Characterising the intersection of QMA and coQMA

Serge Massar\textsuperscript{1} · Miklos Santha\textsuperscript{2,3}

Received: 8 February 2021 / Accepted: 23 October 2021 / Published online: 23 November 2021
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2021

Abstract
We show that the functional analogue of $\text{QMA} \cap \text{coQMA}$, denoted $\text{F}(\text{QMA} \cap \text{coQMA})$, equals the complexity class Total Functional QMA (TFQMA). To prove this, we need to introduce an alternative definition of \text{QMA} \cap \text{coQMA} in terms of a single quantum verification procedure. We show that if TFQMA equals the functional analogue of BQP (FBQP), then QMA \cap coQMA = BQP. We show that if there is a QMA complete problem that (robustly) reduces to a problem in TFQMA, then QMA \cap coQMA = QMA. Our results thus imply that if some of the inclusions between functional classes FBQP \subseteq TFQMA \subseteq FQMA are in fact equalities, then the corresponding inclusions in BQP \subseteq QMA \cap coQMA \subseteq QMA are also equalities.

Keywords Quantum complexity classes · QMA · coQMA · Total functional QMA · Intersection of QMA and coQMA

1 Introduction

Functional NP (FNP) is the class of search problems defined by polynomial time relations $M(x, y)$ (the verifier) where the length of $y$ is polynomial in the length of $x$. On an input $x$, the task is to find a witness $y$ (if it exists) such that $M$ accepts $(x, y)$.

The complexity class Total Functional NP (TFNP), introduced in [1], is the subset of FNP for which it can be shown that for all inputs $x$, there exists at least one witness $y$. It lies between Functional P (FP) (the subclass of FNP for which a witness can be found in polynomial time) and FNP.
TFNP contains many natural and important problems, including factoring, local search problems [2–4], computational versions of Brouwer’s fixed point theorem [5], finding Nash equilibria [6,7]. Although there probably do not exist complete problems for TFNP, there are many syntactically defined subclasses of TFNP that contain complete problems, and for which some of the above natural problems can be shown to be complete. For recent work in this direction, see [8].

One of the results of the founding paper [1] concerns the relation between Total Functional NP and other complexity classes. The inclusions

\[ \text{FP} \subseteq \text{TFNP} \subseteq \text{FNP} \quad (1) \]

are obvious. But what would be the consequences if some of these inclusions were not strict, but replaced by equality?

In [1], this question is connected with the inclusions

\[ \text{P} \subseteq \text{NP} \cap \text{coNP} \subseteq \text{NP} \quad (2) \]

It was first shown in [1] that Total Functional NP equals the functional analogue of \( \text{NP} \cap \text{coNP} \) denoted \( \text{F}(\text{NP} \cap \text{coNP}) \):

\[ \text{TFNP} = \text{F}(\text{NP} \cap \text{coNP}) \quad (3) \]

Furthermore, it is proven in [1] that an inclusion in Eq. (1) is strict if and only if the corresponding inclusion in Eq. (2) is strict. The inclusions in Eq. (2) are believed to be strict, as there are problems, such as factoring, that belong to \( \text{NP} \cap \text{coNP} \) but are believed to not belong to \( \text{P} \), and there are problems such as 3-SAT that belong to \( \text{NP} \) but are thought not to belong to \( \text{coNP} \). This result therefore provides strong evidence that the inclusions in Eq. (1) are strict. The proofs of these results are very simple, and take only one paragraph, or are even just implicit in [1].

The quantum analogue of \( \text{NP} \) is \( \text{QMA} \) [9]. \( \text{QMA} \) has been extensively studied and contains a rich set of complete problems, see e.g. [10]. Functional \( \text{QMA} \), the problem of producing a quantum state that serves as witness for a \( \text{QMA} \) problem, was first introduced in [11].

In a recent work [12], we introduced the complexity class Total Functional QMA (TFQMA), the subset of \( \text{FQMA} \) for which it can be shown that for all inputs \( x \), there exists at least one witness \( |\psi\rangle \). TFQMA is an expressive class containing several interesting problems. However, in [12] the analog of the complexity results of [1] for TFQMA where left open. Here we prove these results.

The analogs of Eqs. (1) and (2) are

\[ \text{FBQP} \subseteq \text{TFQMA} \subseteq \text{FQMA} \quad (4) \]

and

\[ \text{BQP} \subseteq \text{QMA} \cap \text{coQMA} \subseteq \text{QMA}. \quad (5) \]
We first show that TFQMA equals the functional analogue of QMA ∩ coQMA:

$$\text{TFQMA} = F(\text{QMA} \cap \text{coQMA}).$$ (6)

We then show that if FBQP = TFQMA, then BQP = QMA ∩ coQMA. We finally show that if there is a QMA complete problem that reduces (using a slightly stronger notion of reduction than the natural one, which we call robust reduction) to a problem in TFQMA, then QMA ∩ coQMA = QMA.

But while the proofs in the classical case are elementary, the quantum proofs are more delicate.

Showing that TFQMA = F(QMA ∩ coQMA) requires a detailed enquiry into what is the correct definition of F(QMA ∩ coQMA). The difficulty is that any language $L$ in QMA ∩ coQMA is naturally defined by two quantum verification procedures $Q$ and $Q'$. But these two quantum verification procedures do not necessarily commute. Therefore, it is not clear how to define a witness for QMA ∩ coQMA. Indeed, given an input $x$ and a state $|\psi\rangle$, one cannot test whether both $Q(x, |\psi\rangle)$ and $Q'(x, |\psi\rangle)$ accept, since the act of carrying out one of these tests will modify the state $|\psi\rangle$ and render impossible the other test.

We will see that the solution to this conundrum is to append to the state a bit $z \in \{0, 1\}$, with the convention that if $z = 0$ one only tests $Q$, and if $z = 1$ one only tests $Q'$. Thus, a witness for QMA ∩ coQMA has the form $|z\rangle|\psi\rangle$.

However, while this solution is natural, it is not clear whether it is the unique way to solve this problem. In order to address this, we need a deeper understanding of QMA ∩ coQMA. To this end, we introduce two alternative definitions of QMA ∩ coQMA. The more important is a definition in terms of a single 2-outcome quantum verification procedure which takes as input a single witness. This definition is particularly useful because it allows us to apply to QMA ∩ coQMA the notions of eigenbasis, spectrum, and eigenspace of a quantum verification procedure which we introduced in [12] (based on the earlier work of Marriott and Watrous [13]). These notions are then used to provide a natural definition for F(QMA ∩ coQMA) which parallels the definition for FQMA given in [12].

Furthermore, by extending the notion of QMA amplification as developed in [13], we show that our definition of F(QMA ∩ coQMA) is independent of the completeness and soundness bounds.

Together these results allow us to define precisely the right hand side of Eq. (6), in such a way that it has the same structure as the left hand side of Eq. (6). Proving the equality of the two quantities is then rather easy.

The paper is structured as follows:

Sections 2 to 7 set the stage, defining quantum verification procedures, QMA, coQMA, QMA ∩ coQMA, Functional QMA, Total Functional QMA, and recalling the key notions of eigenbasis, spectrum and eigenspaces of a quantum verification procedure. It closely follows, with appropriate modifications, our recent work [12] on TFQMA.

