axioms

MDPI

Article

Impossibility of Quantum Bit Commitment, a Categorical Perspective

Xin Sun [1,*], Feifei He [2] and Quanlong Wang [3]

1 Department of Foundation of Computer Science, Catholic University of Lublin, 20950 Lublin, Poland
2 Institute of Logic and Cognition, Sun Yat-sen University, Guangzhou 510275, China; hliheng@gmail.com
3 Department of Computer Science, University of Oxford, Oxford OX13QD, UK; quaang@cs.ox.ac.uk
* Correspondence: xin.sun.logic@gmail.com

Received: 3 January 2020; Accepted: 3 March 2020; Published: 9 March 2020

Abstract: Bit commitment is a cryptographic task in which Alice commits a bit to Bob such that she cannot change the value of the bit after her commitment and Bob cannot learn the value of the bit before Alice opens her commitment. According to the Mayers–Lo–Chau (MLC) no-go theorem, ideal bit commitment is impossible within quantum theory. In the information theoretic-reconstruction of quantum theory, the impossibility of quantum bit commitment is one of the three information-theoretic constraints that characterize quantum theory. In this paper, we first provide a very simple proof of the MLC no-go theorem and its quantitative generalization. Then, we formalize bit commitment in the theory of dagger monoidal categories. We show that in the setting of dagger monoidal categories, the impossibility of bit commitment is equivalent to the unitary equivalence of purification.

Keywords: bit commitment, categorical quantum mechanics, quantum foundation

1. Introduction

Bit commitment, used in a wide range of cryptographic protocols (e.g., zero-knowledge proof, multiparty secure computation, and oblivious transfer), consists of two phases, namely: commit and opening. In the commit phase, Alice the sender chooses a bit a ($a = 0$ or 1) which she wishes to commit to the receiver Bob. Then, Alice presents Bob some evidence about the bit. The committed bit cannot be known by Bob prior to the opening phase. Later, in the opening phase, Alice announces some information for reconstructing a. Bob then reconstructs a bit a' using Alice's evidence and announcement. A correct bit commitment protocol will ensure that $a' = a$. A bit commitment protocol is concealing if Bob cannot know the bit Alice committed before the opening phase and it is binding if Alice cannot change the bit she committed after the commit phase. It is secure if it is both concealing and binding. It is unconditionally secure if it is secure and the security does not rely on any computational assumption.

Quantum bit commitment (QBC) [1–16] protocol was first proposed by Bennett and Brassard in 1984 [1]. Later, several QBC protocols were designed to achieve unconditional security, such as those in [17,18]. However, in 1996, Mayers [19] and Lo and Chau [20,21] showed that all previously proposed QBC protocols were vulnerable to an entanglement attack which can be launched by Alice. This result was later referred to as the Mayers–Lo–Chau (MLC) no-go theorem.

This no-go theorem has been continuously challenged in the past two decades. Yuen [22,23] repeatedly argued that the no-go proof is not general enough to exhaust all conceivable quantum bit commitment protocols. On the other hand, the no-go theorem has also been extended by several scholars. Nambu and Chiba-Kohno [24] gave a constructive proof of the theorem from the viewpoint of quantum information theory. Spekkens and Rudolph [25] and He [26] extended the no-go theorem

with quantitative bounds on the degree of concealment and bindingness. D'Ariano et al. [27] provided a strengthened and explicit impossibility proof exhausting all conceivable protocols in which not only quantum information, but also classical information is exchanged between the two parties. However, the considerable length of the proof in [27] makes it still hard to follow. Chiribella et al. [28] simplified the proof in [27]. In the works of Cohn-Gordon [29] and Heunen and Kissinger [30], a clear and rigorous formalization of QBC is developed in the setting of categorical quantum mechanics. Cohn-Gordon [29] also provided a proof of the no-go theorem. While this proof is already simpler than all previous proofs, we find there is still room for simplification and extension.

In Clifton et al.'s information theoretic-reconstruction of quantum theory [31], the impossibility of bit commitment is conceived as one of the three fundamental information-theoretic constraints that characterize quantum theory. In [31], the authors partially proved that the impossibility of bit commitment is equivalent to the existence of entangled, or nonlocal, states. This result was questioned by Heunen and Kissinger [30], who demonstrated that, in the categorical setting, the impossibility of bit commitment is not equivalent to the existence of entangled states. Which quantum feature is the one that is equivalent to the impossibility of bit commitment is left unanswered in [30].

The contributions of this paper are ass follows.

1. The length of the proof in Cohn-Gordon [29] is more than two pages. We provide a simpler proof which takes only a few lines.
2. The proof in [29] only concerns the qualitative version of the no-go theorem. We formalize and prove the quantitative version of the no-go theorem.
3. We show that the impossibility of bit commitment is equivalent to the unitary equivalence of purification in the setting of dagger monoidal categories. This provides an answer to the problem left by Heunen and Kissinger [30].

The structure of this paper is as follows. We simplify and extend the proof of Cohn-Gordon [29] in Section 2. Then, in Section 3, we study the impossibility of bit commitment in the setting of dagger monoidal categories and demonstrate that the quantum feature corresponding to the impossibility of bit commitment in the categorical setting is the unitary equivalence of purification. In Section 4, we discuss some related work. We conclude this paper with future work in Section 5.

2. The No-Go Theorem of Quantum Bit Commitment

In the literature [19,20,25,29,30], it is acknowledged that a general model of QBC protocols should at least includes the following ingredients:

1. The Hilbert space required to describe the protocol is the tensor product of the Hilbert spaces that play a role in the protocol.
2. The total system is initially in a pure state.
3. Every action taken by a party corresponds to that party performing a unitary operation on the systems in his/her possession.
4. Every communication corresponds to a party sending a subset of the systems in his/her possession to the other party.

Bearing this common knowledge in mind, we propose the most rigorous and simplest formalization of quantum bit commitment as follows.

