bipartite questions from individuals, results in one permissible generator candidate per pair of pentagon sets and in precisely the 15 candidate generators exhibited here and in Appendix B 2 a. The time evolution group can thus not be generated by any other than these 15 surviving generator candidates; in fact, the remaining 45 possible sign distributions can be argued to correspond to different conventions (see Appendix B 2 a).

Using a computer algebra program, one can easily check that these 15 surviving information swap generators (B5) and (B7) (see Appendix B 2 a)

(a) satisfy the commutator algebra of $\mathrm{su}(4) \simeq \mathrm{so}(6) \simeq \mathrm{psu}(4) \subset \mathrm{so}(15)$, and

(b) coincide exactly (in some cases up to an unimportant overall sign) with the adjoint representation

$$(G^i)_{jk} := f^{ijk} = \tfrac{1}{4}\,\mathrm{tr}([\sigma_j,\sigma_k]\,\sigma_i)$$

of the 15 fundamental generators of the unitary group SU(4). f^{ijk} are the structure constants of SU(4), the indices i,j,k take the 15 values $x_1,y_1,z_1,x_2,\dots,xz,xy,\dots,zz$ (as in our reconstruction) and $\sigma_{x_1} := \sigma_x \otimes \mathbb{1},\dots,\ \sigma_{x_2} := \mathbb{1} \otimes \sigma_x,\dots,\ \sigma_{xx} := \sigma_x \otimes \sigma_x,\dots,\ \sigma_{zz} := \sigma_z \otimes \sigma_z$, and $\sigma_x,\sigma_y,\sigma_z$ are the usual Pauli matrices. In particular, the ordering of coincidence is $G^i \equiv \pm G^{\mathrm{Pent}_a,\mathrm{Pent}_b}$ where Q_i is the single question in $\mathrm{Pent}_a \cap \mathrm{Pent}_b$ which is left invariant by the swap; e.g., $G^{xx} \equiv G^{\mathrm{Pent}_1,\mathrm{Pent}_2}$, etc.

Next, we must check whether the (image of any state under the) full group $\mathcal{T}_2'$ generated by exponentiating the 15 surviving swap generators (B5) and (B7) and their linear combinations is consistent with the principles and thus by Principle 4 whether $\mathcal{T}_2'$ is contained in $\mathcal{T}_2$. Clearly, $\mathcal{T}_2'$ obeys Principle 3 by construction and the only background assumption which it is not evidently consistent with are the complementarity inequalities (2.1). Similarly, the only structure entailed by Principles 1 and 2 that $\mathcal{T}_2'$ is not evidently consistent with is the correlation structure of Fig. 3. We thus have to expose $\mathcal{T}_2'$ to a few nontrivial consistency checks. In Appendix B it is shown as follows:

(i) Equation (3.5) results in 15 independent conservation equations, one for each swap generator:

$$\sum_{i\in \mathrm{Pent}_a, 1\leqslant j\leqslant 15} r_i\, G^{\mathrm{Pent}_a,\mathrm{Pent}_b}_{ij}\, r_j = 0, \quad a<b, \quad a,b = 1,\dots,6. \tag{3.13}$$

All other combinations of the swap generators with the Bloch vector components of some pentagon lead via (3.5) to conservation equations which are either trivial or implied by (3.13). (Appendix B 2 c)

(ii) Together with the six pentagon equalities (3.3), these 15 conservation equations (3.13) constitute 21 equations which define an invariant set under $\mathcal{T}_2'$, i.e., for *any* Bloch vector $\vec{r}$ solving (3.3) and (3.13), $T(t)\cdot\vec{r}$ will again solve these 21 equations for all $T(t) \in \mathcal{T}_2'$. In particular, writing $T(t) = \exp(t\,G)$ with G in the Lie algebra of $\mathcal{T}_2'$, the pentagon equalities will be preserved to all orders in t [recall that (3.5) was only the preservation condition to linear order in t] (Appendix B 2 c).

(iii) The complementarity inequalities (2.1) are preserved by $\mathcal{T}_2'$ and all Bloch vectors $\vec{r}$ satisfying (3.3) and (3.13) also necessarily obey all complementarity inequalities (Appendix B 2 f).

(iv) $\mathcal{T}_2'$ preserves the correlation structure of Fig. 3 and, fixing the convention to only employ the XNOR for constructing multipartite questions from individuals, (3.3) and (3.13), implies unambiguously the correlation structure of Fig. 3 (Appendix B 2 g).

Accordingly, $\mathcal{T}_2'$ maps states satisfying Principles 1–3, all background assumptions, and (3.3) and (3.13) to other such states. Principle 4 requires the existence of *any* time evolution fulfilling these conditions such that we must indeed conclude $\mathcal{T}_2' \subseteq \mathcal{T}_2$.

But, which group is $\mathcal{T}_2'$? In (a) it was seen that the swap generators form the Lie algebra of $\mathrm{su}(4) \simeq \mathrm{so}(6) \simeq \mathrm{psu}(4)$. SU(4) is a double cover of SO(6) which, in turn, is a double cover of $\mathrm{PSO}(6) \simeq \mathrm{PSU}(4)$. The exponentiation of the swap generators (B5) and (B7) can*not* result in a faithful representation of either SU(4) or SO(6), which feature a nontrivial center, because by Schur's lemma all center elements read as $c \cdot \mathbb{1}$ with $c^{15} = 1$ such that $c \equiv 1$ and the representation is centerless. The exponentiation will thus result in a faithful representation of PSU(4). Hence, $\mathrm{PSU}(4) \subseteq \mathcal{T}_2 \subset \mathrm{SO}(15)$.

Can $\mathcal{T}_2$ contain any additional transformations not contained in $\mathcal{T}_2'$? Given that the 15 surviving swap generators (B5) and (B7) constitute a maximal set consistent with (3.5) and the correlation structure of Fig. 3, we must conclude that the answer is negative. In fact, in Appendix B 2 d it is further shown that PSU(4) is a *maximal subgroup*[14] of SO(15). Since $\mathcal{T}_2$ must be a proper subgroup of SO(15), we conclude that

$$\mathcal{T}_2 \simeq \mathrm{PSU}(4).$$

This is the correct time evolution group for two qubits in quantum theory and, thanks to (b), we obtain it in the correct Bloch vector representation.[15]

It is interesting to note that the six generators (B7) of the information swaps between the pentagons which overlap in an individual question satisfy the commutator algebra of $\mathrm{so}(3) \oplus \mathrm{so}(3)$ and therefore generate the subgroup $\mathrm{PSU}(2) \times \mathrm{PSU}(2) \simeq \mathrm{SO}(3) \times \mathrm{SO}(3)$ of product unitaries corresponding to the Bloch sphere rotations of the two individual qubits. By contrast, the nine generators (B5) of the swaps between pentagons overlapping in a composite question generate the entangling unitaries in PSU(4) (see Appendix B 2 a).

4. State space reconstruction

Now that we have concluded that $\mathcal{T}_2 = \mathrm{PSU}(4)$ is the correct time evolution group, we are also in a position to determine Σ_2. The 21 equations [Eqs. (3.3) and (3.13)] define a $\mathcal{T}_2$-invariant set of Bloch vectors and every legal pure state must lie within it. One may be worried that these 21 equations overconstrain the 15 components of the Bloch vector $\vec{r}$. However, the legitimate

[14] A maximal subgroup H of a group G is a proper subgroup which is not contained in any other subgroup other than H itself and the full group G.

[15] The adjoint action of $U \in \mathrm{SU}(4)$ in an evolution $\rho \mapsto U\,\rho\,U^\dagger$ of a 4×4 density matrix is ignorant of the phase in U and therefore yields a representation of PSU(4).

"product" states (3.6) satisfy all 21 equations and $\mathcal{T}_2$ preserves these equations such that the set defined by (3.3) and (3.13) is clearly nonempty. In fact, in Appendix B 2 e it is shown, using the information distribution results of Sec. III A 2, that for *any* Bloch vector fulfilling (3.3) and (3.13), there exists a time evolution in $\mathcal{T}_2$ which maps all information to the "product state" form $\alpha_{z_1} = \alpha_{z_2} = \alpha_{zz} = 1$ bit and all other $\alpha_i = 0$. This informational configuration has eight solutions in terms of the Bloch vector which can be divided into two mutually exclusive sets (all other $r_i = 0$)

$$\begin{aligned} \mathcal{S}_{\text{XNOR}} : 1./2.\ & r_{zz} = +1,\ r_{z_1} = \pm 1,\ r_{z_2} = \pm 1, \\ 3./4.\ & r_{zz} = -1,\ r_{z_1} = \pm 1,\ r_{z_2} = \mp 1, \\ \mathcal{S}_{\text{XOR}} : 5./6.\ & r_{zz} = -1,\ r_{z_1} = \mp 1,\ r_{z_2} = \mp 1, \\ 7./8.\ & r_{zz} = +1,\ r_{z_1} = \mp 1,\ r_{z_2} = \pm 1, \end{aligned}$$

the first of which is consistent with the XNOR conjunction $Q_{zz} = Q_{z_1} \leftrightarrow Q_{z_2}$, the second of which corresponds to the XOR connective $Q_{zz} = \neg(Q_{z_1} \leftrightarrow Q_{z_2})$. These are two perfectly consistent conventions for building up the composite questions (the information measure cannot distinguish between XNOR and XOR) [35].

It can be easily verified that the four solutions in $\mathcal{S}_{\text{XNOR}}$ are connected by elements of $\mathcal{T}_2$, as are the four solutions in $\mathcal{S}_{\text{XNOR}}$.[16] However, the two sets of Bloch vectors generated by acting with $\mathcal{T}_2$ on each of $\mathcal{S}_{\text{XNOR}}$ and $\mathcal{S}_{\text{XOR}}$ are *not* connected by time evolution since, using the time connectedness of each set,

$$\begin{aligned} \mathcal{T}_2(\mathcal{S}_{\text{XOR}}) &:= \{T \cdot (-1)(\vec{\delta}_{z_1} + \vec{\delta}_{z_2} + \vec{\delta}_{z_1 z_2}) \mid T \in \mathcal{T}_2\} \\ &= -\{T \cdot (\vec{\delta}_{z_1} + \vec{\delta}_{z_2} + \vec{\delta}_{z_1 z_2}) \mid T \in \mathcal{T}_2\} \\ &=: -\mathcal{T}_2(\mathcal{S}_{\text{XNOR}}) \end{aligned}$$

such that $\mathcal{T}_2(\mathcal{S}_{\text{XOR}})$ and $\mathcal{T}_2(\mathcal{S}_{\text{XNOR}})$ are related by a global multiplication with $-\mathbb{1}_{15\times 15} \notin \mathcal{T}_2 \subset \text{SO}(15)$ which commutes with all elements in $\mathcal{T}_2$. This corresponds precisely to a change of convention of building composite questions with XOR rather than XNOR.

In conclusion, the 21 equations [(3.3) and (3.13)] define exactly *two* isomorphic sets $\mathcal{T}_2(\mathcal{S}_{\text{XOR}})$ and $\mathcal{T}_2(\mathcal{S}_{\text{XNOR}})$ which are disconnected by time evolution, however, on each of which the time evolution group $\mathcal{T}_2$ acts transitively.

It is well known that, thanks to transitivity, $\mathcal{T}_2 \simeq \text{PSU}(4)$ generates *all* two-qubit pure states of quantum theory by acting with all its elements on *any* legal pure state (in the Bloch or Hermitian representation) [22,24,46]. The seed pure state $\vec{r} = \vec{\delta}_{z_1} + \vec{\delta}_{z_2} + \vec{\delta}_{z_1 z_2}$ in $\mathcal{S}_{\text{XNOR}}$, written in the basis defined by the informationally complete question set $\{Q_{x_1}, \ldots, Q_{zz}\}$, coincides with the generalized Bloch vector representation of the two-qubit product state density matrix $\rho = 1/4\,(\mathbb{1}_{4\times 4} + \sigma_z \otimes \mathbb{1} + \mathbb{1} \otimes \sigma_z + \sigma_z \otimes \sigma_z)$, written in the basis of the informationally complete Pauli operators $\mathbb{1} \otimes \sigma_i, \sigma_j \otimes \mathbb{1}, \sigma_i \otimes \sigma_j$, $i,j = x,y,z$. We also recall from (b) in Sec. III A 3 that the 15 swap generators (B5) and (B7), expressed in the question basis, coincide with the adjoint representation of the fundamental generators of the quantum time evolution group SU(4), written in the Pauli operator basis. It is thus clear that the orbit $\mathcal{T}_2(\mathcal{S}_{\text{XNOR}})$, expressed in the question basis, is *exactly* the set of two-qubit pure states of quantum theory, expressed in the Pauli operator basis.[17] Furthermore, since the seed states in $\mathcal{S}_{\text{XNOR}}$ are legal pure states in Σ_2 and since the time evolution image of any legal state must again be legal, we conclude that $\mathcal{T}_2(\mathcal{S}_{\text{XNOR}})$ is fully contained in the set of pure states implied by the principles. Geometrically, this set of two-qubit pure states is $\mathcal{T}_2(\mathcal{S}_{\text{XNOR}}) \simeq \mathbb{CP}^3$ [49], of which $\mathcal{T}_2 \simeq \text{PSU}(4)$ is the isometry group.

Evidently, $\mathcal{T}_2(\mathcal{S}_{\text{XOR}}) \simeq \mathbb{CP}^3$ also defines a representation of the pure state space which is physically perfectly equivalent to $\mathcal{T}_2(\mathcal{S}_{\text{XNOR}})$. However, since it corresponds to the "XOR convention," it leads to a correlation structure as in Fig. 3, except that the signs in all triangles would be flipped.

Hence, adopting the convention, as we did so far, to build up composite questions from individuals solely by XNOR connectives, we conclude that the $N = 2$ pure state space implied by the principles is precisely (one copy of) the pure state space for two qubits in quantum theory. Accordingly, upon fixing the XNOR convention, a Bloch vector $\vec{r}$ represents a pure two-qubit quantum state if and only if it satisfies the six pentagon equations (3.3), which are ignorant of the correlation structure, and the 15 conservation equations (3.13), which also encode the correlation structure (up to an overall XNOR vs XOR ambiguity).[18]

The pure states form the set of extremal Bloch vector length within the full state space Σ_2 which must be convex. Thus, clearly, the convex hull of the pure states is contained in Σ_2. But, can there by any further legal extremal states? If there was another extremal state it could not be a state of maximal information and it could also not be a convex linear combination of pure states. In Sec. II, we required that O can prepare any extremal state in a single shot interrogation relative to the state of no information with questions from an informationally complete set, and possibly a subsequent time evolution. However, it follows from our constraints on the state update rule in Sec. II that any posterior state of a system of two qubits in such a single shot interrogation will be a quantum state[19] which is already contained in the convex hull of the

[16]For instance, solutions 1 and 2 (or 5 and 6) are mapped to solutions 4 and 3 (or 8 and 7), respectively, by $T = \exp(\pi\, G^{\text{Pent}_3,\text{Pent}_5})$ or $T = \exp(\pi\, G^{\text{Pent}_1,\text{Pent}_5})$. Similarly, solutions 1 and 2 (or 5 and 6) are mapped to solutions 3 and 4 (or 7 and 8), respectively, by $T = \exp(\pi\, G^{\text{Pent}_4,\text{Pent}_6})$ or $T = \exp(\pi\, G^{\text{Pent}_2,\text{Pent}_6})$. (See Appendix B for the explicit representations of the swap generators and formulas for their exponentiation.)

[17]Indeed, it can be easily checked, using a computer algebra program, that *all* two-qubit pure states of quantum theory satisfy the 21 equations [Eqs. (3.3) and (3.13)].

[18]Clearly, the 21 equations cannot be fully independent. In fact, only 9 of the 21 equations can be locally independent on $\mathbb{R}^{15}$ to produce a $(15 - 9 = 6)$-dimensional pure state space $\mathbb{CP}^3$. It is not possible, however, thanks to pairwise independence of the questions in an informationally complete set, to globally parametrize the pure state space in terms of the probabilities (or Bloch vector components) of six fixed questions only.

[19]Any two questions in the informationally complete set are pairwise independent and either maximally complementary or maximally

pure states. Since the pure states are closed under all possible time evolutions, so is their convex hull. We thus conclude that there can be no further extremal states than the pure states. The Krein-Milman theorem [43] states that a (compact) convex set is the closed convex hull of its extreme points. Hence, we find

$$\Sigma_2 = \text{closed convex hull of } \mathbb{CP}^3.$$

Σ_2 contains the *state of no information* $\vec{r} = 0$ (e.g., multiply each of the four solutions in $\mathcal{S}_{\text{XNOR}}$ with $\frac{1}{4}$ and sum up) and indeed coincides with the set of unit trace density matrices over the two-qubit Hilbert space $\mathbb{C}^2 \otimes \mathbb{C}^2$. From the fact that all pure states satisfy all complementarity inequalities (2.1), it follows that all convex mixtures of them will satisfy them too since the information measure (2.4) satisfies $\alpha_i[\lambda \vec{r}_1 + (1-\lambda)\vec{r}_2] < \max\{\alpha_i(\vec{r}_1),\alpha_i(\vec{r}_2)\}$ if $\lambda \in (0,1)$ and if the pure states $\vec{r}_1 \neq \vec{r}_2$ are distinct [35].

B. $N > 2$ qubits

Principles 1, 2, and 6 imply that an informationally complete set for N gbits contains $4^N - 1$ questions $Q_{\mu_1\mu_2\ldots\mu_N} = Q_{\mu_z} \leftrightarrow Q_{\mu_2} \leftrightarrow \cdots \leftrightarrow Q_{\mu_N}$, $\mu_i = 0,x,y,z$, where $Q_0 = 1$, such that the Bloch vector $\vec{r}$ is $(4^N - 1)$ dimensional [35]. Pure state Bloch vectors have (squared) length $2^N - 1$ bits, corresponding to having maximal information about N mutually independent and compatible questions (Principle 1), as well as their (dependent) multipartite correlations.

1. Derivation of the unitary group

Again, any given time evolution $T(t)$ acts linearly on the Bloch vector $r_i(t) = T_{ij}(t)\,r_j(0)$ and constitutes a one-parameter subgroup of $\mathcal{T}_N$ [35]. For analogous reasons to the $N = 2$ case, $\mathcal{T}_N$ must be a proper subgroup of $\mathrm{SO}(4^N - 1)$ for $N \geqslant 2$.

We label the N gbits by $1,\ldots,N$. Consider the gbit pair labeled by (12). We shall say that this pair evolves as an isolated subsystem under $\mathcal{T}_2^{(12)} = \mathrm{PSU}(4)$ (to avoid confusion, we label the copy of the two-gbit time evolution group by the pair of gbits) if the components of the N-gbit Bloch vector $\vec{r} \in \mathbb{R}^{4^N-1}$:

(i) $r_{\mu_1\mu_2 00\ldots 0}$ corresponding to the 15 questions $Q_{\mu_1\mu_2 00\ldots 0}$ (excluding $\mu_1 = \mu_2 = 0$) forming an informationally complete set (see Sec. III A) for the gbit pair (12) evolve under $\mathcal{T}_2^{(12)}$ as derived in Sec. III A 3, independently of the other components;[20] and

(ii) $r_{00\mu_3\mu_4\ldots\mu_N}$ corresponding to all questions $Q_{00\mu_3\mu_4\ldots\mu_N}$ *not* involving gbits (12) are left *invariant* under $\mathcal{T}_2^{(12)}$.

Recall that $\mathcal{T}_2^{(12)} \supset \mathrm{SO}(3) \times \mathrm{SO}(3)$ contains the local qubit unitaries such that this definition also accounts for the isolated evolution of individual gbits.

Since N gbits form a composite system, it must be physically possible for every pair of gbits to evolve in time together as an isolated subsystem, as derived in Sec. III A 3, and for any individual gbit to evolve isolated of the others, as described in Ref. [35], thus without affecting O's information distribution over any other gbits. Accordingly, we shall require the time evolutions $\mathcal{T}_2 \simeq \mathrm{PSU}(4)$ for any pair of gbits and $\mathcal{T}_1 \simeq \mathrm{SO}(3)$ for any single gbit, respectively, to be contained in $\mathcal{T}_N$. Of course, given three or more gbits, the different copies of PSU(4) cannot act simultaneously on all pairs due to monogamy of entanglement (which also naturally follows from the principles [35]).

In Appendix B 3 a, it is shown that this requirement of isolated $\mathcal{T}_2$ or $\mathcal{T}_1$ evolution, together with the results of Sec. III A, leads to an unambiguous promotion of the representation of the PSU(4) time evolution elements for every gbit pair from $\mathbb{R}^{15}$ to $\mathbb{R}^{4^N-1}$. In particular, the $\mathcal{T}_2^{(12)}$ generators of the gbit pair (12) take the form

$$G^{\mathrm{Pent}_a^{(12)},\mathrm{Pent}_b^{(12)}}_{(\mu_1\mu_2\mu_3\mu_4\ldots\mu_N)(\nu_1\nu_2\nu_3\nu_4\ldots\nu_N)} = G^{\mathrm{Pent}_a,\mathrm{Pent}_b}_{(\mu_1\mu_2)(\nu_1\nu_2)}\,\delta_{\mu_3\nu_3}\delta_{\mu_4\nu_4}\ldots\delta_{\mu_N\nu_N}, \tag{3.14}$$

where $G^{\mathrm{Pent}_a,\mathrm{Pent}_b}_{(\mu_1\mu_2)(\nu_1\nu_2)}$ is the representation of the corresponding two-qubit swap generators on $\mathbb{R}^{15}$ of Sec. III A 3 (and Appendix B 2 a)[21] and we define $G^{\mathrm{Pent}_a,\mathrm{Pent}_b}_{(00)(\nu_1\nu_2)} := 0 =: G^{\mathrm{Pent}_a,\mathrm{Pent}_b}_{(\mu_1\mu_2)(00)}$. In Appendix B 3 b, it is furthermore shown that the generators (3.14) coincide precisely with the adjoint representation of the fundamental generators $\sigma_i \otimes \mathbb{1} \otimes \mathbb{1} \otimes \cdots \mathbb{1}, \mathbb{1} \otimes \sigma_i \otimes \mathbb{1} \cdots \mathbb{1}, \sigma_i \otimes \sigma_j \otimes \mathbb{1} \cdots \mathbb{1}$ of pairwise unitaries in quantum theory. The ordering of coincidence is such that, first, $Q_{\mu_1\mu_2 0\ldots 0}$ corresponds to $\sigma_{\mu_1\mu_2 0\ldots 0} := \sigma_{\mu_1} \otimes \sigma_{\mu_2} \otimes \mathbb{1} \otimes \cdots \otimes \mathbb{1}$ where $\sigma_0 = \mathbb{1}$ and, second, $G^{\mathrm{Pent}_a^{(1,2)},\mathrm{Pent}_b^{(1,2)}}$ coincides with the adjoint representation of $\sigma_{\mu_1\mu_2 0\ldots 0}$ corresponding to the unique question $Q_{\mu_1\mu_2 0\ldots 0}$ in $\mathrm{Pent}_a^{(12)} \cap \mathrm{Pent}_b^{(12)}$. For example, $G^{\mathrm{Pent}_1^{(12)},\mathrm{Pent}_2^{(12)}}$ coincides with the adjoint representation of $\sigma_x \otimes \sigma_x \otimes \mathbb{1} \otimes \cdots \otimes \mathbb{1}$. This coincidence holds analogously for arbitrary pairs among the N gbits. Clearly, also the $\mathcal{T}_N$ subgroups generated by these bipartite generators will have exactly the same form (at the Bloch vector level) as in quantum theory.

It is well known that two-qubit unitaries PSU(4) (between any pair) and local evolutions SO(3) generate the full projective unitary group $\mathrm{PSU}(2^{\mathrm{N}})$ [50,51].[22] Since all local evolutions and pairwise unitaries are required to be contained in $\mathcal{T}_N$ and since these have the same representation as in quantum theory, we must conclude, abstractly, that $\mathrm{PSU}(2^{\mathrm{N}}) \subseteq \mathcal{T}_{\mathrm{N}} \subset \mathrm{SO}(4^{\mathrm{N}} - 1)$ and, more explicitly, that the generated copy of $\mathrm{PSU}(2^{\mathrm{N}})$ appears in a Bloch vector representation, relative to the

compatible. Given the two constraints of Sec. II on the update rule [(1) questions are repeatable, and (2) independent compatible information is preserved], it is clear that any single shot interrogation on the prior state $\vec{r} = 0$ with the questions of the informationally complete set will result in a posterior state $\vec{r}\,'$ with any component being one of $0,\pm 1$. Any such posterior state must obey Principle 1, complementarity, and the correlation structure in Fig. 3 and thus has either precisely one or three components equal to ± 1 and the rest 0. But, any such state respecting the correlation structure corresponds to a quantum state. In particular, the 3 bit states are legal pure states.

[20] Note that these 15 Bloch vector components define an invariant subspace under $\mathcal{T}_2^{(12)}$ of $\mathbb{R}^{4^N-1}$.

[21] In agreement with the more general notation of this section, we have exchanged the indices i,j in $G^{\mathrm{Pent}_a,\mathrm{Pent}_b}_{ij}$ [Eqs. (B5) and (B7)] for the equivalent $(\mu_1\mu_2)$ and $(\nu_1\nu_2)$ indices, respectively.

[22] This universality result has also been used in other reconstructions [24,28].

question basis, which is identical to the Bloch vector (or adjoint) representation of the quantum unitaries relative to the Pauli operator basis. As in the $N=2$ case, $\mathrm{PSU}(2^N)$ is a maximal subgroup of $\mathrm{SO}(4^N-1)$ (see Appendix B 2 d) and since $\mathcal{T}_N$ must be a proper subgroup of the latter, we conclude

$$\mathcal{T}_N \simeq \mathrm{PSU}(2^{\mathrm{N}})$$

which is the correct time evolution group for N qubits. The fact that we obtain the full group $\mathrm{PSU}(2^{\mathrm{N}})$ (rather than some of its subgroups) follows from the maximality requirement of Principle 4 which demands *every* time evolution compatible with the principles (and the background assumptions). As a consistency check, we show in Appendix B 3 d that $\mathrm{PSU}(2^N)$ indeed preserves all complementarity inequalities (2.1), as required.

2. State space reconstruction

We show in Appendix B 3 c that for every Bloch vector $\vec{r}$ which could be a legal N gbit pure state there exists a time evolution in $\mathcal{T}_N$ which transfers all 2^N-1 bits to the "product state" form $\alpha_{z_1}=\cdots=\alpha_{z_N}=\alpha_{z_1z_2}=\alpha_{z_1z_3}=\cdots=\alpha_{z_1z_2z_3}=\cdots=\alpha_{z_1\cdots z_N}=1$ bit (and all other $\alpha_i=0$). This informational configuration has 2^{2^N-1} Bloch vector solutions $r_{z_1},\ldots,r_{z_1z_2},\ldots,r_{z_1\cdots z_N}\in\{-1,+1\}$ and the remaining $r_i=0$. Since by Principle 1 only N of the 2^N-1 corresponding questions $Q_{z_1},\ldots,Q_{z_1\cdots z_N}$ are mutually independent, these Bloch vectors can be grouped into $2^{2^N-1}/2^N$ sets $\mathcal{S}^N_1,\ldots,\mathcal{S}^N_{2^{2^N-1-N}}$, each consistent with a specific convention of distributing XNOR or XOR connectives among the different individual gbit questions $Q_{\mu_1},\ldots,Q_{\mu_N}$ to build up multipartite questions, in analogy to Sec. III A 4. Evidently, only one of these sets agrees with our choice of employing solely the XNOR connective $\leftrightarrow$ to define multipartite questions $Q_{\mu_1\mu_2\ldots\mu_N}=Q_{\mu_1}\leftrightarrow Q_{\mu_2}\leftrightarrow\cdots\leftrightarrow Q_{\mu_N}$ from the individuals Q_{μ_i}, namely, the set of 2^N solutions defined by

$$\mathcal{S}^N_{\mathrm{XNOR}} := \Bigg\{ (r_{z_1},\ldots,r_{z_N},r_{z_1z_2},\ldots,r_{z_1\cdots z_N}) \,\Big|\, r_{z_1},\ldots,r_{z_N}\in\{-1,+1\}, \quad r_{z_{i_1}\cdots z_{i_m}} = \prod_{k=1}^{m\leqslant N} r_{z_{i_k}}, i_k\in\{1,\ldots,N\}, i_k<i_{k+1}\Bigg\}.$$

It is not difficult to convince oneself that the 2^N Bloch vectors in any convention set $\mathcal{S}^N_i$ are connected through the local rotations $\mathrm{SO}(3)\times\cdots\times\mathrm{SO}(3)\subset\mathcal{T}_N$.[23]

We now focus on $\mathcal{S}^N_{\mathrm{XNOR}}$. The state $\vec{r}_z:=\vec{\delta}_{z_1}+\cdots+\vec{\delta}_{z_1\cdots z_N}$ in $\mathcal{S}^N_{\mathrm{XNOR}}$ coincides with the generalized Bloch vector representation of the N-qubit product state density matrix $\rho=(\mathbb{1}_{2^N\times 2^N}+\sigma_z\otimes\mathbb{1}\otimes\cdots\otimes\mathbb{1}+\cdots+\sigma_z\otimes\cdots\otimes\sigma_z)/2^N$ in quantum theory and is a legal pure state since $Q_{z_1},\ldots,Q_{z_N}$ are mutually compatible and independent [35]. It was shown in the previous section that the Bloch vector representation of $\mathcal{T}_N$ is *exactly* the same as in quantum theory.

[23]Namely, by the local unitaries which map $r_{z_i}=+1\longleftrightarrow r_{z_i}=-1$.