Section 8 introduces the notion of reduction in quantum verification procedures, including the notion of robust reduction mentioned above.

Section 9 recalls the notion of eigenspace preserving map introduced in [12].
Section 10 introduces “iterative procedures”, thereby generalising an idea introduced in [13]. Iterative procedures modify the acceptance probabilities of eigenstates of a quantum verification procedure without changing the eigenstates themselves. We use iterative procedures to show in Theorem 10 that the spectrum of a quantum verification procedure can be modified to a very large extent.

As a first application of iterative procedures, we introduce in Sect. 12 the notion of “nondestructive” procedure which outputs both a classical bit indicating whether the procedure accepts or rejects and a quantum state, in such a way that if the input state is an eigenstate, the output state is also the eigenstate. We show that, essentially without loss of generality, one can take quantum verification procedures to be nondestructive.

In Sect. 13, we present the two additional definitions of $\text{QMA} \cap \text{coQMA}$ mentioned above. We show that the three definitions are equivalent. We then introduce in Sect. 14 functional $\text{QMA} \cap \text{coQMA}$ and use the results of Sect. 10 to show that this definition does not depend on the soundness and completeness thresholds.

In Sect. 15, we show that $F(\text{QMA} \cap \text{coQMA})$ equals the class Total Functional $\text{QMA}$ (TFQMA).

Section 16 contains the proof that if $\text{FBQP} = \text{TFQMA}$, then $\text{BQP} = \text{QMA} \cap \text{coQMA}$.

And finally in Sect. 17 we prove that if there exists a $\text{QMA}$ complete problem that robustly reduces to a problem in TFQMA, then $\text{QMA} = \text{QMA} \cap \text{coQMA}$.

In appendix, we sketch how similar results hold for the classical probabilistic classes MA and coMA. We recommend that the reader interested in the details of the proofs of the paper read appendix simultaneously with the rest of the paper, as it explains which parts of our proofs are quantum and which parts are in fact classical.

2 Preliminary definitions

We denote by $\mathcal{H}_n$ the Hilbert space of $n$ qubits. For pure states, we use the Dirac ket notation $|\psi\rangle$, whereas for density matrices we just use the Greek letter $\rho$. We denote by $|0^k\rangle$ the state of $k$ qubits all in the $|0\rangle$ state. We denote by $I_m$ the identity operator acting on $m$ qubits.

We denote by poly the set of all nonzero polynomials with nonnegative integer coefficients. Note that if $f \in \text{poly}$, then $f$ maps positive integers to positive integers.

We denote by $1/\text{poly}$ the set of all functions that are the inverse of a polynomial in poly:

$$1/\text{poly} = \{g : \mathbb{N} \to \mathbb{R} : \exists p \in \text{poly} \text{ AND } g = 1/p\}.$$ (7)

3 Quantum verification procedures

Definition 1 ($d$-Outcome Quantum Verification Procedure.) For any integer $d$ larger or equal to 2, a $d$-outcome quantum verification procedure is a polynomial time uniform family of quantum circuits $Q = \{Q_n : n \in \mathbb{N}\}$ with $Q_n$ taking as input $(x, |\psi\rangle \otimes |0^k\rangle)$, where $x \in \{0, 1\}^n$ is a binary string of length $n$, $|\psi\rangle$ is a state of $m$ qubits, and both
m = m(n) and k = k(n) belong to poly. The last k qubits, initialised to the state \(|0^k]\), form the ancilla Hilbert space \(\mathcal{H}_k\), and the m-qubit states \(|\psi]\) form the witness Hilbert space \(\mathcal{H}_m\). The outcome of the run of \(Q_n\) is a word \(w \in \{0, \ldots, d - 1\}\). It is obtained by measuring the first \(\lceil \log d \rceil\) qubits in the computational basis, interpreting the result as an integer in \(\{0, \ldots, 2^{\lceil \log d \rceil} - 1\}\) and, if this integer is greater or equal to \(d\), replacing it by \(d - 1\). We denote this outcome by \(Q_n(x, |\psi]\)).

In most of this article, we will consider 2-outcome quantum verification procedures. For brevity, throughout this work we use the following terminology which is standard in the literature:

**Definition 2 (Quantum Verification Procedure).** A 2-outcome quantum verification procedure is called a quantum verification procedure.

Note that a \(d\)-outcome quantum verification procedure can of course also take as input a mixed state \(\rho\), rather than a pure state \(|\psi]\). Mixed states can be written as convex combinations of pure states. The acceptance (rejection) probability for the mixed state is the convex combination of the acceptance (rejection) probabilities for the constituent pure states.

In order to simplify notation, in what follows we will mainly consider the case where \(Q_n\) takes as input a pure state. In view of the above remark, the extension to mixed state inputs is immediate. In some cases, the argument requires that \(Q_n\) takes as input a mixed state, in which case, abusing slightly the notation, we write \(Q_n(x, \rho)\) for the outcome of the quantum verification procedure on the mixed state \(\rho\).

### 4 QMA

**Definition 3 ((a,b)-Quantum Verification Procedure).** Let \(a, b : \mathbb{N} \rightarrow (0, 1)\) be polynomially time computable functions which satisfy

\[
a(n) - b(n) \geq 1/q(n),
\]

for some \(q \in \text{poly}\). We say that a quantum verification procedure \(Q\) is an \((a, b)\)-quantum verification procedure (or shortly an \((a, b)\)-procedure) if for every \(x\) of length \(n\), one of the following holds:

\[
\exists |\psi]\), \Pr[Q_n(x, |\psi]\) = 1] \geq a,
\]

\[
\forall |\psi]\), \Pr[Q_n(x, |\psi]\) = 1] \leq b.
\]

We call \(a\) and \(b\) the completeness and soundness probabilities of the quantum verification procedure.

Note that taking the completeness or soundness probabilities equal 1 or 0 requires a specific formulation dealing with exact quantum computation, which while theoretically interesting is not implementable in practice (real quantum computation will have some, possibly exponentially small, error probability). One of the results of the present
work is to show that several complexity classes do not depend on the completeness and soundness probabilities used to define them. More precisely, in these results we show that the completeness and soundness probabilities can be taken exponentially close to 1 and 0, respectively. These results do not extend to showing that $a$ and $b$ can be taken equal to 1 and 0. For these reasons, we explicitly exclude in Definition 3 and all similar definitions the cases when $a = 1$ and $b = 0$, and take them to belong to the open interval $(0, 1)$.

**Definition 4 (QMA and coQMA).** Let $a, b$ be functions as in Definition 3. The class $\text{QMA}(a, b)$ is the set of languages $L \subseteq \{0, 1\}^*$ such that there exists an $(a, b)$-procedure $Q$, where for every $x$, we have $x \in L$ if and only if $a$ holds (and consequently, $x \notin L$ if and only if $b$ holds).

We call $Q$ a quantum verification procedure for $L$, and for $x \in L$, we say that a $|\psi\rangle$ satisfying Eq. (9) is a witness for $x$.

The class $\text{coQMA}(a, b)$ is the set of languages $L \subseteq \{0, 1\}^*$ such that there exists an $(a, b)$-quantum verification procedure $Q'$, where for every $x$, we have $x \notin L$ if and only if $\exists |\psi\rangle$ satisfying Eq. (9) holds (and consequently, $x \in L$ if and only if $\forall |\psi\rangle$ satisfying Eq. (9) holds).