Definition 1. *A quantum bit commitment protocol consists of the following:*

(1) Two finite-dimensional Hiblert spaces A and B
(2) Two pure states $|H\rangle, |T\rangle \in A \otimes B$
(3) A quantum operation (i.e., completely positive, trace-preserving super operator) Open on $A \otimes B$ such that $Open(|H\rangle\langle H|) \neq Open(|T\rangle\langle T|)$

This QBC protocol is concealing if $Tr_A(|H\rangle\langle H|) = Tr_A(|T\rangle\langle T|)$. *It is binding if there is no unitary* U *on* A *such that* $(U \otimes I_B)|H\rangle = |T\rangle$.

This formalization provides a high level description of quantum bit commitment. Initially, Alice (possibly with the help of Bob) prepares a state $|H\rangle$ or $|T\rangle$ of quantum system $A \otimes B$ depending on the value of Alice's bit. Note that $|H\rangle$ and $|T\rangle$ are not the initial states of the QBC protocol, but the final states of the commit phase. Starting from a pure state, a commit phase may involve many rounds of actions and communications. Alice sends $Tr_A(|H\rangle\langle H|)$ or $Tr_A(|T\rangle\langle T|)$ to Bob to perform the commitment. At the opening stage, Alice sends the rest sub-state of $|H\rangle$ or $|T\rangle$ to Bob to allow him to verify her commitment. Bob applies the quantum operation $Open$ to determine Alice's commitment.

In our definition of bindingness, we only consider the situation in which Alice applies unitary operators to the pure state in her possession, instead of complete positive maps on mixed states. This is a reasonable assumption in the sense that complete positive maps on mixed states can be purified to unitary map on pure states via Stinespring representation [32]. This notion of bindingness is very strong: Alice must be able to alter $|H\rangle$ to $|T\rangle$ with certainty. In Section 2.2, we introduce ϵ-binding, a weaker notion of bindingness that allows Alice to alter $|H\rangle$ to a state which is similar to $|T\rangle$. Another issue concerning bindingness is that the operation $Open$ plays no role in the current definition of bindingness. We discuss an alternative notion of bindingness which involves $Open$ in Section 4.

Example 1. *The QBC protocol due to Bennett and Brassard [1] goes as follows: Alice and Bob first agree on a security parameter, a positive integer* s.

1. *Commit phase:*
   - (a) *Alice chooses the value of the committed bit* c *and the auxiliary bits* $a_1, \ldots, a_s$.
   - (b) *If* $c = 0$, *she prepares and sends Bob* s *qubits, which are chosen to be either* $|0\rangle$ *or* $|1\rangle$. *The value of* c *is kept secret during the commit phase. If* $a_i = 0$, *then Alice sets the* i*th qubit to be* $|0\rangle$. *If* $a_i = 1$, *then she sets the* i*th qubit to be* $|1\rangle$. *The value of* $a_1, \ldots, a_n$ *are also kept secret during the commit phase.*
   - (c) *Similarly, if* $c = 1$, *she prepares and sends Bob* s *qubits, which are chosen to be either* $|+\rangle$ *or* $|-\rangle$. *If* $a_i = 0$, *then Alice sets the* i*th qubit to be* $|+\rangle$. *If* $a_i = 1$, *and then she sets the* i*th qubit to be* $|-\rangle$. *The value of* $c, a_1, \ldots, a_n$ *are kept secret during the commit phase.*
2. *Opening phase:*
   - (a) *Bob randomly prepares auxiliary bits* $b_1, \ldots, b_s$. *If* $b_i = 0$, *and then Bob measures the* i*th qubit in the* $\{|0\rangle, |1\rangle\}$ *basis. If* $b_i = 1$, *then Bob measures the* i*th qubit in the* $\{|+\rangle, |-\rangle\}$ *basis.*
   - (b) *Alice announces the value of* $c, a_1, \ldots, a_s$.
   - (c) *Bob accepts Alice's commitment if and only if, for all indexes* $i \in \{1, \ldots, s\}$ *with* $c = b_i$, *Bob's measurement outcome agrees with Alice's announcement.*

We can formalize this QBC protocol as follows:

- *Let* $A = \mathbb{C}^{(2^{1+s})}$ *and* $B = \mathbb{C}^{(2^s)}$.
- *Let* $|H\rangle = \sum_{a_1 \ldots a_s} |0a_1 \ldots a_s\rangle \otimes U_{0,a_1}|0\rangle \ldots U_{0,a_s}|0\rangle$, *where* $U_{0,0}$ *is the identity operator and* $U_{0,1}$ *is the Pauli X operator.*
- *Let* $|T\rangle = \sum_{a_1 \ldots a_s} |1a_1 \ldots a_s\rangle \otimes U_{1,a_1}|0\rangle \ldots U_{1,a_s}|0\rangle$, *where* $U_{1,0}$ *is the Hadamard operator* H *and* $U_{1,1}$ *is* HX.
- *Let Open be a completely positive map such that*
  - $Open(|H\rangle\langle H|) = \sum_{a_1 \ldots a_s} (|0a_1 \ldots a_s\rangle\langle 0a_1 \ldots a_s|) \otimes M_{b_1}(U_{0,a_1}|0\rangle\langle 0|U_{0,a_1}^\dagger) \otimes \ldots \otimes M_{b_s}(U_{0,a_s}|0\rangle\langle 0|U_{0,a_s}^\dagger)$, *where* M_0 *is the completely positive map which represents the measurement*

on the $\{|0\rangle, |1\rangle\}$ *basis and* M_1 *is the completely positive map which represents the measurement on the* $\{|+\rangle, |-\rangle\}$ *basis.*

– $Open(|T\rangle\langle T|) = \sum_{a_1 \ldots a_s} (|1a_1 \ldots a_s\rangle\langle 1a_1 \ldots a_s|) \otimes M_{b_1}(U_{1,a_1}|0\rangle\langle 0|U_{1,a_1}^\dagger) \otimes \ldots \otimes M_{b_s}(U_{1,a_s}|0\rangle\langle 0|U_{1,a_s}^\dagger)$.

Note that, although our formalization of QBC protocols in Definition 1 looks simple, it is in fact already more general than the formalizations by Lo and Chau [20] and Cohn-Gordon [29]. It is also a proper extension of the purification bit commitment protocol by Spekkens and Rudolph [25].