As for $N=2$, $\mathcal{T}_N$ acts transitively on the pure states of qubit quantum theory and therefore the *complete* pure quantum state space is generated when $\mathcal{T}_N$ acts on any pure quantum state [22,24,46]. Hence, the orbit $\mathcal{T}_N(\mathcal{S}^N_{\mathrm{XNOR}})$, expressed in our question basis, coincides exactly with the Bloch vector representation of the N-qubit pure state space of quantum theory, written in the Pauli operator basis. Since the time evolution image of any legal pure state must be again a legal pure state, we conclude that all of $\mathcal{T}_N(\mathcal{S}^N_{\mathrm{XNOR}})$ is contained in the set of pure states implied by the principles.

But, can there be more pure states? Since all other sets $\mathcal{S}^N_i\neq\mathcal{S}^N_{\mathrm{XNOR}}$ correspond to distinct conventions of building up composite questions from the individuals Q_{μ_i}, the answer is negative. Indeed, the seed states in any $\mathcal{S}^N_i\neq\mathcal{S}^N_{\mathrm{XNOR}}$ are not legal quantum states, featuring a correlation structure distinct from quantum theory. (There are only 2^N pure quantum states with only ±1 in the z components and these precisely constitute $\mathcal{S}^N_{\mathrm{XNOR}}$.) Hence, these sets are not connected via $\mathcal{T}_N$ to our legal pure states $\mathcal{T}_N(\mathcal{S}^N_{\mathrm{XNOR}})$. Some of these other conventions will yield a distinct, but physically equivalent, representation of the set of quantum pure states (e.g., as in the $N=2$ case the set corresponding to the convention of building up all composite questions with the XOR, rather than XNOR connective).

Consequently, adhering to our usual convention to build up all composite questions of an informationally complete set *only* with XNOR operations from the Q_{μ_i} implies that the set of all pure states allowed by the principles $\mathcal{T}_N(\mathcal{S}^N_{\mathrm{XNOR}})$ is precisely the set of pure quantum states. Geometrically, for N qubits this space is given by $\mathcal{T}_N(\mathcal{S}^N_{\mathrm{XNOR}})\simeq\mathbb{CP}^{2^N-1}$ [49] of which $\mathrm{PSU}(2^N)$ is the transitive isometry group. In complete analogy to the $N=2$ case in Sec. III A 4, we thus obtain

$$\Sigma_N = \text{closed convex hull of } \mathbb{CP}^{2^N-1}$$

which contains the *state of no information* and coincides with the set of normalized density matrices over the N-fold tensor product of single-qubit Hilbert spaces $\mathbb{C}^2\otimes\cdots\otimes\mathbb{C}^2$. For consistency, we show in Appendix B 3 d that all states in Σ_N are compatible with the principles and, in particular, satisfy all complementarity inequalities (2.1).

In conclusion, we arrive precisely at the correct state spaces and time evolution groups for arbitrarily many qubits.

C. The set of allowed questions $\mathcal{Q}_N$ and the Born rule

The reconstruction of the time evolution groups $\mathcal{T}_N$ and the state spaces Σ_N did not require the derivation of the precise structure of $\mathcal{Q}_N$, but only of the structure of an informationally complete set $\mathcal{Q}_{M_N}\subset\mathcal{Q}_N$. But, what is the structure of the question set $\mathcal{Q}_N$? And what is the action of $\mathcal{T}_N$ on $\mathcal{Q}_N$? To answer these questions, we invoke Principle 5 which did not yet come into play.

1. Characterization of the question set

We begin by phrasing the derived probability rule (2.3) in terms of Bloch vectors $y(Q|\vec{r}):=Y(Q|\vec{y}=\frac{1}{2}\vec{r}+\vec{1})$; the probability for $Q=$ "yes", given the state $\vec{r}$, then reads as

$$y(Q|\vec{r})=y(\vec{q}|\vec{r})=\tfrac{1}{2}(1+\vec{q}\cdot\vec{r}). \tag{3.15}$$

The structure of the landscape in Sec. II implies that to every $Q \in \mathcal{Q}_N$ there corresponds, via (3.15), a question vector $\vec{q} \in \mathbb{R}^{4^N-1}$ such that $y(\vec{q}|\vec{r}) \in [0,1]\ \forall\ \vec{r} \in \Sigma_N$ and a 1 bit state $\vec{r}_Q$ such that $y(\vec{q}|\vec{r}_Q) = 1$, i.e., such that O "knows" that $Q =$ "yes" if S is in the state $\vec{r}_Q$. Conversely, Principle 5 asserts that each such vector $\vec{q}$ corresponds to a question $Q \in \mathcal{Q}_N$. In Appendix C 1, we show that any such vector $\vec{q}$ is a 1 bit quantum state, in fact, coinciding with $\vec{r}_Q = \vec{q}$. We thus arrive at the following question vector characterization:

Consequence (*Question vector characterization*). A vector $\vec{q} \in \mathbb{R}^{4^N-1}$ corresponds to $Q \in \mathcal{Q}_N$ if and only if it is a quantum state with $|\vec{q}|^2 = 1$ bit and $y(\vec{q}|\vec{r}) \in [0,1]\ \forall\ \vec{r} \in \Sigma_N$.

Given that every question vector corresponds to a unique $Q \in \mathcal{Q}_N$ and vice versa (see Sec. II), we immediately have

$$\mathcal{Q}_N \simeq \{\vec{q} \in \mathbb{R}^{4^N-1}\ |\ y(\vec{q}|\vec{r}) \in [0,1]\ \forall\ \vec{r} \in \Sigma_N \text{ and } \vec{q} \text{ is a 1 bit quantum state}\}. \tag{3.16}$$

Among other things, operationally this means that every $Q \in \mathcal{Q}_N$ is in one-to-one correspondence with a unique 1 bit state $\vec{r}_Q \in \Sigma_N$ which represents the truth value $Q =$ "yes" and which does not represent the truth value "yes" for any other question in $\mathcal{Q}_N$. This state $\vec{r}_Q$ encodes the situation that O has asked *only* the single question Q to S in the state of no information $\vec{r} = \vec{0}$ and received a "yes" answer (i.e., $\vec{r}_Q$ is the updated state after receiving $Q =$ "yes" relative to $\vec{r} = \vec{0}$). For $N = 1$, each question in $\mathcal{Q}_N$ will therefore be described by the *pure* state in which it is answered with "yes", while for $N > 1$ each question is represented by the *mixed* state in which it is answered with "yes" by S. We also note that $\neg Q \in \mathcal{Q}_N$ iff $Q \in \mathcal{Q}_N$ and that $\neg Q$ will be described by a distinct question vector.

Thus, the full set of legitimate 1 bit question vectors, corresponding to $\mathcal{Q}_N$, coincides with a subset of the 1 bit quantum states in Σ_N. First, notice that not every Bloch vector of length 1 bit represents a legal state in Σ_N for $N > 1$. For instance, consider $N = 2$ qubits and the vector $\vec{r}_{\text{ill}} = \frac{1}{\sqrt{2}}(1,1,0,\dots,0)$ which naively could be interpreted as O having half a bit of information about each of Q_{x_1} and Q_{x_2}. But, this would specify the probabilities that O receives "yes" answers to the latter two questions as $y_{x_1} = y_{x_2} = (r_{x_1} + 1)/2 = (1 + 1/\sqrt{2})/2 > 0.85$. In this case, it is impossible that the probability y_{xx} that Q_{xx} gives "yes" is $1/2$. Accordingly, r_{xx} must be larger than 0 and $\vec{r}_{\text{ill}}$ is an illegal state. In fact, one can convince oneself that $\vec{r}_{\text{ill}}$ is *not* a convex combination of pure states and that this Bloch vector would produce a nonpositive density matrix.[24] We conclude that, for $N > 1$, not all vectors of length 1 bit can correspond to questions in $\mathcal{Q}_N$.

Second, we proceed with the observation that also not every legal 1 bit mixed state corresponds to a "yes" answer of a question in $\mathcal{Q}_N$. For example, for any pure state $\vec{r}_{\text{pure}}$, the rescaling $\vec{r}_{\text{pure}}/\sqrt{2^N-1}$ corresponds to a convex sum of the original pure state and the state of no information and thus yields a legal 1 bit mixed state.[25] This state cannot correspond to a question vector of any $Q \in \mathcal{Q}_N$ because (3.15) implies that the probability for measuring a "yes" outcome for Q in the state $\vec{r}_{\text{pure}}$ would be larger than one, $y(Q|\vec{r}_{\text{pure}}) = (1 + \sqrt{2^N-1})/2 > 1$ for $N > 1$.

2. Born rule for projective measurements

As an interlude, we note that (3.15) coincides precisely with the Born rule of quantum theory for projective measurements onto the Pauli operators $\vec{n}\cdot\vec{\sigma}$,[26] where $\vec{n} \in \mathbb{R}^{4^N-1}$ with $|\vec{n}| = 1$. Namely, it can be easily checked that the projector onto the $+1$ eigenspace of a Pauli operator $\sigma_{\mu_1\dots\mu_N}$ is given by $P_{\mu_1\dots\mu_N} = \frac{1}{2}(\mathbb{1} + \sigma_{\mu_1\dots\mu_N})$. Indeed, using $\sigma^2_{\mu_1\dots\mu_N} = \mathbb{1}$ it follows that $P^2_{\mu_1\dots\mu_N} = P_{\mu_1\dots\mu_N}$ and $P_{\mu_1\dots\mu_N}\,\rho_{\mu_1\dots\mu_N} = \rho_{\mu_1\dots\mu_N}$ where $\rho_{\mu_1\dots\mu_N} = \frac{1}{2^N}(\mathbb{1} + \sigma_{\mu_1\dots\mu_N})$ is the density matrix corresponding to only $\sigma_{\mu_1\dots\mu_N}$ being measured with $+1$ and all other $\sigma_{\nu_1\dots\nu_N}$ unknown. Using that all Pauli operators are connected by unitary conjugation (see Appendix C 2), one finds that $P_{\vec{n}} = \frac{1}{2}(\mathbb{1} + \vec{n}\cdot\vec{\sigma})$ constitutes the projector onto the $+1$ eigenspace of the Pauli operator $\vec{n}\cdot\vec{\sigma}$. But then for all permitted $\vec{n}$ and all density matrices we find

$$\mathrm{tr}(P_{\vec{n}}\,\rho) = \tfrac{1}{2}(1 + \vec{n}\cdot\vec{r})$$

in agreement with (3.15) under the identification $\vec{n} = \vec{q}$.

We have thus reconstructed the Born rule of quantum theory for projective measurements onto Pauli operators. Next, we show that $\mathcal{Q}_N$ also coincides with the set of projective measurements onto the Pauli operators.

3. Questions as projective measurements onto Pauli operators

For a single qubit, (3.16) immediately implies $\mathcal{Q}_1 \simeq \{\vec{q} \in \mathbb{R}^3\ |\ |\vec{q}| = 1\} \simeq \mathbb{CP}^1 \simeq S^2$ such that $\mathcal{Q}_1$ is isomorphic to the set of pure states. This has two consequences. (1) It induces a transitive action of the time evolution group $\mathcal{T}_1 \simeq \mathrm{SO}(3)$ on $\mathcal{Q}_1$: if the Bloch vector $\vec{r}$ ($|\vec{r}| = 1$) incarnates the "yes" answer to Q, represented by $\vec{q}$, then $T\cdot\vec{r}$ is the "yes" answer to the question $T(Q)$, represented by $T\cdot\vec{q}$, for any $T \in \mathcal{T}_1$ (we can imagine the time evolution of a question to correspond to a rotation of the measurement device by means of which O asks the questions). (2) $\mathcal{Q}_1$ is isomorphic to the set of projective measurements on single-qubit Pauli operators $\vec{n}\cdot\vec{\sigma}$, $\vec{\sigma} = (\sigma_x,\sigma_y,\sigma_z)$, which likewise are parametrized by $\vec{n} \in \mathbb{R}^3$, $|\vec{n}| = 1$.

---

[24] It must hold $r_{xx} \geqslant \sqrt{2} - 1$ in order for the state to be positive.

[25] We note that such a state is *not* connected via time evolution to the 1 bit states corresponding to the questions in an informationally complete set. For example, $\vec{r}_{\text{pure}}/\sqrt{2^N-1}$ cannot be time connected to $\vec{q}_{x_1} = \vec{\delta}_{x_1}$, corresponding to Q_{x_1}, for this would be equivalent to $\vec{r}_{\text{pure}}$ being time connected to $\sqrt{2^N-1}\,\vec{\delta}_{x_1}$ which is impossible for $N > 1$. Thus, there are subsets of 1 bit mixed states for $N > 1$ which cannot be related via time evolution.

[26] Pauli operators are those Hermitian operators on $\mathbb{C}^{2^N}$ which have two eigenvalues ± 1 with equal dimensionality of the corresponding eigenspaces. These are exactly the Hermitian, traceless operators σ satisfying $\sigma^2 = \mathbb{1}$ (see Sec. III C 1 below, but also [52,53]). As we shall see in Appendix C 2, not every $\vec{n} \in \mathbb{R}^{4^N-1}$ with $|\vec{n}| = 1$ yields a Pauli operator.

For $N > 1$ the situation is more intricate. However, in Appendix C we derive the analogous results also for $N > 1$. First, on the quantum side, we show the following in Appendix C 2:

(a) The Pauli operators on an N-qubit Hilbert space $\mathbb{C}^{2^N}$ can be written as $\vec{n}\cdot\vec{\sigma}$, where

$$\vec{\sigma} = \big(\sigma_{x_1}\otimes \mathbb{1}\otimes\cdots\otimes\mathbb{1},\mathbb{1}\otimes\sigma_{x_2}\otimes\cdots\otimes\mathbb{1},\ldots,\sigma_{z_1}\otimes\sigma_{z_2}\otimes\cdots\otimes\sigma_{z_N}\big) \tag{3.17}$$

constitutes a basis of Pauli operators and the set of permissible unit vectors $\vec{n}$ is the orbit $\{T\cdot\vec{\delta}_{z_1}\mid T\in\mathcal{T}_N\}\simeq\mathbb{CP}^{2^N-1}$ which is thus isomorphic to the set of quantum pure states. (Note that this set of permissible $\vec{n}$ is a strict subset of the unit sphere for $N>1$.) In particular, $\mathcal{T}_N = \mathrm{PSU}(2^N)$ acts transitively on the unit vectors $\vec{n}$ defining the Pauli operators. Equivalently, for any Pauli operator $\vec{n}\cdot\vec{\sigma}$ there exists $U\in\mathrm{SU}(2^N)$ such that $\sigma_{z_1} = U\,(\vec{n}\cdot\vec{\sigma})\,U^\dagger$, where $\sigma_{z_1} := \sigma_z\otimes\mathbb{1}\times\cdots\otimes\mathbb{1}$. The set of Pauli operators accounts for all traceless Hermitian operators on $\mathbb{C}^{2^N}$ with ±1 eigenvalues because all diagonal operators on $\mathbb{C}^{2^N}$ featuring equally many ±1 along their diagonals are related to σ_{z_1} by conjugation with permutation matrices lying in $\mathrm{SU}(2^N)$.

Second, on the reconstruction side, we establish in Appendix C 3 the below consequences of (3.16):

(b) In its 1 bit vector representation, the question set $\mathcal{Q}_N$ inherits an action of the time evolution group $\mathcal{T}_N$ from the states Σ_N and $\mathcal{T}_N$ acts transitively on $\mathcal{Q}_N$. In particular, the basis question vectors $\vec{q}_{x_1}=\vec{\delta}_{x_1},\ldots,\vec{q}_{x_N}=\vec{\delta}_{x_N},\ldots,\vec{q}_{z_1\cdots z_N}=\vec{\delta}_{z_1\cdots z_N}$, corresponding to the informationally complete set $\mathcal{Q}_{M_N}=\{Q_{x_1},\ldots,Q_{x_N},\ldots,Q_{z_1\cdots z_N}\}$, are connected by time evolution $\mathcal{T}_N$ and no question in $\mathcal{Q}_N$ exists whose question vector is not connected by time evolution to these basis vectors.

(c) Under the identification $\vec{q}\equiv\vec{n}$, $\mathcal{Q}_N$ is isomorphic to the set of Pauli operators on an N-qubit Hilbert space. Hence, $\mathcal{Q}_N\simeq\mathbb{CP}^{2^N-1}$ and the set of allowed questions is thanks to (a) therefore isomorphic to the pure state space also for $N>1$.

We conclude that the set of binary questions $\mathcal{Q}_N$, which we have restricted O to, corresponds to a strict subset of all possible N-qubit observables: the Pauli operators. In fact, any $\vec{n}\in\mathbb{R}^{4^N-1}$ produces a Hermitian operator $\vec{n}\cdot\vec{\sigma}$ on $\mathbb{C}^{2^N}$ and thus legitimate N-qubit observable. However, these operators can feature 2^N arbitrary real eigenvalues, corresponding to many different measurement outcomes per observable such that the latter cannot be represented by a single binary question. These observables are not captured by $\mathcal{Q}_N$.

The above results have strong implications for the question set. In particular, under the identification $\vec{n}\equiv\vec{q}$, we ultimately obtain the correspondence

$$Q_{\mu_1}\leftrightarrow Q_{\mu_2}\leftrightarrow\cdots\leftrightarrow Q_{\mu_N}$$
$$\Leftrightarrow P_{\mu_1\ldots\mu_N} := \tfrac{1}{2}\big(\mathbb{1}+\sigma_{\mu_1}\otimes\sigma_{\mu_2}\otimes\cdots\otimes\sigma_{\mu_N}\big),$$

where $P_{\mu_1\ldots\mu_N}$ is the projector onto the $+1$ eigenspace of $\sigma_{\mu_1}\otimes\sigma_{\mu_2}\otimes\cdots\otimes\sigma_{\mu_N}$. Indeed, $Q_{\mu_1\ldots\mu_N}$ yields 1 or 0 if an even or odd number of Q_{μ_i} is 0, respectively, and thus corresponds to the question "is the product of the spin projections of $\sigma_{\mu_1}\otimes\sigma_{\mu_2}\otimes\cdots\otimes\sigma_{\mu_N}$ +1?" (see also [53] for a related discussion of Pauli operators). We thus see that the XNOR connective $\leftrightarrow$ at the question level corresponds to the tensor product at the operator level.

In the remainder of this section, we shall discuss further consequences of (a)–(c).

4. Dual time evolution of questions: Heisenberg versus Schrödinger

We just observed that the set of permissible questions $\mathcal{Q}_N$ inherits an action of the time evolution group $\mathcal{T}_N$ from the states Σ_N. Specifically, any two legal question vectors are connected by a time evolution element and the time evolution of a legal question always yields another legal question.[27] At this point, this might be taken as just a mathematical observation. However, we might as well interpret the action of the time evolution group on the questions as transformations (e.g., rotations) of the measurement device(s) by means of which O interrogates the systems.

The evolution of questions is dual to the evolution of states. Namely, the Born rule (3.15) implies $y(Q|T\cdot\vec{r}) = [1+\vec{q}\cdot(T\cdot\vec{r})]/2 = [1+(T^t\cdot\vec{q})\cdot\vec{r}]/2 = y[T^{-1}(Q)|\vec{r}]$. That is, we may describe O's interrogation of a system of N qubits as it evolves in time in two equivalent ways: (1) the state vector $\vec{r}(t)$ evolves in time while the questions are time independent, or (2) the state vector is time independent and the questions $\vec{q}(t)$ evolve under the inverse of the time evolution. In particular, if both the state and question are evolved simultaneously, the probability remains invariant. (1) corresponds to the usual Schrödinger picture of quantum theory, while (2) parallels the Heisenberg picture; our reconstruction thus admits these dual interpretations of qubit quantum theory.

Importantly, for the Heisenberg picture, the time evolution invariance of the Born rule (3.15) immediately implies that the compatibility and independence structure of the questions is invariant if time evolved simultaneously. Indeed, using that the question vectors are identical to 1 bit states in which only the corresponding question is positively answered, we can express the independence relations of two arbitrary questions $Q_1,Q_2\in\mathcal{Q}_N$ via $y(Q_1|\vec{q}_2)$ and clearly it holds

$$y[T(Q_1)|T\cdot\vec{q}_2] = y(Q_1|\vec{q}_2).$$

By similar arguments, using the Born rule with respect to states, it follows that also their compatibility relations remain invariant.

Finally, this also entails that every question $Q\in\mathcal{Q}_N$ is indeed contained in an informationally complete set, a mutually complementary set, and a maximal set of compatible questions. Namely, consider some set of mutually complementary $\{\vec{q}_1,\vec{q}_2',\ldots,\vec{q}_k'\}$ and another of mutually compatible $\{\vec{q}_1,\vec{q}_2'',\ldots,\vec{q}_j''\}$ questions. Since for any $Q\in\mathcal{Q}_N$ there is a $T\in\mathcal{T}_N$ such that $\vec{q}=T\cdot\vec{q}_1$, the following time evolved sets $\{\vec{q},T\cdot\vec{q}_{i_2}',\ldots,T\cdot\vec{q}_{i_k}'\}$ and $\{\vec{q},T\cdot\vec{q}_{i_2}'',\ldots,T\cdot\vec{q}_{i_j}''\}$ constitute a

[27] For example, let $T_1\in\mathcal{T}_1$ be a local rotation of qubit 1 and let $\tilde{T}\in\mathcal{T}_1^{(1)}$ be its product representation within $\mathcal{T}_N$. Denote by $T(Q)$ the action of some $T\in\mathcal{T}_N$ on a question $Q\in\mathcal{Q}_N$ (understood at the question vector level). Since $T_1(Q_{\mu_1})$ is a legal question on qubit 1, so must be

$$T_1(Q_{\mu_1})\leftrightarrow Q_{\mu_2}\leftrightarrow\cdots\leftrightarrow Q_{\mu_N} = \tilde{T}(Q_{\mu_1}\leftrightarrow Q_{\mu_2}\leftrightarrow\cdots\leftrightarrow Q_{\mu_N}).$$

mutually complementary and a compatible set of questions, respectively, both of which contain $\vec{q}$. In the sense of compatibility and independence relations, no question in $\mathcal{Q}_N$ is special.

5. (Non)uniqueness of pure state decompositions in terms of questions

Every pure state can be decomposed in terms of a sum of 2^N-1 mutually compatible question vectors. The reason is that, thanks to the transitivity of $\mathcal{T}_N$ on the set of pure states, every pure state $\vec{r}_{\text{pure}}$ can be written as $\vec{r}_{\text{pure}} = T\cdot(\vec{\delta}_{z_1}+\vec{\delta}_{z_2}+\cdots+\vec{\delta}_{z_1\cdots z_N})$ for some $T\in\mathcal{T}_N$. The vectors $T\cdot\vec{\delta}_{z_1},\ldots,T\cdot\vec{\delta}_{z_1\cdots z_N}$ within the decomposition are time connected to the question vectors $\vec{q}_{z_1},\ldots,\vec{q}_{z_1\cdots z_N}$ and are therefore themselves legal question vectors, featuring the same compatibility and independence relations. The Born rule (3.15) implies that the probability for each of these 2^N-1 questions in the pure state decomposition to be answered by S_N with "yes" equals one in this state. In fact, (b) above implies that, by running through all elements T in $\mathcal{T}_N$, all question vectors will appear in some pure state. This raises the question as to whether such a question decomposition of a pure state is unique or not and, in consequence, whether S_N, prepared in a pure state, answers a unique set of questions in $\mathcal{Q}_N$ with "yes".

For $N=1$ this is trivially the case since every pure state vector is also a legal question vector. For $N>1$ the situation, however, turns out to be less trivial. More precisely, in Appendix C 4, we demonstrate the peculiar fact that

The decomposition of a pure state vector $\vec{r}_{\text{pure}} = \vec{q}_1+\cdots+\vec{q}_{2^N-1}$ in terms of question vectors $\vec{q}_i$ for $Q_i\in\mathcal{Q}_N$ is *unique* for $N=1,2$ and *nonunique* for $N\geqslant 3$.

This is a consequence of the fact that the isotropy subgroup $\mathrm{PSU}(2^N-1)$ of $\mathcal{T}_N=\mathrm{PSU}(2^N)$ on $\mathbb{CP}^{2^N-1}$ corresponding to a pure state $\vec{r}_{\text{pure}}$ contains elements for $N\geqslant 3$ which are not part of the isotropy subgroups associated to every question vector $\vec{q}_i$ in the decomposition.

In other words, for $N=1,2$, S_N, prepared in any pure state, answers a unique set of 2^N-1 questions from $\mathcal{Q}_N$ positively. For $N\geqslant 3$, S_N answers in every pure state multiple distinct sets of 2^N-1 questions from $\mathcal{Q}_N$ simultaneously with "yes". However, for $N\geqslant 3$ the total information contained in one of these sets of 2^N-1 questions is evidently equivalent to that carried by any other such set, even though a question in the first set might be (partially) independent from all questions in any other set.

D. The von Neumann evolution equation

For completeness, we discuss briefly how the von Neumann evolution equation of density matrices follows from the reconstruction. After having established coincidence between Σ_N and the set of N-qubit density matrices, nothing stops us from passing from the Bloch vector representation of states to the equivalent Hermitian representation in terms of density matrices on $\mathbb{C}^{2^N}$:

$$\rho = \frac{1}{2^N}\left(\mathbb{1}_{2^N\times 2^N} + \vec{r}\cdot\vec{\sigma}\right),$$

where $\vec{r}$ is the Bloch vector and $\vec{\sigma}$ is given in Eq. (3.17). We have seen (e.g., in Appendix B 3) that the linear evolution $\vec{r}(t) = T(t)\,\vec{r}(0)$ with $T(t)=e^{t\,G}\in\mathrm{PSU}(2^N)$ is equivalent to the adjoint action of $U(t)=e^{-i\,H\,t}\in\mathrm{SU}(2^N)$ on its Lie algebra

$$\rho(t) = U(t)\,\rho(0)\,U^\dagger(t), \tag{3.18}$$

for some Hermitian operator H on $\mathbb{C}^{2^N}$ [49]. In particular, using that $\mathrm{Tr}(\sigma_i\,\sigma_j) = 2^N\,\delta_{ij}$ [53], $T_{ij}(t) = \frac{1}{2^N}\,\mathrm{Tr}\,[\sigma_i\,U(t)\,\sigma_j\,U^\dagger(t)]$. This yields a relation between time evolution generators $G\in\mathrm{psu}(2^N)$ at the Bloch vector level and a "Hamiltonian" H on a Hilbert space. But, (3.18) is equivalent to $\rho(t)$ satisfying the von Neumann evolution equation

$$i\frac{\partial\rho}{\partial t} = [H,\rho]$$

which, in turn, is well known to be equivalent to the Schrödinger equation for pure states.

IV. DISCUSSION AND CONCLUSIONS

We have shown that one can derive qubit quantum theory from transparent rules on an observer's acquisition of information about an observed system. These rules constitute a set of physical statements, equivalent to the usual textbook axioms, characterizing the quantum formalism. This paper, together with [35], thereby offers a solution to a longstanding problem and completes related informational reconstruction ideas put forward in the context of Rovelli's *relational quantum mechanics* [9] and the Brukner-Zeilinger informational interpretation of quantum theory [10,11] for the case of qubit systems. (It also can be regarded as a completion of some ideas put forward by Spekkens in his epistemic toy model [16] which, however, relies on ontic states.) One of the salient conclusions to be drawn from the present reconstruction is that it is sufficient to speak about the information that an observer has access to through measurement. This information is associated to the relation between the observer and the system, established through interaction; the state represents the observer's "catalog of knowledge" about the system and it is not necessary to consider the notion of intrinsic state of the system. This highlights that quantum theory can be understood as an inference framework governing an observer's acquisition of information and pertaining to what the observer can say about Nature, rather than to how Nature "really" is.

In addition, the reconstruction provides new structural insights into qubit quantum theory which were previously unnoticed. Specifically, we have derived new constraints on the distribution of information over the various questions in an informationally complete set (orthonormal basis of Pauli operators) of N qubits. This employs the quadratic information measure derived from the principles in Ref. [35] and earlier proposed from a different perspective in Refs. [11,12,14,48]. Most importantly, we have shown for two qubits that the maximal mutually complementary question sets each carry precisely 1 bit of information for pure states, constituting six *conserved informational charges* of time evolution for two qubits. These six equalities define the unitary group and, together with 15 conservation equalities, fully characterize the pure state space. This generalizes the single-qubit case where a similar statement holds. While it was not necessary for the completion of the reconstruction, it is tempting to conjecture that this is a general property, namely, that the unitary group and pure states are characterized by maximal mutually complementary sets carrying precisely 1 bit of information for arbitrarily many qubits. We leave this as an open question.

These observations highlight information as a "charge of quantum theory" in the sense of providing the conserved quantities of the unitary groups. In analogy to charges in other areas of physics which can be transferred without loss among different carrier systems, these informational charges can be redistributed without loss among different questions in-between measurements.

Such conserved charges thus form part of the invariant structure that observers in distinct reference frames should agree on. As such, they might be useful, say, in a quantum communication protocol as in Ref. [54] which permits distinct observers, who have never met before but can communicate, to efficiently agree on their respective descriptions of quantum states. In this manner, one can derive the appropriate reference frame transformation group operationally from the structure of the communicated physical objects, rather than imposing it on the theory "by hand." For instance, depending on the conditions on such a quantum communication protocol, one can show that either the rotation group SO(3) or the orthochronous Lorentz group $\mathrm{O}^{+}(3,1)$ constitutes the dictionary among distinct observer's quantum descriptions, without presupposing any specific space-time structure [54].

We have also derived the Born rule for projective measurements and shown that the time evolution of states implied by the principles is equivalent to the von Neumann evolution equation. While it was not necessary for us to derive the Born rule for state transition probabilities, this could presumably be accomplished by using arguments similar to the ones in [22–24]. We emphasize that it was also not necessary to fully specify (or derive) the precise state update rule in order to arrive at the structure of quantum theory. We shall similarly leave the full clarification of this update rule as an open matter.

The binary question framework in its present form is limited to reconstructing qubit (and rebit [35,44]) quantum theory and requires a generalization in order to be applicable to arbitrary n-level quantum systems. A treatment of *mechanical* systems may even necessitate an entirely novel approach.