**Definition 5 (QMA $\cap$ coQMA).** Let $a, b$ and $a', b'$ be pairs of functions as in Definition 3. The class $\text{QMA} \cap \text{coQMA}(a, b; a', b')$ is the set of languages $L \subseteq \{0, 1\}^*$ such that $L \in \text{QMA}(a, b)$ and $L \in \text{coQMA}(a', b')$.

More explicitly, $\text{QMA} \cap \text{coQMA}$ is the class of languages $L \subseteq \{0, 1\}^*$ such that there exist an $(a, b)$-procedure $Q = \{Q_n\}$ and an $(a', b')$-procedure $Q' = \{Q'_n\}$, such that for every $x$ we have $x \in L$ if and only if both the following hold:

$$\exists |\psi\rangle, \Pr[Q_n(x, |\psi\rangle) = 1] \geq a,$$

$$\forall |\psi\rangle, \Pr[Q'_n(x, |\psi\rangle) = 1] \leq b';$$

and $x \notin L$ if and only if both the following hold:

$$\forall |\psi\rangle, \Pr[Q_n(x, |\psi\rangle) = 1] \leq b,$$

$$\exists |\psi\rangle, \Pr[Q'_n(x, |\psi\rangle) = 1] \geq a'.$$

It is of course essential to understand to what extent the above definitions depend on the bounds $(a, b)$ and $(a', b')$. It was shown by Kitaev that the separation $a - b$ in the definition of QMA could be amplified exponentially by using multiple copies of the input state, and multiple copies of the verification circuit [9], that is, by increasing both $m$ and $k$. This was further improved in [13] (see also [14]) where it was shown that by running forwards and backwards the original quantum verification procedure, only one copy of the input state was needed to obtain the same amplification, that is, one needs only increase $k$.

**Theorem 1 (QMA Amplification [9,13,14]).** Let $a, b$ be functions as in Definition 3. For any polynomial $r$, we have $\text{QMA}(a, b) \subseteq \text{QMA}(1 - 2^{-r}, 2^{-r})$.

As a consequence of Theorem 1, the precise values of the bounds $(a, b)$ are irrelevant. Traditionally, they are taken to be $2/3$ and $1/3$. We will do here the same.
Definition 6 We define the class $\text{QMA}$ as $\text{QMA}(2/3, 1/3)$.

Definition 7 We define the class $\text{QMA} \cap \text{coQMA}$ as $\text{QMA} \cap \text{coQMA}(2/3, 1/3; 2/3, 1/3)$.

Definition 8 (a-Total Quantum Verification Procedure). Let $a : \mathbb{N} \to [0, 1]$ be a polynomially time computable function. We say that a quantum verification procedure is an $a$-total quantum verification procedure (or shortly an $a$-total procedure) if for every $x$ of length $n$, the following holds:

$$\exists |\psi\rangle, \Pr[Q_n(x, |\psi\rangle) = 1] \geq a.$$ (15)

Note that an $a$-total procedure is also an $(a, b)$-procedure for all $b$ satisfying the conditions of Definition 3. Note that the language associated with an $a$-total procedure is $L = \{0, 1\}^*$. That is the decision problem for total procedures is trivial, since for all $x \in \{0, 1\}^*$ there exists a witness for $x$. Therefore, for total procedures, the only interesting questions concern the witnesses. The main topic of the present work is to understand the relation between $a$-total procedures and $\text{QMA} \cap \text{coQMA}$.

5 BQP

5.1 Efficiently implementable channels and states

Recall that a quantum channel is a completely positive (CP) trace preserving map between spaces of operators.

Definition 9 (Efficiently implementable quantum channel). A family $\Phi$ of efficiently implementable quantum channels is defined by a polynomial time uniform family of quantum circuits $Q = \{Q_n : n \in \mathbb{N}\}$ with $Q_n$ taking as input $(x, |\psi\rangle \otimes |0^k\rangle)$ where $x \in \{0, 1\}^n$, where $|\psi\rangle \in \mathcal{H}_m$ where $m = m(n)$ and $k = k(n)$ belong to poly, and the output of the channel is obtained by keeping the first $m'$ qubits and tracing over the remaining $m + k - m'$ qubits, where where $m' = m'(n)$ belongs to poly and $m' \leq m + k$. We denote the output of the channel by $\Phi(x, |\psi\rangle)$:

$$\Phi(x, |\psi\rangle) = \text{Tr}_{m+k-m'}Q_n(x, |\psi\rangle \otimes |0^k\rangle).$$ (16)

Note that a quantum channel can of course also act on a mixed state $\rho$ of $m$ qubits.

Definition 10 (Efficiently preparable states). Let $m' \in \text{poly}$. A family of density matrices $\{\rho(x) : x \in \{0, 1\}^n, n \in \mathbb{N}\}$ is efficiently preparable if $\rho(x)$ acts on $\mathcal{H}_{m'(n)}$ and if there exists a polynomial time uniform family of quantum circuits $Q = \{Q_n : n \in \mathbb{N}\}$ with $Q_n$ taking as input $(x, |0^k\rangle)$ with $x \in \{0, 1\}^n$, with $k = k(n)$ belonging to poly and $k \geq m'$, and where $\rho(x)$ is obtained by tracing out the last $k - m'$ qubits of $Q_n(x)$.

This definition is equivalent to saying that a family of efficiently preparable states $\{\rho(x)\}$ is the output of a family of efficiently implementable quantum channels $\Phi$ which does not take any quantum state as input, i.e. if one sets $m = 0$ in Definition 9: $\rho(x) = \Phi(x, \emptyset)$. 

Springer
5.2 BQP

Bounded-error quantum polynomial time (BQP) is the class of decision problems solvable by a quantum computer in polynomial time, with bounded error probability for all instances. We give two equivalent definitions of BQP, following the formulation of [12].

**Definition 11** (BQP). Let $a, b$ be functions as in Definition 3. The class $BQP(a, b)$ is the set of languages $L \subseteq \{0, 1\}^*$ such that there exists an $(a, b)$-procedure $Q = \{Q_n : n \in \mathbb{N}\}$, with $Q_n$ taking as input $(x, |0^k\rangle)$ (i.e. there is no witness Hilbert space), where $x \in \{0, 1\}^n$ is a binary string of length $n$ and where for every $x$ we have

\[
x \in L \iff \Pr[Q_n(x) = 1] \geq a, \tag{17}
\]

\[
x \notin L \iff \Pr[Q_n(x) = 1] \leq b. \tag{18}
\]

By repeating the procedure a polynomial number of times, the thresholds can be made exponentially close to 1 and 0, respectively. Therefore, the exact values of the bounds $a$ and $b$ are irrelevant. Traditionally they are taken to be $2/3$ and $1/3$. We will do here the same.

**Definition 12** We define the class BQP as $BQP(2/3, 1/3)$.

We give an alternative definition of BQP which is closer to the definition of QMA.