Example 2. *A purification bit commitment protocol [25] makes use of two systems, the token system and the proof system. These are associated with Hilbert spaces* H_t *and* H_p*. A purification bit commitment protocol also specifies two orthogonal states* $|\phi_0\rangle$ *and* $|\phi_1\rangle$*, which are states of the system* $H_t \otimes H_p$*. At the commit phase, Alice prepares the two systems in the state* $|\phi_b\rangle$ *in order to commit to bit* b*, and sends the token system to Bob. At the opening phase, Alice sends the proof system to Bob, and Bob performs a measurement of the projector valued measure* $\{P_0, P_1, P_{fail}\}$*, where* $P_b = |\phi_b\rangle\langle\phi_b|$*.*

We further discuss the generality of our formalism in Section 4.

2.1. The Qualitative No-Go Theorem

Within our formalization, the no-go theorem of quantum bit commitment becomes a precise mathematical statement. To prove this statement, we make use of the unitary equivalence of purification, which can be found in standard textbooks of quantum information [32,33].

Definition 2 (purification)**.** *Let* A *and* B *be two Hilbert spaces and* $Pos(A)$ *be the set of all positive semidefinite operators on* A*. For* $\rho \in Pos(A)$ *and* $|\phi\rangle \in A \otimes B$*,* $|\phi\rangle$ *is a purification of* ρ *if* $Tr_B(|\phi\rangle\langle\phi|) = \rho$*.*

Lemma 1 (unitary equivalence of purification)**.** *Let* $|\phi\rangle \in A \otimes B$ *and* $|\psi\rangle \in A \otimes B$ *be two purifications of a positive smiedefinite operator* $\rho \in Pos(A)$*. There is a unitary transformation* U *acting on* B *such that* $|\phi\rangle = (I_A \otimes U)|\psi\rangle$*.*

Theorem 1 (no-go theorem, the qualitative version)**.** *If a quantum bit commitment protocol is concealing, then it is not binding.*

Proof. If a QBC is concealing, then $Tr_A(|H\rangle\langle H|) = Tr_A(|T\rangle\langle T|)$. Hence, $|H\rangle$ and $|T\rangle$ are two purifications of the same mixed state. By Lemma 1, we know there is a unitary operator U_A such that $|H\rangle = (U_A \otimes I_B)|T\rangle$, which means that the QBC is not binding. □

The astonishing simplicity of the above proof suggests a close relationship between the unitary equivalence of purification and the impossibility of quantum bit commitment. In Section 3, we show that they are actually equivalent in an abstract categorical framework.

2.2. The Quantitative No-Go Theorem

The qualitative version of the no-go theorem states that it is impossible for a QBC protocol to be both absolute concealing and absolute binding. However, it does not exclude the possibility of a QBC protocol to be both partially concealing and partially binding. We now formalize and prove the quantitative version of the no-go theorem, which establishes a relation between partially concealing and partially binding. The key notion we use is the fidelity between quantum states.

Definition 3 (fidelity [33])**.** *Let* $|\phi\rangle$ *and* $|\psi\rangle$ *be two pure states of a Hilbert space. The fidelity of* $|\phi\rangle$ *and* $|\psi\rangle$ *is* $F(|\phi\rangle, |\psi\rangle) = |\langle\phi|\psi\rangle|$*. Let* ρ *and* σ *be two mix states of a Hilbert space. The fidelity of* ρ *and* σ *is* $F(\rho, \sigma) = Tr(\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}})$*.*

After some careful calculation, we know that $F(|\phi\rangle, |\psi\rangle) = F(|\phi\rangle\langle\phi|, |\psi\rangle\langle\psi|)$. We define the relation $\overset{\epsilon}{=}$, where $\epsilon \in [0,1]$, between quantum states as follows: $\rho \overset{\epsilon}{=} \sigma$ iff $F(\rho,\sigma) \geq \epsilon$. Apparently, $\rho = \sigma$ iff $\rho \overset{1}{=} \sigma$.

Definition 4 (ϵ-concealing, ϵ-binding). *A quantum bit commitment protocol is ϵ-concealing if $Tr_A(|H\rangle\langle H|) \overset{\epsilon}{=} Tr_A(|T\rangle\langle T|)$. It is ϵ-binding if there is no unitary U on A such that $(U \otimes I_B)|H\rangle \overset{\epsilon}{=} |T\rangle$.*

The following Uhlmann's theorem is used in the proof of the quantitative version of the no-go theorem.

Theorem 2 (Uhlmann's theorem [33]). *$F(\rho,\sigma) = \max_{|\phi\rangle,|\psi\rangle} |\langle\phi|\psi\rangle|$, where $|\phi\rangle$ ranges over all purifications of ρ and ψ ranges over all purifications of σ. If $|\phi\rangle$ is a fixed purification of ρ, then $F(\rho,\sigma) = \max_{|\psi\rangle} |\langle\phi|\psi\rangle|$, where ψ ranges over all purifications of σ.*

Theorem 3 (no-go theorem, the quantitative version). *If a quantum bit commitment protocol is ϵ-concealing, then it is not ϵ-binding.*

Proof. If a QBC protocol is ϵ-concealing, then $Tr_A(|H\rangle\langle H|) \overset{\epsilon}{=} Tr_A(|T\rangle\langle T|)$. Thus, we have $F(Tr_A(|H\rangle\langle H|), Tr_A(|T\rangle\langle T|)) \geq \epsilon$. Now, by Uhlmann's theorem, we know there exists a purification $|T'\rangle$ of $Tr_A(|T\rangle\langle T|)$ such that $|\langle H|T'\rangle| = F(Tr_A(|H\rangle\langle H|), Tr_A(|T\rangle\langle T|)) \geq \epsilon$. Therefore, $F(|H\rangle, |T'\rangle) \geq \epsilon$ and $|H\rangle \overset{\epsilon}{=} |T'\rangle$. Note that, by the unitary equivalence of purification, we have $|T'\rangle = (U_A \otimes I_B)|T\rangle$. This means that $(U_A \otimes I_B)|T\rangle \overset{\epsilon}{=} |H\rangle$. Therefore, the QBC protocol is not ϵ-binding. □

3. Bit Commitment in Categorical Quantum Mechanics

Categorical quantum mechanics (CQM) [34–45] is the study of quantum computation and quantum foundations using category theory, as well as the graphical language closely related to category theory. In CQM, dagger monoidal categories (DMC) are used as an axiomatic basis for quantum mechanics, providing a generalization of the usual axiomatization in terms of Hilbert spaces.