ACKNOWLEDGMENTS

We are indebted to M. Müller for numerous discussions, helpful comments, and the proof of Lemma 10. We would also like to thank L. Hardy and R. Spekkens for many useful discussions and comments. P.H., furthermore, thanks Č. Brukner, S. Carrozza, B. Dakić, and C. Rovelli for discussion. C.W. is grateful for the hospitality of Perimeter Institute, where a large part of this work was done. P.H. similarly thanks the Demokritos Institute in Athens for hospitality during a visit and both authors also appreciate the hospitality of the Institute for Theoretical Physics of Universiteit Utrecht. Research at Perimeter Institute is supported by the Government of Canada through the Department of Innovation, Science and Economic Development Canada and by the Province of Ontario through the Ministry of Research, Innovation and Science. During the main part of this research project, C.W. worked at NCSR "Demokritos" and was supported by the Research Funding Program ARISTEIA, HOCTools [cofinanced by the European Union (European Social Fund ESF) and Greek national funds through the Operational Program "Education and Lifelong Learning" of the National Strategic Reference Framework (NSRF)].

APPENDIX A: AFFINE LINEARITY OF THE PROBABILITY FUNCTION

In Sec. II, we argued operationally that the probability function is at least convex linear

$$Y[Q|\lambda\,\vec{y}_1+(1-\lambda)\,\vec{y}_2]=\lambda\,Y(Q|\vec{y}_1)+(1-\lambda)\,Y(Q|\vec{y}_2),\quad 0\leqslant\lambda\leqslant 1.$$

This holds for all $Q\in\mathcal{Q}$ and $\vec{y}_i\in\Sigma$. More generally, this means that

$$Y\left(Q\,\middle|\,\sum_i\lambda_i\,\vec{y}_i\right)=\sum_i\lambda_i\,Y(Q|\vec{y}_i),\quad \lambda_i\geqslant 0,\quad \sum_i\lambda_i=1. \tag{A1}$$

It will be convenient to parametrize states equivalently by $\vec{r}_i=2\,\vec{y}_i-\vec{1}$. Setting $y(Q|\vec{r}):=Y(Q|\vec{y}=1/2\,\vec{r}+\vec{1})$, it is clear that (A1) if and only if

$$y\left(Q\,\middle|\,\sum_i\lambda_i\,\vec{r}_i\right)=\sum_i\lambda_i\,y(Q|\vec{r}_i),\quad \lambda_i\geqslant 0,\quad \sum_i\lambda_i=1. \tag{A2}$$

We shall now show that this implies that $y(Q|\vec{r})$ is affine linear as claimed in Eq. (2.3). This result and its following proof are a twisted version of linearity results in Hardy [22] and Barrett [45]. The biggest twist is that here we work with "normalized" states only and with $y(Q|\vec{0})\neq 0$.

Setting one of the $\vec{r}_i$ in Eq. (A2) equal to the state of no information, $\vec{r}=\vec{0}$, it is easy to see that for $\vec{r}_i\in\Sigma$ also

$$y\left(Q\,\middle|\,\sum_i\lambda_i\,\vec{r}_i\right)=\sum_i\lambda_i\,y(Q|\vec{r}_i)+\left(1-\sum_i\lambda_i\right)y(Q|\vec{0}),\quad \lambda_i\geqslant 0,\quad \sum_i\lambda_i\leqslant 1. \tag{A3}$$

Suppose now that $\sum_i\lambda_i=\gamma<1$. It is then not difficult to convert (A3) to

$$y\left(Q\,\middle|\,\sum_i\tilde{\lambda}_i\,\tilde{\vec{r}}_i\right)=\sum_i\tilde{\lambda}_i\,y(Q|\tilde{\vec{r}}_i)+\left(1-\sum_i\tilde{\lambda}_i\right)y(Q|\vec{0}),$$

where $\tilde{\lambda}_i=\lambda_i/\gamma^2$ and $\tilde{\vec{r}}_i=\gamma\,\vec{r}_i$. Since $\sum_i\tilde{\lambda}_i=\gamma^{-1}>1$ and $\tilde{\vec{r}}_i\in\Sigma$ if $\vec{r}_i\in\Sigma$ ($\tilde{\vec{r}}_i$ is a convex combination of $\vec{r}_i$ and $\vec{0}$), we have even more generally

$$y\left(Q\,\middle|\,\sum_i\lambda_i\,\vec{r}_i\right)=\sum_i\lambda_i\,y(Q|\vec{r}_i)+\left(1-\sum_i\lambda_i\right)y(Q|\vec{0}),\quad \lambda_i\geqslant 0, \tag{A4}$$

as long as $\vec{r}_i,\ \sum_i\lambda_i\,\vec{r}_i\in\Sigma$. A special case of this is

$$y(Q|\lambda\,\vec{r})=\lambda\,y(Q|\vec{r})+(1-\lambda)\,y(Q|\vec{0}),$$

$$\lambda > 0, \quad \vec{r},\lambda\vec{r} \in \Sigma.$$

For $\lambda\,\vec{r} \notin \Sigma$ this equation is *a priori* not defined. Since this does not correspond to a physical situation, we are free to demand that also

$$y(Q|\lambda\,\vec{r}) = \lambda\, y(Q|\vec{r}) + (1-\lambda)\, y(Q|\vec{0}), \quad \forall\,\vec{r} \in \Sigma,\lambda \geqslant 0. \tag{A5}$$

Consider now the set $\Sigma_+ := \{\lambda\,\vec{r}\,|\,\forall\,\vec{r} \in \Sigma,\lambda \geqslant 0\}$. As Σ is convex, Σ_+ is a convex cone. Using (A4) and (A5), one easily shows that this implies

$$y\left(Q\middle|\sum_i \lambda_i\,\vec{r}_i\right) = \sum_i \lambda_i\, y(Q|\vec{r}_i) + \left(1 - \sum_i \lambda_i\right) y(Q|\vec{0}), \quad \forall\,\vec{r} \in \Sigma_+,\lambda_i \geqslant 0. \tag{A6}$$

Next, suppose

$$\vec{r} = \sum_i t_i\,\vec{r}_i, \quad \text{where} \quad \vec{r},\vec{r}_i \in \Sigma_+, \quad t_i \in \mathbb{R}. \tag{A7}$$

Split the indices according to $i \in A_-$ if $t_i < 0$ and $i \in A_+$ if $t_i \geqslant 0$. Then, we have

$$\vec{r} + \sum_{i\in A_-} |t_i|\,\vec{r}_i = \sum_{i\in A_+} t_i\,\vec{r}_i$$

and each side of the equation is in Σ_+ such that (A6) holds. Upon reorganization, this yields

$$y\left(Q\middle|\sum_i \lambda_i\,\vec{r}_i\right) = \sum_i \lambda_i\, y(Q|\vec{r}_i) + \left(1 - \sum_i \lambda_i\right) y(Q|\vec{0}), \quad \forall\,\lambda_i \in \mathbb{R}. \tag{A8}$$

This may be linearly extended to any vector that lies in the span of Σ_+; $y(Q|\vec{r})$ on the rest of $\mathbb{R}^D$ is arbitrary and may be freely chosen to be of the affine form (A8) as well.

Finally, setting $f_Q(\vec{r}) := y(Q|\vec{r}) - y(Q|\vec{0})$, (A8) implies that $f_Q(\vec{r})$ is *linear*

$$f_Q\left(\sum_i t_i\,\vec{r}_i\right) = \sum_i t_i\, f_Q(\vec{r}_i), \quad t_i \in \mathbb{R}$$

such that

$$y(Q|\vec{r}) = \vec{f}_Q \cdot \vec{r} + y(Q|\vec{0})$$

for some $\vec{f}_Q \in \mathbb{R}^D$. Remembering that by definition $y(Q|\vec{r} = \vec{0}) = \frac{1}{2}$ for all $Q \in \mathcal{Q}$ in the state of no information $\vec{r} = \vec{0}$, and setting $\vec{f}_Q = 1/2\,\vec{q}$, we immediately have

$$y(Q|\vec{r}) = \tfrac{1}{2}(\vec{q}\cdot\vec{r} + 1), \tag{A9}$$

where $\vec{q} \in \mathbb{R}^D$ is a vector depending on $Q \in \mathcal{Q}$. Hence, $Y(Q|\vec{y}) = 1/2[\vec{q}\cdot(2\vec{y} - \vec{1}) + 1]$.

APPENDIX B: RECONSTRUCTION OF THE UNITARY GROUP AND STATE SPACES

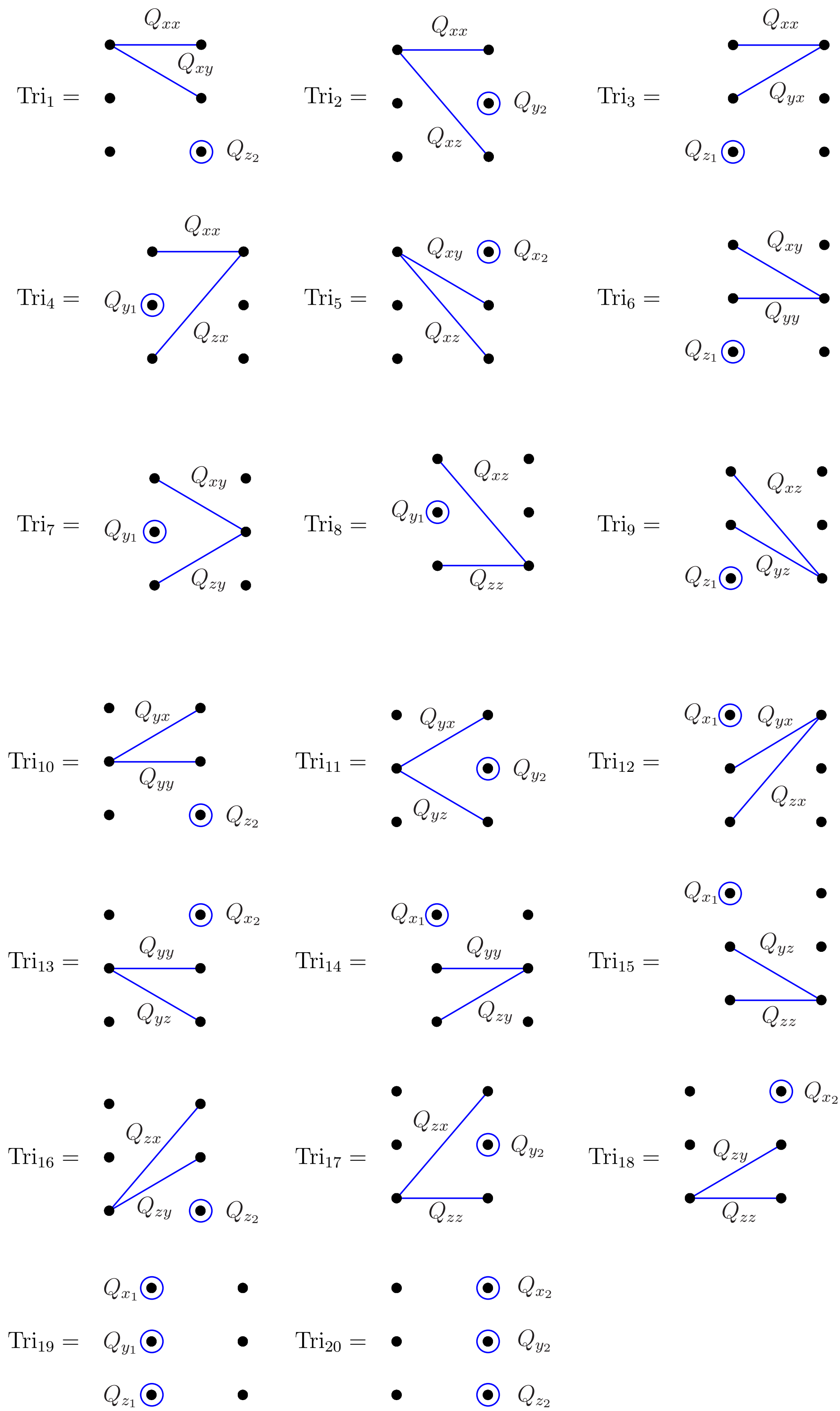
In order to present a flowing text in the main part of the paper, some proofs, derivations, and other statements were left out. These are collected in this Appendix.

1. Maximal mutually complementary triangle sets for $N = 2$ qubits

The maximal mutually complementary pentagon sets are important for the derivation of the time evolution group since their information contents constitute conserved charges under time evolution. In addition to the maximal pentagon sets, there are also maximal mutually complementary sets which contain three questions:

$$\begin{aligned}
\mathrm{Tri}_1 &= \{Q_{xx},Q_{xy},Q_{z_2}\},\\
\mathrm{Tri}_2 &= \{Q_{xx},Q_{xz},Q_{y_2}\},\\
\mathrm{Tri}_3 &= \{Q_{xx},Q_{yx},Q_{z_1}\},\\
\mathrm{Tri}_4 &= \{Q_{xx},Q_{zx},Q_{y_1}\},\\
\mathrm{Tri}_5 &= \{Q_{xy},Q_{xz},Q_{x_2}\},\\
\mathrm{Tri}_6 &= \{Q_{xy},Q_{yy},Q_{z_1}\},\\
\mathrm{Tri}_7 &= \{Q_{xy},Q_{zy},Q_{y_1}\},\\
\mathrm{Tri}_8 &= \{Q_{xz},Q_{zz},Q_{y_1}\},\\
\mathrm{Tri}_9 &= \{Q_{xz},Q_{yz},Q_{z_1}\},\\
\mathrm{Tri}_{10} &= \{Q_{yx},Q_{yy},Q_{z_2}\},\\
\mathrm{Tri}_{11} &= \{Q_{yx},Q_{yz},Q_{y_2}\},\\
\mathrm{Tri}_{12} &= \{Q_{yx},Q_{zx},Q_{x_1}\},\\
\mathrm{Tri}_{13} &= \{Q_{yy},Q_{yz},Q_{x_2}\},\\
\mathrm{Tri}_{14} &= \{Q_{yy},Q_{zy},Q_{x_1}\},\\
\mathrm{Tri}_{15} &= \{Q_{yz},Q_{zz},Q_{x_1}\},\\
\mathrm{Tri}_{16} &= \{Q_{zx},Q_{zy},Q_{z_2}\},\\
\mathrm{Tri}_{17} &= \{Q_{zx},Q_{zz},Q_{y_2}\},\\
\mathrm{Tri}_{18} &= \{Q_{zy},Q_{zz},Q_{x_2}\},\\
\mathrm{Tri}_{19} &= \{Q_{x_1},Q_{y_1},Q_{z_1}\},\\
\mathrm{Tri}_{20} &= \{Q_{x_2},Q_{y_2},Q_{z_2}\}.
\end{aligned} \tag{B1}$$

Similarly as for the pentagon sets, they can be represented by question graphs as given in Eq. (B2). Again, the vertices correspond to individual questions and edges connecting them represent the corresponding correlation questions. However, contrary to the maximal pentagon sets, for pure states the total information carried by each triangle set is not necessarily equal to the 1 bit bound in Eq. (2.1) (e.g., for entangled states the information content in Tri_{19},Tri_{20} is 0 bits) and is furthermore not conserved under time evolution. The pentagon and triangle sets are the only maximal mutually complementary sets for $N = 2$ qubits:



(B2)

We note that Tri_2, Tri_4, Tri_{19}, and Tri_{20} are represented as green triangles in the pentagon lattice of Fig. 4.

These triangle sets define via (2.1) complementarity inequalities $0 \leqslant I(\mathrm{Tri}_i) \leqslant 1$ bit, where $I(\mathrm{Tri}_i)$ is the information contained in triangle set i. Together with the pentagon equalities (3.3), these triangle complementarity inequalities define all independent complementarity inequalities which pure states have to satisfy as there are no other maximal mutually complementary sets. That is, any set of mutually complementary questions among the informationally complete set will be contained in either the pentagons or the triangles.

It is easy to show, however, that for pure states the 20 complementarity inequalities following from the triangle sets (B2) are not all independent. In fact, the pentagon equalities (3.3) imply that

$$
\begin{aligned}
I(\mathrm{Tri}_1) &:= \alpha_{z_2} + \alpha_{xx} + \alpha_{xy} = \alpha_{x_1} + \alpha_{yz} + \alpha_{zz} =: I(\mathrm{Tri}_{15}),\\
I(\mathrm{Tri}_2) &:= \alpha_{y_2} + \alpha_{xx} + \alpha_{xz} = \alpha_{x_1} + \alpha_{yy} + \alpha_{zy} =: I(\mathrm{Tri}_{14}),\\
I(\mathrm{Tri}_3) &:= \alpha_{z_1} + \alpha_{xx} + \alpha_{yx} = \alpha_{x_2} + \alpha_{zy} + \alpha_{zz} =: I(\mathrm{Tri}_{18}),\\
I(\mathrm{Tri}_4) &:= \alpha_{y_1} + \alpha_{xx} + \alpha_{zx} = \alpha_{x_2} + \alpha_{yy} + \alpha_{yz} =: I(\mathrm{Tri}_{13}),\\
I(\mathrm{Tri}_5) &:= \alpha_{x_2} + \alpha_{xy} + \alpha_{xz} = \alpha_{x_1} + \alpha_{yx} + \alpha_{zx} =: I(\mathrm{Tri}_{12}),\\
I(\mathrm{Tri}_6) &:= \alpha_{z_1} + \alpha_{yy} + \alpha_{xy} = \alpha_{y_2} + \alpha_{zx} + \alpha_{zz} =: I(\mathrm{Tri}_{17}),\\
I(\mathrm{Tri}_7) &:= \alpha_{y_1} + \alpha_{zy} + \alpha_{xy} = \alpha_{y_2} + \alpha_{yx} + \alpha_{yz} =: I(\mathrm{Tri}_{11}),\\
I(\mathrm{Tri}_8) &:= \alpha_{y_1} + \alpha_{xz} + \alpha_{zz} = \alpha_{z_2} + \alpha_{yx} + \alpha_{yy} =: I(\mathrm{Tri}_{10}),\\
I(\mathrm{Tri}_9) &:= \alpha_{z_1} + \alpha_{yz} + \alpha_{xz} = \alpha_{z_2} + \alpha_{zx} + \alpha_{zy} =: I(\mathrm{Tri}_{16}),\\
I(\mathrm{Tri}_{19}) &:= \alpha_{x_1} + \alpha_{y_1} + \alpha_{z_1} = \alpha_{x_2} + \alpha_{y_2} + \alpha_{z_2} =: I(\mathrm{Tri}_{20}).
\end{aligned}
$$

Note the symmetry pattern of these relations in terms of the graphical representation of the triangle sets in Eq. (B2); the encircled individual question of the triangle set on the left-hand side is the vertex where the two correlation questions of the triangle set on the right-hand side meet and vice versa.

2. Swap generators for $N = 2$ qubits

In this section, we discuss the swap generators defining the group $\mathcal{T}_2 = \mathrm{PSU}(4)$, their exponentiation, the pentagon preservation equations, and the consistency conditions arising from the complementarity inequalities (2.1) and the correlation structure of Fig. 3.

a. Derivation of the swap generators

We shall present the derivation of the 15 swap generators of Sec. III A 3 which are consistent with the correlation structure of Fig. 3. Subsequently, we shall argue that by varying the relative signs in these swap generators one accounts for all possible 60 linearly independent generators which could satisfy (3.5) and (3.8).

At the Bloch vector level, the swap transformation (3.9) between Pent_1 and Pent_2 is of the form

$$
\begin{aligned}
r_{y_1} &\longleftrightarrow \pm r_{zx}\ (\mathrm{Pent}_5), \quad r_{z_1} \longleftrightarrow \pm r_{yx}\ (\mathrm{Pent}_3),\\
r_{xy} &\longleftrightarrow \pm r_{z_2}\ (\mathrm{Pent}_4), \quad r_{xz} \longleftrightarrow \pm r_{y_2}\ (\mathrm{Pent}_6).
\end{aligned}
$$

Writing the transformation as $\vec{r}\,' = T\,\vec{r} = \exp[(\pi/2)\,G^{\mathrm{Pent}_1,\mathrm{Pent}_2}]\,\vec{r}$, the corresponding generator is, without loss of generality, of the following form:

$$
\begin{aligned}
G_{ij}^{\mathrm{Pent}_1,\mathrm{Pent}_2} &= \delta_{iy_1}\delta_{jzx} + s_1\,\delta_{iz_1}\delta_{jyx} + s_2\,\delta_{ixy}\delta_{jz_2}\\
&\quad + s_3\,\delta_{ixz}\delta_{jy_2} - (i \longleftrightarrow j),
\end{aligned}
$$

where $s_1,s_2,s_3 \in \{-1,+1\}$ are relative signs which must be determined. As can be easily checked, (3.5) is trivially satisfied for $i \in \mathrm{Pent}_k$ with $k \neq 1,2$ and $G_{ij} = G_{ij}^{\mathrm{Pent}_1,\mathrm{Pent}_2}$ thanks to symmetry and antisymmetry. For both the two swapped pentagons $k = 1,2$, on the other hand, the conservation equations (3.5) with $G^{\mathrm{Pent}_1,\mathrm{Pent}_2}$ are equivalent to

$$
r_{y_1}\,r_{zx} + s_1\,r_{z_1}\,r_{yx} + s_2\,r_{xy}\,r_{z_2} + s_3\,r_{xz}\,r_{y_2} = 0. \tag{B3}
$$

The sign structure of the generator $G_{ij}^{\mathrm{Pent}_1,\mathrm{Pent}_2}$ can be derived by considering three separate information distributions, all of which correspond to legal states:

$$
\begin{aligned}
&\text{Configuration 1: } \alpha_{x_2} = 1\text{ bit} \Rightarrow \alpha_{y_1} = \alpha_{yx},\ \alpha_{z_1} = \alpha_{zx},\\
&\qquad \alpha_{xy} = \alpha_{z_2} = \alpha_{xz} = \alpha_{y_2} = 0,\\
&\text{Configuration 2: } \alpha_{x_1} = 1\text{ bit} \Rightarrow \alpha_{y_2} = \alpha_{xy},\ \alpha_{z_2} = \alpha_{xz},\\
&\qquad \alpha_{y_1} = \alpha_{zx} = \alpha_{z_1} = \alpha_{yx} = 0,\\
&\text{Configuration 3: } \alpha_{zz} = 1\text{ bit} \Rightarrow \alpha_{z_1} = \alpha_{z_2},\ \alpha_{xy} = \alpha_{yx},\\
&\qquad \alpha_{y_1} = \alpha_{zx} = \alpha_{xz} = \alpha_{y_2} = 0.
\end{aligned}
$$

On the right-hand sides, we have made use of the constraints on the information distribution at the end of Sec. III A 2, in particular, Fig. 5, and complementarity (e.g., Q_{x_2},Q_{xy} being complementary implies that $\alpha_{x_2} = 1$ bit necessitates $\alpha_{xy} = 0$, etc.).

In configuration 1, (B3) reduces to

$$
r_{y_1}\,r_{zx} + s_1\,r_{z_1}\,r_{yx} = 0. \tag{B4}
$$

The relevant correlation triangles are represented in Fig. 6(a). Since both triangles represent *even* correlations, we have that $r_{x_2} = \pm 1$ implies $r_{z_1} = \pm r_{zx}$, $r_{y_1} = \pm r_{yx}$ (in this sign order). Accordingly, (B4) requires $s_1 = -1$ in order to be satisfied.[28] Using configuration 2 and Fig. 6(b), one shows similarly that $s_2 s_3 = -1$ and, finally, employing configuration 3 and Fig. 6(c), one easily verifies that (B3) requires $s_2 = +1$ and, hence, $s_3 = -1$. This yields $G^{\mathrm{Pent}_1,\mathrm{Pent}_2}$ in the form (3.11).

The generators of the eight other swaps between pentagons in Fig. 4 sharing composite questions are derived similarly. As will become clear shortly, together with $G^{\mathrm{Pent}_1,\mathrm{Pent}_2}$ these constitute the

9 generators of entangling unitaries:

$$
\begin{aligned}
G_{ij}^{\mathrm{Pent}_1,\mathrm{Pent}_2} &= \delta_{iy_1}\delta_{jzx} + \delta_{ixy}\delta_{jz_2} - \delta_{iz_1}\delta_{jyx} - \delta_{ixz}\delta_{jy_2}\\
&\quad - (i \longleftrightarrow j),
\end{aligned}
$$

[28] There must be a state which has all the Bloch components r_{z_1}, r_{zx}, r_{y_1}, and r_{yx} being nonzero. If this was not the case it would imply that whenever the observer O knows the answer to Q_{x_2} completely, O would then also know the answer to either the pairs Q_{z_1},Q_{zx} or Q_{y_1},Q_{yx} completely as well. However, this is not possible since then the question pairs Q_{z_1},Q_{zx} or Q_{y_1},Q_{yx} would be (partially) dependent on Q_{x_2}, which contradicts the fact that they are part of an informationally complete set.

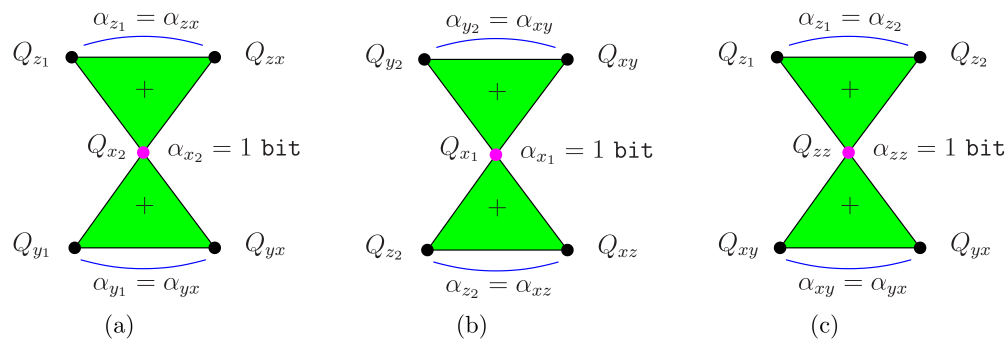


FIG. 6. The relevant correlation triangles of Fig. 3 for (B3) in configurations (a) 1, (b) 2, and (c) 3.

$$
\begin{aligned}
G_{ij}^{\mathrm{Pent}_1,\mathrm{Pent}_4} &= \delta_{iz_1}\delta_{jyy} + \delta_{ixx}\delta_{jz_2} - \delta_{iy_1}\delta_{jzy} - \delta_{ixz}\delta_{jx_2} \\
&\quad -(i \longleftrightarrow j),\\
G_{ij}^{\mathrm{Pent}_1,\mathrm{Pent}_6} &= \delta_{iy_1}\delta_{jzz} + \delta_{ixx}\delta_{jy_2} - \delta_{iz_1}\delta_{jyz} - \delta_{ixy}\delta_{jx_2} \\
&\quad -(i \longleftrightarrow j),\\
G_{ij}^{\mathrm{Pent}_2,\mathrm{Pent}_3} &= \delta_{iy_2}\delta_{jyz} + \delta_{izx}\delta_{jx_1} - \delta_{iz_2}\delta_{jyy} - \delta_{ixx}\delta_{jz_1} \\
&\quad -(i \longleftrightarrow j),\\
G_{ij}^{\mathrm{Pent}_2,\mathrm{Pent}_5} &= \delta_{iy_2}\delta_{jzz} + \delta_{ixx}\delta_{jy_1} - \delta_{iz_2}\delta_{jzy} - \delta_{iyx}\delta_{jx_1} \\
&\quad -(i \longleftrightarrow j),\\
G_{ij}^{\mathrm{Pent}_3,\mathrm{Pent}_4} &= \delta_{iyz}\delta_{jx_2} + \delta_{iz_1}\delta_{jxy} - \delta_{iyx}\delta_{jz_2} - \delta_{ix_1}\delta_{jzy} \\
&\quad -(i \longleftrightarrow j),\\
G_{ij}^{\mathrm{Pent}_3,\mathrm{Pent}_6} &= \delta_{iyy}\delta_{jx_2} + \delta_{ix_1}\delta_{jzz} - \delta_{iyx}\delta_{jy_2} - \delta_{iz_1}\delta_{jxz} \\
&\quad -(i \longleftrightarrow j),\\
G_{ij}^{\mathrm{Pent}_4,\mathrm{Pent}_5} &= \delta_{ix_2}\delta_{jzz} + \delta_{iyy}\delta_{jx_1} - \delta_{iz_2}\delta_{jzx} - \delta_{ixy}\delta_{jy_1} \\
&\quad -(i \longleftrightarrow j),\\
G_{ij}^{\mathrm{Pent}_5,\mathrm{Pent}_6} &= \delta_{izy}\delta_{jx_2} + \delta_{iy_1}\delta_{jxz} - \delta_{izx}\delta_{jy_2} - \delta_{ix_1}\delta_{jyz} \\
&\quad -(i \longleftrightarrow j). \qquad \text{(B5)}
\end{aligned}
$$

Note from the index structure that these generators always swap information between a pair of an individual and a composite question, thus transferring information from composite to individual questions and vice versa, as appropriate for an entangling transformation.