**Definition 13** (The language class $BQP'$). Let $a, b$ be functions as in Definition 3. Let $BQP'(a, b) \subseteq QMA(a, b)$ be the set of languages $L \subseteq \{0, 1\}^*$ such that there exists:

1. an $(a, b)$ quantum verification procedure $Q = \{Q_n : n \in \mathbb{N}\}$ with $Q_n$ taking as input $(x, |\psi\rangle \otimes |0^k\rangle)$, where $x \in \{0, 1\}^n$ is a binary string of length $n$, $|\psi\rangle$ is a state of $m$ qubits, with $m, k \in \text{poly}$;
2. an efficiently preparable set of density matrices $\{\rho(x)\}$ where $\rho(x)$ acts on $\mathcal{H}_m$;

and where for every $x$, we have $x \in L$ if and only if

\[
\Pr[Q_n(x, \rho(x)) = 1] \geq a, \tag{19}
\]

and $x \notin L$ if and only if

\[
\forall |\psi\rangle, \Pr[Q_n(x, |\psi\rangle) = 1] \leq b. \tag{20}
\]

**Theorem 2** ($BQP'$=BQP[12]). For all $a, b$ functions as in Definition 3, $BQP'(a, b) = BQP$.

6 Structure of the witness space

The witness space has a structure that will be central in what follows. This structure can be derived using the methods of [13,14] based on Jordan’s lemma, or more easily using the structure of the POVM element corresponding to the quantum verification procedure accepting, see [15]. We repeat here the formulation of [12].
Theorem 3 (Structure of witness space [13,15]). Given a quantum verification procedure $Q = \{Q_n\}$, for all $x \in \{0, 1\}^n$, there exists a basis $B_Q(x) = \{|\psi_i\rangle : 1 \leq i \leq 2^m\}$ of the witness space $\mathcal{H}_m$ such that the acceptance probability of linear combinations of the basis states does not involve interferences, that is, for all $\alpha_i$ such that $\sum_i |\alpha_i|^2 = 1$, we have

$$\Pr[Q_n(x, \sum_i \alpha_i|\psi_i\rangle) = 1] = \sum_i |\alpha_i|^2 \Pr[Q_n(x, |\psi_i\rangle) = 1].$$

(21)

Definition 14 (Eigenbasis, spectrum and eigenspaces of a quantum verification procedure). Given a quantum verification procedure $Q = \{Q_n\}$, for all $x \in \{0, 1\}^n$ and for any eigenbasis $B_Q(x) = \{|\psi_i\rangle\}$ of $Q$ for $x$,

1. for all $|\psi_i\rangle \in B_Q(x)$, we call

$$p_i = \Pr[Q_n(x, |\psi_i\rangle) = 1]$$

(22)

the acceptance probability of $|\psi_i\rangle$;

2. we call the set of acceptance probabilities the spectrum of $Q$ for $x$:

$$\text{Spect}(Q, x) = \{p \in [0, 1] : \exists |\psi_i\rangle \in B_Q(x) \text{ such that } \Pr[Q_n(x, |\psi_i\rangle) = 1] = p\};$$

(23)

3. for $p \in \text{Spect}(Q, x)$, we call

$$\mathcal{H}_Q(x, p) = \text{Span}(\{|\psi_i\rangle \in B_Q(x) : \Pr[Q_n(x, |\psi_i\rangle) = 1] = p\})$$

(24)

the eigenspace of $Q$ for $x$ with acceptance probability $p$.

Theorem 4 (Uniqueness of the spectrum and eigenspaces of $Q$ [12,15]). Given a quantum verification procedure $Q = \{Q_n\}$, for all $x \in \{0, 1\}^*$, the spectrum $\text{Spect}(Q, x)$ of $Q$ and the eigenspaces $\mathcal{H}_Q(x, p)$ of $Q$ with acceptance probability $p \in \text{Spect}(Q, x)$ are unique and do not depend on the choice of eigenbasis $B_Q(x)$.

The spectrum of quantum verification procedures plays an important role in the study of QMA and related complexity classes. It is closely related (but distinct) from the energy spectrum of local Hamiltonians. Several complexity classes with conditions on the spectrum have been studied, such as Polynomially Gaped QMA (PGQMA) in which the gap between the largest and second largest eigenvalue is inverse polynomial [15], and Exponentially Gaped QMA (EGQMA) in which the gap between the largest and second largest eigenvalue is exponentially small [16].

7 Functional classes

In this section, we are interested in the set of states on which a quantum verification procedure $Q$ accepts with high probability. We may also be interested in the set of
states on which $Q$ rejects with high probability. These sets will allow us to characterise
the functional analogs of the complexity classes introduced previously.

There are two approaches to characterising these sets. The first is based on the
notion of witness introduced in Definition 4. The second uses the notion of eigenbasis
of a quantum verification procedure, see Theorems 3 and 4.

7.1 Functional classes based on witnesses

**Definition 15 (Accepting density matrices).** Let $Q = \{Q_n\}$ be a quantum verification
procedure and fix $a \in [0, 1]$.

We define the following relations over binary strings and density matrices:

\[
R^\geq_a(x, \rho) = 1 \text{ if } \Pr[Q_n(x, \rho) = 1] \geq a, \tag{25}
\]

\[
R^\leq_a(x, \rho) = 1 \text{ if } \Pr[Q_n(x, \rho) = 1] \leq a. \tag{26}
\]

To simplify notation, we denote

\[
R^\geq_a(x) = \left\{ \rho : R^\geq_a(x, \rho) = 1 \right\}, \tag{27}
\]

\[
R^\leq_a(x) = \left\{ \rho : R^\leq_b(x, \rho) = 1 \right\}. \tag{28}
\]

Consider an $(a, b)$-procedure $Q$. We are interested in the functional task of outputting a witness for $Q$ and in defining the corresponding complexity class. This motivates the following definitions, where the subscript $W$ stands for “Witness”.

**Definition 16 (Witness based definition of Functional QMA (FQMA$_W$)).** Let $a, b$ be functions as in Definition 3. The class FQMA$_W(a)$ is the set \{ $R^\geq_a(x, \rho)$ \} where $Q$ is an $(a, b)$-procedure.

We can also define the functional class total functional QMA.

**Definition 18 (Witness based definition of total Functional QMA (TFQMA$_W$)).** Let $a : \mathbb{N} \to [0, 1]$ be a polynomially time computable function. The class TFQMA$_W(a) \subseteq$ FQMA$_W(a)$ is the set of relations \{ $R^\geq_a(x, \rho)$ \} where $Q$ is an $a$-total procedure.

7.2 Functional classes based on eigenstates

The above definitions are natural. However, they are not completely satisfactory for
several reasons.
First, we do not know whether FQMA\(_W(a)\) is independent of the threshold \(a\). We obviously have that FQMA\(_W(a') \subseteq FQMA\(_W(a)\) if \(a' \leq a\), but we do not know if the reverse is true, as FQMA\(_W(a)\) does not transform simply under amplification.

Second, while the sets \(R^{\geq a}_Q(x, \rho)\) are convex, they are not closed under linear combinations of pure states. That is, if the projectors onto \(|\psi\rangle\) and \(|\psi'\rangle\) belong to \(R^{\geq a}_Q(x, \rho)\), then the projector onto the linear combination \(a|\psi\rangle + b|\psi'\rangle\) does not necessarily belong to \(R^{\geq a}_Q(x, \rho)\).