Definition 5 (strict monoidal category [43]). *A strict monoidal category $\mathcal{C}$ is a category equipped with:*

1. *a parallel composition operation for objects:*

$$\otimes : ob(\mathcal{C}) \times ob(\mathcal{C}) \to ob(\mathcal{C});$$

2. *a unit object $I \in ob(\mathcal{C})$; and*
3. *a parallel composition operation for morphisms:*

$$\otimes : \mathcal{C}(A,B) \times \mathcal{C}(C,D) \to \mathcal{C}(A \otimes C, B \otimes D)$$

satisfying the following conditions:

1. *$\otimes$ is associative and unital on objects:*

$$(A \otimes B) \otimes C = A \otimes (B \otimes C) \qquad A \otimes I = A = I \otimes A;$$

2. *$\otimes$ is associative and unital on morphisms:*

$$(f \otimes g) \otimes h = f \otimes (g \otimes h) \qquad f \otimes 1_I = f = 1_I \otimes f; \text{ and}$$

3. *$\otimes$ and $\circ$ satisfy the interchange law:*

$$(g_1 \otimes g_2) \circ (f_1 \otimes f_2) = (g_1 \circ f_1) \otimes (g_2 \circ f_2).$$

Definition 6 (dagger functor †[43]). *A dagger functor for a strict monoidal category is an operation † that satisfies the following:*

- *identity on objects:* $A^\dagger = A$;
- *reserves morphisms:* $(f : A \to B)^\dagger := f^\dagger : B \to A$;
- *is involutive:* $(f^\dagger)^\dagger = f$; *and*
- *respects the symmetric monoidal category structure:*

$$(g \circ f)^\dagger = f^\dagger \circ g^\dagger \qquad (f \otimes g)^\dagger = f^\dagger \otimes g^\dagger.$$

A dagger monoidal category is a strict monoidal category equipped with a dagger functor.

Example 3. *The category of finite dimensional Hilbert spaces* ***FinHilb*** *is a DMC. In* ***FinHilb****, objects are finite-dimensional Hilbert spaces over complex numbers, morphisms are linear maps, parallel composition is the tensor product, I is the one-dimensional Hilbert spaces* $\mathbb{C}$*, and † is the adjoin operator.*

Example 4. *The category* ***Dens*** *of density operators and completely positive maps is a DMC. The objects of* ***Dens*** *are the same as the objects of* ***FinHilb****. A morphism from object* $\mathbb{C}^m$ *to object* $\mathbb{C}^n$ *is a completely positive map* $f : \mathbb{C}^{m\times m} \to \mathbb{C}^{n\times n}$*. Parallel composition is the tensor product, I is the one-dimensional Hilbert spaces* $\mathbb{C}$*, and † is the adjoin operator.*

Example 5. *The category of arbitrary dimensional Hilbert spaces* ***Hilb*** *is a DMC. In* ***Hilb****, objects are Hilbert spaces over complex numbers, morphisms are bounded linear maps, parallel composition is the tensor product, I is the one-dimensional Hilbert spaces* $\mathbb{C}$*, and † is the adjoin operator.*

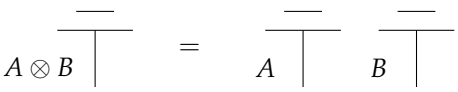
To formalize bit commitment in DMC, we further need concepts such as environment structure and purification.

3.1. Environment Structure and Purification

Definition 7 (environment structure [46]). *Let* $\mathcal{C}$ *be a dagger monoidal category. An environment structure for* $\mathcal{C}$ *is a monoidal category* $\mathcal{C}^\top$ *with the same objects as* $\mathcal{C}$*, together with a strict monoidal functor* $\mathfrak{F} : \mathcal{C} \to \mathcal{C}^\top$ *with* $\mathfrak{F}(A) = A$*, and for each object A a morphism* $\top_A : A \to I$ *in* $\mathcal{C}^\top$*, which we depict as:*

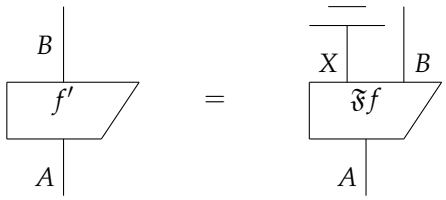
satisfying:

1. *We have* $\top_I = 1_I$*, and for all objects A and B:* $\top_{A\otimes B} = \top_A \otimes \top_B$.



2. *For morphisms* $f : A \to X \otimes B$ *and* $g : A \to X \otimes B$ *in* $\mathcal{C}$*,* $f = g$ *in* $\mathcal{C}$ *if and only if* $(\top_X \otimes 1_B) \circ \mathfrak{F}f = (\top_X \otimes 1_B) \circ \mathfrak{F}g$ *in* $\mathcal{C}^\top$.

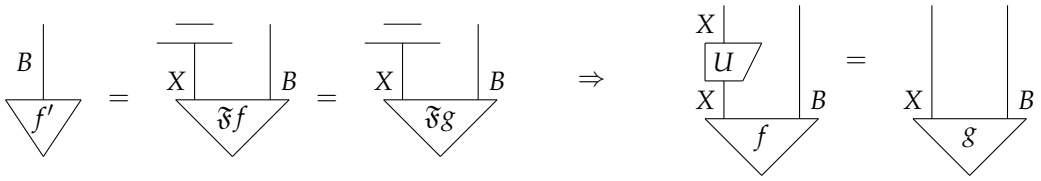
3. *For each $f' \in \mathcal{C}^\top(A,B)$, there is $f \in \mathcal{C}(A, X \otimes B)$ for some object X such that $f' = (\top_X \otimes 1_B) \circ \mathfrak{F}f$ in $\mathcal{C}^\top$. Such an f is called a purification of f'.*



Intuitively, if we think of the category $\mathcal{C}$ as consisting of pure states, then the category $\mathcal{C}^\top$ consists of mixed states. The morphisms $\top_A$ can be viewed as discarding system A to the environment, or, in other words, trace out A.