Next, we shall briefly explain how to derive the specific form of the swap generators for pentagon pairs in Fig. 4, overlapping in an individual question. For example, for the swap between Pent_3 and Pent_5, overlapping in Q_{x_1}, one arrives in analogy to above at

$$
G_{ij}^{\mathrm{Pent}_3,\mathrm{Pent}_5} = \delta_{iy_1}\delta_{jz_1} + s_1'\,\delta_{iyx}\delta_{jzx} + s_2'\,\delta_{iyy}\delta_{jzy} + s_3'\,\delta_{iyz}\delta_{jzz} -(i \longleftrightarrow j)
$$

such that (3.5) for $k = 3,5$ (again, the latter is trivially satisfied for $k \neq 3,5$ and $G^{\mathrm{Pent}_3,\mathrm{Pent}_5}$) is equivalent to

$$
r_{y_1}r_{z_1} + s_1'\,r_{yx}r_{zx} + s_2'\,r_{yy}r_{zy} + s_3'\,r_{yz}r_{zz} = 0. \qquad \text{(B6)}
$$

The sign structure can be determined by considering the information distributions

$$
\begin{aligned}
\text{Configuration } 1':\ & \alpha_{x_2} = 1 \text{ bit} \Rightarrow \alpha_{y_1} = \alpha_{yx},\\
& \alpha_{z_1} = \alpha_{zx},\ \alpha_{yy} = \alpha_{zy} = \alpha_{yz} = \alpha_{zz} = 0,\\
\text{Configuration } 2':\ & \alpha_{y_2} = 1 \text{ bit} \Rightarrow \alpha_{y_1} = \alpha_{yy},\\
& \alpha_{z_1} = \alpha_{zy},\ \alpha_{yx} = \alpha_{zx} = \alpha_{zz} = \alpha_{yz} = 0,\\
\text{Configuration } 3':\ & \alpha_{z_2} = 1 \text{ bit} \Rightarrow \alpha_{z_1} = \alpha_{zz},\\
& \alpha_{y_1} = \alpha_{yz},\ \alpha_{yx} = \alpha_{zx} = \alpha_{yy} = \alpha_{zy} = 0.
\end{aligned}
$$

The relevant correlation triangles for configurations $1'$–$3'$ are represented in Figs. 7(a)–7(c). Now, one proceeds as before, using that all relevant triangles represent *even* correlations, to show that $s_1' = s_2' = s_3' = -1$. The different sign structure (three, compared to the two minus signs for the entangling swaps) results from the fact that for *all* configurations $1'$–$3'$ the sign is determined by relating the last three terms in Eq. (B6) to the first (signless) term $r_{y_1}r_{z_1}$. By contrast, e.g., configuration

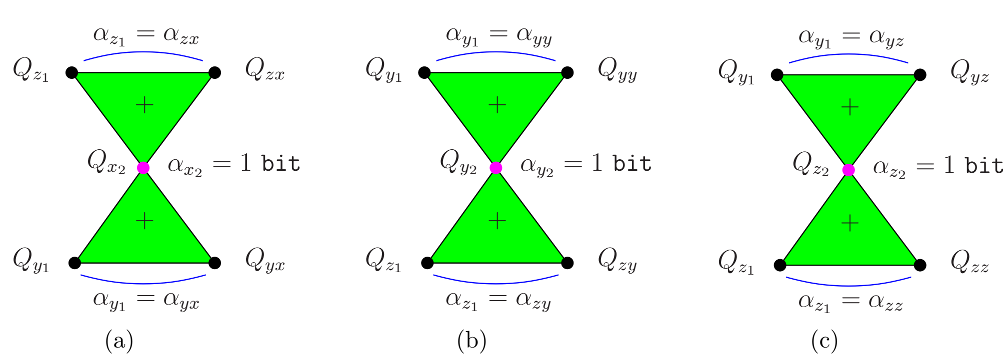


FIG. 7. The relevant correlation triangles of Fig. 3 for (B6) in configurations (a) $1'$, (b) $2'$, and (c) $3'$.

2 for the swap between Pent_1 and Pent_2 relates the last two terms with signs in Eq. (B3) against each other.

This yields $G^{\text{Pent}_3,\text{Pent}_5}$ in the form (3.12) and, in analogy, the full set of swap generators for pentagon pairs overlapping in an individual. As will be discussed below, these are the

6 generators of product unitaries:

$$\begin{aligned}
G^{\text{Pent}_1,\text{Pent}_3}_{ij} &= \delta_{ix_1}\delta_{jy_1} - \delta_{iyz}\delta_{jxz} - \delta_{iyy}\delta_{jxy} - \delta_{iyx}\delta_{jxx}\\
&\quad -(i \longleftrightarrow j),\\
G^{\text{Pent}_1,\text{Pent}_5}_{ij} &= \delta_{iz_1}\delta_{jx_1} - \delta_{ixz}\delta_{jzz} - \delta_{ixy}\delta_{jzy} - \delta_{ixx}\delta_{jzx}\\
&\quad -(i \longleftrightarrow j),\\
G^{\text{Pent}_2,\text{Pent}_4}_{ij} &= \delta_{iy_2}\delta_{jx_2} - \delta_{izx}\delta_{jzy} - \delta_{iyx}\delta_{jyy} - \delta_{ixx}\delta_{jxy}\\
&\quad -(i \longleftrightarrow j),\\
G^{\text{Pent}_2,\text{Pent}_6}_{ij} &= \delta_{iz_2}\delta_{jx_2} - \delta_{izx}\delta_{jzz} - \delta_{iyx}\delta_{jyz} - \delta_{ixx}\delta_{jxz}\\
&\quad -(i \longleftrightarrow j),\\
G^{\text{Pent}_3,\text{Pent}_5}_{ij} &= \delta_{iz_1}\delta_{jy_1} - \delta_{iyz}\delta_{jzz} - \delta_{iyy}\delta_{jzy} - \delta_{iyx}\delta_{jzx}\\
&\quad -(i \longleftrightarrow j),\\
G^{\text{Pent}_4,\text{Pent}_6}_{ij} &= \delta_{iz_2}\delta_{jy_2} - \delta_{izy}\delta_{jzz} - \delta_{iyy}\delta_{jyz} - \delta_{ixy}\delta_{jxz}\\
&\quad -(i \longleftrightarrow j).
\end{aligned} \tag{B7}$$

It can be easily checked that the six generators in Eq. (B7) satisfy the commutator algebra of $\text{so}(3) \oplus \text{so}(3)$. Note from the index structure that these six generators always swap information between pairs of individual questions or pairs of composite questions, as appropriate for the generators of the product unitaries.

With a computer algebra program one may check that, remarkably, the 15 generators [Eqs. (B5) and (B7)] coincide exactly (in some cases up to an unimportant overall sign) with the adjoint representation of the 15 fundamental generators of the Lie group SU(4):

$$(G^i)_{jk} := f^{ijk} = \tfrac{1}{4}\,\text{tr}([\sigma_j,\sigma_k]\,\sigma_i), \tag{B8}$$

where f^{ijk} are the structure constants of SU(4), the indices i,j,k take the 15 values $x_1,y_1,z_1,x_2,\dots,xz,xy,\dots,zz$ (as in our reconstruction) and $\sigma_{x_1} := \sigma_x \otimes \mathbb{1},\dots,\sigma_{x_2} := \mathbb{1}\otimes\sigma_x,\dots,$ $\sigma_{xx} := \sigma_x\otimes\sigma_x,\dots,\sigma_{zz} := \sigma_z\otimes\sigma_z$, and $\sigma_x,\sigma_y,\sigma_z$ are the usual Pauli matrices. In particular, the ordering of coincidence is $G^i \equiv \pm G^{\text{Pent}_a,\text{Pent}_b}$ where Q_i is the single question in $\text{Pent}_a \cap \text{Pent}_b$ which is left invariant by the swap; e.g., $G^{xx} \equiv G^{\text{Pent}_1,\text{Pent}_2}$, etc. This ultimately also clarifies that indeed (B5) constitute the generators of entangling unitaries, while (B7) are the generators of the product unitaries. Clearly, the 15 swap generators thus satisfy the commutator algebra of $\text{su}(4) \simeq \text{so}(6) \simeq \text{psu}(4)$,

$$[G^i,G^j] = f^{ijk}\,G^k,$$

with f^{ijk} given by (B8).

Let us now explain how the full information swaps account for all 60 linearly independent generators which *could* solve (3.5) and (3.8). While deriving the 15 generators [Eqs. (B5) and (B7)] we have made use of the correlation structure in Fig. 3 in order to fix the relative signs in the generators, e.g., in Eqs. (B3) and (B6). It is clear, however, that by varying these relative signs, one can produce four linearly independent generators from each generator in Eqs. (B5) and (B7) since each such generator contains four linearly independent components. By inspection, the reader may also verify that each of the 60 distinct pairs of complementary questions is encoded in precisely one of the 15 generators in terms of a nonvanishing component, corresponding to the pair of indices representing the pair of complementary questions. This immediately entails that by varying the relative signs in the 15 generators [Eqs. (B5) and (B7)], one obtains precisely the maximal amount of 60 linearly independent generators which satisfy (3.8). The relative sign structure only affects the correlation structure but not the fact that each of these 60 linearly independent generators represents a full swap of information between a pair of pentagon sets. As evident from the derivation in this section, however, it is only the 15 generators in Eq. (B5) and (B7) which are consistent with the correlation structure in Fig. 3 and which thus are legitimate candidates for time evolution generators in our reconstruction.

As an aside, let us briefly note that the sign structure of the 15 generators would be exactly the same, had we instead followed the alternative convention to build composite questions with the XOR connective, e.g., $\tilde{Q}_{xx} := \neg(Q_{x_1} \leftrightarrow Q_{x_2})$, etc., rather than the XNOR as done thus far (see also [35] on this). $\tilde{Q}_{xx}$ represents an *anticorrelation* question "are the answers to Q_{x_1} and Q_{x_2} anticorrelated?" In this case, the correlation structure for the XOR composites would coincide with the one in Fig. 3 except that all even correlation triangles would be replaced by odd ones and vice versa. However, this would leave the relative sign structure, determined via Figs. 6(a)–7(c) invariant. This has to be expected, of course, since both conventions are physically equivalent.

However, we note that the 15 generators for mirror quantum theory [23,35,46], obtained by swapping the assignment "yes" $\leftrightarrow$ "no" of a single individual question and adhering to the convention of building composite questions with the XNOR as before, would be distinct. Indeed, the swap of the answer assignment for, say, Q_{x_1} is equivalent to $Q_{x_1} \mapsto \neg Q_{x_1}$ (a partial transpose at the density matrix level) and $Q_{xx},Q_{xy},Q_{xz} \mapsto \neg Q_{xx},\neg Q_{xy},\neg Q_{xz}$. This produces a flip of the sign of the correlation triangles in *only* the upper graph in Fig. 3 (involving *only* the correlation questions), while leaving the lower graph invariant (see [35] for details). This has the consequence that Figs. 7(a)–7(c) and, more generally, the six product generators in Eq. (B7) remain invariant. However, the nine generators (B5) of the entangling transformations change their sign structure. In particular, Fig. 6(c) involves an *even* correlation triangle of the composites Q_{xy},Q_{yx},Q_{zz}, which would be replaced by an *odd* triangle for mirror quantum theory. This would result in $s_2 = -1$ and thus $s_3 = +1$ for mirror quantum theory (and analogously for the other generators). Mirror quantum theory thus has distinct entangling Hamiltonians (corresponding to the partial transpose relating it to standard quantum theory). Nevertheless, mirror quantum theory is physically perfectly equivalent to standard quantum theory and just employs a distinct convention for "yes" and "no" outcomes of questions [35,46]. The example of mirror quantum theory thus demonstrates that those swap generators among the 60 linearly independent ones mentioned above which differ in their relative sign structure from (B5) and (B7) simply correspond to distinct conventions.

b. Exponentiation of the generators

For the reasons mentioned in Sec. III A 3, the exponentiation of the swap generators results in the connected, simple Lie group $\mathcal{T}_2' = \mathrm{PSU}(4) \simeq \mathrm{PSO}(6)$ [rather than in SU(4) or SO(6)]. The exponential of any single generator G^a acts as 2×2 rotation matrices on the planes spanned by each pair of swapped questions. For example, $T^{\mathrm{Pent}_1,\mathrm{Pent}_2}(t) = \exp(t\, G^{\mathrm{Pent}_1,\mathrm{Pent}_2})$ acts as rotations of angle $\pm t$ in the planes (r_{y_1},r_{zx}), (r_{z_1},r_{yx}), (r_{xy},r_{z_2}), (r_{xz},r_{y_2}), where the signs are fixed by the swap generator (3.11). Furthermore, as one can easily convince oneself, the six generators (B7) exponentiate to the $\mathrm{SO}(3)\times\mathrm{SO}(3)\simeq\mathrm{PSU}(2)\times\mathrm{PSU}(2)$ product unitaries. For instance, $T^{\mathrm{Pent}_3,\mathrm{Pent}_5}(t) = \exp(t\, G^{\mathrm{Pent}_3,\mathrm{Pent}_5})$, generated by the swap which leaves α_{x_1} invariant, describes rotations of the Bloch vector around the r_{x_1} axis (leaving $r_{x_1},r_{xx},r_{xy},r_{xz}$ and r_{x_2},r_{y_2},r_{z_2} invariant). Similarly, the other generators in Eq. (B7) generate rotations around the Bloch vector axis corresponding to the individual question which constitutes the overlap of the respective pentagon pairs.

In general, the exponential of any single swap generator $G^{\mathrm{Pent}_i,\mathrm{Pent}_j}$ is of the form

$$\begin{aligned} T^{\mathrm{Pent}_a,\mathrm{Pent}_b}(t) &= \exp(t\, G^{\mathrm{Pent}_a,\mathrm{Pent}_b}) \\ &= [\cos(t)-1]\tilde{\mathbb{1}}^{\mathrm{Pent}_a,\mathrm{Pent}_b} \\ &\quad + \sin(t) G^{\mathrm{Pent}_a,\mathrm{Pent}_b} + \mathbb{1}, \\ \tilde{\mathbb{1}}^{\mathrm{Pent}_a,\mathrm{Pent}_b}_{kl} &= \sum_{\bar{k},\bar{l}\in(\mathrm{Pent}_a\cup\mathrm{Pent}_b)\setminus(\mathrm{Pent}_a\cap\mathrm{Pent}_b)} \delta_{k\bar{k}}\delta_{l\bar{l}}. \end{aligned} \tag{B9}$$

The matrix $\tilde{\mathbb{1}}^{\mathrm{Pent}_a,\mathrm{Pent}_b}_{kl} \sim (G^{\mathrm{Pent}_a,\mathrm{Pent}_b})^2_{kl}$ is the diagonal matrix with ones at the positions of the eight questions which are swapped by $G^{\mathrm{Pent}_a,\mathrm{Pent}_b}$ and otherwise zeros.

c. Pentagon conservation equations for $N = 2$ qubits

Every swap generator $G = G^{\mathrm{Pent}_a,\mathrm{Pent}_b}$ puts constraints on the potential pure states according to Eq. (3.5). These equalities follow from the requirement that for pure states the total information in each pentagon set Pent_c must be a conserved charge under the time evolution group $\mathcal{T}_2$. Equation (3.5) defines the pentagon conservation equations to linear order in t. However, clearly, if the group $\mathcal{T}_2' = \mathrm{PSU}(4)$ generated by (B5) and (B7) did constitute the correct time evolution group $\mathcal{T}_2$, then acting with an arbitrary $T(t)\in\mathcal{T}_2'$ on a legal pure state state $\vec{r}$ must produce another pure state $\vec{r}\,' := T(t)\cdot\vec{r}$ which satisfies the pentagon equalities (3.3) to all orders in t. In this section, we shall show that the linear order conservation conditions (3.5) are, in fact, sufficient to guarantee preservation of the pentagon equalities to all orders in t and for all $T\in\mathcal{T}_2$.

To this end, we first consider the action of the exponential map (B9) for an arbitrary of the 15 generators on some pure state $\vec{r}$. Surely, $\vec{r}\,' = T^{\mathrm{Pent}_a,\mathrm{Pent}_b}(t)\,\vec{r}$ must again satisfy the pentagon equalities (time evolution preserves the total information and must map states to states), i.e., we must have

$$1 = \sum_{l\in\mathrm{Pent}_c} r_l^2 \overset{!}{=} \sum_{l\in\mathrm{Pent}_c} (r_l')^2, \quad c = 1,\dots,6. \tag{B10}$$

We shall now show in Lemma 1 below that, if the first equation in Eq. (B10) is satisfied, then

$$\sum_{l\in\mathrm{Pent}_c} (r_l')^2 = \sum_{l\in\mathrm{Pent}_c} r_l^2 + 2\sin(t)\cos(t) \sum_{l\in\mathrm{Pent}_c,1\leqslant m\leqslant 15} r_l\, G^{\mathrm{Pent}_a,\mathrm{Pent}_b}_{lm}\, r_m$$

such that (B10) is satisfied for arbitrary t iff the linear constraints (3.5) hold:

$$\sum_{l\in\mathrm{Pent}_c,1\leqslant m\leqslant 15} r_l\, G^{\mathrm{Pent}_a,\mathrm{Pent}_b}_{lm}\, r_m = 0. \tag{B11}$$

For this purpose, we introduce the projector $P^{\mathrm{Pent}_a}_{kl} := \sum_{\bar{k},\bar{l}\in\mathrm{Pent}_a}\delta_{k\bar{k}}\delta_{l\bar{l}}$ onto the Bloch vector components corresponding to Pent_a and the symmetric matrix $R_{kl} := (\vec{r}\cdot\vec{r}^{\,t})_{kl} = r_k r_l$. In the following, we choose the shorthand notation $P^a := P^{\mathrm{Pent}_a}, G^{ab} := G^{\mathrm{Pent}_a,\mathrm{Pent}_b}$ with $a<b$. The pentagon equalities and generator constraints (B11) can now be equivalently expressed as

$$\begin{aligned} &\text{Pentagon eq.}: \mathrm{tr}[P^a R] = 1 \quad \text{for all } 1\leqslant a\leqslant 6, \\ &\text{Generator eq.}: \mathrm{tr}[P^a G^{bc} R] = \tfrac{1}{2}\mathrm{tr}[[P^a,G^{bc}]R] = 0 \quad \text{for all} \\ &\qquad 1\leqslant a\leqslant 6 \text{ and } 1\leqslant b<c\leqslant 6. \end{aligned} \tag{B12}$$

Before we show the above-mentioned result, we first require a few identities. Using the explicit expressions (B5) and (B7) for the 15 generators, one can check that the following statements are valid for any $1\leqslant a,b,c,d\leqslant 6$:

(a) $[P^a,G^{bc}] = (\delta_{ab}+\delta_{ac})G^{bc}(\mathbb{1}-2P^a)$, which also implies $\{P^a,G^{ab}\} = \{P^b,G^{ab}\} = G^{ab}$.

(b) $[P^a,G^{ab}] = -[P^b,G^{ab}]$.

(c) $[G^{ab},G^{cd}] = 0$, whenever G^{ab} and G^{cd} swap different pentagons, i.e., a,b are both different from c,d.

Note that (a) and (b) imply that there are only 15 independent pentagon conservation equations arising from (3.5) and (B11). These are exhibited in Eq. (3.13). Furthermore, (c) corresponds to the vanishing of the structure constants $f^{(ab)(cd)(eg)}$ of PSU(4) whenever G^{ab} and G^{cd} swap different pentagons or similarly to the commutation of PSO(6) rotations in the different planes (ab) and (cd). Throughout the derivation, we will also use the relation

$$\tilde{\mathbb{1}}^{ab} := \tilde{\mathbb{1}}^{\mathrm{Pent}_a,\mathrm{Pent}_b} = P^a + P^b - 2P^aP^b.$$

Lemma 1. Define $\vec{r}\,' = \exp(tG^{ab})\cdot\vec{r}$ where G^{ab} is any of the 15 swap generators (B5) and (B7). If $\mathrm{tr}[P^cR]=1$ for all $1\leqslant c\leqslant 6$, then $\mathrm{tr}[P^cR'] = \mathrm{tr}[P^cR] + 2\sin(t)\cos(t)\mathrm{tr}[P^cG^{ab}R]$.

Proof. By using the fact that the diagonal matrices $\tilde{\mathbb{1}}^{ab}$ and P^c commute, together with $(\tilde{\mathbb{1}}^{ab})^2 = \tilde{\mathbb{1}}^{ab}, \tilde{\mathbb{1}}^{ab}\cdot G^{ab} = G^{ab}$, the properties of the trace $\mathrm{tr}[M]=\mathrm{tr}[M^t]$, $\mathrm{tr}[MN]=\mathrm{tr}[NM]$ and further straightforward trigonometry we can show

$$\begin{aligned} \mathrm{tr}[P^cR'] &= \mathrm{tr}(\{[\cos(t)-1]\tilde{\mathbb{1}}^{ab} - \sin(t)G^{ab} \\ &\quad + \mathbb{1}\}P^cR\{[\cos(t)-1]\tilde{\mathbb{1}}^{ab} + \sin(t)G^{ab} + \mathbb{1}\}) \\ &= \mathrm{tr}[P^cR] + 2\sin(t)\cos(t)\mathrm{tr}[P^cG^{ab}R] \\ &\quad - \sin^2(t)(\mathrm{tr}[P^c\tilde{\mathbb{1}}^{ab}R] + \mathrm{tr}[P^cG^{ab}RG^{ab}]), \end{aligned}$$

where we denoted by $R' = \vec{r}\,'\cdot\vec{r}\,'^t = \exp(-tG^{ab})\vec{r}\cdot\vec{r}^{\,t}\exp(tG^{ab}) = \exp(-tG^{ab})R\exp(tG^{ab})$. The last term

$\sim\mathrm{tr}[P^c\tilde{\mathbb{1}}^{ab}R]+\mathrm{tr}[P^cG^{ab}RG^{ab}]$ on the second line above vanishes. To see this we use (a), together with $\tilde{\mathbb{1}}^{ab}=P^a+P^b-2P^aP^b$, $(G^{ab})^2=-\tilde{\mathbb{1}}^{ab}$ to get

$$\begin{aligned}&\mathrm{tr}[P^cG^{ab}RG^{ab}]+\mathrm{tr}[P^c\tilde{\mathbb{1}}^{ab}R]\\&\quad=\mathrm{tr}[P^c(G^{ab})^2R]-\mathrm{tr}[[P^c,G^{ab}]G^{ab}R]+\mathrm{tr}[P^c\tilde{\mathbb{1}}^{ab}R]\\&\quad=(\delta_{ca}+\delta_{cb})\mathrm{tr}[(\mathbb{1}-2P^c)\tilde{\mathbb{1}}^{ab}R]\\&\quad=(\delta_{ca}+\delta_{cb})\mathrm{tr}\{(\mathbb{1}-2P^c)[P^a+(\mathbb{1}-2P^a)P^b]R\}.\end{aligned}$$

If $c\neq a,b$ the above vanishes because of the δ's. Choosing $c=a$ without loss of generality, it vanishes again because of $P^cP^c=P^c$ and thus $(\mathbb{1}-2P^c)^2=1$, which implies $\mathrm{tr}\{(\mathbb{1}-2P^a)[P^a+(\mathbb{1}-2P^a)P^b]R\}=\mathrm{tr}\{[(\mathbb{1}-2P^a)P^a+P^b]R\}=\mathrm{tr}[(P^b-P^a)R]=\mathrm{tr}[P^bR]-\mathrm{tr}[P^aR]=1-1=0.$ ■

Using his result, we can now move on to show that, in fact, the 21 equations (B12) define a $\mathcal{T}_2'$-invariant set, where $\mathcal{T}_2'=\mathrm{PSU}(4)$ is the *full* group generated by exponentiating the 15 generators (B5) and (B7) and their linear combinations. That is, not only the pentagon, but also the pentagon conservation equations are preserved by $\mathcal{T}_2'$.[29]

Lemma 2. If $\vec{r}$ satisfies (B12), then so does $\vec{r}\,'=T\cdot\vec{r}$ for any $T\in\mathcal{T}_2'$.

Proof. We start by showing that every time evolution $T\in\mathcal{T}_2'=\mathrm{PSU}(4)$ can be written as a product of exponentials, i.e., $T=\prod_{ab}\exp(t_{ab}G^{ab})$ where always a single generator G^{ab} (from a given basis) appears in every exponent. First note that *any* matrix $T\in GL(\mathbb{R},n^2)$ lying in $\mathrm{SO}(n)$ can be expressed as a product of rotation matrices $\exp(tG_F^{lm})$, each in some plane (lm) [55,56] by the use of generalized Euler angles, where G_F^{lm} are the antisymmetric generators of the *fundamental* representation of $\mathrm{SO}(n)$, i.e., $(G_F^{lm})_{ij}=\delta_{li}\delta_{mj}-\delta_{lj}\delta_{mi}$. This statement is true for the entire equivalence class of generators, where the equivalence relation amounts to similarity transformations of the fundamental generators. That is, all of the choices of Lie algebra bases in that equivalence class have the same structure constants. The statement that any group element can be written as products of exponentials of single generators (of a basis from this equivalence class) can also be understood abstractly at the manifold level of the Lie group and hence must be true for any representation (of the equivalence class of bases).

The same therefore holds true for the fundamental generators of $\mathrm{PSU}(4)\simeq\mathrm{PSO}(6)$. Our 15×15 swap generator matrices G^{ab} are exactly in a one-to-one correspondence with the fundamental 6×6 generator matrices $(G_F^{lm})_{ij}=\delta_{li}\delta_{mj}-\delta_{lj}\delta_{mi}$ of SO(6). This has also been explicitly checked for the matrices corresponding to (B5) and (B7). In other words, also in the adjoint representation all the $\mathrm{PSU}(4)\simeq\mathrm{PSO}(6)$ group elements generated by the generators (B5) and (B7) are expressible as products of *single* exponentials of our swap generators G^{ab}, where only *one* swap generator appears in each exponent as in Eq. (B9). For this reason, it suffices to consider $T=\exp(tG^{ab})$ in the following and then the case of a general $T=\prod_{ab}\exp(t_{ab}G^{ab})\in\mathcal{T}_2'\simeq\mathrm{PSU}(4)$ follows by induction.

Consider $\vec{r}\,'=\exp(tG^{ab})\cdot\vec{r}$ where $\vec{r}$ satisfies (B12), i.e., $\mathrm{tr}[P^cR]=1$ (pentagon equalities) and $\mathrm{tr}[P^cG^{de}R]=0$ (generator equalities) for all $1\leqslant c,d,e\leqslant6$. From Lemma 1 it follows that $\mathrm{tr}[P^cR']=\mathrm{tr}[P^cR]+2\sin(t)\cos(t)\mathrm{tr}[P^cG^{ab}R]=\mathrm{tr}[P^cR]=1$ and thus $\vec{r}\,'$ also satisfies the pentagon equalities. It remains to show that $\vec{r}\,'$ satisfies the generator equalities $\mathrm{tr}[P^cG^{de}R']=0$ as well. Note that if $d=a$ and $e=b$, then $\mathrm{tr}[P^cG^{de}R']\sim\mathrm{tr}[P^c\exp(-t'G^{ab})R'\exp(t'G^{ab})]-\mathrm{tr}[P^cR']=\mathrm{tr}\{P^c\exp[-(t'+t)G^{ab}]R\exp[(t'+t)G^{ab}]\}-\mathrm{tr}[P^cR]=2\sin(t'+t)\cos(t'+t)\mathrm{tr}[P^cG^{ab}R]=0$ because of Lemma 1. Therefore, we should only consider the case where $a\neq d,e$ and/or $b\neq d,e$. Using the explicit expression for $\exp(tG^{ab})$ in Eq. (B9), one finds

$$\begin{aligned}\mathrm{tr}[P^cG^{de}R']&=\mathrm{tr}(\{[\mathrm{c}(t)-1]\tilde{\mathbb{1}}^{ab}-\mathrm{s}(t)G^{ab}+\mathbb{1}\}P^cG^{de}R\{[\mathrm{c}(t)-1]\tilde{\mathbb{1}}^{ab}+\mathrm{s}(t)G^{ab}+\mathbb{1}\})\\&=\tfrac{1}{2}\{[\mathrm{c}(t)-1]^2M_1+2\mathrm{s}(t)[\mathrm{c}(t)-1]M_2-\mathrm{s}^2(t)M_3+2[\mathrm{c}(t)-1]M_4+2\mathrm{s}(t)M_5\},\\&\mathrm{c}(t):=\cos(t),\quad \mathrm{s}(t):=\sin(t),\quad M_1=\mathrm{tr}[[P^c,G^{de}](\tilde{\mathbb{1}}^{ab}R\tilde{\mathbb{1}}^{ab})],\quad M_2=\mathrm{tr}[[P^c,G^{de}](G^{ab}R\tilde{\mathbb{1}}^{ab})],\\M_3&=\mathrm{tr}[[P^c,G^{de}](G^{ab}RG^{ab})],\quad M_4=\mathrm{tr}[[P^c,G^{de}](R\tilde{\mathbb{1}}^{ab})],\quad M_5=\mathrm{tr}[[P^c,G^{de}](G^{ab}R)].\end{aligned}$$

We will now show that $M_1=-M_3=M_4$, $M_2=M_5=0$, such that $\mathrm{tr}[P^cG^{de}R']=\frac{1}{2}\{[\mathrm{c}(t)-1]^2+\mathrm{s}^2(t)+2[\mathrm{c}(t)-1]\}M_4=0$. Because of (a), we will take without loss of generality $c=d$ throughout the derivation and use $\mathrm{tr}[[G^{ab},G^{de}]P^gR]=f^{(ab)(de)(cg)}\mathrm{tr}[G^{cg}P^gR]=\mathrm{tr}[P^gG^{cg}R]=0$, and thus (d): $\mathrm{tr}[G^{ab}G^{de}P^gR]=\mathrm{tr}[G^{ab}G^{de}RP^g]$. From (d) it follows that $M_5=\mathrm{tr}[[P^d,G^{de}](G^{ab}R)]=-\mathrm{tr}[G^{de}[P^d,G^{ab}]R]$. Furthermore, using (b) and then (d) implies as well $M_5=-\mathrm{tr}[[P^e,G^{de}](G^{ab}R)]=\mathrm{tr}[G^{de}[P^e,G^{ab}]R]$. Note that $[P^d,G^{ab}]=0$ or $[P^e,G^{ab}]=0$ because of (a) and also $a\neq d,e$ and/or $b\neq d,e$ and therefore $M_5=0$. For showing the three remaining equalities $M_1=-M_3=M_4,M_2=0$ we consider two separate cases: c_1: $a=d$ and $b\neq d,e$, c_2: $a\neq d,e$ and $b\neq d,e$. The symmetric case $a=e$ and $b\neq d,e$ is also captured because of (b).