Third, the very useful concept of eigenstate and eigenspace is not captured by the functional classes based on witnesses. This is illustrated in the following example:

**Example 1** Consider a function \(\delta : \mathbb{N} \to [0, 1/3]\) that decreases faster than \(1/\text{poly}(n)\) for any polynomial \(\text{poly}(n)\), for instance \(\delta(n) = 2^{-n^2}\). The example consists of a \((1/3, 2/3)\)-quantum verification procedure \(Q^{\text{example}}\) whose spectrum is the set

\[
\text{Spect}(Q^{\text{example}}, x) = \left\{ \frac{1}{3}, \frac{2}{3} - \delta^2(n), \frac{2}{3} + \delta(n) \right\}
\]

where \(n = |x|\).

Let us denote by \(|\psi_{2/3+\delta}\rangle\) and \(|\psi_{2/3-\delta^2}\rangle\) two eigenstates with acceptance probability \(2/3 + \delta\) and \(2/3 - \delta^2\), respectively. Then, the following state

\[
|\psi\rangle = \sqrt{\frac{\delta}{1 + \delta}} |\psi_{2/3+\delta}\rangle + \sqrt{\frac{1}{1 + \delta}} |\psi_{2/3-\delta^2}\rangle
\]

(30)

is a witness (it has acceptance probability \(2/3\)) and hence belongs to \(R_Q(x, \cdot)\). But it has exponentially small overlap with the eigenspace \(H_Q(x, \frac{2}{3} + \delta(n))\).

These difficulties are avoided by the following definitions, based on the notion of eigenspace of a quantum verification procedure.

**Definition 19** (*Accepting and rejecting subspaces*). Let \(Q = \{Q_n\}\) be a quantum verification procedure and fix \(a, b \in [0, 1]\).

We define the following relations over binary strings and quantum states:

\[
H^{\geq a}_Q(x, |\psi\rangle) = 1 \text{ if } |\psi\rangle \in \text{Span}(\{H_Q(x, p) : p \geq a\}),
\]

(31)

\[
H^{\leq b}_Q(x, |\psi\rangle) = 1 \text{ if } |\psi\rangle \in \text{Span}(\{H_Q(x, p) : p \leq b\}),
\]

(32)

where \(H_Q(x, p)\) are the eigenspaces of \(Q\) for \(x\).

To simplify notation, we denote

\[
H^{\geq a}_Q(x) = \left\{ |\psi\rangle : H^{\geq a}_Q(x, |\psi\rangle) = 1 \right\},
\]

(33)

\[
H^{\leq b}_Q(x) = \left\{ |\psi\rangle : H^{\leq b}_Q(x, |\psi\rangle) = 1 \right\},
\]

(34)

and we will generally express results in terms of the subspaces \(H^{\geq a}_Q(x), H^{\leq b}_Q(x)\), rather than the corresponding relations.
These relations provide the basis for an alternative definition of functional classes. These classes are denoted without the subscript $W$.

**Definition 20** (Functional QMA ($F\text{QMA}$)). Let $a, b$ be functions as in Definition 3. The class $F\text{QMA}(a, b)$ is the set $\{(H^\geq_Q(x, |\psi\rangle), H^\leq_Q(x, |\psi\rangle))\}$ of pairs of relations, where $Q$ is an $(a, b)$-verification procedure.

This definition is in terms of two relations $(H^\geq_Q$ and $H^\leq_Q$) for reasons which were presented in [12].

One can show that this definition of $F\text{QMA}$ does not depend on the bounds $(a, b)$:

**Theorem 5** (FQMA is independent of the soundness and completeness bounds [12]). Let $Q$ be a quantum verification procedure. Let $a, b$ be a pair of functions as in Definition 3. For any $r \in \text{poly}$ and pair of functions $a', b'$ as in Definition 3 satisfying $a' < 1 - 2^{-r}$ and $b' > 2^{-r}$, we have $F\text{QMA}(a, b) \subseteq F\text{QMA}(a', b')$.

Hence, we take the traditional values $2/3$ and $1/3$:

**Definition 21** We define the class $F\text{QMA}$ as $F\text{QMA}(2/3, 1/3)$.

We introduced $a$-total procedures in Definition 8. We can now define the corresponding functional classes.

**Definition 22** (Totality). A pair of relations $(H^\geq_Q(x, |\psi\rangle), H^\leq_Q(x, |\psi\rangle))$ in $F\text{QMA}(a, b)$ is called total if for all inputs $x$ there exists at least one witness $|\psi\rangle$, i.e. if $H^\geq_Q(x)$ is non empty.

**Definition 23** (Total Functional QMA ($T\text{FQMA}$)). Let $a, b$ be functions as in Definition 3. The class $T\text{FQMA}(a, b)$ is the set $\{(H^\geq_Q(x, |\psi\rangle), H^\leq_Q(x, |\psi\rangle))\}$ of pairs of total relations, i.e. the set of pairs of relations in $F\text{QMA}$ where $Q$ is an $a$-total verification procedure.

Theorem 5 implies that we can take the thresholds to have their traditional values:

**Definition 24** We define the class of total relations in $F\text{QMA}$ as $T\text{FQMA} = T\text{FQMA}(2/3, 1/3)$.

A similar definition can be given for the functional analog of BQP. However, the definition of BQP is that there is a witness that can be efficiently prepared. Therefore, functional BQP needs to be expressed in terms of the existence of an efficiently preparable witness. The definition $F\text{BQP}_W$ thus seems the natural one in this case.

### 7.3 Relation between the two definitions of functional QMA

We discuss here how the two definitions of Functional QMA are related.

**Theorem 6** (Relation between definitions of Functional QMA [12]). Let $a, b$ be functions as in Definition 3 and let $Q$ be an $(a, b)$-procedure. Then
1. we have the inclusion
\[ \mathcal{H}_{Q}^{\geq a}(x) \subseteq R_{Q}^{\geq a}(x), \]
where we view \( \mathcal{H}_{Q}^{\geq a}(x) \) not as a set of pure states, but as the set of density matrices associated with these pure states. It also holds that the convex hull of \( \mathcal{H}_{Q}^{\geq a}(x) \) is included in \( R_{Q}^{\geq a}(x) \). In general, these inclusions are strict, see Example 1 for an illustration.

2. In the other direction, if \( R_{Q}^{\geq a}(x) \) is nonempty, then \( \mathcal{H}_{Q}^{\geq a}(x) \) is nonempty.

8 Reductions

8.1 Reductions in procedures

**Definition 25 (Reduction).** Let \( a, b \) and \( a', b' \) be pairs of functions as in Definition 3.

Let \( L \) be a language in QMA\( (a, b) \), and denote by \( Q = \{ Q_{n} : n \in \mathbb{N} \} \) the associated \( (a, b) \)-quantum verification procedure.

Let \( L' \) be a language in QMA\( (a', b') \), and denote by \( Q' = \{ Q'_{n} : n \in \mathbb{N} \} \) the associated \( (a', b') \)-quantum verification procedure.