Example 6. ***Dens*** *provides an environment structure for* ***FinHilb****, in which $\top_{\mathbb{C}^n}$ is the trace operator $Tr : \mathbb{C}^{n\times n} \to \mathbb{C}$. The functor $\mathfrak{F}$ maps a liner map $f \in$ **FinHilb**$(\mathbb{C}^m, \mathbb{C}^n)$ to a completely positive operator $\mathfrak{F}f$ such that $\mathfrak{F}f(\rho) = f\rho f^\dagger$.*

Definition 8 (unitary equivalence of purification)**.** *An environment structure $\mathcal{C}^\top$ for $\mathcal{C}$ satisfies the unitary equivalence of purification if the following is satisfied: for all $B \in ob(\mathcal{C}^\top)$, $f' \in \mathcal{C}^\top(I,B)$, if $f, g \in \mathcal{C}(I, X \otimes B)$ are purifications of f', then there exists a unitary morphism $U : X \to X$ such that $(U \otimes 1_B) \circ f = g$.*



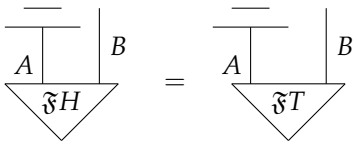
3.2. Bit Commitment in Dagger Monoidal Category

Now, we formalize bit commitment in the setting of dagger monoidal categories. We do not assume compactness in our formalization. This is because assuming compactness will impose finite dimensionality on Hilbert spaces [47]: the DMC **FinHilb** is compact, while **Hilb** is not compact. Assuming no compactness makes our formalization more general than most formalizations in the literature, which only formalize bit commitment in finite dimensional Hilbert spaces.

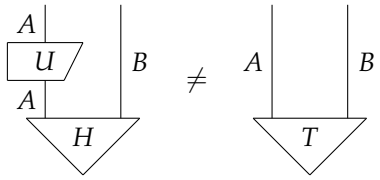
Definition 9 (bit commitment in DMC)**.** *Let $\mathcal{C}$ be a dagger monoidal category with an environment structure $\mathcal{C}^\top$. A bit commitment protocol on $(\mathcal{C}, \mathcal{C}^\top)$ consists of the following:*

1. *Two objects A and B*
2. *Two states $H, T : I \to A \otimes B$ in $\mathcal{C}$*
3. *A morphism $Open$ on $A \otimes B$ in $\mathcal{C}^\top$ such that $Open(\mathfrak{F}H) \neq Open(\mathfrak{F}T)$ in $\mathcal{C}^\top$*

A bit commitment protocol on $(\mathcal{C}, \mathcal{C}^\top)$ is concealing if $(\top_A \otimes 1_B) \circ \mathfrak{F}H = (\top_A \otimes 1_B) \circ \mathfrak{F}T$ in $\mathcal{C}^\top$.



It is binding if there is no unitary morphism $U : A \to A$ such that $(U \otimes 1_B) \circ H = T$ in $\mathcal{C}$. Equivalently, it is binding if, for all unitary morphisms $U : A \to A$, it holds that $(U \otimes 1_B) \circ H \neq T$ in $\mathcal{C}$.

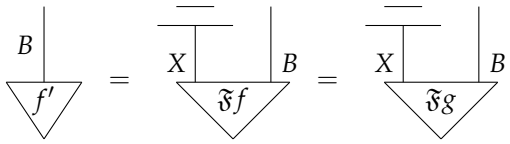


Theorem 4. *Let $\mathcal{C}$ be a dagger monoidal category with an environment structure $\mathcal{C}^\top$. The following are equivalent:*

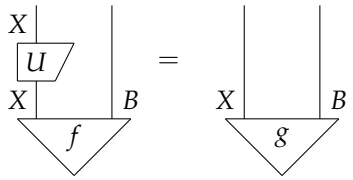
(1) The unitary equivalence of purification is satisfied.
(2) For all bit commitment protocols on $(\mathcal{C}, \mathcal{C}^\top)$, if it is concealing, then it is not binding.

Proof. (1) $\Rightarrow$ (2) Assume the unitary equivalence of purification is satisfied. If a bit commitment protocol $(A, B, H, T, Open)$ on $(\mathcal{C}, \mathcal{C}^\top)$ is concealing, then $(\top_A \otimes 1_B) \circ \mathfrak{F}H = (\top_A \otimes 1_B) \circ \mathfrak{F}T$ in $\mathcal{C}^\top$. By the third requirement in the definition of environment structure, we know H and T are two purifications of the same state. By the unitary equivalence of purification, we know there is a unitary morphism $U : A \to A$ such that $H = (U \otimes 1_B) \circ T$, which means that the bit commitment protocol is not binding.

(2) $\Rightarrow$ (1) Assume for all bit commitment protocol on $(\mathcal{C}, \mathcal{C}^\top)$, if it is concealing then it is not binding. Let B be an arbitrary object in $\mathcal{C}^\top$ and $f' \in \mathcal{C}^\top(I, B)$. Assume $f, g \in \mathcal{C}(I, X \otimes B)$ are purifications of f'. This means that $f' = (\top_X \otimes 1_B) \circ \mathfrak{F}f = (\top_X \otimes 1_B) \circ \mathfrak{F}g$.



1. If $\mathfrak{F}f = \mathfrak{F}g$, then by the second requirement in the definition of environment structure, we know that $f = g$. Now, we let $U = 1_X$. Then, it holds that $(U \otimes 1_B) \circ f = g$.
2. If $\mathfrak{F}f \neq \mathfrak{F}g$, then we design a bit commitment protocol $(X, B, f, g, Open)$ in which $Open = 1_{X \otimes B}$. Since $(\top_X \otimes 1_B) \circ \mathfrak{F}f = (\top_X \otimes 1_B) \circ \mathfrak{F}g$, we know this protocol is concealing. Hence, it cannot be binding, which means there is a unitary morphism $U : X \to X$ such that $(U \otimes 1_B) \circ f = g$.