[29]We note that the pentagon equalities (3.3) alone are generally not preserved under $\mathcal{T}_2'$ without the generator conservation equations in Eq. (B12). For instance, the information distribution $\alpha_{xy}=\alpha_{z_2}=\alpha_{xz}=\alpha_{y_2}=\frac{1}{2}$ bit and $\alpha_{x_1}=1$ bit (and all other $\alpha_i=0$) satisfies all pentagon equalities, however, violates the generator conservation equations. Under a finite evolution with $T^{\mathrm{Pent}_4\mathrm{Pent}_6}(t)$ in Eq. (B9) (this is a rotation around the x_2 axis) this can be evolved to $\alpha_{xy}+\alpha_{z_2}>1$ bit, thereby violating the equality for Pent_4.

Let us start with the case c_1, for which $[G^{de},P^b]=0$ because of (a). Then, for M_2

$$\begin{aligned}
M_2 &= \mathrm{tr}[[P^d,G^{de}](G^{db}R\tilde{\mathbb{1}}^{db})] = \mathrm{tr}[[P^d,G^{de}]P^bG^{db}R] + \mathrm{tr}\{P^d[P^d,G^{de}][(\mathbb{1}-2P^b)G^{db}R]\}\\
&= \tfrac{1}{2}(\mathrm{tr}[[P^d,G^{de}][P^b,G^{db}]R] - \mathrm{tr}\{[G^{db},[P^d,G^{de}]]P^bR\}) + \mathrm{tr}[P^d[P^d,G^{de}][G^{db},P^b]R]\\
&= \tfrac{1}{2}(-\mathrm{tr}[(\mathbb{1}-2P^d)[P^d,G^{de}][P^d,G^{db}]R] - \tfrac{1}{2}\mathrm{tr}\{[\{G^{db},P^b\},[P^d,G^{de}]]R\})\\
&= \tfrac{1}{2}(\mathrm{tr}[G^{de}[P^d,G^{db}]R] - \tfrac{1}{2}\mathrm{tr}\{[G^{db},[P^d,G^{de}]]R\}) = 0-0=0.
\end{aligned}$$

Similarly, for M_3 we can show

$$\begin{aligned}
M_3 &= \mathrm{tr}[[P^d,G^{de}](G^{db}RG^{db})] = -\mathrm{tr}[[P^e,G^{de}](G^{db}RG^{db})]\\
&= -(\mathrm{tr}\{[P^e,[G^{de},G^{db}]]RG^{db}\} + \mathrm{tr}[[P^e,G^{de}]R(G^{db})^2])\\
&= -(f^{(de)(db)(rs)}\mathrm{tr}[[P^e,G^{rs}]RG^{db}] - \mathrm{tr}[[P^e,G^{de}](R\tilde{\mathbb{1}}^{db})])\\
&= \mathrm{tr}[[P^e,G^{de}](R\tilde{\mathbb{1}}^{db})] = -\mathrm{tr}[[P^d,G^{de}](R\tilde{\mathbb{1}}^{db})] = -M_4.
\end{aligned}$$

Finally, for M_1 it also follows

$$\begin{aligned}
M_1 &= \mathrm{tr}[[P^d,G^{de}](\tilde{\mathbb{1}}^{db}R\tilde{\mathbb{1}}^{db})] = \mathrm{tr}[[P^d,G^{de}]P^dR\tilde{\mathbb{1}}^{db}(\mathbb{1}-2P^b)] + \mathrm{tr}[[P^d,G^{de}]R\tilde{\mathbb{1}}^{db}P^b]\\
&= \mathrm{tr}\{[[P^d,G^{de}],P^d]R\tilde{\mathbb{1}}^{db}(\mathbb{1}-2P^b)\} + \mathrm{tr}[[P^d,G^{de}]R\tilde{\mathbb{1}}^{db}]\\
&= \tfrac{1}{2}\mathrm{tr}\{[P^d,[P^d,G^{de}],P^d]R\} + M_4 = -\tfrac{1}{2}\mathrm{tr}[[P^d,G^{de}]R] + M_4 = M_4.
\end{aligned}$$

Lastly, we consider the simplest case c_2, for which $[G^{de},P^a]=[G^{de},P^b]=0$ and $[G^{de},G^{ab}]=0$ because of (a) and (c). In particular, also $[G^{de},\tilde{\mathbb{1}}^{ab}]=0$. Working out M_2 results again in

$$\begin{aligned}
M_2 &= \mathrm{tr}[[P^d,G^{de}](G^{ab}R\tilde{\mathbb{1}}^{ab})] = \mathrm{tr}[[P^d,G^{de}]\tilde{\mathbb{1}}^{ab}G^{ab}R]\\
&= \mathrm{tr}[[P^d,G^{de}]G^{ab}R] = 0.
\end{aligned}$$

For M_3 the same derivation as in the case of c_1 can be used to show $M_3=-M_4$. Finally, for $M_1 = \mathrm{tr}[[P^d,G^{de}](\tilde{\mathbb{1}}^{ab}R\tilde{\mathbb{1}}^{ab})] = \mathrm{tr}[[P^d,G^{de}]R(\tilde{\mathbb{1}}^{ab})^2] = M_4$. ■

d. PSU(2^N) *is a maximal subgroup of* SO(4^N-1)

In the main text we argue that PSU(2^N) is a subgroup of the time evolution group $\mathcal{T}_N$, which itself is (isomorphic to) a subgroup of SO(4^N-1). In order to conclude that $\mathcal{T}_N \simeq$ PSU(2^N), we prove here that PSU(2^N) is (isomorphic to) a maximal subgroup of the larger group SO(4^N-1):

Lemma 3. PSU(2^N) acts in the adjoint representation on the state space of N qubits and is a maximal subgroup of SO(4^N-1) for all $N \geqslant 2$.

Proof. The irreducible representations of PSU(N_F) are categorized by N_F-1 numbers. Each representation corresponds to a Young tableau to which its dimension is intimately related [57]. A survey of the irreducible representations of PSU(N_F) shows that whenever $N_F \geqslant 9$, the dimensions of the irreducible representations can be ranked from lowest to highest as 1, N_F, $\frac{1}{2}N_F(N_F-1)$, $\frac{1}{2}N_F(N_F+1)$, $\dim(\mathrm{Ad}) = N_F^2-1,\ldots$, where the ellipsis refers to higher-dimensional representations with dimensions larger than N_F^2-1. The N-qubit state space transforms in some representation R of PSU($N_F=2^N$). Let us first consider the case of $N>3$, for which $N_F=2^N>9$. If R was reducible, it would have at least one copy of the trivial representation in its direct sum since $\dim(R)=\dim(\mathrm{Ad})$ is uneven and all lower-dimensional representations are even except the trivial one, which would imply that R leaves a one-dimensional subspace invariant. However, this is not possible because the subgroup PSU(2) $\times\cdots\times$ PSU(2) $\subseteq$ PSU(2^N) which corresponds to the rotations of the individual qubits lies inside the subgroup PSU(2^N) and these transformations would certainly not leave any one-dimensional subspace invariant. Therefore, the representation R must be irreducible and it *must* be the adjoint representation since all other representations are of larger dimension. For $N \leqslant 3$, one observes from explicit tables of group dimensions [58] that the same reasoning applies and R again equals the adjoint representation. The maximality of PSU(2^N) in SO(4^N-1) now directly follows from Dynkin's theorem [59] and the fact that PSU(2^N) is simple and its adjoint representation is faithful and irreducible [acting on the fundamental representation space of SO(4^N-1)]. ■

e. Evolving to product states

We shall now demonstrate the following claim of Sec. III A 4.

Lemma 4. Any $\vec{r}$ satisfying (B12) can be brought to the configuration $\alpha_{z_1}=\alpha_{z_2}=\alpha_{zz}=1$ bit and all other $\alpha_i=0$ by performing successive $\mathcal{T}_2'$ transformations of the form (B9).

Proof. First note that when two questions are swapped *within* one pentagon, the other three questions remain unchanged (cf. Fig. 4). This is the case because the remaining three questions do *not* appear in any of the two pentagons whose information contents are being swapped. For example, this can be explicitly seen in Fig. 4, where as α_{y_1} and α_{zx} are swapped within Pent$_5$ via $G^{\mathrm{Pent}_1,\mathrm{Pent}_2}$, the information content of $\alpha_{x_1},\alpha_{zz},\alpha_{zy}$ in Pent$_5$ are left invariant. Because of this property we can by repeating (at most four different) swap transformations (B9) put all 1 bit of information contained in Pent$_5$ in, e.g., question Q_{y_1}: (1) first rotate all information from

Q_{zx} to Q_{y_1} with $T^{\text{Pent}_1,\text{Pent}_2}(t_1)$ for some t_1 such that $\alpha_{zx}=0$,[30] (2) then use $T^{\text{Pent}_3,\text{Pent}_5}(t_2)$ for some t_2 to rotate the information contained in Q_{zy} into Q_{y_1} which leaves $\alpha_{zx}=\alpha_{zy}=0$, (3) use $T^{\text{Pent}_1,\text{Pent}_6}(t_3)$ for some t_3 to map the information content of Q_{zz} into Q_{y_1} which leaves $\alpha_{zx}=\alpha_{zy}=\alpha_{zz}=0$, and (4) finally use $T^{\text{Pent}_1,\text{Pent}_3}(t_4)$ for some t_4 to rotate the information from Q_{x_1} into Q_{y_1} which leaves $\alpha_{zx}=\alpha_{zy}=\alpha_{zz}=\alpha_{x_1}=0$. Since the time evolution group maps pure states to pure states and $I(\text{Pent}_5)=1$ bit, we conclude $\alpha_{y_1}=1$ bit after the four steps. The information content of questions in other pentagons is also transformed during these four successive transformations. However, since every employed transformation leaves the other three questions in Pent_5 invariant, this is not relevant for the argument. Nevertheless, all eight questions complementary to Q_{y_1} will necessarily have $\alpha_i=0$ too, while the remaining 2 bits will be distributed over the six questions compatible with Q_{y_1}.

The above information redistribution algorithm, by using appropriate combinations of transformations, can similarly be performed on *any* state satisfying (B12) to get $\alpha_{z_1}=1$ bit. In that case, the remaining 2 bits will be contained in the boundary of the three compatible triangles with central vertex $\alpha_{z_1}=1$ bit [cf. (3.4) and Fig. 5] and $\alpha_{x_2}=\alpha_{zx}$, $\alpha_{zy}=\alpha_{y_2}$, $\alpha_{zz}=\alpha_{z_2}$. Using the three latter equalities and the fact that the six boundary questions contain 2 bits of information, it follows that $\alpha_{x_2}+\alpha_{y_2}+\alpha_{z_2}=1$ bit. We can evolve this 1 bit of information into $\alpha_{z_2}=1$ bit by using local rotations of qubit 2: (1) first rotate around the r_{x_2} axis with $T^{\text{Pent}_4,\text{Pent}_6}$ to get $\alpha_{y_2}=0$, (2) then rotate around the r_{y_2} axis with $T^{\text{Pent}_2,\text{Pent}_6}$ while leaving $\alpha_{y_2}=0$ and setting $\alpha_{x_2}=0$ and thus $\alpha_{z_2}=1$ bit. Finally, we therefore reach the required product configuration $\alpha_{z_1}=\alpha_{z_2}=\alpha_{zz}=1$ bit, starting from any pure state. Note that this required at most six *different* successive transformations of the form (B9). ∎

f. Preservation of the complementarity inequalities

Next, we show that $\mathcal{T}_2'=\text{PSU}(4)$ preserves all complementarity inequalities (2.1), provided (B12) is fulfilled. Since $\mathcal{T}_2'$ preserves all pentagon equalities by construction, it suffices to check it for the triangle complementarity sets in Appendix B 1 since all sets of mutually complementary questions are either contained in the pentagon or triangle sets on account of their maximality.

Lemma 5. Any $\vec{r}$ solving (B12) also satisfies all triangle complementarity inequalities following from (2.1) for the triangle complementarity sets (B2).

Proof. By inspection one verifies that any of the three pairs of questions contained in each of the triangle sets Tri_i [Eq. (B2)] also lies in a common pentagon set (3.1). However, clearly not all three questions in a triangle set can lie in the same pentagon, for otherwise maximality of the triangle set would be violated. This implies that for every triangle set and every pair of questions contained in it there exists an information swap generator in Eqs. (B5) and (B7) which swaps the information between the two questions of that pair and leaves the third question in the triangle set invariant (see the arguments in the proof of Lemma 4). For example, for Tri_1, $G^{\text{Pent}_1,\text{Pent}_4}$ swaps the information between Q_{xx} and Q_{z_2} and leaves Q_{xy} invariant. Accordingly, the exponentiation (B9) of $G^{\text{Pent}_1,\text{Pent}_4}$ rotates information continuously between Q_{xx} and Q_{z_2} and leaves Q_{xy} invariant. In particular, there will always exist values of t such that *all* information carried by Q_{xx} and Q_{z_2} can be evolved into one of the two questions, e.g., Q_{xx}. By subsequently applying the analogous rotation generated by $G^{\text{Pent}_2,\text{Pent}_4}$ to the pair Q_{xx},Q_{xy} (which leaves Q_{z_2} invariant), one can always evolve the entire information $I(\text{Tri}_1)(t)=\alpha_{xx}(t)+\alpha_{xy}(t)+\alpha_{z_2}(t)$, carried by Tri_1, into $I(\text{Tri}_1)(t)=I(\text{Tri}_1)(t+\Delta t)=\alpha_{xx}(t+\Delta t)$ such that $\alpha_{xy}(t+\Delta t)=\alpha_{z_2}(t+\Delta t)=0$ bits and no information has leaked out of the triangle [where $\alpha_i(t)=r_i(t)^2$]. That is, if the triangle complementarity inequality following from (2.1) for Tri_1 was ever violated, $\alpha_{xx}+\alpha_{xy}+\alpha_{z_2}>1$ bit, there would exist a $T\in\mathcal{T}_2'$ which evolves this configuration to $\alpha_{xx}>1$ bit. But, this would violate the pentagon equalities which, by Lemma 2, can never happen under $\mathcal{T}_2'$ if (B12) is fulfilled. The same argument can be repeated for all 20 triangle sets such that we conclude that (B12), in fact, implies that the triangle complementarity inequalities hold. ∎

In particular, $\mathcal{T}_2'$ thus preserves all complementarity inequalities (2.1) once (B12) holds.

g. Preservation of the correlation structure

We also have to check that $\mathcal{T}_2'=\text{PSU}(4)$ leaves the correlation structure of Fig. 3 invariant, provided (B12) is fulfilled. For this purpose we recall that the correlation structure in Fig. 3 encodes that a question in an (anti)correlation triangle is the (anti)correlation of the other two questions in the triangle. The correlation structure thus means that if (a) $Q_i=Q_j\leftrightarrow Q_k$ then $y_i=1$ implies $r_j=r_k$ and $y_i=0$ implies $r_j=-r_k$,[31] and if (b) $Q_i=\neg(Q_j\leftrightarrow Q_k)$ then $y_i=1$ implies $r_j=-r_k$ and $y_i=0$ implies $r_j=r_k$, where $i,j,k=x_1,y_1,\dots,zz$ and $i\neq j\neq k\neq i$ are question indices compatible with a triangle in Fig. 3. That is, since any Q_i is contained in three triangles (c) if $Q_i=Q_j\leftrightarrow Q_k=\neg(Q_l\leftrightarrow Q_m)$, then $y_i=1$ implies $r_j=r_k$ and $r_l=-r_m$ simultaneously and $y_i=0$ implies $r_j=-r_k$ and $r_l=r_m$ simultaneously. Finally, (d) if $Q_i=Q_j\leftrightarrow Q_k=Q_l\leftrightarrow Q_m$, then $y_i=1$ implies $r_j=r_k$ and $r_l=r_m$ simultaneously and $y_i=0$ implies $r_j=-r_k$ and $r_l=-r_m$ simultaneously. We thus only show the statement for states with at least one $\alpha_i=1$ bit for which the correlation structure has meaning.

We recall from Lemma 4 and the arguments of Sec. III A 4 that there exist precisely two $\mathcal{T}_2'$-transitive sets solving (B12), namely,

$$\mathcal{S}_{QT}^{+}:=\{T\cdot(\vec{\delta}_{z_1}+\vec{\delta}_{z_2}+\vec{\delta}_{z_1z_2})\,|\,T\in\mathcal{T}_2'\},$$
$$\mathcal{S}_{QT}^{-}:=-\{T\cdot(\vec{\delta}_{z_1}+\vec{\delta}_{z_2}+\vec{\delta}_{z_1z_2})\,|\,T\in\mathcal{T}_2'\}.$$

[30]Recall from above that $T^{\text{Pent}_1,\text{Pent}_2}(t_1)$ acts as a rotation by $\pm t_1$ in the plane (r_{y_1},r_{zx}).

[31]For example, $Q_{xx}=Q_{x_1}\leftrightarrow Q_{x_2}$ is the question "are the answers to Q_{x_1},Q_{x_2} correlated?" Since y_{xx} is thus also the probability that the answers to Q_{x_1},Q_{x_2} are correlated, this means that whenever $y_{xx}=1$ we must have $y_{x_1}=y_{x_2}$ and whenever $y_{xx}=0$ we must have $r_{x_1}=-r_{x_2}$.

$\mathcal{S}^+_{QT}$ is the set of pure quantum states, while $\mathcal{S}^-_{QT}$ constitutes an equivalent but different representation of the pure quantum state space. These two sets are *not* connected via $\mathcal{T}_2'$.

Claim:

(1) Any $\vec{r}$ which solves (B12) and satisfies the correlation structure of Fig. 3 lies in $\mathcal{S}^+_{QT}$. This is the set corresponding to the convention of building bipartite questions from the individuals $Q_{x_1},Q_{x_2},Q_{y_1},Q_{y_2},Q_{z_1},Q_{z_2}$ using the XNOR connective $\leftrightarrow$.

(2) Any $\vec{r}$ which solves (B12) and satisfies the correlation structure obtained by replacing correlation triangles in Fig. 3 by anticorrelation triangles and vice versa lies in $\mathcal{S}^-_{QT}$. This is the set corresponding to the convention of building bipartite questions from the individuals using the XOR connective $\neg(\cdot\leftrightarrow\cdot)$.

Thus, in particular, in the XNOR convention, (B12) implies the correlation structure of Fig. 3 which therefore is $\mathcal{T}_2'$ invariant.

Proof. Suppose $\vec{r}$ solves (B12). This implies that whenever $\alpha_i=1$ bit, then $\alpha_j=\alpha_k$ if either $Q_i=Q_j\leftrightarrow Q_k$ or $Q_i=\neg(Q_j\leftrightarrow Q_k)$ [as mentioned at the end of Sec. III A 2 this follows from the pentagon identities contained in Eq. (B12)]. This means that $r_i=\pm1$ and either $r_j=r_k$ or $r_j=-r_k$. We wish to show consistency with (a)–(d). We shall illustrate the argument with the example of $\alpha_{z_1}=1$ bit. While the proof is straightforward, it involves many details such that we restrict to a sketch.

We adopt the notation of Appendix B 2 c and note that the conservation equation

$$(P^4\cdot\vec{r})\cdot G^{46}\cdot\vec{r}=r_{z_2}r_{y_2}-r_{zy}r_{zz}-r_{yy}r_{yz}-r_{xy}r_{xz}=0$$

reads as $r_{z_2}r_{y_2}=r_{zy}r_{zz}$ once $\alpha_{z_1}=1$ bit such that all questions complementary to Q_{z_1} carry 0 bits. Together with $r_{y_2}=\pm r_{zy}$ and $r_{zz}=\pm r_{z_2}$, which is implied by the pentagon equalities as noted above, this entails for the right and lower triangles in Fig. 5 that

$$r_{y_2}=+r_{zy}\Leftrightarrow r_{zz}=+r_{z_2}\quad\text{and}$$
$$r_{y_2}=-r_{zy}\Leftrightarrow r_{zz}=-r_{z_2}.$$

We can now employ finite-time evolutions $T^{46}(t)=\exp(t\,G^{46})$ as in Eq. (B9) which generate rotations in the (y_2,z_2) and (zy,zz) planes, both by an angle $-t$. Such a time evolution leaves r_{x_2},r_{z_1},r_{zx}, corresponding to the upper left triangle in Fig. 5 invariant. In particular, we can start with a Bloch vector $r_{z_1}=r_{y_2}=r_{zy}=+1$ and all other $r_i=0$. This Bloch vector solves (B12) and is compatible with constructing the bipartite question $Q_{zy}=Q_{z_1}\leftrightarrow Q_{y_2}$ via the XNOR connective $\leftrightarrow$. Applying $T^{46}(t)=\exp(t\,G^{46})$ for all $t\in[0,2\pi]$ to this vector generates *all* configurations for which $r_{z_1}=+1$ and simultaneously $r_{y_2}=+r_{zy}$ and $r_{zz}=+r_{z_2}$, while all other $r_i=0$ and thus preserving that all of $I(\vec{r})=|\vec{r}|^2=3$ bits is carried by the five questions in the upper right and the lower triangle in Fig. 5. Similarly, by starting with the Bloch vector $r_{z_1}=r_{y_2}=-1$, $r_{zy}=+1$ and all other $r_i=0$, which again solves (B12) and is compatible with $Q_{zy}=Q_{z_1}\leftrightarrow Q_{y_2}$, one can generate all configurations for which $r_{z_1}=-1$ and simultaneously $r_{y_2}=-r_{zy}$ and $r_{zz}=-r_{z_2}$, while all other $r_i=0$ and thus preserving that all of $I(\vec{r})=|\vec{r}|^2=3$ bits is carried by the five questions in the upper right and the lower triangle in Fig. 5. Note, first, that the two states $r_{z_1}=r_{y_2}=r_{zy}=+1$ (all other $r_i=0$) and $r_{z_1}=r_{y_2}=-1$, $r_{zy}=+1$ (all other $r_i=0$) are connected by $T(t=\pi)=\exp(\pi\,G^{12})$ such that all the states we just discussed are connected by time evolution and thus clearly satisfy (B12). Second, note that *all* of these Bloch vectors are consistent with building the bipartite $Q_{zz}=Q_{z_1}\leftrightarrow Q_{z_2}$ using XNOR and, accordingly, with $Q_{zy}\leftrightarrow Q_{y_2}=Q_{z_1}=Q_{zz}\leftrightarrow Q_{z_2}$. Third, note that we could have arrived at the same result by using the conservation equation $(P^2\cdot\vec{r})\cdot G^{25}\cdot\vec{r}=0$ and $T^{25}(t)$ which also leaves the questions in the upper left triangle of Fig. 5 invariant.

One can repeat the analogous argument with G^{26} or G^{45}, both of which leave the upper right triangle in Fig. 5 invariant and solely rotate the information between the other two triangles (while leaving r_{z_1} invariant), to show that from $r_{z_1}=r_{z_2}=r_{zz}=1$ (all other $r_i=0$) one can generate by time evolution *all* states with $r_{z_1}=+1$ and simultaneously $r_{z_2}=r_{zz}$ and $r_{x_2}=r_{zx}$ and *all* states with $r_{z_1}=-1$ and simultaneously $r_{z_2}=-r_{zz}$ and $r_{x_2}=-r_{zx}$ and all other $r_i=0$. Since $r_{z_1}=r_{z_2}=r_{zz}=1$ (all other $r_i=0$) is connected by time evolution to the states of the previous paragraph, all of these states are likewise related through time evolution group elements to all states of the previous paragraph. We again note that all of these states are consistent with constructing the bipartite $Q_{zx}=Q_{z_1}\leftrightarrow Q_{x_2}$ with the XNOR from the individuals Q_{z_1},Q_{x_2} and, accordingly, with $Q_{zx}\leftrightarrow Q_{x_2}=Q_{z_1}=Q_{zz}\leftrightarrow Q_{z_2}$.

Next, we repeat the analogous argument with G^{24} or G^{56}, both of which leave the lower triangle in Fig. 5 invariant, to show that from $r_{z_1}=r_{y_2}=r_{zy}=+1$ (all other $r_i=0$) one can produce through time evolution group elements *all* states with $r_{z_1}=+1$ and simultaneously $r_{y_2}=r_{zy}$ and $r_{x_2}=r_{zx}$ and *all* states with $r_{z_1}=-1$ and simultaneously $r_{y_2}=-r_{zy}$ and $r_{x_2}=-r_{zx}$ and all other $r_i=0$. All of these states are clearly connected via time evolution group elements to all states of the previous two paragraphs and consistent with $Q_{zx}\leftrightarrow Q_{x_2}=Q_{z_1}=Q_{zy}\leftrightarrow Q_{y_2}$.

Combining the previous arguments, it is clear that by applying all possible products of $T^{46},T^{25},T^{26},T^{45},T^{24},T^{56}$ for all possible values of $t\in[0,2\pi]$ to the states of the previous three paragraphs one generates *all* states with $r_{z_1}=+1$ and simultaneously $r_{x_2}=r_{zx}$ and $r_{zy}=r_{y_2}$ and $r_{zz}=r_{z_2}$ and *all* states with $r_{z_1}=-1$ and simultaneously $r_{x_2}=-r_{zx}$ and $r_{zy}=-r_{y_2}$ and $r_{zz}=-r_{z_2}$ and all other $r_i=0$ and $I(\vec{r})=|\vec{r}|^2=3$ bits. It is also clear that all these states satisfy (B12) and that no other states can be produced by combinations of $T^{46},T^{25},T^{26},T^{45},T^{24},T^{56}$. But, these are precisely all the states consistent with $Q_{z_1}=Q_{zy}\leftrightarrow Q_{y_2}=Q_{zz}\leftrightarrow Q_{z_2}=Q_{zx}\leftrightarrow Q_{x_2}$ and $\alpha_{z_1}=1$ bit and thus all the states consistent with the correlation structure of Fig. 5. In conclusion, all of these states are thus implied by (B12), provided one follows the convention to only build up bipartite questions with the XNOR connective from individual questions.

Had we instead started the above arguments with the state $r_{z_1}=-1,r_{y_2}=r_{zy}=+1$, and all other $r_i=0$, corresponding to the XOR connective $Q_{zy}=\neg(Q_{z_1}\leftrightarrow Q_{y_2})$ and solving (B12), we would have produced through time evolution all states consistent with $Q_{z_1}=\neg(Q_{zy}\leftrightarrow Q_{y_2})=\neg(Q_{zz}\leftrightarrow Q_{z_2})=\neg(Q_{zx}\leftrightarrow Q_{x_2})$ and $\alpha_{z_1}=1$ bit. These correspond to the correlation structure of Fig. 5, except that all correlation triangles in it are replaced by anticorrelation triangles.

Clearly, one can repeat the same arguments for any question Q_i and Bloch vectors with $\alpha_i = 1$ bit, finding that *all* states compatible with $\alpha_i = 1$ bit and building bipartite questions with the XNOR are connected via $\mathcal{T}_2'$ and likewise that *all* states compatible with $\alpha_i = 1$ bit and building bipartite questions with the XOR are connected via $\mathcal{T}_2'$.

Together with Lemma 4 and the arguments of Sec. III A 4 it follows that *all* 3 bit states consistent with the correlation structure of Fig. 3 lie in $\mathcal{S}_{QT}^+$. Similarly, it follows that *all* 3 bit states consistent with the correlation structure corresponding to the convention of constructing bipartite questions with the XOR from individuals lie in $\mathcal{S}_{QT}^-$. ■

3. Reconstructing $\mathcal{T}_N$ and Σ_N for $N > 2$

a. Deriving the "swap generators" for $N > 2$

All pairwise unitaries must be contained in $\mathcal{T}_N$ and therefore require a representation on $\mathbb{R}^{4^N-1}$. Consider the gbit pair (1,2). It is not difficult to convince oneself that the definition (and requirement) of isolated evolution under $\mathcal{T}_2^{(12)} \subset \mathcal{T}_N$ from Sec. III B 1 implies that *every* $T^{(12)}(t) \in \mathcal{T}_2^{(12)}$ must be of the block-diagonal form

$$T^{(12)}(t) = \begin{pmatrix} \bar{T}^{(12)}(t) & 0 & 0 \\ 0 & \tilde{T}^{(12)}(t) & 0 \\ 0 & 0 & \mathbb{1}_{(4^{N-2}-1)\times(4^{N-2}-1)} \end{pmatrix}, \tag{B13}$$

where $\bar{T}^{(12)}(t)$ is the corresponding 15×15 $\mathcal{T}_2$ matrix of Sec. III A 3 and $\tilde{T}^{(12)}(t)$ is a $[4^N - 1 - 15 - (4^{N-2} - 1)] \times [4^N - 1 - 15 - (4^{N-2} - 1)]$ matrix which acts on the indices $(\mu_1\mu_2 0\ldots0)$ and $(\mu_1\mu_2\mu_3\ldots\mu_N)$, respectively, of a Bloch vector $\vec{r} \in \Sigma_N$, where $(\mu_1\mu_2) \neq (00)$ and $(\mu_3\ldots\mu_N) \neq (0\ldots0)$. Therefore, the generators of $\mathcal{T}_2^{(12)}$ must be of the following block-diagonal form:

$$G^{(12)} = \begin{pmatrix} \bar{G}^{(12)} & 0 & 0 \\ 0 & g^{(12)} & 0 \\ 0 & 0 & 0_{(4^{N-2}-1)\times(4^{N-2}-1)} \end{pmatrix}, \tag{B14}$$

where $\bar{G}^{(12)}$ are (linear combinations of) the two-qubit information swap generators (B5) and (B7) and $g^{(12)}$ are the generators of $\tilde{T}^{(12)}$. The latter clearly also have to form a representation of psu(4) in order for the $G^{(12)}$ to generate a $(4^N - 1) \times (4^N - 1)$ matrix representation of psu(4) such that $g^{(12)}$ must be antisymmetric too. Note that this resulting psu(4) representation will thus be reducible. The analogous block-diagonal form holds for the pairwise unitaries and their generators of all other gbit pairs.