A reduction from \( Q \) to \( Q' \) is a pair \((f, \Phi)\) where \( f : \mathbb{N} \to \mathbb{N} \) is a polynomial time computable function and \( \Phi \) is a family of efficiently implementable channel, such that:

1. For all \( x \in L \), it holds that \( f(x) \in L' \).
   In other words, for all \( x \) such that there exists \( |\psi\rangle \) satisfying
   \[ \Pr[Q_{|x|}(x, |\psi\rangle) = 1] \geq a \]
   (i.e. \( |\psi\rangle \) is a witness for \( Q \) for \( x \)), it holds that there exists \( |\psi'\rangle \) satisfying
   \[ \Pr[Q'_{|f(x)|}(f(x), |\psi'\rangle) = 1] \geq a', \]
   (i.e. \( |\psi'\rangle \) is a witness for \( Q' \) for \( f(x) \)).

2. For all \( x \), for all witnesses \( |\psi'\rangle \) for \( Q' \) for \( f(x) \), it holds that \( \Phi(x, |\psi'\rangle) \) is a witness for \( Q \) for \( x \).
   In other words, for all \( x \), for all \( |\psi'\rangle \) such that
   \[ \Pr[Q'_{|f(x)|}(f(x), |\psi'\rangle) = 1] \geq a', \]
   it holds that
   \[ \Pr[Q_{|x|}(x, \Phi(x, |\psi'\rangle) = 1] \geq a. \]

To illustrate this definition, we recall briefly Kitaev’s construction that \( k \)-local-Hamiltonian is QMA complete [9].
The $k$-local Hamiltonian problem, which is a promise problem, is defined as follows. The input $x$ is a classical description of a $k$-local Hamiltonian acting on $n$ qubits, where we recall that a $k$-local Hamiltonian $H$ is the sum of polynomially many Hermitian matrices (whose norm is bounded by a polynomial) that act on only $k$ qubits. The input also contains two numbers $a < b$, such that $b - a \in 1/poly$. The problem is to determine whether the smallest eigenvalue of this Hamiltonian is less than $a$ or greater than $b$, promised that one of these is the case.

Kitaev showed that if $Q \in QMA$, then for every instance $x$, there exists an instance $f(x)$ of $k$-local Hamiltonian—which we write $H(f(x))$—such that:

1) if $x \in L$, there exists a low energy eigenstate of $H(f(x))$;
2) if $x \notin L$, then $H(f(x))$ does not have low energy eigenstates.

Recall that the witnesses in Kitaev’s construction have the form

$$\frac{1}{\sqrt{L} + 1} \sum_{j=0}^{L} U_j(|\psi\rangle|0^k\rangle)|j\rangle$$  \hspace{1cm} (40)

where the first register is the witness space, the second register is the ancilla space, and the third register is the time counter, $L$ is the number of gates in $Q$, and $U_j$ is the unitary that implements the $j$ first gates of the procedure $Q$ (with $U_0$ the identity).

A reduction from $Q$ to $k$-local Hamiltonian consists of: 1) the function $f(x)$; 2) the channel $\Phi_1$ which consists in measuring the time counter of the witness to obtain $j$ and then undo the computation conditional on $j$ (i.e. apply $U_j^\dagger$).

**Theorem 7** Let $a, b, a', b', L, L', Q, Q'$ be functions, languages and procedures as in Definition 25.

Suppose $(f, \Phi)$ is a reduction from $Q$ to $Q'$.

Then there exists an $(a, b)$-procedure $Q^R$ such that

- The language associated with $Q^R$ is $L$;
- If $|\psi\rangle$ is a witness for $Q'$ for $f(x)$, then $|\psi\rangle$ is a witness for $Q^R$ for $x$, or expressed differently

$$R_{Q'}^{a'}(f(x)) \subseteq R_{Q^R}^a(x)$$  \hspace{1cm} (41)

**Proof** Trivial. The procedure $Q^R$ is given by $Q^R(x, |\psi\rangle) = Q(x, \Phi(|\psi\rangle))$. \hfill \Box

We note that it would be interesting to generalise slightly the definition of reduction in procedures, and only require that the channel $\Phi$ succeeds with probability greater than $1/poly$. For instance in the case of a reduction from $Q$ to $k$-local Hamiltonian, the channel $\Phi$ could consists in measuring the time counter of the witness and rejecting except if the result is $j = 0$. However, as the above discussion of $k$-local Hamiltonian suggests, a channel $\Phi$ that always succeeds seems sufficient. In the present work, we will suppose that $\Phi$ always succeeds. The case where $\Phi$ is probabilistic would be interesting to study, but is a nontrivial generalisation. For instance, it is not obvious whether Theorem 7 holds in this case.
Definition 26 (QMA Completeness). Let \( a, b \) be functions as in Definition 3.

Let \( L \) be a language in QMA\((a, b)\), and denote by \( Q = \{ Q_n : n \in \mathbb{N} \} \) the associated \((a, b)\)-quantum verification procedure.

The procedure \( Q \) is QMA-complete if, for every \( a', b' \) functions as in Definition 3, for every language \( L' \) in QMA\((a', b')\) with \( Q' = \{ Q'_n : n \in \mathbb{N} \} \) the associated \((a', b')\)-quantum verification procedure, there exists a reduction from \( Q' \) to \( Q \).

8.2 Robust reductions

For many questions concerning QMA, the above notion of reduction is sufficient. However, Example 1 shows that it may not be appropriate in some cases. Suppose there exists a reduction \((f, \Phi)\) from a procedure \( Q_{\text{example}} \) to procedure \( Q \). This reduction tells us how the witness of \( Q_{\text{example}} \) (the eigenstates which accept with probability \( 2/3 + \delta \)) transforms under \( \Phi \). But it tells us nothing about how eigenstates with acceptance probability \( 2/3 - \delta^2 \) transform under \( \Phi \). But these eigenstates are operationally indistinguishable (except possibly by using the structure of \( Q_{\text{example}} \)) from the genuine witnesses, since their acceptance probability is so close to \( 2/3 \).

In Sect. 17, we will need a slightly stronger form of reduction which we call robust reduction, and which does not suffer from this problem.

Definition 27 (Robust Reduction). Let \( a, b, a', b', L, L', Q, Q' \) be functions, languages and procedures as in Definition 25.

Recall that \( a' - b' \geq 1/q' \) for some \( q' \in \text{poly} \). Let \( \epsilon \in 1/\text{poly} \) be such that \( \epsilon \leq 1/(2q') \). (As a consequence \( a' - \epsilon \) lies between \( a' \) and \( b' \), at a distance \( \geq 1/\text{poly} \) from either bound).

A robust reduction from \( Q \) to \( Q' \) with parameter \( \epsilon \) is a reduction from \( Q \) to \( Q' \) via the pair \((f, \Phi)\) where condition 2 of Definition 25 is replaced by the stronger condition

\[ a' - \epsilon, (42) \]

it holds that

\[ a, (43) \]

Note that a robust reduction with parameter \( \epsilon = 0 \) is a reduction according to Definition 25.

Proposition 1 The following hold for all \( \epsilon, \epsilon' \geq 0 \):

1. A robust reduction with parameter \( \epsilon \) is also a robust reduction with parameter \( \epsilon' \) for all \( 0 \leq \epsilon' \leq \epsilon \).
2. Transitivity of reductions. If there exists a robust reduction from \( Q \) to \( Q' \) with parameter \( \epsilon \), and if there exists a robust reduction from \( Q' \) to \( Q'' \) with parameter \( \epsilon' \), then there exists a robust reduction from \( Q \) to \( Q'' \) with parameter \( \epsilon' \).