To conclude, no matter $\mathfrak{F}f = \mathfrak{F}g$ or $\mathfrak{F}f \neq \mathfrak{F}g$, the unitary equivalence of purification is satisfied. □

4. Related Work and Discussion

4.1. An Alternative Notion of Bindingness

The definition of bindingness described in Section 2 essentially says that Alice cannot change $|H\rangle$ to $|T\rangle$ by operating on the quantum system under her control. This definition is reasonable, but not uniquely reasonable. Another reasonable definition of bindingness, which says that Alice cannot change $Open(|H\rangle\langle H|)$ to $Open(|T\rangle\langle T|)$ by operating on the quantum system under her control, is formally given as follows.

Definition 10 (ϵ-posterior binding)**.** *A quantum bit commitment protocol is ϵ-posterior binding if there is no unitary U on A such that $Open((U \otimes I_B)|H\rangle\langle H|(U^\dagger \otimes I_B)) \overset{\epsilon}{=} Open(|T\rangle\langle T|)$.*

We can prove that, if a QBC protocol is ϵ-concealing, then it is not ϵ-posterior binding by combining Theorem 3 and the following theorem.

Theorem 5. *If a quantum bit commitment protocol is not ϵ-binding, then it is not ϵ-posterior binding.*

Proof. If a QBC protocol is not ϵ-binding, then there is a unitary map U on A such that $(U \otimes I_B)|H\rangle \stackrel{\epsilon}{=} |T\rangle$. Therefore, $F((U \otimes I_B)|H\rangle, |T\rangle) \geq \epsilon$. Note that $F((U \otimes I_B)|H\rangle, |T\rangle) = F((U \otimes I_B)|H\rangle\langle H|(U^\dagger \otimes I_B), |T\rangle\langle T|)$. Now, by the monotonicity of the fidelity function under quantum operations [32], we know that $F(Open((U \otimes I_B)|H\rangle\langle H|(U^\dagger \otimes I_B)), Open(|T\rangle\langle T|)) \geq F((U \otimes I_B)|H\rangle\langle H|(U^\dagger \otimes I_B), |T\rangle\langle T|) = F((U \otimes I_B)|H\rangle, |T\rangle) \geq \epsilon$. Therefore, the QBC protocol is not ϵ-posterior binding. □

4.2. Mixed State Formalization of QBC

To the best of our knowledge, the most mathematically involved formalization of QBC was given by D'Ariano et al. [27] and Chiribella et al. [28]. In their formalization, the original state is a mixed state and the strategies that Alice and Bob can use are represented by super operators. These super operators are decomposed to a sequence of super operators to characterize the actions Alice and Bob may take at different steps of the protocol. Some distance functions between super operators are adopted to define ϵ-concealing and ϵ-binding.

Since super operators on mixed states can be represented by linear maps on pure states with some ancillary states by the Stinespring dilation, we conject that our formalism is equivalent to the mixed state formalism. A detailed comparison of these formalism is left as future work.

5. Conclusions and Future Work

In this paper, we first provide a very simple proof of the no-go theorem of quantum bit commitment and its quantitative generalization. Then, we formalize the no-go theorem in the theory of dagger monoidal categories. We show that, in the setting of dagger monoidal categories, the impossibility of bit commitment is equivalent to the unitary equivalence of purification.

The presented material also indicates some directions for future research:

1. Sikora and Selby [48] formalized bit commitment in generalized probabilistic theories and showed that the no-go theorem holds by presenting a quantitative trade-off between Alice's and Bob's cheating probabilities. A comparison between our formalization and theirs will be carried out in the future.
2. It was shown by Kent et al. [5–7,12] that perfect bit commitment is possible in the theory of relativity. Baez [49] pointed out that, from a categorical perspective, the theory of relativity and quantum theory resemble each other quite well. DMC plays an important role in both theories. In particular, nCob, the DMC which contains manifold as object and cobordism as morphism, plays an important role in general relativity. It will be interesting to formalize bit commitment in nCob and use it to analyze the similarity and difference of quantum theory and the theory of relativity.
3. We also plan to apply the axiomatic and graphical language of categorical quantum mechanics in the formal verification of concrete QBC protocols in the future.
4. The MLC no-go theorem does not rule out the feasibility of designing secure QBC in practice. Several practically secure QBC protocols have been devised and experimentally implemented in the last decade [50–52]. The security of those protocols typically relies on the current technological limitation on non-demolition measurement and long-term quantum memory. The implementation of those protocols often uses quantum optical devices such as nanosecond pulse laser, single mode optical fiber, and Mach–Zehnder interferometer for the generation, communication, and operation of non-entangled photons. With the recent development on the generation and manipulation of entangled photons [53], in the future,we are also interested in implementing QBC protocols based on (low-dimensional) entangled states [9,16].

Author Contributions: Conceptualization, X.S. and Q.W.; Formal analysis, X.S.; Methodology, F.H.; Validation, Q.W.; Writing – original draft, X.S.; Writing – review and editing, F.H. All authors have read and agreed to the published version of the manuscript.