We shall now prove Eq. (3.14). We shall do this in three steps, each given by a lemma. Note that the indices of the matrix $\tilde{T}^{(12)}_{(\mu_1\ldots\mu_N)(\nu_1\ldots\nu_N)}$ are *always* such that $(\mu_1\mu_2) \neq (00)$ and $(\mu_3\ldots\mu_N) \neq (0\ldots0)$ (and similarly for the ν indices). However, we can trivially extend $\tilde{T}^{(12)}$ to an $(4^N - 1) \times (4^N - 1)$ matrix by simply setting all new components corresponding to all remaining index combinations to zero. In this case, we can let the indices μ,ν run over all possible values.

Lemma 6. $\tilde{T}^{(12)}_{(\mu_1\mu_2\mu_3\ldots\mu_N)(\nu_1\nu_2\nu_3\ldots\nu_N)} = M_{(\mu_1\mu_2)(\nu_1\nu_2)}(\mu_3,\ldots,\mu_N)\,\delta_{\mu_3\nu_3}\ldots\delta_{\mu_N\nu_N}$. Here, the factor $M_{(\mu_1\mu_2)(\nu_1\nu_2)}(\mu_3,\ldots,\mu_N)$ is a 16×16 matrix which might depend on the values of the indices $(\mu_3\ldots\mu_N)$, and $M_{(00)(\nu_1\nu_2)}(\mu_3,\ldots,\mu_N) = 0 = M_{(\mu_1\mu_2)(00)}(\mu_3,\ldots,\mu_N)$.

Proof. We shall show that the matrix components $\tilde{T}^{(12)}_{(\mu_1\ldots\mu_N)(\nu_1\ldots\nu_N)}$ (for simplicity we drop here the argument t) vanish whenever $\mu_3 \neq \nu_3$. By symmetry in the qubit labels, it then follows more generally that $\tilde{T}^{(12)}$ vanishes unless $\mu_3 = \nu_3,\ldots,\mu_N = \nu_N$. (Clearly, the proof below can also be performed for the fourth, fifth, and higher indices.) Throughout this proof, we use that two questions $Q_{\mu_1\ldots\mu_N}$ and $Q_{\nu_1\ldots\nu_N}$ are complementary iff their indices differ in an odd number of nonzero indices [35].

Consider now $\tilde{T}^{(12)}_{(\mu_1\ldots\mu_N)(\nu_1\ldots\nu_N)}$ with the indices $(\mu_1\ldots\mu_N)$ and $(\nu_1\ldots\nu_N)$ *fixed* and $\mu_3 \neq \nu_3$. We shall henceforth also assume that $(\mu_1\mu_2) \neq (00) \neq (\nu_1\nu_2)$ and, likewise, $(\mu_3\ldots\mu_N) \neq (0,\ldots0) \neq (\nu_3\ldots\nu_N)$ for otherwise this component of $\tilde{T}^{(12)}$ is trivially zero. These two index sets will correspond to two questions $Q_{\mu_1\ldots\mu_N}, Q_{\nu_1\ldots\nu_N}$. We shall now choose a further question $Q_{00\nu_3'\ldots\nu_N'}$ such that it is complementary to $Q_{\mu_1\ldots\mu_N}$ and compatible with $Q_{\nu_1\ldots\nu_N}$. At the end of the proof, we shall show that this is always possible.

Since $Q_{\nu_1\ldots\nu_N}, Q_{00\nu_3'\ldots\nu_N'}$ are compatible, whenever O knows the answer to the two with certainty, he will also know with certainty the answer to their correlation $Q_{\nu_1\nu_2\tilde{\nu_3}\ldots\tilde{\nu_N}} = Q_{\nu_1\nu_2\nu_3\ldots\nu_N} \leftrightarrow Q_{00\nu_3'\ldots\nu_N'}$, where $(\tilde{\nu_3}\ldots\tilde{\nu_N})$ depend on $(\nu_3\ldots\nu_N)$ and $(\nu_3'\ldots\nu_N')$. Since $(\nu_3\ldots\nu_N) \neq (0\ldots0)$, it also holds that $(\tilde{\nu_3}\ldots\tilde{\nu_N}) \neq (0\ldots0)$ [35], however, the precise values of the $\tilde{\nu}_i$ will not matter. There exists a 3 bit state in which only these three questions are answered with certainty, while for all other Bloch vector components $r_i = 0$. Namely, after asking only $Q_{\nu_1\ldots\nu_N}, Q_{00\nu_3'\ldots\nu_N'}$ to a system S in the state of no information, O will have certain information about these two questions and their correlation, however, will not know anything about any further question in the informationally complete set. We shall work with such 3 bit states henceforth.

Thanks to the form of (B13), the component $r_{00\nu_3'\ldots\nu_N'} = \pm1$ of the Bloch vector $\vec{r}$ corresponding to such a state is left invariant under the time evolution $\vec{r}\,' := T^{(12)} \cdot \vec{r}$, i.e., $r'_{00\nu_3'\ldots\nu_N'} = r_{00\nu_3'\ldots\nu_N'} = \pm1$. The complementarity inequalities (2.1) therefore imply that

$$0 = r'_{\mu_1\ldots\mu_N} = \sum_{\beta_i} \tilde{T}^{(12)}_{(\mu_1\ldots\mu_N)(\beta_1\ldots\beta_N)} r_{\beta_1\ldots\beta_N}$$

since $Q_{00\nu_3'\ldots\nu_N'}$ was chosen complementary to $Q_{\mu_1\ldots\mu_N}$. Given that $r_{00\nu_3'\ldots\nu_N'} = \pm1$ is left invariant and thus only the $r_{\nu_1\ldots\nu_N}, r_{\nu_1\nu_2\tilde{\nu_3}\ldots\tilde{\nu_N}} \in \{-1,+1\}$ can contribute (recall that all other $r_i = 0$), the previous equation reduces to[32]

$$\begin{aligned} 0 &= r'_{\mu_1\mu_2\mu_3\ldots\mu_N} \\ &= \tilde{T}^{(12)}_{(\mu_1\ldots\mu_N)(\nu_1\ldots\nu_N)} r_{\nu_1\ldots\nu_N} + \tilde{T}^{(12)}_{(\mu_1\ldots\mu_N)(\nu_1\nu_2\tilde{\nu_3}\ldots\tilde{\nu_N})} r_{\nu_1\nu_2\tilde{\nu_3}\ldots\tilde{\nu_N}} \end{aligned} \tag{B15}$$

[32]We note that $\tilde{T}^{(12)}_{(\mu_1\ldots\mu_N)(\nu_1\nu_2\tilde{\nu}_3\ldots\tilde{\nu}_N)}$ is not necessarily zero since $(\nu_1\nu_2) \neq (00)$ and $(\tilde{\nu}_3\ldots\tilde{\nu}_N) \neq (0\ldots0)$.

(no further summation over ν_i or $\tilde{\nu}_j$). Consider now the two specific configurations[33] (a) $r_{\nu_1\nu_2\nu_3\ldots\nu_N} = r_{\nu_1\nu_2\tilde{\nu}_3\ldots\tilde{\nu}_N} = 1$ and (b) $r_{\nu_1\nu_2\nu_3\ldots\nu_N} = 1, r_{\nu_1\nu_2\tilde{\nu}_3\ldots\tilde{\nu}_N} = -1$. (B15) must hold true for *both* (a) and (b) which is only possible if $\tilde{T}^{(12)}_{(\mu_1\mu_2\mu_3\ldots\mu_N)(\nu_1\nu_2\nu_3\ldots\nu_N)} = 0 = \tilde{T}^{(12)}_{(\mu_1\mu_2\mu_3\ldots\mu_N)(\tilde{\nu}_1\tilde{\nu}_2\tilde{\nu}_3\ldots\tilde{\nu}_N)}$.

In this argument it was crucial that the invariant $Q_{00\nu'_3\ldots\nu'_N}$ was complementary to $Q_{\mu_1\ldots\mu_N}$ and compatible with $Q_{\nu_1\ldots\nu_N}$. Clearly, no such $Q_{00\nu'_3\ldots\nu'_N}$ with this property could exist if we had $(\mu_3\ldots\mu_N) = (\nu_3\ldots\nu_N)$. Hence, all that remains to be checked is whether we can always find a $Q_{00\nu'_3\cdots\nu'_N}$ with this property if $\mu_3 \neq \nu_3$. By considering all the possible cases this can easily be shown to be true. For ease of notation, let us denote the relevant question as $Q^* := Q_{00\nu'_3\ldots\nu'_N}$. First, for $N = 3$ we must have $\mu_3,\nu_3 \neq 0$ in order for $\tilde{T}^{(12)}$ not to vanish and we can choose $Q^* = Q_{00\nu_3}$. For $N > 3$, we choose the question Q^* according to the two cases where the indices $(\mu_4\ldots\mu_N)$ and $(\nu_4\ldots\nu_N)$ differ in either an *odd* or *even* amount of nonzero indices cases (we remind the reader that $\mu_3 \neq \nu_3$):

(i) *Odd* number of differing nonzero indices such that $Q_{000\mu_4\ldots\mu_N}$ and $Q_{000\nu_4\ldots\nu_N}$ are complementary: take $Q^* = Q_{000\nu_4\ldots\nu_N}$.

(ii) *Even* number of differing nonzero indices such that $Q_{000\mu_4\ldots\mu_N}$ and $Q_{000\nu_4\ldots\nu_N}$ are compatible:

$\mu_3 \neq 0$: take $Q^* = Q_{00\nu_3\nu_4\ldots\nu_N}$ if $\nu_3 \neq 0$ or $Q^* = Q_{00\nu'_3\nu_4\ldots\nu_N}$, where any $\nu'_3 \neq \mu_3$ suffices, if $\nu_3 = 0$.

$\mu_3 = 0$ (and thus $\nu_3 \neq 0$) and without loss of generality we assume that $\mu_4 \neq 0$ since there *must* be a nonzero index among $\mu_4,\ldots,\mu_N$: (i) if $\nu_4 \neq 0$, take $Q^* = Q_{00\nu'_3\nu'_4\nu_5\ldots\nu_N}$ with $\nu'_4 \neq \mu_4$, and also $(\nu_3\nu_4)$ and $(\nu'_3\nu'_4)$ differ in an even amount of nonzero indices,[34] (ii) if $\nu_4 = 0$ take $Q^* = Q_{000\nu'_4\nu_5\ldots\nu_N}$, where any $\nu'_4 \neq \mu_4$ suffices.

We thus conclude that $\tilde{T}^{(12)}_{(\mu_1\mu_2\mu_3\ldots\mu_N)(\nu_1\nu_2\nu_3\ldots\nu_N)}$ vanishes unless $(\mu_3\ldots\mu_N) \equiv (\nu_3\ldots\nu_N)$ and thus $\tilde{T}^{(12)}_{(\mu_1\mu_2\mu_3\ldots\mu_N)(\nu_1\nu_2\nu_3\ldots\nu_N)} \sim \delta_{\mu_3\nu_3}\ldots\delta_{\mu_N\nu_N}$. The factor multiplying the delta's might depend on either the indices $\nu_3,\ldots,\nu_N$ or $\mu_3,\ldots,\mu_N$ which are fixed to be equal. ■

It follows from Lemma 6 that the block matrix in the generators (B14) is of the form

$$g^{(12)}_{(\mu_1\mu_2\mu_3\ldots\mu_N)(\nu_1\nu_2\nu_3\ldots\nu_N)} = \tilde{G}_{(\mu_1\mu_2)(\nu_1\nu_2)}(\mu_3,\ldots,\mu_N)\,\delta_{\mu_3\nu_3}\ldots\delta_{\mu_N\nu_N} \tag{B16}$$

with $\tilde{G}_{(00)(\nu_1\nu_2)}(\mu_3,\ldots,\mu_N) = 0 = \tilde{G}_{(\mu_1\mu_2)(00)}(\mu_3,\ldots,\mu_N)$. Note that

$$\begin{aligned} &g^{(12)}_{(\mu_1\ldots\mu_N)(\nu'_1\ldots\nu'_N)}\,g^{(12)}_{(\nu'_1\ldots\nu'_N)(\nu_1\ldots\nu_N)} \\ &= \tilde{G}_{(\mu_1\mu_2)(\nu'_1\nu'_2)}(\mu_3,\ldots,\mu_N)\,\delta_{\mu_3\nu'_3}\ldots\delta_{\mu_N\nu'_N} \\ &\quad\times\tilde{G}_{(\nu'_1\nu'_2)(\nu_1\nu_2)}(\nu'_3\ldots\nu'_N)\,\delta_{\nu'_3\nu_3}\ldots\delta_{\nu'_N\nu_N} \\ &= \tilde{G}_{(\mu_1\mu_2)(\nu'_1\nu'_2)}(\mu_3,\ldots,\mu_N) \\ &\quad\times\tilde{G}_{(\nu'_1\nu'_2)(\nu_1\nu_2)}(\mu_3,\ldots,\mu_N)\,\delta_{\mu_3\nu_3}\ldots\delta_{\mu_N\nu_N} \end{aligned}$$

and similarly for the higher powers of $g^{(12)}$ and therefore $M(t) = \exp(t\,\tilde{G})$ for M given in Lemma 6. We are now interested in the representation of the pentagon swap generators corresponding to (B5) and (B7) on $\mathbb{R}^{4^N-1}$:

$$G^{\mathrm{Pent}^{(12)}_a,\mathrm{Pent}^{(12)}_b} = \begin{pmatrix} G^{\mathrm{Pent}_a,\mathrm{Pent}_b} & 0 & 0 \\ 0 & g^{\mathrm{Pent}^{(12)}_a,\mathrm{Pent}^{(12)}_b} & 0 \\ 0 & 0 & 0_{(4^{N-2}-1)\times(4^{N-2}-1)} \end{pmatrix}, \tag{B17}$$

where $G^{\mathrm{Pent}_a,\mathrm{Pent}_b}$ is one of the 15 two-qubit swap generators in Eqs. (B5) and (B7) and by (B16)

$$g^{\mathrm{Pent}^{(12)}_a,\mathrm{Pent}^{(12)}_b}_{(\mu_1\mu_2\mu_3\ldots\mu_N)(\nu_1\nu_2\nu_3\ldots\nu_N)} = \tilde{G}^{\mathrm{Pent}_a,\mathrm{Pent}_b}_{(\mu_1\mu_2)(\nu_1\nu_2)}(\mu_3,\ldots,\mu_N)\,\delta_{\mu_3\nu_3}\ldots\delta_{\mu_N\nu_N}. \tag{B18}$$

Lemma 7. $\tilde{G}^{\mathrm{Pent}_a,\mathrm{Pent}_b}_{(\mu_1\mu_2)(\nu_1\nu_2)}(\mu_3,\ldots,\mu_N) = 0$ in Eq. (B18) if $Q_{\mu_1\mu_2}$ or $Q_{\nu_1\nu_2}$ is a question whose Bloch vector component is preserved under the two-qubit evolutions generated by the $G^{\mathrm{Pent}_a,\mathrm{Pent}_b}$.

Proof. It is instructive to consider a specific example, say, $G^{\mathrm{Pent}_1,\mathrm{Pent}_2}$ which, as seen in Fig. 4, preserves $r_{x_1},r_{x_2},r_{xx},r_{yy},r_{zz},r_{yz},r_{zy}$. Next, notice that $Q_{x_100\ldots}, Q_{0x_20\ldots}, Q_{xx0\ldots0}, Q_{00\mu_3\ldots\mu_N}$ for $(\mu_3\ldots\mu_N) \neq (0,\ldots0)$ are pairwise compatible since the indices of the questions disagree in none of the nonzero indices [35]. In fact, by Theorem 3.1 in Ref. [35] (Specker's principle), they must also be mutually compatible such that there must exist a state in which the answers to all of these questions are known with certainty to O. For example, $r_{x_100\ldots0} = r_{0x_20\ldots0} = r_{xx0\ldots0} = r_{00\mu_3\ldots\mu_N} = +1$ and therefore, due to the XNOR properties, also $r_{x_10\mu_3\ldots\mu_N} = r_{0x_2\mu_3\ldots\mu_N} = r_{xx\mu_3\ldots\mu_N} = +1$ and all other $r_i = 0$ must exist. This is a 7 bits state. By construction, $T^{\mathrm{Pent}^{(12)}_1,\mathrm{Pent}^{(12)}_2}(t) = \exp(t\,G^{\mathrm{Pent}^{(12)}_1,\mathrm{Pent}^{(12)}_2})$ leaves the components $r_{x_100\ldots0} = r_{0x_20\ldots0} = r_{xx0\ldots0} = r_{00\mu_3\ldots\mu_N} = +1$ invariant. Consequently, $T^{\mathrm{Pent}^{(12)}_1,\mathrm{Pent}^{(12)}_2}(t)$ must also leave $r_{x_10\mu_3\ldots\mu_N} = r_{0x_2\mu_3\ldots\mu_N} = r_{xx\mu_3\ldots\mu_N} = +1$ invariant since these components are implied by $r_{x_100\ldots0} = r_{0x_20\ldots0} = r_{xx0\ldots0} = r_{00\mu_3\ldots\mu_N} = +1$. Furthermore, since time evolution cannot change the total information, also $r_i = 0$ for all other components must be preserved. That is, $T^{\mathrm{Pent}^{(12)}_1,\mathrm{Pent}^{(12)}_2}(t)$ must leave this state invariant for all t. The above arguments and their conclusion are independent of the signs of the nonzero Bloch vector components. In other words, the time evolution must leave, for example, the following two states also invariant[35]: (1) $r_{x_100\ldots0} = r_{00\mu_3\ldots\mu_N} = +1, r_{0x_20\ldots0} = -1$ and (2) $r_{x_100\ldots0} = -1, r_{0x_20\ldots0} = r_{00\mu_3\ldots\mu_N} = +1$. This is only

[33] Both are allowed since $Q_{\nu_1\nu_2\nu_3\ldots\nu_N}, Q_{\nu_1\nu_2\tilde{\nu}_3\ldots\tilde{\nu}_N}$ are pairwise independent [35].

[34] This comes down to the question if, given any two questions $Q_{0\mu_4}$ and $Q_{\nu_3\nu_4}$ where $\nu_3,\nu_4 \neq 0$, there is a third question which is complementary to $Q_{0\mu_4}$ *and* compatible with $Q_{\nu_3\nu_4}$. This is always possible [35].

[35] As before, the XNOR properties dictate the sign of the other nonzero Bloch components as (1) $r_{x_10\mu_3\ldots\mu_N} = 1, r_{0x_2\mu_3\ldots\mu_N} = r_{xx\mu_3\ldots\mu_N} = r_{xx0\ldots0} = -1$ and (2) $r_{x_10\mu_3\ldots\mu_N} = r_{xx\mu_3\ldots\mu_N} = r_{xx0\ldots0} = -1, r_{0x_2\mu_3\ldots\mu_N} = 1$. The remaining components are $r_i = 0$.

possible if

$$\begin{aligned} &M^{\mathrm{Pent}_1,\mathrm{Pent}_2}_{(x_10)(x_10)}[(\mu_3,\ldots,\mu_N);t] \\ &\quad= M^{\mathrm{Pent}_1,\mathrm{Pent}_2}_{(0x_2)(0x_2)}[(\mu_3,\ldots,\mu_N);t] \\ &\quad= M^{\mathrm{Pent}_1,\mathrm{Pent}_2}_{(xx)(xx)}[(\mu_3,\ldots,\mu_N);t] = 1 \end{aligned}$$

and

$$\begin{aligned} &M^{\mathrm{Pent}_1,\mathrm{Pent}_2}_{(\mu_1\mu_2)(x_10)}[(\mu_3,\ldots,\mu_N);t] \\ &\quad\equiv M^{\mathrm{Pent}_1,\mathrm{Pent}_2}_{(\mu_1\mu_2)(0x_2)}[(\mu_3,\ldots,\mu_N);t] \\ &\quad\equiv M^{\mathrm{Pent}_1,\mathrm{Pent}_2}_{(\mu_1\mu_2)(xx)}[(\mu_3,\ldots,\mu_N);t] \equiv 0 \end{aligned}$$

for all t and whenever $(\mu_1\mu_2)$ is neither of $(x_10),(0x_2),(xx)$, respectively. But, this is only possible if $\tilde{G}^{\mathrm{Pent}_1,\mathrm{Pent}_2}_{(\mu_1\mu_2)(x_10)}(\mu_3,\ldots,\mu_N) \equiv \tilde{G}^{\mathrm{Pent}_1,\mathrm{Pent}_2}_{(\mu_1\mu_2)(0x_2)}(\mu_3,\ldots,\mu_N) \equiv \tilde{G}^{\mathrm{Pent}_1,\mathrm{Pent}_2}_{(\mu_1\mu_2)(xx)}(\mu_3,\ldots,\mu_N) \equiv 0$ for all μ_1,μ_2.

By means of an analogous state, one can show similarly that $\tilde{G}^{\mathrm{Pent}_1,\mathrm{Pent}_2}_{(\mu_1\mu_2)(yy)}(\mu_3,\ldots,\mu_N) \equiv \tilde{G}^{\mathrm{Pent}_1,\mathrm{Pent}_2}_{(\mu_1\mu_2)(zz)}(\mu_3,\ldots,\mu_N) \equiv \tilde{G}^{\mathrm{Pent}_1,\mathrm{Pent}_2}_{(\mu_1\mu_2)(yz)}(\mu_3,\ldots,\mu_N) \equiv \tilde{G}^{\mathrm{Pent}_1,\mathrm{Pent}_2}_{(\mu_1\mu_2)(zy)}(\mu_3,\ldots,\mu_N) \equiv 0$ for all μ_1,μ_2.

One argues in complete analogy for all other $\tilde{G}^{\mathrm{Pent}_a,\mathrm{Pent}_b}$. Using the antisymmetry of $\tilde{G}$ one finds the claimed result. ■

We have thus shown that $\tilde{G}^{\mathrm{Pent}_a,\mathrm{Pent}_b}_{(\mu_1\mu_2)(\nu_1\nu_2)}(\mu_3,\ldots,\mu_N)$ could only be nonzero if both questions $Q_{\mu_1\mu_2},Q_{\nu_1\nu_2}$ are among the eight questions whose information content is swapped under the swaps corresponding to $G^{\mathrm{Pent}_a,\mathrm{Pent}_b}$. We shall now strengthen this result further.

Lemma 8. $\tilde{G}^{\mathrm{Pent}_a,\mathrm{Pent}_b}_{(\mu_1\mu_2)(\nu_1\nu_2)}(\mu_3,\ldots,\mu_N) \equiv G^{\mathrm{Pent}_a,\mathrm{Pent}_b}_{(\mu_1\mu_2)(\nu_1\nu_2)}$ for all $(\mu_3\ldots\mu_N)$, where $G^{\mathrm{Pent}_a,\mathrm{Pent}_b}_{(\mu_1\mu_2)(\nu_1\nu_2)}$ is one of the 15 two-qubit swap generators (B5) and (B7), and we define $G^{\mathrm{Pent}_a,\mathrm{Pent}_b}_{(00)(\nu_1\nu_2)} := 0 =: G^{\mathrm{Pent}_a,\mathrm{Pent}_b}_{(\mu_1\mu_2)(00)}$.

Proof. For concreteness, consider, again, $\tilde{G}^{\mathrm{Pent}_1,\mathrm{Pent}_2}$.

(a) We first argue that $\tilde{G}^{\mathrm{Pent}_1,\mathrm{Pent}_2}_{(\mu_1\mu_2)(\nu_1\nu_2)}(\mu_3,\ldots,\mu_N) = 0$ if $G^{\mathrm{Pent}_1,\mathrm{Pent}_2}_{(\mu_1\mu_2)(\nu_1\nu_2)} = 0$. To this end, consider a state with $r_{xy0\ldots0} = r_{zx0\ldots0} = r_{zx\mu_3\ldots\mu_N} = +1$ for $(\mu_3\ldots\mu_N) \neq (0\ldots0)$. Such a state must exist since $Q_{xy0\ldots0},Q_{zx0\cdots0},Q_{zx\mu_3\ldots\mu_N}$ are compatible and pairwise independent. [Recall that two questions are compatible iff they disagree in an even number (including zero) of nonzero indices [35].] By Theorem 3.1 in Ref. [35] (Specker's principle), these are also mutually compatible such that a state must exist in which the answers to these questions are fully known to O. Furthermore, since by Fig. 3 $Q_{xy} \leftrightarrow Q_{zx} = \neg Q_{yz}$ we must also have $r_{yz} = r_{yz\mu_3\ldots\mu_N} = -1$ and, similarly, $r_{00\mu_3\ldots\mu_N} = r_{xy\mu_3\ldots\mu_N} = +1$. For all other components, we may have $r_i = 0$.

Consider now $T^{\mathrm{Pent}^{(12)}_1,\mathrm{Pent}^{(12)}_2}(t) = \exp(t\,G^{\mathrm{Pent}^{(12)}_1,\mathrm{Pent}^{(12)}_2})$ acting on this state. By construction, $r_{yz} = r_{yz\mu_3\ldots\mu_N} = -1$ and $r_{00\mu_3\ldots\mu_N} = +1$ are left invariant (the first two since Q_{yz} is contained in neither of $\mathrm{Pent}_1,\mathrm{Pent}_2$ and thanks to Lemma 7). Furthermore, it follows from Appendix B 2 that $T^{\mathrm{Pent}^{(12)}_1,\mathrm{Pent}^{(12)}_2}(t)$ preserves the pentagon identities (3.3) at the two-qubit level. Given that $T^{\mathrm{Pent}^{(12)}_1,\mathrm{Pent}^{(12)}_2}(t)$ transfers information within the pairs $Q_{xy0\ldots0},Q_{0z_20\ldots0}$ and $Q_{zx0\ldots0},Q_{y_100\ldots0}$ (see Fig. 4) and given the state above, it is clear that

$$r^2_{0z_20\ldots0}(t) + r^2_{zx0\ldots0}(t) = 1 \tag{B19}$$

must thus hold for all $t \in \mathbb{R}$ under $T^{\mathrm{Pent}^{(12)}_1,\mathrm{Pent}^{(12)}_2}(t)$ acting on our initial state.

Next, we note that $Q_{0z_20\ldots0},Q_{zx0\ldots0},Q_{yx\mu_3\ldots\mu_N}$ form a mutually complementary set. Hence, by (2.1), it must always hold $r^2_{0z_20\ldots0}(t) + r^2_{zx0\ldots0}(t) + r_{yx\mu_3\ldots\mu_N}(t) \leqslant 1$ and thanks to (B19) therefore also $r_{yx\mu_3\ldots\mu_N}(t) = 0$ for all $t \in \mathbb{R}$. Given the behavior of our state under $T^{\mathrm{Pent}^{(12)}_1,\mathrm{Pent}^{(12)}_2}(t)$, by Lemma 6 we must therefore have

$$\begin{aligned} r_{yx\mu_3\ldots\mu_N}(t) &= M^{\mathrm{Pent}_1,\mathrm{Pent}_2}_{(yx)(zx)}[(\mu_3,\ldots,\mu_N);t]\,r_{zx\mu_3\ldots\mu_N} \\ &\quad+ M^{\mathrm{Pent}_1,\mathrm{Pent}_2}_{(yx)(xy)}[(\mu_3,\ldots,\mu_N);t]\,r_{xy\mu_3\ldots\mu_N} \\ &= M^{\mathrm{Pent}_1,\mathrm{Pent}_2}_{(yx)(zx)}[(\mu_3,\ldots,\mu_N);t] \\ &\quad+ M^{\mathrm{Pent}_1,\mathrm{Pent}_2}_{(yx)(xy)}[(\mu_3,\ldots,\mu_N);t] \overset{!}{=} 0, \quad \forall\, t \in \mathbb{R}. \end{aligned}$$

Repeating the same steps with the initial state $r_{xy0\ldots0} = r_{zx\mu_3\ldots\mu_N} = r_{yz0\ldots0} = r_{yz\mu_3\ldots\mu_N} = +1$, $r_{00\mu_3\ldots\mu_N} = r_{xy\mu_3\ldots\mu_N} = -1$ (and all other $r_i = 0$), one concludes that also

$$\begin{aligned} &M^{\mathrm{Pent}_1,\mathrm{Pent}_2}_{(yx)(zx)}[(\mu_3,\ldots,\mu_N);t] \\ &\quad- M^{\mathrm{Pent}_1,\mathrm{Pent}_2}_{(yx)(xy)}[(\mu_3,\ldots,\mu_N);t] \overset{!}{=} 0, \quad \forall\, t \in \mathbb{R} \end{aligned}$$

such that

$$\begin{aligned} &M^{\mathrm{Pent}_1,\mathrm{Pent}_2}_{(yx)(zx)}[(\mu_3,\ldots,\mu_N);t] \\ &\quad= M^{\mathrm{Pent}_1,\mathrm{Pent}_2}_{(yx)(xy)}[(\mu_3,\ldots,\mu_N);t] \overset{!}{=} 0, \quad \forall\, t \in \mathbb{R}. \end{aligned}$$

But, this can only be true if also

$$\tilde{G}^{\mathrm{Pent}_1,\mathrm{Pent}_2}_{(yx)(zx)}(\mu_3,\ldots,\mu_N) = \tilde{G}^{\mathrm{Pent}_1,\mathrm{Pent}_2}_{(yx)(xy)}(\mu_3,\ldots,\mu_N) = 0.$$

These components also vanish for $G^{\mathrm{Pent}_1,\mathrm{Pent}_2}$ at the two-qubit level (B5). By complete analogy, one shows that also for all other cases $\tilde{G}^{\mathrm{Pent}_1,\mathrm{Pent}_2}_{(\mu_1\mu_2)(\nu_1\nu_2)}(\mu_3,\ldots,\mu_N) = 0$ if $G^{\mathrm{Pent}_1,\mathrm{Pent}_2}_{(\mu_1\mu_2)(\nu_1\nu_2)} = 0$.