\( \text{Springer} \)
Proof Immediate. □

We note that \(k\)-local Hamiltonian is also QMA complete using the stronger notion of robust reduction. This follows from the promise that the smallest eigenvalue of the \(k\)-local Hamiltonian is less than \(a\) or greater than \(b\). This, together with the fact that we need robust reductions to prove Theorem 18, suggests that robust reductions may in fact be the natural notion to use when considering reductions in procedures.

9 Eigenspace preserving maps

Reductions (robust or not) do not preserve the eigenspace structure of a quantum verification procedure. The following definitions and results repeated from [12] define a mapping between procedures that preserves this structure.

Definition 28 (Eigenspace preserving map of quantum verification procedures). Let \(Q\) and \(Q'\) be two quantum verification procedures with the same witness space dimensions. We say that there exists an eigenspace preserving map from \(Q\) to \(Q'\) if there exists a polynomial time computable strictly increasing family of functions \(\{f_n : n \in \mathbb{N}\}\), \(f_n : [0, 1] \rightarrow [0, 1]\), such that for all \(x \in \{0, 1\}^*\) with \(n = |x|\):

1. there exists a basis \(B_Q(x) = \{|\psi_i\rangle\}\) of the witness Hilbert space \(\mathcal{H}_m\) which is a joint eigenbasis of \(Q\) and \(Q'\) for \(x\);
2. for all \(|\psi_i\rangle \in B_Q(x)\) with \(p_i = \Pr[Q_n(x, |\psi_i\rangle) = 1]\) the acceptance probability of \(|\psi_i\rangle\) for \(Q_n\), and \(p'_i = \Pr[Q'_n(x, |\psi_i\rangle) = 1]\) the acceptance probability of \(|\psi_i\rangle\) for \(Q'_n\), it holds that \(p'_i = f_n(p_i)\).

In what follows, we will refer to an eigenspace preserving map simply as an e-map.

The reason why we require that the functions \(f_n\) be polynomial time computable is because we wish that the soundness and completeness thresholds of \(Q\) be mapped onto the soundness and completeness thresholds of \(Q'\), where we recall that the soundness and completeness thresholds must be polynomial time computable, see Definition 3. That is, if \(Q\) is an \((a, b)\)-procedure that e-maps to \(Q'\) via \(f_n\), then \(Q'\) is an \(a', b'\)-procedure with \(a'(n) = f_n(a(n))\) and \(b'(n) = f_n(b(n))\).

Proposition 2 ([12]) The following hold:

1. Conservation of eigenspaces. If \(Q\) e-maps to \(Q'\) via \(\{f_n\}\), then the eigenspace of \(Q\) for \(x\) with acceptance probability \(p\) equals the eigenspace of \(Q'\) for \(x\) with acceptance probability \(f_n(p)\):

\[
\mathcal{H}_Q(x, p) = \mathcal{H}_{Q'}(x, f_n|_x(p)).
\]

2. Conservation of accepting and rejecting subspaces. Let \(Q\) be an \((a, b)\)-procedure and let \(Q'\) be an \((a', b')\), and suppose that \(Q\) e-maps to \(Q'\) via \(f_n\) with \(a'(n) = f_n(a(n))\) and \(b'(n) = f_n(b(n))\), then

\[
\mathcal{H}^{\geq a}_Q(x) = \mathcal{H}^{\geq a'}_{Q'}(x),
\]
\[
\mathcal{H}^{\leq b}_Q(x) = \mathcal{H}^{\leq b'}_{Q'}(x).
\]
3. Transitivity of reductions. If $Q$ e-maps to $Q'$, and $Q'$ e-maps to $Q''$, then $Q$ e-maps to $Q''$.

Eigenspace preserving maps are characterised by the family of functions $\{f_n\}$. What freedom do we have in choosing the functions $f_n$? The next section introduced iterative procedures, which are of interest in themselves. Iterative procedures are then used in Sect. 11 to show that we have a lot of freedom in choosing the functions $f_n$.

10 Iterative procedures

The amplification result for $FQMA$, Theorem 5, is based on the method introduced in [13] in which a quantum verification procedure is run repeatedly backwards and forwards. Here we generalise this approach.

Definition 29 (Iterative Procedures). Let $Q = \{Q_n : n \in \mathbb{N}\}$ be a quantum verification procedure with parameters $m$ (the size of the witness space) and $k$ (the size of the ancilla space).

Recall that the Hilbert space $\mathcal{H}$ on which $Q_n$ acts can be decomposed into $\mathcal{H} = \mathcal{H}_m^w \otimes \mathcal{H}_k^a$ where $\mathcal{H}_m^w$ is the witness Hilbert space comprising $m$ qubits, and $\mathcal{H}_k^a$ is the ancilla Hilbert space comprising $k$ qubits. The Hilbert space can also be decomposed into $\mathcal{H} = \mathcal{H}_{m+k-1}^{\text{out}} \otimes \mathcal{H}_{m+k-1}^{\text{rest}}$ where $\mathcal{H}_{m+k-1}^{\text{out}}$ of dimension 2 is the qubit which is measured at the end of the quantum verification procedure, and $\mathcal{H}_{m+k-1}^{\text{rest}}$ is the Hilbert space of the remaining $m+k-1$ qubits.

Define the following two projectors

$$\Pi_0 = I_m \otimes |0^k\rangle\langle 0^k|$$

$$\Pi_1 = V_x^\dagger (|0\rangle \langle 0| \otimes I_{m+k-1}^{\text{rest}}) V_x$$

where $V_x$ is the unitary transformation realised by the quantum verification procedure. That is $\Pi_0$ projects onto valid inputs to the quantum verification procedure, and $\Pi_1$ projects onto states on which the quantum verification procedure will accept with certainty.

Let $N \in \text{poly}$ and let

$$G = \{g_n : \{0, \ldots, N(n)\} \to \{0, 1\} : x \in \mathbb{N}\}$$

be a family of polynomially time computable functions.

The $(N, G)$-iterative procedure obtained from $Q$ is a quantum verification procedure $Q_{it}$ with the same witness space dimension $m$ as $Q$, and an ancilla space which we decompose into a first space of $k$ qubits (the same dimension as for $Q$) and an additional working space of dimension $k'$. This second space can be classical. The input space of $Q_{it}$ is thus $\mathcal{H}_m \otimes \mathcal{H}_k \otimes \mathcal{H}_{k'}$. We view the projectors $\Pi_0$ and $\Pi_1$ as acting on the space $\mathcal{H}_m^w \otimes \mathcal{H}_k$.

On input $(x, |\psi\rangle |0^k\rangle |0^k\rangle)$ with $|\psi\rangle \in \mathcal{H}_m$, $Q_{it}$ acts as follows:

1. Repeat until $N + 1$ measurement outcomes have been registered:
(a) measure \( \{\Pi_0, 1 - \Pi_0\} \); 
(b) measure \( \{\Pi_1, 1 - \Pi_1\} \).

(Note: the result of the first measurement will necessarily be 1 since the initial state of the first \( m + k \) qubits \((|\psi\rangle |0^k\rangle)\) is an eigenstate of \( \Pi_0 \) with eigenvalue 1).