Funding: The project is funded by the Minister of Science and Higher Education within the program under the name "Regional Initiative of Excellence" in 2019-2022, project number: 028/RID/2018/19, the amount of funding: 11 742 500 PLN.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Bennetta, C.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **1984**, *560*, 175–179. [CrossRef]
2. Hardy, L.; Kent, A. Cheat Sensitive Quantum Bit Commitment. *Phys. Rev. Lett.* **2004**, *92*, 1–4. [CrossRef] [PubMed]
3. Buhrman, H.; Christandl, M.; Hayden, P.; Lo, H.K.; Wehner, S. Possibility, impossibility, and cheat sensitivity of quantum-bit string commitment. *Phys. Rev. A* **2008**, *78*, 1–10. [CrossRef]
4. Shimizu, K.; Fukasaka, H.; Tamaki, K.; Imoto, N. Cheat-sensitive commitment of a classical bit coded in a block of m × n round-trip qubits. *Phys. Rev. A* **2011**, *84*, 1–14. [CrossRef]
5. Kent, A. Unconditionally secure bit commitment with flying qudits. *New J. Phys.* **2011**, *13*, 1–16. [CrossRef]
6. Kent, A. Unconditionally Secure Bit Commitment by Transmitting Measurement Outcomes. *Phys. Rev. Lett.* **2012**, *109*, 130501. [CrossRef]
7. Lunghi, T.; Kaniewski, J.; Bussières, F.; Houlmann, R.; Tomamichel, M.; Kent, A.; Gisin, N.; Wehner, S.; Zbinden, H. Experimental Bit Commitment Based on Quantum Communication and Special Relativity. *Phys. Rev. Lett.* **2013**, *111*, 180504. [CrossRef]
8. He, G.P. Simplified quantum bit commitment using single photon nonlocality. *Quantum Inf. Process.* **2014**, *13*, 2195–2211. doi:10.1007/s11128-014-0728-8. [CrossRef]
9. Li, Y.; Wen, Q.; Li, Z.; Qin, S.; Yang, Y. Cheat sensitive quantum bit commitment via pre- and post-selected quantum states. *Quantum Inf. Process.* **2014**, *13*, 141–149. [CrossRef]
10. Adlam, E.; Kent, A. Device-independent relativistic quantum bit commitment. *Phys. Rev. A* **2015**, *92*, 1–9. [CrossRef]
11. Lunghi, T.; Kaniewski, J.; Bussières, F.; Houlmann, R.; Tomamichel, M.; Wehner, S.; Zbinden, H. Practical Relativistic Bit Commitment. *Phys. Rev. Lett.* **2015**, *115*, 030502. [CrossRef] [PubMed]
12. Verbanis, E.; Martin, A.; Houlmann, R.; Boso, G.; Bussières, F.; Zbinden, H. 24-Hour Relativistic Bit Commitment. *Phys. Rev. Lett.* **2016**, *117*, 140506. [CrossRef] [PubMed]
13. Song, Y.; Yang, L. Practical Quantum Bit Commitment Protocol Based on Quantum Oblivious Transfer. *Appl. Sci.* **2018**, *8*, 1990. doi:10.3390/app8101990. [CrossRef]
14. Nagy, M.; Nagy, N. An Information-Theoretic Perspective on the Quantum Bit Commitment Impossibility Theorem. *Entropy* **2018**, *20*, 193. doi:10.3390/e20030193. [CrossRef]
15. He, G.P. Unconditionally secure quantum bit commitment based on the uncertainty principle. *Proc. R. Soc. Math. Phys. Eng. Sci.* **2019**, *475*, 20180543.
16. Zhou, L.; Sun, X.; Su, C.; Liu, Z.; Choo, K.R. Game theoretic security of quantum bit commitment. *Inf. Sci.* **2019**, *479*, 503–514. doi:10.1016/j.ins.2018.03.046. [CrossRef]
17. Brassard, G.; Crépeau, C. Quantum Bit Commitment and Coin Tossing Protocols. In *Advances in Cryptology—CRYPTO '90, Proceedings of the 10th Annual International Cryptology Conference, Santa Barbara, CA, USA, 11–15 August 1990*; Menezes, A., Vanstone, S.A., Eds.; Springer: Berlin/Heidelberg, Germany, 1990, pp. 49–61.
18. Brassard, G.; Crépeau, C.; Jozsa, R.; Langlois, D. A Quantum Bit Commitment Scheme Provably Unbreakable by both Parties. In Proceedings of the 34th Annual Symposium on Foundations of Computer Science, Palo Alto, CA, USA, 3–5 November 1993; IEEE Computer Society: Washington, DC, USA, 1993, pp. 362–371. doi:10.1109/SFCS.1993.366851. [CrossRef]
19. Mayers, D. Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.* **1997**, *78*, 3414–3417. [CrossRef]