(b) Second, we now show $\tilde{G}^{\mathrm{Pent}_1,\mathrm{Pent}_2}_{(\mu_1\mu_2)(\nu_1\nu_2)}(\mu_3,\ldots,\mu_N) \equiv G^{\mathrm{Pent}_1,\mathrm{Pent}_2}_{(\mu_1\mu_2)(\nu_1\nu_2)}$. For this purpose, consider again the state above. Under (a) we have just shown that $\tilde{G}^{\mathrm{Pent}_1,\mathrm{Pent}_2}_{(\mu_1\mu_2)(\nu_1\nu_2)}(\mu_3,\ldots,\mu_N) \neq 0$ is only possible if $G^{\mathrm{Pent}_1,\mathrm{Pent}_2}_{(\mu_1\mu_2)(\nu_1\nu_2)} \neq 0$. This means that $M^{\mathrm{Pent}_1,\mathrm{Pent}_2}[(\mu_3,\ldots,\mu_N);t] = \exp(t\,\tilde{G}^{\mathrm{Pent}_1,\mathrm{Pent}_2})$ could at most transfer information within the pairs $(Q_{y_10\mu_3\ldots\mu_N},Q_{zx\mu_3\ldots\mu_N})$, $(Q_{xy\mu_3\ldots\mu_N},Q_{0z_2\mu_3\ldots\mu_N})$, $(Q_{z_10\mu_3\ldots\mu_N},Q_{yx\mu_3\ldots\mu_N})$, and $(Q_{xz\mu_3\ldots\mu_N},Q_{0y_2\mu_3\ldots\mu_N})$ for $(\mu_3\ldots\mu_N) \neq (0\ldots0)$. But, since the total information must be preserved this implies that

$$r^2_{xy\mu_3\ldots\mu_N}(t) + r^2_{0z_2\mu_3\ldots\mu_N}(t) = 1, \quad \forall\, t \in \mathbb{R} \tag{B20}$$

must hold for $\vec{r}(t) = T^{\mathrm{Pent}^{(12)}_1,\mathrm{Pent}^{(12)}_2}(t)\,\vec{r}(0)$, where $\vec{r}(0)$ is our initial state above. Similarly, from the pentagon equalities (3.3) it follows for the time evolution of this state that also

$$r^2_{xy0\ldots0}(t) + r^2_{0z_20\ldots0}(t) = 1, \quad \forall\, t \in \mathbb{R}. \tag{B21}$$

From the complementarity inequalities (2.1) it must also hold

$$\begin{aligned} &r^2_{xy0\ldots0}(t) + r^2_{0z_2\mu_3\ldots\mu_N}(t) \leqslant 1, \\ &r^2_{0z_20\ldots0}(t) + r^2_{xy\mu_3\ldots\mu_N}(t) \leqslant 1, \quad \forall\, t \in \mathbb{R}. \end{aligned}$$

From adding up (B20) and (B21) it, in fact, follows, that these inequalities must be saturated:

$$r^2_{xy0\dots0}(t)+r^2_{0z_2\mu_3\dots\mu_N}(t)=1,$$
$$r^2_{0z_20\dots0}(t)+r^2_{xy\mu_3\dots\mu_N}(t)=1,\quad \forall\, t\in\mathbb{R}.$$

This implies that for the time evolution of our initial state,

$$\begin{pmatrix} r_{0z_20\dots0}(t)\\ r_{xy0\dots0}(t)\end{pmatrix}=\begin{pmatrix} s_1\, r_{0z_2\mu_3\dots\mu_N}(t)\\ s_2\, r_{xy\mu_3\dots\mu_N}(t)\end{pmatrix},\quad \forall\, t\in\mathbb{R}$$

where s_1,s_2 are two signs to be determined. From the state at $t=0$, however, we know that $s_2=+1$. Furthermore, we noted above that $r_{00\mu_3\dots\mu_N}=+1$ is invariant under $T^{\mathrm{Pent}_1^{(12)},\mathrm{Pent}_2^{(12)}}(t)$. But, this implies that whenever $r_{0z_20\dots0}(t)=\pm1$, we must also have $r_{0z_2\mu_3\dots\mu_N}=\pm1$ since $Q_{0z_2\mu_3\dots\mu_N}=Q_{0z_20\dots0}\leftrightarrow Q_{00\mu_3\dots\mu_N}$. This entails also $s_1=+1$ and, therefore,

$$\begin{pmatrix} r_{0z_20\dots0}(t)\\ r_{xy0\dots0}(t)\end{pmatrix}=\begin{pmatrix} r_{0z_2\mu_3\dots\mu_N}(t)\\ r_{xy\mu_3\dots\mu_N}(t)\end{pmatrix},\quad \forall\, t\in\mathbb{R}.$$

This is only possible if, indeed, $\tilde G^{\mathrm{Pent}_1,\mathrm{Pent}_2}_{(xy)(0z_2)}(\mu_3,\dots,\mu_N)\equiv G^{\mathrm{Pent}_1,\mathrm{Pent}_2}_{(xy)(0z_2)}$ for *all* values of the indices $\mu_3,\dots,\mu_N$. By completely analogous reasoning, it follows for all other components that $\tilde G^{\mathrm{Pent}_1,\mathrm{Pent}_2}_{(\mu_1\mu_2)(\nu_1\nu_2)}(\mu_3,\dots,\mu_N)\equiv G^{\mathrm{Pent}_1,\mathrm{Pent}_2}_{(\mu_1\mu_2)(\nu_1\nu_2)}$. This implies that $\tilde G^{\mathrm{Pent}_1,\mathrm{Pent}_2}_{(\mu_1\mu_2)(\nu_1\nu_2)}(\mu_3,\dots,\mu_N)$ only depends on its indices $(\mu_1\mu_2)$ and $(\nu_1\nu_2)$ and thus it can be interpreted as a proper 16×16 matrix.

Finally, using similar states and arguments, one shows that, in generality, the above also holds for the other pair of pentagon indices $\tilde G^{\mathrm{Pent}_a,\mathrm{Pent}_b}_{(\mu_1\mu_2)(\nu_1\nu_2)}(\mu_3,\dots,\mu_N)\equiv G^{\mathrm{Pent}_a,\mathrm{Pent}_b}_{(\mu_1\mu_2)(\nu_1\nu_2)}$ for all $a,b=1,\dots,6$. ■

Lemmas 6–8, together with (B17) and (B18) thus indeed give the desired result (3.14). It is also clear that (3.14) generates a (reducible) representation of $\mathcal{T}_2^{(12)}\simeq \mathrm{PSU}(4)$ on $\mathbb{R}^{4^N-1}$.

b. Quantum theory generators of pairwise unitaries for $N>2$ qubits in the adjoint representation

Here, we shall argue that in the adjoint representation, the fundamental generators of the PSU(4) subgroup of PSU(2^N) that involves all time evolutions of the subsystem made up of qubits 1 and 2 are of the following form:

$$\begin{aligned} &G^{(\omega_1\omega_20\dots0)}_{(\mu_1\dots\mu_N)(\nu_1\dots\nu_N)}\\ &\quad:=f^{(\omega_1\omega_20\dots0)}_{(\mu_1\dots\mu_N)(\nu_1\dots\nu_N)}=\frac{1}{2^N}\,\mathrm{tr}\big[[\sigma_{\omega_1\omega_20\dots0},\sigma_{\mu_1\dots\mu_N}]\,\sigma_{\nu_1\dots\nu_N}\big]\\ &\quad=f^{(\omega_1\omega_2)}_{(\mu_1\mu_2)(\nu_1\nu_2)}\delta_{\mu_3\nu_3}\dots\delta_{\mu_N\nu_N}, \end{aligned}\qquad\text{(B22)}$$

where $f^{(\omega_1\omega_2)}_{(\mu_1\mu_2)(\nu_1\nu_2)}$ are the generators of PSU(4) in the adjoint representation corresponding to the 4×4 Pauli operators as given in Eq. (B8). The above generalizes trivially to the generators of the PSU(4) time evolution subgroup of the subsystem of any pair of qubits i and j. The Pauli operators are $\sigma_{\mu_1\dots\mu_N}=(\sigma_{\mu_1}\otimes\dots\otimes\sigma_{\mu_N})$ and satisfy $\mathrm{tr}[\sigma_{\mu_1\dots\mu_N}\cdot\sigma_{\nu_1\dots\nu_N}]=2^N\delta_{\mu_1\nu_1}\dots\delta_{\mu_N\nu_N}$. Working out the trace in Eq. (B22) and using the tensor property $\mathrm{tr}[A\otimes B]=\mathrm{tr}[A]\mathrm{tr}[B]$ results in

$$\begin{aligned} &\frac{1}{2^N}\,\mathrm{tr}\big[(\sigma_{\omega_1}\cdot\sigma_{\mu_1}\cdot\sigma_{\nu_1})\otimes(\sigma_{\omega_2}\cdot\sigma_{\mu_2}\cdot\sigma_{\nu_2})\otimes(\sigma_{\mu_3}\cdot\sigma_{\nu_3})\otimes\dots\otimes(\sigma_{\mu_N}\cdot\sigma_{\nu_N})\\ &\qquad-(\sigma_{\mu_1}\cdot\sigma_{\omega_1}\cdot\sigma_{\nu_1})\otimes(\sigma_{\mu_2}\cdot\sigma_{\omega_2}\cdot\sigma_{\nu_2})\otimes(\sigma_{\mu_3}\cdot\sigma_{\nu_3})\otimes\dots\otimes(\sigma_{\mu_N}\cdot\sigma_{\nu_N})\big]\\ &\quad=\frac{1}{2^N}\,\mathrm{tr}\big[(\sigma_{\omega_1}\cdot\sigma_{\mu_1}\cdot\sigma_{\nu_1})\otimes(\sigma_{\omega_2}\cdot\sigma_{\mu_2}\cdot\sigma_{\nu_2})-(\sigma_{\mu_1}\cdot\sigma_{\omega_1}\cdot\sigma_{\nu_1})\otimes(\sigma_{\mu_2}\cdot\sigma_{\omega_2}\cdot\sigma_{\nu_2})\big]\mathrm{tr}[\sigma_{\mu_3}\cdot\sigma_{\nu_3}]\dots\mathrm{tr}[\sigma_{\mu_N}\cdot\sigma_{\nu_N}]\\ &\quad=\frac{1}{2^N}\,\big(4f^{(\omega_1\omega_2)}_{(\mu_1\mu_2)(\nu_1\nu_2)}\big)(2\delta_{\mu_3\nu_3})\dots(2\delta_{\mu_N\nu_N})=f^{(\omega_1\omega_2)}_{(\mu_1\mu_2)(\nu_1\nu_2)}\delta_{\mu_3\nu_3}\dots\delta_{\mu_N\nu_N}. \end{aligned}$$

We noted before in Appendix B 2 a that the two-qubit adjoint generators $(G^{(\omega_1\omega_2)})_{(\mu_1\mu_2)(\nu_1\nu_2)}:=f^{(\omega_1\omega_2)}_{(\mu_1\mu_2)(\nu_1\nu_2)}$ of quantum theory coincide with the swap generators (B5) and (B7) of the reconstruction. Using the correspondence $Q_{\mu_1\mu_2}\longleftrightarrow\sigma_{\mu_1\mu_2}:=\sigma_{\mu_1}\otimes\sigma_{\mu_2}$ with $\sigma_0=\mathbb{1}$, the ordering of coincidence was such that $G^{(\omega_1\omega_2)}\equiv\pm G^{\mathrm{Pent}_a,\mathrm{Pent}_b}$ where $Q_{\omega_1\omega_2}$ is the unique question in $\mathrm{Pent}_a\cap\mathrm{Pent}_b$ left invariant by the swap.[36]

But, this immediately implies that also (B22) coincides with the reconstructed $\mathcal{T}_2^{(12)}=\mathrm{PSU}(4)$ generators (3.14) (see also Appendix B 3 a). Namely, the ordering of coincidence is such that, first, $Q_{\mu_1\mu_20\dots0}$ corresponds to $\sigma_{\mu_1\mu_20\dots0}:=\sigma_{\mu_1}\otimes\sigma_{\mu_2}\otimes\mathbb{1}\otimes\dots\otimes\mathbb{1}$ and, second, $G^{\mathrm{Pent}_a^{(1,2)},\mathrm{Pent}_b^{(1,2)}}$ coincides with the adjoint representation of $\sigma_{\mu_1\mu_20\dots0}$ corresponding to the unique question $Q_{\mu_1\mu_20\dots0}$ in $\mathrm{Pent}_a^{(12)}\cap\mathrm{Pent}_b^{(12)}$.

c. Evolving to product states for $N>2$ in the reconstruction

Also, for $N>2$ all candidate pure states can be evolved to a product form.

Lemma 9. Using the time evolution group $\mathcal{T}_N\simeq\mathrm{PSU}(2^N)$, any N-gbit pure state $\vec r$ can be transformed to a state with information distribution $\alpha_{z_1}=\dots=\alpha_{z_1\cdots z_N}=1$ bit and all remaining questions in the informationally complete set $\mathcal{Q}_{M_N}$ carrying zero bits.

Proof. Consider the Hermitian traceless matrix $\chi:=\sum_{\mu_i}r_{\mu_1\dots\mu_N}\sigma_{\mu_1}\otimes\dots\otimes\sigma_{\mu_N}$, where $r_{\mu_1\dots\mu_N}$ are the Bloch vector components relative to our question basis. In Sec. III B and Appendixes B 3 a and B 3 b, it was shown that the representation of $\mathcal{T}_N=\mathrm{PSU}(2^N)$, written in the Bloch vector question basis, is exactly the adjoint representation of SU(2^N)

[36] In Appendix B 2 a, we still used the distinct but equivalent index notation with i,j labeling the questions. However, the equivalence is immediate by identifying $i:=\omega_1\omega_2$.

relative to a basis of Pauli operators, which are themselves the generators of the fundamental representation of $SU(2^N)$. The ordering of coincidence of the respective generators corresponds precisely to the pairing between $r_{\mu_1\ldots\mu_N}$ and $\sigma_{\mu_1\ldots\mu_N} := \sigma_{\mu_1}\otimes\cdots\otimes\sigma_{\mu_N}$ in χ. χ thus transforms as $\chi \to U\,\chi\,U^\dagger$ with $U\in SU(2^N)$ in the fundamental representation whenever $\vec r \to T\cdot\vec r$ with $T\in\mathcal{T}_N$. Since χ is Hermitian, it is possible to diagonalize it with some matrix $U\in SU(2^N)$, i.e., such that $\chi' = \sum_{\mu_i} r'_{\mu_1\ldots\mu_N}\sigma_{\mu_1\ldots\mu_N}$ is diagonal and $\vec r\,' = T\cdot\vec r$ with $T\in\mathcal{T}_N$. The Pauli operators $\vec\sigma$ form a basis of all Hermitian matrices and therefore *only* those $r'_{\mu_1\ldots\mu_N}$ which multiply the diagonal $\sigma_{\mu_1\ldots\mu_N}$'s will be nonzero and the other components of $\vec r$ must be zero. There are exactly 2^N-1 of such $\sigma_{\mu_1\ldots\mu_N}$'s, namely, exactly the ones where only σ_z or $\mathbb{1}$ appear in the tensor products [53], i.e., $\sigma_{z_1}=\sigma_z\otimes\mathbb{1}\otimes\cdots\otimes\mathbb{1}$, $\sigma_{z_2}=\mathbb{1}\otimes\sigma_z\otimes\mathbb{1}\otimes\cdots\otimes\mathbb{1},\cdots$, $\sigma_{z_1\ldots z_N}=\sigma_z\otimes\cdots\otimes\sigma_z$ and therefore only the 2^N-1 components $r'_{z_1},\ldots,r'_{z_1\ldots z_N}$ are nonzero. If $\vec r$ was a pure state, then $|\vec r|^2 = 2^N-1$ bits and also $|\vec r\,'|^2=\sum_{\mu_i}(r'_{\mu_1\ldots\mu_N})^2 = 2^N-1$ bits because $\mathcal{T}_N$ preserves the Bloch vector length. There are now two possibilities: (1) less than 2^N-1 of the $(r'_{z_1},\ldots,r'_{z_1\ldots z_N})$ are nonzero. This is only possible if at least one of them has $|r'_i|>1$ and thus $\alpha'_i>1$ bit which is illegal such that in this case the original $\vec r$ could not[37] have been a legal pure state. (2) Exactly 2^N-1 of the $(r'_{z_1},\ldots,r'_{z_1\ldots z_N})$ are nonzero. Since $\alpha'_i=(r_i)^2\leqslant 1$ bit, it follows that precisely $\alpha'_i=(r'_i)^2=1$ bit for $i=z_1,\ldots,z_1\ldots z_N$. Hence, every legal pure state can be time evolved to a state with information distribution $\alpha_{z_1}=\cdots=\alpha_{z_1\ldots z_N}=1$ bit. ∎

d. PSU(2^N) *preserves all complementarity inequalities*

In Sec. III B 2, we concluded that the set of states Σ_N implied by the principles (and background assumptions) is precisely the set of (pure and mixed) N-qubit quantum states. We shall now check for consistency that all states in Σ_N (and thus all quantum states) indeed satisfy the complementarity inequalities (2.1).[38] To this end, we might as well perform the check directly in quantum theory. In particular, we recall that in the correspondence $Q_{\mu_1\ldots\mu_N}\longleftrightarrow\sigma_{\mu_1\ldots\mu_N}$ the Bloch vector description relative to our question basis and the quantum description relative to the Pauli operator basis fully coincide. Thus, in order to show that *all* states in Σ_N satisfy all complementarity inequalities (2.1), we may show that the quantum states satisfy these equalities relative to the Pauli operator basis.

Using our knowledge of quantum theory, we may henceforth effortlessly switch between the Bloch and Hermitian representation by defining for any $\vec r\in\Sigma_N$ the density matrix $\rho := (\mathbb{1}+\vec r\cdot\vec\sigma)/2^N := (\mathbb{1}+\sum r_{\mu_1\ldots\mu_N}\sigma_{\mu_1}\otimes\cdots\otimes\sigma_{\mu_N})/2^N$, for which the following statements will hold:

(i) For any state $\vec r\in\Sigma_N$, ρ transforms as $\rho\to U\rho U^\dagger$ with $U\in SU(2^N)$, whenever $\vec r\to T\cdot\vec r$ for some $T\in\mathcal{T}_N\simeq PSU(2^N)$.

(ii) The density matrix ρ is positive semidefinite and the quantum probability function $\mathrm{tr}[\rho(\mathbb{1}+\sigma_i)/2]\in[0,1]$ for any Pauli operator σ_i.

(iii) For any pair of states $\vec r,\vec r\,'\in\Sigma_N$ with corresponding density matrices ρ,ρ', respectively, the quantum transition probability $\mathrm{tr}[\rho\rho']\in[0,1]$.

We begin with a lemma restricting the Bloch vector components of states featuring information solely in a single set of noncommuting Pauli operators:

Lemma 10. [39] Suppose we have a collection of n traceless, $2^N\times 2^N$ Hermitian and unitary matrices $\{\sigma_i\}_{i=1}^n$ that anticommute:

$$\sigma_i^\dagger=\sigma_i,\quad \sigma_i^2=\mathbb{1},\quad \sigma_i\sigma_j=-\sigma_j\sigma_i\ \ (i\neq j).$$

The operator

$$S=\mathbb{1}+\sum_{i=1}^n r_i\sigma_i\geqslant 0$$

is positive semidefinite if and only if $|r|^2:=\sum_{i=1}^n r_i^2\leqslant 1$.

Proof. Consider the traceless and Hermitian matrix $M := S-\mathbb{1}=\sum_i r_i\sigma_i$. Then,

$$M^2=\sum_{ij} r_ir_j\sigma_i\sigma_j=\sum_i r_i^2\sigma_i^2+\sum_{i<j} r_ir_j\sigma_i\sigma_j+\sum_{i>j} r_ir_j\sigma_i\sigma_j$$
$$=|r|^2\mathbb{1}+\sum_{i<j} r_ir_j\sigma_i\sigma_j-\sum_{i>j} r_ir_j\sigma_j\sigma_i.$$

Exchanging the names of the variables in the last sum, $i\leftrightarrow j$, shows that both sums are actually equal, and we get

$$M^2=|r|^2\mathbb{1}.$$

It follows that every eigenvalue of the Hermitian matrix M must be either $+|r|$ or $-|r|$. In fact, since M is traceless, it must have *both* $+|r|$ or $-|r|$ as eigenvalues. The eigenvalues of the matrix S are therefore $1\pm|r|$ and S is positive semidefinite if and only if $|r|\leqslant 1$. ∎

A set of Hermitian and traceless Pauli operators $\{\sigma_{\mu_1^{(1)}}\otimes\cdots\otimes\sigma_{\mu_N^{(1)}},\ldots,\sigma_{\mu_1^{(n)}}\otimes\cdots\otimes\sigma_{\mu_N^{(n)}}\}$ which, under $Q_{\mu_1\ldots\mu_N}\longleftrightarrow\sigma_{\mu_1\ldots\mu_N}$, correspond to a set of mutually complementary questions[40] $\{Q_{\mu_1^{(1)}\ldots\mu_N^{(1)}},\ldots,Q_{\mu_1^{(n)}\ldots\mu_N^{(n)}}\}$ will satisfy the conditions in the above lemma. The reason is that the $N=1$ qubit 2×2 Pauli operators anticommute themselves and therefore any pair of $2^N\times 2^N$ Pauli operators $P_1=\sigma_{\mu_1}\otimes\cdots\otimes\sigma_{\mu_N}$, $P_2=\sigma_{\mu'_1}\otimes\cdots\otimes\sigma_{\mu'_N}$, which differ in an uneven amount of nonzero indices, *must* anticommute as[41] $P_1\cdot P_2=(\sigma_{\mu_1}\cdot\sigma_{\mu'_1})\otimes\cdots\otimes(\sigma_{\mu_n}\cdot\sigma_{\mu'_n})\otimes\cdots=(-1)^n(\sigma_{\mu'_1}\cdot$

[37] By construction, the time evolution group must map legal states to legal states.

[38] Principles 1 and 3 are trivially satisfied because all pure Bloch vectors, which are generated by the length-conserving group action of $\mathcal{T}_N$ on $\vec r_z:=\vec\delta_{z_1}+\cdots+\vec\delta_{z_1\ldots z_N}$, have a length of 2^N-1 bits (corresponding to N independent bits) and the mixed state vectors are of length smaller than 2^N-1 bits since they are convex combinations of pure state vectors.

[39] The authors are indebted to M. Müller for the proof of this lemma.

[40] We remind the reader that the questions $Q_{\mu_1\ldots\mu_N}$ and $Q_{\mu'_1\ldots\mu'_N}$ are complementary if and only if they have exactly an uneven amount of nonzero indices in which they differ.

[41] Without loss of generality, we assume that the first uneven n indices are nonzero and different between the two Pauli operators.

$\sigma_{\mu_1}) \otimes \cdots \otimes (\sigma_{\mu'_n} \cdot \sigma_{\mu_n}) \otimes \cdots = -P_2 \cdot P_1$. Therefore, all Bloch vectors with a length of exactly 1 bit whose only nonzero components $r_{\mu_1^{(1)}\ldots\mu_N^{(1)}},\ldots,r_{\mu_1^{(n)}\ldots\mu_N^{(n)}}$ correspond to a set of mutually complementary questions $\{Q_{\mu_1^{(1)}\ldots\mu_N^{(1)}},\ldots,Q_{\mu_1^{(n)}\ldots\mu_N^{(n)}}\}$ (including maximal sets) will constitute a valid quantum state because its corresponding density matrix $\rho = (\mathbb{1} + \sum r_{\mu_1\ldots\mu_N}\sigma_{\mu_1}\otimes\cdots\otimes\sigma_{\mu_N})/2^N$ will be positive semidefinite as follows from the lemma above. (The same is true, of course, if the length of the vector would be less than 1 bit.)

Note that this lemma does not immediately imply the same for *arbitrary* quantum states which can also have nonzero Bloch vector components outside of just one noncommuting Pauli operator set. We shall, however, establish this generalization next.

Lemma 11. Every quantum state satisfies the complementarity inequalities (2.1) in the correspondence $Q_{\mu_1\ldots\mu_N} \longleftrightarrow \sigma_{\mu_1\ldots\mu_N}$. Equivalently, every state in Σ_N satisfies (2.1).

Proof. Suppose there was a state $\vec{r}$ featuring *more* than 1 bit of information in a set of mutually complementary questions $\{Q_{\mu_1^{(1)}\ldots\mu_N^{(1)}},\ldots,Q_{\mu_1^{(n)}\ldots\mu_N^{(n)}}\}$. This implies that the length of the Bloch vector components corresponding to those complementary questions is larger than 1 bit, i.e., $r_c := \sqrt{\sum_{i=1}^n r^2_{\mu_1^{(i)}\ldots\mu_N^{(i)}}} > 1$. Lemma 10 entails that all Bloch vectors whose only nonzero components are labeled by these indices $\{(\mu_1^{(1)}\ldots\mu_N^{(1)}),\ldots,(\mu_1^{(n)}\ldots\mu_N^{(n)})\}$, and that are exactly of length 1 bit are legal quantum states and thus also legal states in Σ_N. Hence, we may define the legal Bloch vector $\vec{r}\,' = -\sum_{i=1}^n r_{\mu_1^{(i)}\ldots\mu_N^{(i)}}\vec{\delta}_{\mu_1^{(i)}\ldots\mu_N^{(i)}}/r_c \in \Sigma_N$ of length 1 bit, which corresponds to a legal quantum state. The transition probability $\mathrm{tr}[\rho\cdot\rho'] = \mathrm{tr}[(\mathbb{1}+\vec{r}\cdot\vec{\sigma})\cdot(\mathbb{1}+\vec{r}\,'\cdot\vec{\sigma})]/4^N = (1+\vec{r}\cdot\vec{r}\,')/2^N = (1-r_c)/2^N < 0$, however, is negative for this pair of states and therefore $\vec{r}$ *cannot* have been a legal quantum state. Thus, it can not be contained in Σ_N. ■

APPENDIX C: QUESTION SET

In this Appendix, we derive the characteristic attributes of the question set $\mathcal{Q}_N$, quoted in Sec. III C.

1. Question vectors are 1 bit states

We begin with a result that helps to characterize $\mathcal{Q}_N$.

Lemma 12. Every $\vec{q} \in \mathbb{R}^{D_N}$ with $y(\vec{q}|\vec{r}) \in [0,1]\ \forall\, \vec{r} \in \Sigma_N$ is a quantum state (in the Bloch vector representation). If, in addition, there exists $\vec{r}_Q \in \Sigma_N$ with $I(\vec{r}_Q) = |\vec{r}_Q|^2 = 1$ bit such that $y(\vec{q}|\vec{r}_Q) = 1$, then $\vec{q} \equiv \vec{r}_Q$.

Proof. Having established the coincidence of Σ_N with the set of density matrices over $\mathbb{C}^{2^N}$, we are permitted to work in the Hermitian representation of quantum states. Consider $\tilde{\rho} = \frac{1}{2^N}(\mathbb{1} + \vec{q}\cdot\vec{\sigma})$. It is well known that $\tilde{\rho}$ is a quantum state if and only if $\tilde{\rho} \geqslant 0$ and $\mathrm{tr}\,\tilde{\rho} = 1$. Since $\mathrm{tr}\,\tilde{\rho} = 1$ by construction, $\tilde{\rho}$ could only fail to be a quantum state if $\tilde{\rho}$ was not positive semidefinite. But, then there would exist a quantum state ρ such that $\mathrm{tr}(\rho\tilde{\rho}) < 0$. This is equivalent to $\vec{q}\cdot\vec{r} < -1$, where $\vec{r}$ is the Bloch vector representation of ρ. Since this would be in contradiction with $y(\vec{q}|\vec{r}) = 1/2(\vec{r}\cdot\vec{q}+1) \in [0,1]$ we conclude that $\vec{q}$ is a quantum state also.

It is clear that $|\vec{q}|^2 > 1$ bit is impossible for otherwise $y(\vec{q}|\vec{r} = \vec{q}) > 1$. Suppose now that there exists $\vec{r}_Q \in \Sigma_N$ with $|\vec{r}_Q|^2 = 1$ bit such that $y(\vec{q}|\vec{r}_Q) = 1$. This condition can only be fulfilled if $\vec{r}_Q = \vec{q}$ which also implies $|\vec{q}|^2 = 1$ bit. ■

2. Geometry of the set of Pauli operators

We prove two geometric properties of the set of Pauli operators on $\mathbb{C}^{2^N}$, ultimately showing the set to be isomorphic to $\mathbb{CP}^{2^N-1}$.

Lemma 13. $\mathrm{PSU}(2^N)$ acts transitively on the Pauli operators and these account for all traceless Hermitian operators on $\mathbb{C}^{2^N}$ with eigenvalues equal to ± 1.

Proof. By definition, any Pauli operator P is Hermitian and traceless. Therefore, P can be represented as $P = \vec{n}\cdot\vec{\sigma}$ for some $\vec{n} \in \mathbb{R}^{4^N-1}$ since the matrices $\vec{\sigma}$ in Eq. (3.17) form a basis of Hermitian and traceless matrices. Any Hermitian matrix is diagonalizable by some matrix $U \in \mathrm{SU}(2^N)$ and thus we can write $P = \vec{n}\cdot\vec{\sigma} = UDU^\dagger$ where D is a diagonal matrix with the eigenvalues of P along its diagonal. Since P is a Pauli operator, the diagonal matrix D will contain equal amounts of plus and minus ones along its diagonal. Given any diagonal matrix D of the form above, there *always* exists an orthogonal permutation matrix P_σ which will permute the ± 1's on the diagonal of D to the $\pm$ configuration found for the matrix $\sigma_{z_1} := \sigma_z \otimes \mathbb{1}\cdots\otimes\mathbb{1}$, i.e., $D = P_\sigma\cdot\sigma_{z_1}\cdot P_\sigma^t$. If P_σ happens to be an odd permutation matrix, we may consider the even permutation $P_\sigma\cdot P_{\sigma_0} \in \mathrm{SU}(2^N)$ instead with determinant 1, where P_{σ_0} is any 2-cycle permutation which permutes two rows (and the corresponding columns) of σ_{z_1} that both contain $+1$ and thus that leaves σ_{z_1} invariant. Therefore, without loss of generality, we have $D = P_\sigma\cdot\sigma_{z_1}\cdot P_\sigma^t$ for some $P_\sigma \in \mathrm{SU}(2^N)$ and thus $P = \vec{n}\cdot\vec{\sigma} = (UP_\sigma)\sigma_{z_1}(UP_\sigma)^\dagger$ with $UP_\sigma \in \mathrm{SU}(2^N)$. We conclude that all Pauli operators are related by conjugation with unitaries to the diagonal Pauli operator σ_{z_1}. ■

Lemma 14. The set of Pauli operators is isomorphic to the set of pure quantum states $\mathbb{CP}^{2^N-1}$.

Proof. We may use the fact that the matrices $\vec{\sigma}$ are exactly the *fundamental* generators of $\mathrm{PSU}(2^N)$ and, therefore, by an appropriate adjoint transformation $T \in \mathcal{T}_N$ on the vector $\vec{n}$, we get $(T\cdot\vec{n})\cdot\vec{\sigma} = (UP_\sigma)^\dagger\cdot(\vec{n}\cdot\vec{\sigma})\cdot(UP_\sigma) = \sigma_{z_1}$ and thus $T\cdot\vec{n} = \vec{\delta}_{z_1}$ because the $\vec{\sigma}$ matrices are linearly independent. We have thus shown that the vector $\vec{n}$ which parametrizes the Pauli operator P is connected via the time evolution group to $\vec{\delta}_{z_1}$ and the set of Pauli operators is therefore isomorphic to[42] $\mathcal{T}_N\cdot\vec{\delta}_{z_1}$. Note now that the unit vector $\vec{\delta}_{z_1} \in \mathbb{R}^{4^N-1}$ is related by an $\mathrm{SO}(4^N-1)$ rotation O to the vector $(\vec{\delta}_{z_1} + \cdots + \vec{\delta}_{z_1\ldots z_N})/\sqrt{2^N-1}$. The group action of $\mathcal{T}_N$ on $\vec{\delta}_{z_1}$ therefore results in $\mathcal{T}_N\cdot\vec{\delta}_{z_1} = O^t(O\cdot\mathcal{T}_N\cdot O^t)O\cdot\vec{\delta}_{z_1} = O^t(O\cdot\mathcal{T}_N\cdot O^t)(\vec{\delta}_{z_1}+\cdots+\vec{\delta}_{z_1\cdots z_N})/\sqrt{2^N-1} \simeq \mathbb{CP}^{2^N-1}$. We used first that equivalent representations lead to isomorphic orbits, second that because of transitivity of the pure state space under the action of $\mathcal{T}_N$, the orbit of the pure state $\vec{r} = (\vec{\delta}_{z_1} + \cdots + \vec{\delta}_{z_1\cdots z_N})$ equals $\mathbb{CP}^{2^N-1}$, and last that $(O^t/\sqrt{2^N-1})$ is an

[42]We denote the orbit of some vector $\vec{q} \in \mathbb{R}^{4^N-1}$ under the time evolution group action as $\mathcal{T}_N\cdot\vec{q} := \{T\cdot\vec{q}\mid T\in\mathcal{T}_N\}$ for short.

invertible matrix. We conclude that the set of Pauli operators is isomorphic to $\mathbb{CP}^{2^N-1}$ and parametrized by $\mathcal{T}_N \cdot \vec{\delta}_{z_1}$. ■

3. Structure of $\mathcal{Q}_N$

As argued in the main text and in Ref. [35], for $N = 1$ qubit the question set $\mathcal{Q}_1$ is isomorphic to the set of pure states $\mathbb{CP}^1$. In the following, we show that (3.16) in Sec. III C similarly implies that the question set $\mathcal{Q}_N$ is also isomorphic to the set of pure states $\mathbb{CP}^{2^N-1}$ for $N > 1$ qubits.

Lemma 15. Equation (3.16) implies that the set of vectors $\vec{n}$ parametrizing the Pauli operators $\vec{n} \cdot \vec{\sigma}$ coincides with the set of all question vectors $\vec{q}$. Therefore, $\mathcal{Q}_N$ is isomorphic to the set of Pauli operators and thereby to the set of pure states such that $\mathcal{Q}_N \simeq \mathbb{CP}^{2^N-1}$. In particular, $\mathcal{Q}_N$, in its 1 bit vector representation, inherits a transitive action of the time evolution group $\mathcal{T}_N = \mathrm{PSU}(2^N)$ from Σ_N.

Proof. By Eq. (3.16) the question vectors correspond to legal quantum states, which themselves evolve in the adjoint representation of $\mathrm{PSU}(2^N)$. Therefore, we may form a Hermitian operator by contracting the question vector components with the Pauli operators $\vec{q} \cdot \vec{\sigma} := q_{\mu_1 \ldots \mu_N} \sigma_{\mu_1} \otimes \cdots \otimes \sigma_{\mu_N}$ in the same component ordering as for the state vectors. Hence, for every $U \in \mathrm{SU}(2^N)$ we have $U \cdot (\vec{q} \cdot \vec{\sigma}) \cdot U^\dagger \equiv (T \cdot \vec{q}) \cdot \vec{\sigma}$ for $T \in \mathcal{T}_N$ and thus an action of $\mathcal{T}_N$ on $\mathcal{Q}_N$ inherited from the states.

We may equivalently reformulate (3.16) in terms of the operator $\vec{q} \cdot \vec{\sigma}$ corresponding to a question $Q \in \mathcal{Q}_N$:

(a) The condition $|\vec{q}|^2 = 1$ bit implies

$$\mathrm{tr}[(\vec{q} \cdot \vec{\sigma})^2] = 2^N\, |\vec{q}|^2 = 2^N.$$

(b) The requirement of $0 \leqslant y(Q|\vec{r}) = (1 + \vec{q} \cdot \vec{r})/2 \leqslant 1 \forall\, \vec{r} \in \Sigma_N$ is equivalent to

$$0 \leqslant \mathrm{tr}[\rho(\mathbb{1} + \vec{q} \cdot \vec{\sigma})]/2 \leqslant 1$$
$$\Rightarrow -1 \leqslant \mathrm{tr}[\rho(\vec{q} \cdot \vec{\sigma})] \leqslant 1,$$

for all quantum states ρ, where $\rho = (\mathbb{1} + \vec{r} \cdot \vec{\sigma})/2^N$ is the density matrix corresponding to $\vec{r}$.

All Hermitian operators are diagonalizable and thus there must exist a $T \in \mathcal{T}_N$ which diagonalizes $[(T \cdot \vec{q}) \cdot \vec{\sigma}] = U \cdot (\vec{q} \cdot \vec{\sigma}) \cdot U^\dagger = D = \mathrm{diag}(D_1, D_2, \ldots, D_{2^N})$, with diagonal elements D_i. Note that if $\vec{q} \cdot \vec{\sigma}$ satisfies (a) and (b) above, then so will the operator D since the first constraint is left invariant and the second is related to a valid time evolved state $T^t \cdot \vec{r}$. (a) implies $\mathrm{tr}[D^2] = \sum_{i=1}^{2^N} D_i^2 = 2^N$. By taking now the diagonal density matrices $\rho_1 = \mathrm{diag}(1,0,\ldots,0)$, $\rho_2 = \mathrm{diag}(0,1,\ldots,0)$, ..., $\rho_{2^N} = \mathrm{diag}(0,\ldots,0,1)$, corresponding to the pure states[43] $(r_{z_1} = 1, r_{z_2} = 1, \ldots, r_{z_N} = 1)$, $(r_{z_1} = -1, r_{z_2} = 1, \ldots, r_{z_N} = 1)$, ..., $(r_{z_1} = -1, r_{z_2} = -1, \ldots, r_{z_N} = -1)$, respectively, (b) becomes $-1 \leqslant \mathrm{tr}[\rho_i\, D] = D_i \leqslant 1$. These constraints can only be satisfied if $D_i^2 = 1$ for every index i and therefore $D_i = \pm 1$. Together with $\mathrm{tr}[D] = 0$, we have that D is a Pauli operator as follows from the proof of Lemma 13. Since according to Lemma 13 $\mathcal{T}_N$ acts transitively on the set of all Pauli operators, we get directly that $\mathcal{T}_N$ also acts *transitively* on $\mathcal{Q}_N$ and that the set of Hermitian operators $\vec{q} \cdot \vec{\sigma}$ corresponding to all questions $Q \in \mathcal{Q}_N$, forms a subset of the Pauli operators. Conversely, every Pauli operator $\vec{n} \cdot \vec{\sigma}$ is of the form $T \cdot \vec{\delta}_{z_1}$ for some $T \in \mathcal{T}_N$ and satisfies (a) and (b). From (3.16) (and Lemma 12), it then follows that the vectors $\vec{n}$ which parametrize the Pauli operators correspond to valid questions $Q \in \mathcal{Q}_N$.

Therefore, the set of question vectors coincides with the set of vectors that parametrize the Pauli operators $\vec{n} \cdot \vec{\sigma}$, under the identification $\vec{n} = \vec{q}$. We have shown in Lemma 14 that these vectors are all connected to $\vec{\delta}_{z_1}$ by time evolution and they form a set that is isomorphic to $\mathcal{T}_N \cdot \vec{q}_{z_1} \simeq \mathbb{CP}^{2^N-1}$. Accordingly, we obtain an explicit isomorphism between the set of Pauli operators and the question set $\mathcal{Q}_N$ by contracting each question vector $\vec{q}$ (corresponding to some $Q \in \mathcal{Q}_N$) with the matrices $\vec{\sigma}$ in Eq. (3.17). We conclude that $\mathcal{T}_N$ acts transitively on $\mathcal{Q}_N$ and that $\mathcal{Q}_N$ is isomorphic to the set of Pauli operators. Therefore, $\mathcal{Q}_N$ is also isomorphic to the set of pure states such that $\mathcal{Q}_N \simeq \mathbb{CP}^{2^N-1}$. ■

4. (Non)uniqueness of pure state decompositions

In Sec. III C 5, we quoted the following result:

Lemma 16. The decomposition of a pure state vector $\vec{r}_{\mathrm{pure}} = \vec{q}_1 + \cdots + \vec{q}_{2^N-1}$ in terms of question vectors $\vec{q}_i$ for $Q_i \in \mathcal{Q}_N$ is *unique* for $N = 1,2$ and *nonunique* for $N \geqslant 3$.

Proof. The transitivity of the $\mathcal{T}_N$ group action on the set of pure states and $\mathcal{Q}_N$ entails that such a decomposition of any pure state is unique if and only if it is unique for the pure state $(\vec{\delta}_{z_1} + \vec{\delta}_{z_2} + \cdots + \vec{\delta}_{z_1 \ldots z_N})$. The "only if" direction is trivial, so let us assume now that the decomposition of $\vec{\delta}_{z_1} + \cdots \vec{\delta}_{z_1 \ldots z_N}$ was unique. There is a $T \in \mathcal{T}_N$ such that $\vec{\delta}_{z_1} + \cdots \vec{\delta}_{z_1 \ldots z_N} = T \cdot \vec{r}_{\mathrm{pure}} = (T \cdot \vec{q}_1) + \cdots + (T \cdot \vec{q}_{2^N-1})$. Since $(T \cdot \vec{q}_1), \ldots, (T \cdot \vec{q}_{2^N-1})$ are valid question vectors, they must be uniquely equal (up to permutations) to $\vec{\delta}_{z_1}, \ldots, \vec{\delta}_{z_1 \ldots z_N}$ by assumption. Thus, $\vec{q}_1, \ldots, \vec{q}_{2^N-1}$ are uniquely equal to $T^{-1} \cdot \vec{\delta}_{z_1}, \ldots, T^{-1} \cdot \vec{\delta}_{z_1 \ldots z_N}$ and the decomposition of $\vec{r}_{\mathrm{pure}}$ is thus unique. Therefore, without loss of generality, we will consider henceforth the pure state $\vec{r}_{\mathrm{pure}} = (\vec{\delta}_{z_1} + \vec{\delta}_{z_2} + \cdots + \vec{\delta}_{z_1 \ldots z_N})$.

Suppose now that there was a second, decomposition of $\vec{r}_{\mathrm{pure}}$ in terms of a question set $\vec{q}_i$, $i = 1, \ldots, 2^N - 1$. Since any $\vec{q}_i$ must be answered with "yes" in $\vec{r}_{\mathrm{pure}}$, the Born rule (3.15) implies $y(\vec{q}_i|\vec{r}_{\mathrm{pure}}) = 1 \Leftrightarrow \vec{q}_i \cdot (\vec{\delta}_{z_1} + \vec{\delta}_{z_2} + \cdots + \vec{\delta}_{z_1 \ldots z_N}) = 1$, $i = 1, \ldots, 2^N - 1$. The triangle inequalities then imply

$$\sum_{j \in \{z_1, \ldots, z_1 \ldots z_N\}} (\vec{q}_i \cdot \vec{\delta}_j)^2 \geqslant \left(\sum_{j \in \{z_1, \ldots, z_1 \ldots z_N\}} \vec{q}_i \cdot \vec{\delta}_j \right)^2 = 1.$$

As each question $\vec{q}_i$ must be of length 1 bit and the $4^N - 1$ question vectors $\vec{\delta}_{x_1}, \ldots, \vec{\delta}_{z_1 \ldots z_N}$ of an informationally complete

[43]The other Bloch components are fixed by the correlation and complementarity structure.

set are orthonormal, it also follows that

$$1=\sum_{j\in\{x_1,\dots,z_1\dots z_N\}}(\vec{q}_i\cdot\vec{\delta}_j)^2\geqslant\sum_{j\in\{z_1,\dots,z_1\dots z_N\}}(\vec{q}_i\cdot\vec{\delta}_j)^2,$$

and therefore

$$\sum_{j\in\{z_1,\dots,z_1\dots z_N\}}(\vec{q}_i\cdot\vec{\delta}_j)^2=1.$$

Hence, the questions $\vec{q}_i$ lie in the span of $\vec{\delta}_{z_1},\dots,\vec{\delta}_{z_1\dots z_N}$, i.e., $\vec{q}_i=\sum_{j\in\{z_1,\dots,z_1\dots z_N\}}(\vec{q}_i\cdot\vec{\delta}_j)\,\vec{\delta}_j$.

Let us now consider the Hermitian matrix $\vec{r}_{\text{pure}}\cdot\vec{\sigma}=\sum_i\vec{q}_i\cdot\vec{\sigma}=\sum_{j\in\{z_1,\dots,z_1\dots z_N\}}\vec{\delta}_j\cdot\vec{\sigma}$. Every individual Hermitian matrix $\vec{q}_i\cdot\vec{\sigma}$ appearing in the sum *must* be diagonal because $\vec{q}_i$ lies in the span of the questions $\vec{\delta}_{z_1},\dots,\vec{\delta}_{z_1\dots z_N}$ which, when contracted with $\vec{\sigma}$, yield the diagonal Pauli operators $\sigma_{z_1}\otimes\mathbb{1}\otimes\dots\otimes\mathbb{1},\dots,\sigma_{z_1}\otimes\dots\otimes\sigma_{z_N}$. Moreover, $\vec{q}_i\cdot\vec{\sigma}$ must be a Pauli operator since $\vec{q}_i$ is a legal question vector. Therefore, $\vec{q}_i\cdot\vec{\sigma}$ is a diagonal matrix with 2^{N-1} plus ones and 2^{N-1} minus ones along the diagonal and there are exactly $\binom{2^N}{2^{N-1}}$ of such diagonal Pauli operators. The decomposition of the pure state $\vec{r}_{\text{pure}}$ is now unique if and only if the decomposition of the matrix $\vec{r}_{\text{pure}}\cdot\vec{\sigma}$ in terms of diagonal Pauli operators is unique.

For $N=1$ this decomposition is trivially unique. For $N=2$ there are precisely six diagonal Pauli operators; these are exactly the three operators $\sigma_{z_1}\otimes\mathbb{1}$, $\mathbb{1}\otimes\sigma_{z_2}$, and $\sigma_{z_1}\otimes\sigma_{z_2}$, as well as the operators formed by multiplying them by -1. The Pauli operators form a basis of traceless Hermitian matrices and therefore the matrices $\vec{q}_i\cdot\vec{\sigma}$ must be exactly the three Pauli operators $\sigma_{z_1}\otimes\mathbb{1}$, $\mathbb{1}\otimes\sigma_{z_2}$, $\sigma_{z_1}\otimes\sigma_{z_2}$ and we conclude that the decomposition for $N=2$ is also unique.

For $N>2$ the decomposition is, however, no longer unique. Consider, for example, the simplest case of $N=3$ and $\vec{r}_{\text{pure}}=\vec{\delta}_{z_1}+\vec{\delta}_{z_2}+\dots+\vec{\delta}_{z_1z_2}+\dots+\vec{\delta}_{z_1z_2z_3}$. Let us conjugate the Hermitian matrix $P\cdot(\vec{r}_{\text{pure}}\cdot\vec{\sigma})\cdot P^t=P\cdot\text{diag}(7,-1,\dots,-1)\cdot P^t=\text{diag}(7,-1,\dots,-1)$ with a permutation matrix P which permutes two pairs of rows and columns, $2\leftrightarrow3,4\leftrightarrow5$, and therefore leaves $\vec{r}_{\text{pure}}\cdot\vec{\sigma}$ invariant. The permutation is even such that $P\in\text{SU}(8)$ and P thus defines an element in the isotropy subgroup associated to $\vec{r}_{\text{pure}}$. However, we note that the conjugation with P will not leave the matrices $(\vec{\delta}_{z_1}\cdot\vec{\sigma})=\sigma_{z_1}\otimes\mathbb{1}\otimes\mathbb{1}=\text{diag}(1,1,1,1,-1,-1,-1,-1),\dots,(\vec{\delta}_{z_1z_2z_3}\cdot\vec{\sigma})=\sigma_{z_1}\otimes\sigma_{z_2}\otimes\sigma_{z_3}=\text{diag}(1,-1,-1,1,-1,1,1,-1)$ invariant.[44] A simple check shows that the conjugation with P results in seven new Pauli operators $P\cdot(\vec{\delta}_i\cdot\vec{\sigma})\cdot P^t$, $i=z_1,z_2,\dots,z_1z_2,\dots,z_1z_2z_3$, which all correspond to legal *but different* question vectors than the questions $\vec{\delta}_{z_1},\dots,\vec{\delta}_{z_1z_2z_3}$ appearing in the original decomposition. P is thus *not* contained in the isotropy subgroup associated to $\vec{\delta}_{z_1},\dots,\vec{\delta}_{z_1z_2z_3}$ and the seven new Pauli operators define a distinct decomposition of the pure state.

One may convince oneself that $P\cdot(\vec{\delta}_{z_1}\cdot\vec{\sigma})\cdot P^t=\text{diag}(1,1,1,-1,1,-1,-1,-1)$, in fact, represents the question $Q=(Q_{z_1}\wedge Q_{z_2})\vee(Q_{z_1}\wedge Q_{z_3})\vee(Q_{z_2}\wedge Q_{z_3})$. Similarly, the other Pauli operators $P\cdot(\vec{\delta}_j\cdot\vec{\sigma})\cdot P^t$ will also correspond to legal questions. Note that whenever Q gives "yes", the probability that the question Q_{z_1} is also answered with "yes" cannot be 1/2 as 3 out of 4 states representing $Q=$ "yes" also feature $Q_{z_1}=$ "yes", and similarly for the questions Q_{z_2} and Q_{z_3}. This question Q is therefore *not* fully pairwise independent of either of the questions $\vec{\delta}_{z_1},\dots,\vec{\delta}_{z_1z_2z_3}$.

Since $P\in\text{SU}(8)$ we have $P\cdot(\vec{\delta}_j\cdot\vec{\sigma})\cdot P^t=[(T\cdot\vec{\delta}_j)\cdot\vec{\sigma}]$ for some $T\in\mathcal{T}_3$. The seven questions $(T\cdot\vec{\delta}_{z_1}),\dots,(T\cdot\vec{\delta}_{z_1z_2z_3})$ are independent and compatible because so are the $\vec{\delta}_j$. Accordingly, a system of three qubits, in the pure state $\vec{r}_{\text{pure}}$, also answers "yes" to these seven questions because of the Born rule. In other words, even though having full information of either of the questions $\vec{\delta}_j$ individually is *not* the same as having full information of either of the $T\cdot\vec{\delta}_j$ individually, knowing the answer to *all* seven questions $\vec{\delta}_{z_1},\dots,\vec{\delta}_{z_1\dots r_{z_3}}$ at the same time is equivalent to knowing the answer to $T\cdot\vec{\delta}_{z_1},\dots,T\cdot\vec{\delta}_{z_1z_2z_3}$ simultaneously.

The same conclusion of nonuniqueness of the pure state decomposition in terms of question vectors holds for all $N\geqslant3$ because the $2(2^N-1)$ diagonal Pauli operators given by $\sigma_{z_1},\dots,\sigma_{z_1\dots z_N}$ and their negatives is a strict subset of the $\binom{2^N}{2^{N-1}}$ diagonal Pauli operators for $N\geqslant3$. ■

[44] The diagonal elements here correspond to choosing the ordering of the diagonal of the density matrix $(\mathbb{1}+\vec{r}\cdot\vec{\sigma})/8$ in terms of z "up" or "down" of the three qubits as $|{+}{+}{+}\rangle,|{-}{+}{+}\rangle,|{+}{-}{+}\rangle,|{-}{-}{+}\rangle,|{+}{+}{-}\rangle,|{-}{+}{-}\rangle,|{+}{-}{-}\rangle,|{-}{-}{-}\rangle$.

[1] J. S. Bell, On the einstein-podolsky-rosen paradox, Physics **1**, 195 (1964).

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

[3] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Proposed Experiment to Test Local Hidden-Variable Theories, Phys. Rev. Lett. **23**, 880 (1969).

[4] S. Popescu and D. Röhrlich, Quantum nonlocality as an axiom, Found. Phys. **24**, 379 (1994).

[5] M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Żukowski, Information causality as a physical principle, Nature (London) **461**, 1101 (2009).

[6] D. I. Fivel, How interference effects in mixtures determine the rules of quantum mechanics, Phys. Rev. A **50**, 2108 (1994).

[7] R. D. Sorkin, Quantum mechanics as quantum measure theory, Mod. Phys. Lett. A **09**, 3119 (1994).

[8] H. Barnum, M. P. Müller, and C. Ududec, Higher-order interference and single-system postulates characterizing quantum theory, New J. Phys. **16**, 123029 (2014).

[9] C. Rovelli, Relational quantum mechanics, Int. J. Theor. Phys. **35**, 1637 (1996).

[10] A. Zeilinger, A foundational principle for quantum mechanics, Found. Phys. **29**, 631 (1999).

[11] C. Brukner and A. Zeilinger, Information and fundamental elements of the structure of quantum theory, in *Time, Quantum and*

Information, edited by L. Castell and O. Ischebeck (Springer, Berlin, 2003).

[12] C. Brukner and A. Zeilinger, Operationally Invariant Information in Quantum Measurements, Phys. Rev. Lett. **83**, 3354 (1999).

[13] C. Brukner and A. Zeilinger, Young's experiment and the finiteness of information, Philos. Trans. R. Soc. London A **360**, 1061 (2002).

[14] Č. Brukner and A. Zeilinger, Information invariance and quantum probabilities, Found. Phys. **39**, 677 (2009).

[15] C. Brukner, M. Zukowski, and A. Zeilinger, The essence of entanglement, arXiv:quant-ph/0106119.

[16] R. W. Spekkens, Evidence for the epistemic view of quantum states: A toy theory, Phys. Rev. A **75**, 032110 (2007).

[17] R. W. Spekkens, Quasi-quantization: classical statistical theories with an epistemic restriction, arXiv:1409.5041.

[18] T. Paterek, B. Dakic, and C. Brukner, Theories of systems with limited information content, New J. Phys. **12**, 053037 (2010).

[19] C. F. von Weizsäcker, *The Structure of Physics* (Springer, Dordrecht, 2006).

[20] T. Görnitz, An Introduction to Carl Friedrich von Weizsäcker's Program for a Reconstruction of Quantum Theory, in *Time, Quantum and Information*, edited by L. Castell and O. Ischebeck (Springer, Berlin, 2003).

[21] H. Lyre, Quantum theory of ur-objects as a theory of information, Int. J. Theor. Phys. **34**, 1541 (1995).

[22] L. Hardy, Quantum theory from five reasonable axioms, arXiv:quant-ph/0101012.

[23] B. Dakic and C. Brukner, Quantum theory and beyond: Is entanglement special? in *Deep Beauty: Understanding the Quantum World through Mathematical Innovation*, edited by H. Halvorson (Cambridge University Press, Cambridge, UK, 2011), pp. 365–392.

[24] L. Masanes and M. P. Müller, A derivation of quantum theory from physical requirements, New J. Phys. **13**, 063001 (2011).

[25] M. P. Müller and L. Masanes, Information-theoretic postulates for quantum theory, arXiv:1203.4516.

[26] L. Masanes, M. P. Müller, R. Augusiak, and D. Perez-Garcia, Existence of an information unit as a postulate of quantum theory, Proc. Natl. Acad. Sci. USA **110**, 16373 (2013).

[27] G. Chiribella, G. M. D'Ariano, and P. Perinotti, Informational derivation of quantum theory, Phys. Rev. A **84**, 012311 (2011).

[28] G. de la Torre, L. Masanes, A. J. Short, and M. P. Müller, Deriving Quantum Theory from its Local Structure and Reversibility, Phys. Rev. Lett. **109**, 090403 (2012).

[29] M. P. Müller and L. Masanes, Three-dimensionality of space and the quantum bit: how to derive both from information-theoretic postulates, New J. Phys. **15**, 053040 (2013).

[30] L. Hardy, Reconstructing quantum theory, arXiv:1303.1538.

[31] A. J. P. Garner, M. P. Müller, and O. C. O. Dahlsten, The quantum bit from relativity of simultaneity on an interferometer, arXiv:1412.7112.

[32] R. Oeckl, A first-principles approach to physics based on locality and operationalism, PoS **14**, 171 (2016).

[33] S. Kochen, A reconstruction of quantum mechanics, arXiv:1306.3951.

[34] P. Goyal, From Information Geometry to Quantum Theory, New J. Phys. **12**, 023012 (2010).

[35] P. A. Höhn, Toolbox for reconstructing quantum theory from rules on information acquisition, arXiv:1412.8323.

[36] M. Smerlak and C. Rovelli, Relational EPR, Found. Phys. **37**, 427 (2007).

[37] J. B. Hartle, Quantum mechanics of individual systems, Am. J. Phys. **36**, 704 (1968).

[38] Q. Zheng and T. Kobayashi, Quantum optics as a relativistic theory of light, Phys. Essays **9**, 447 (1996).

[39] C. A. Fuchs, Quantum mechanics as quantum information (and only a little more), arXiv:quant-ph/0205039.

[40] C. M. Caves, C. A. Fuchs, and R. Schack, Quantum probabilities as Bayesian probabilities, Phys. Rev. A **65**, 022305 (2002).

[41] C. M. Caves, C. A. Fuchs, and R. Schack, Unknown quantum states: the quantum de Finetti representation, J. Math. Phys. **43**, 4537 (2002).

[42] A. Petersen, The philosophy of Niels Bohr, Bull. At. Sci. **19**, 8 (1963).

[43] M. Krein and D. Milman, On extreme points of regular convex sets, Studia Mathematica **9**, 133 (1940).

[44] P. A. Höhn and C. S. P. Wever (unpublished).

[45] J. Barrett, Information processing in generalized probabilistic theories, Phys. Rev. A **75**, 032304 (2007).

[46] L. Masanes, M. P. Müller, D. Perez-Garcia, and R. Augusiak, Entanglement and the three-dimensionality of the bloch ball, J. Math. Phys. **55**, 122203 (2014).

[47] C. Brukner and A. Zeilinger, Quantum measurement and shannon information, a reply to M. J. W. Hall, arXiv:quant-ph/0008091.

[48] C. Brukner and A. Zeilinger, Conceptual inadequacy of the shannon information in quantum measurements, Phys. Rev. A **63**, 022113 (2001).

[49] I. Bengtsson and K. Zyczkowski, *Geometry of Quantum States: An Introduction to Quantum Entanglement* (Cambridge University Press, Cambridge, UK, 2006).

[50] M. J. Bremner, C. M. Dawson, J. L. Dodd, A. Gilchrist, A. W. Harrow, D. Mortimer, M. A. Nielsen, and T. J. Osborne, Practical Scheme for Quantum Computation with any Two-Qubit Entangling Gate, Phys. Rev. Lett. **89**, 247902 (2002).

[51] A. Harrow, Exact universality from any entangling gate without inverses, Quantum Inf. Comput. **9**, 773 (2009).

[52] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, UK, 2010).

[53] J. Lawrence, Č. Brukner, and A. Zeilinger, Mutually unbiased binary observable sets on n qubits, Phys. Rev. A **65**, 032320 (2002).

[54] P. A. Höhn and M. P. Müller, An operational approach to spacetime symmetries: Lorentz transformations from quantum communication, New J. Phys. **18**, 063026 (2016).

[55] R. C. Raffenetti and K. Ruedenberg, Parametrization of an orthogonal matrix in terms of generalized eulerian angles, Int. J. Quantum Chem. **4**, 625 (1969).

[56] D. K. Hoffman, R. C. Raffenetti, and K. Ruedenberg, Generalization of euler angles to n-dimensional orthogonal matrices, J. Math. Phys. **13**, 528 (1972).

[57] H. Georgi, Lie Algebras in Particle Physics. From Isospin to Unified Theories, Front. Phys. **54**, 1 (1982).

[58] R. Feger and T. Kephart, LieArt – A mathematica application for Lie algebras and representation theory, arXiv:1206.6379.

[59] E. Dynkin, Maximal subgroups of the classical groups, AMS Transl. **6**, 245 (1957).