20. Lo, H.K.; Chau, H.F. Is Quantum Bit Commitment Really Possible? *Phys. Rev. Lett.* **1997**, *78*, 3410–3413. [CrossRef]
21. Lo, H.K.; Chau, H.F. Why quantum bit commitment and ideal quantum coin tossing are impossible. *Phys. Nonlinear Phenom.* **1998**, *120*, 177–187. [CrossRef]
22. Yuen, H. Unconditionally Secure Quantum Bit Commitment Is Possible. 2000. Available online: https://arxiv.org/abs/quant-ph/0006109 (accessed on 6 January 2020).
23. Yuen, H. Unconditionally Secure Quantum Bit Commitment. 2005. Available online: https://arxiv.org/abs/quant-ph/0505132 (accessed on 6 January 2020).
24. Nambu, Y.; Chiba-Kohno, Y. Information-Theoretic Description of No-go Theorem of a Bit Commitment. 2000. Available online: https://arxiv.org/abs/quant-ph/0011068 (accessed on 6 January 2020).
25. Spekkens, R.W.; Rudolph, T. Degrees of concealment and bindingness in quantum bit commitment protocols. *Phys. Rev. A* **2001**, *65*, 012310. doi:10.1103/PhysRevA.65.012310. [CrossRef]
26. He, G.P. Security bound of cheat sensitive quantum bit commitment. *Sci. Rep.* **2015**, *5*, 9398. [CrossRef] [PubMed]
27. D'Ariano, G.M.; Kretschmann, D.; Schlingemann, D.; Werner, R.F. Reexamination of quantum bit commitment: The possible and the impossible. *Phys. Rev. A* **2007**, *76*, 032328. doi:10.1103/PhysRevA.76.032328. [CrossRef]
28. Chiribella, G.; D'Ariano, G.M.; Perinotti, P.; Schlingemann, D.; Werner, R. A short impossibility proof of quantum bit commitment. *Phys. Lett. A* **2013**, *377*, 1076–1087. doi:10.1016/j.physleta.2013.02.045. [CrossRef]
29. Cohn-Gordon, K. Commitment Algorithms. Master's Thesis, University of Oxford, Oxford, UK, 2012.
30. Heunen, C.; Kissinger, A. Can Quantum Theory Be Characterized in Terms of Information-Theoretic Constraints? 2016. Available online: http://homepages.inf.ed.ac.uk/cheunen/publications/2016/cbh/cbh.pdf (accessed on 6 January 2020).
31. Clifton, R.; Bub, J.; Halvorson, H. Characterizing Quantum Theory in Terms of Information-Theoretic Constraints. *Found. Phys.* **2003**, *33*, 1561–1591. [CrossRef]
32. Watrous, J. *The Theory of Quantum Information*; Cambridge University Press: Cambridge, UK, 2018.
33. Nielsen, M.; Chuang, I. *Quantum Computation and Quantum Information*; Cambridge University Press: Cambridge, UK, 2011.
34. Abramsky, S.; Coecke, B. A Categorical Semantics of Quantum Protocols. In Proceedings of the 19th IEEE Symposium on Logic in Computer Science (LICS 2004), Turku, Finland, 14–17 July 2004; IEEE Computer Society: Washington, DC, USA, 2004, pp. 415–425. doi:10.1109/LICS.2004.1319636. [CrossRef]
35. Selinger, P. Dagger Compact Closed Categories and Completely Positive Maps: (Extended Abstract). *Electr. Notes Theor. Comput. Sci.* **2007**, *170*, 139–163. doi:10.1016/j.entcs.2006.12.018. [CrossRef]
36. Coecke, B.; Duncan, R. Interacting Quantum Observables. In *Automata, Languages and Programming, Proceedigs of the 35th International Colloquium, ICALP 2008, Reykjavik, Iceland, 7–11 July 2008, Part II—Track B: Logic, Semantics, and Theory of Programming & Track C: Security and Cryptography Foundations*; Lecture Notes in Computer Science; Aceto, L., Damgård, I., Goldberg, L.A., Halldórsson, M.M., Ingólfsdóttir, A., Walukiewicz, I., Eds.; Springer: Berlin/Heidelberg, Germany, 2008; Volume 5126, pp. 298–310. doi:10.1007/978-3-540-70583-3_25. [CrossRef]
37. Vicary, J. Categorical Formulation of Finite-dimensional C*-algebras. *Electr. Notes Theor. Comput. Sci.* **2011**, *270*, 129–145. doi:10.1016/j.entcs.2011.01.012. [CrossRef]
38. Coecke, B.; Duncan, R. Interacting quantum observables: categorical algebra and diagrammatics. *New J. Phys.* **2011**, *13*, 1–85. [CrossRef]
39. Coecke, B.; Wang, Q.; Wang, B.; Wang, Y.; Zhang, Q. Graphical Calculus for Quantum Key Distribution (Extended Abstract). *Electr. Notes Theor. Comput. Sci.* **2011**, *270*, 231–249. doi:10.1016/j.entcs.2011.01.034. [CrossRef]
40. Selinger, P. Finite Dimensional Hilbert Spaces are Complete for Dagger Compact Closed Categories (Extended Abstract). *Electr. Notes Theor. Comput. Sci.* **2011**, *270*, 113–119. doi:10.1016/j.entcs.2011.01.010. [CrossRef]
41. Coecke, B.; Perdrix, S. Environment and classical channels in categorical quantum mechanics. *Log. Methods Comput. Sci.* **2012**, *8*, 1–24. [CrossRef]
42. Backens, M. The ZX-calculus is complete for stabilizer quantum mechanics. *New J. Phys.* **2014**, *16*, 093021. doi:10.1088/1367-2630/16/9/093021. [CrossRef]

43. Coecke, B.; Kissinger, A. *Picturing Quantum Processes: A First Course in Quantum Theory and Diagrammatic Reasoning*; Cambridge University Press: Cambridge, UK, 2017.
44. Zhou, L.; Wang, Q.; Sun, X.; Kulicki, P.; Castiglione, A. Quantum technique for access control in cloud computing II: Encryption and key distribution. *J. Netw. Comput. Appl.* **2018**, *103*, 178–184. doi:10.1016/j.jnca.2017.11.012. [CrossRef]
45. Hadzihasanovic, A.; Ng, K.F.; Wang, Q. Two complete axiomatisations of pure-state qubit quantum computing. In Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2018, Oxford, UK, 9–12 July 2018; Dawar, A., Grädel, E., Eds.; ACM: New York, NY, USA, 2018; pp. 502–511. doi:10.1145/3209108.3209128. [CrossRef]
46. Coecke, B.; Heunen, C. Pictures of complete positivity in arbitrary dimension. *Inf. Comput.* **2016**, *250*, 50–58. doi:10.1016/j.ic.2016.02.007. [CrossRef]
47. Heunen, C. Compactly Accessible Categories and Quantum Key Distribution. *Log. Methods Comput. Sci.* **2008**, *4*. doi:10.2168/LMCS-4(4:9)2008. [CrossRef]
48. Sikora, J.; Selby, J. Simple proof of the impossibility of bit commitment in generalized probabilistic theories using cone programming. *Phys. Rev. A* **2018**, *97*, 1–5. [CrossRef]
49. Baez, J. Quantum Quandaries: A Category-Theoretic Perspective. In *The Structural Foundations of Quantum Gravity*; Rickles, D., French, S., Saatsi, J.T., Eds.; Oxford Scholarship Online: Oxford, UK, 2006.
50. Danan, A.; Vaidman, L. Practical quantum bit commitment protocol. *Quantum Inf. Process.* **2012**, *11*, 769–775. doi:10.1007/s11128-011-0284-4. [CrossRef]
51. Loura, R.; Almeida, A.J.; André, P.S.; Pinto, A.N.; Mateus, P.; Paunković, N. Noise and measurement errors in a practical two-state quantum bit commitment protocol. *Phys. Rev. A* **2014**, *89*, 052336. doi:10.1103/PhysRevA.89.052336. [CrossRef]
52. Loura, R.; Arsenović, D.c.v.; Paunković, N.; Popović, D.c.v.B.; Prvanović, S. Security of two-state and four-state practical quantum bit-commitment protocols. *Phys. Rev. A* **2016**, *94*, 062335. doi:10.1103/PhysRevA.94.062335. [CrossRef]
53. Li, C.; Jiang, Z.; Zhang, Y.; Zhang, Z.; Wen, F.; Chen, H.; Zhang, Y.; Xiao, M. Controlled Correlation and Squeezing in Pr^{3+} : Y_2SiO_5 to Yield Correlated Light Beams. *Phys. Rev. Appl.* **2017**, *7*, 014023. doi:10.1103/PhysRevApplied.7.014023. [CrossRef]