2. Inspect the sequence of results.

(a) If results \( i \) and \( i + 1 \) differ set \( z_i = 0 \); 
(b) while if results \( i \) and \( i + 1 \) are equal set \( z_i = 1 \).

3. Set \( s = \sum_{i=1}^{N} z_i \).

4. Generate a random bit \( c \in \{0, 1\} \) satisfying \( \Pr[c = 1] = g_{|x|}(s) \) and \( \Pr[c = 0] = 1 - g_{|x|}(s) \).

5. Output \( c \).

Note that, in view of step 2, the functions \( g_n(s) \in [0, 1] \) can be interpreted as probability distributions over the set \( \{0, 1\} \). One can extend the above generalised amplification procedure and take the \( g_n(s) \) to be probability distributions over the alphabet \( \{0, \ldots, d - 1\} \), in which case the generalised amplification would yield a \( d \)-outcome quantum verification procedure.

A particularly interesting case of iterative procedure is when the \( g_n \) are threshold functions:

\[
g_n(s) = 0 \text{ if } s < s_0(n) \\
= 1 \text{ if } s \geq s_0(n)
\]

for some polynomial time computable function \( s_0 : \mathbb{N} \to \mathbb{N} \) with \( s_0(n) \in \{0, \ldots, N(n)\} \). The QMA amplification described in [13] is based on a threshold iterative procedure.

In the following, we will denote by \( f(k; N, p) \) the probability mass function of the binomial distribution with parameters \( N \) and \( p \). Thus, if

\[
X \sim B(N, p),
\]

then

\[
f(k; N, p) = \Pr[X = k] = \binom{N}{k} p^k (1 - p)^{N-k}.
\]

In addition, for any \( g : \{0, \ldots, N\} \to [0, 1] \), we denote by \( P_g \) the function

\[
P_g : [0, 1] \to [0, 1] \quad : p \to P_g(p) = E[g(X)] = \sum_{k=0}^{N} f(k; N, p) g(k).
\]
Theorem 8 (Properties of Iterative Procedures). Let \( Q = \{ Q_n : n \in \mathbb{N} \} \) be a quantum verification procedure, let \((N, G)\) be as in Definition 29, and let \( Q_{it} \) be the \((N, G)\)-iterative procedure obtained from \( Q \). Then, the following hold:

1. There exists a basis \( B_Q(x) = \{ |\psi_i\rangle \} \) of the witness Hilbert space \( \mathcal{H}_m \) which is a joint eigenbasis of \( Q \) and \( Q_{it} \) for \( x \).
2. Let \( |\psi_i\rangle \) be an eigenstate of \( Q \) for \( x \) (and therefore also an eigenstate of \( Q_{it} \) for \( x \)). Denote by \( p_i \) and \( p'_i \) the acceptance probabilities of \( |\psi_i\rangle \) for \( Q \) and \( Q_{it} \), respectively. If the initial state of the witness space is \( |\psi_i\rangle \), then the following hold:
   
   (a) The variables \( z_i \) defined in step 2 are \( 0 - 1 \) i.i.d. random variables satisfying \( \Pr[z_i = 1] = p_i \) (i.e. equals the acceptance probability of \( |\psi_i\rangle \)).
   (b) The acceptance probabilities of the iterative procedure are given by
       \[
       p'_i = P_{g_n}(p_i) = \sum_{k=0}^{N} f(k; N, p_i) g_n(k) \tag{53}
       \]
       where \( n = |x| \).
   (c) Whenever at step (a) Definition 29 the outcome of measurement \( \{ \Pi_0, 1 - \Pi_0 \} \) is \( 1 \), the state of the witness space is the original witness \( |\psi_i\rangle \).

Proof Not given. Simple application of the construction in [13].

11 Iterative procedures and eigenspace preserving maps

We now show how iterative procedures can be used to construct e-maps.

The results in the present section are purely classical, and can be phrased as the following problem. Given \( N \) draws from a coin with bias \( p \), generate a new coin with bias \( f(p) \), where \( p \) is unknown, but the function \( f : [0, 1] \rightarrow [0, 1] \) is known. To this end, introduce a function \( g : \{0, \ldots, N\} \rightarrow [0, 1] \), and upon finding that \( k \) of the coins come out head, toss a coin with bias \( g(k) \). The coin so obtained will have bias \( p' = \sum_{k=0}^{N} f(k; N, p) g(k) \). This is Eq. (53).

In addition, we need to impose the further conditions: the function \( f \) is strictly increasing (see Definition 28 of e-maps), and both \( f \) and \( g \) are polynomial time computable (see Definitions 28 and 29).

First we show in Theorem 9 that, under the natural condition that the function \( g \) is increasing and non constant, the function \( f \) is strictly increasing.

Second, we show in Theorem 10 that by choosing the function \( g \) appropriately, we have a lot of freedom in choosing the function \( f \). More precisely, we show that for any \( M \), if \( N \) is large enough we can choose \( g \) so that \( f \) is strictly increasing and passes through \( M \) predefined points \((s_i, t_i)\), i.e. \( f(s_i) = t_i \), where \( i = 1, \ldots, M \) (to which we add the points \((0, 0)\) and \((1, 1)\)). The main remaining condition is that the \( s_i \) have inverse polynomial gaps.
Theorem 9 (Iterative procedures with increasing functions \( g_n \) are eigenspace preserving maps). Given a quantum verification procedure \( Q \), and \((N, G = \{g_n\})\) as in Definition 29 with the functions \( g_n : \{0, \ldots, N\} \rightarrow [0, 1] \) increasing and nonconstant (by this we mean that \( g(k + 1) \geq g(k) \) and \( g(N) > g(0) \)), then \( Q \) e-maps to the \((N, G)\)-generalised amplification procedure \( Q_{it} \) obtained from \( Q \).

Proof The condition that \( g \) is increasing and nonconstant implies that there is some \( k_0 \in \{0, \ldots, N - 1\} \) such that \( g(k_0 + 1) > g(k_0) \) (with a strict inequality).

We need to show that under the conditions that the functions \( g_n \) are polynomial time computable, increasing and nonconstant, \( p'_i \) given in Eq. (53), viewed as a function of \( p_i \), is a polynomial time computable strictly increasing function.

It is therefore sufficient to show that for any polynomial time computable strictly increasing function \( g \), the function \( P_g(p) \) defined in Eq. (52) is a polynomial time computable strictly increasing function of \( p \).

The fact that \( P_g(p) \) is polynomial time computable follows immediately from the fact that the functions \( g_n \) are polynomial time computable.

We now show that \( P_g(p) \) is strictly increasing.

First note that for all \( p \in [0, 1] \), we have

\[
1 = \sum_{k=0}^{N} f(k; N, p). \tag{54}
\]

Taking the derivative of Eq. (54) with respect to \( p \), we have

\[
0 = \sum_{k=0}^{N} \binom{N}{k} p^{k-1} (1 - p)^{N-k-1} (k - Np). \tag{55}
\]

(Note that as written this expression is well defined only for \( 0 < p < 1 \). However, the limits \( p \to 0 \) and \( p \to 1 \) are finite. We extend Eq. (55) and all expressions below to \( p = 0 \) and \( p = 1 \) by replacing the ill-defined terms by their limit). Hence,

\[
\sum_{k=0}^{\lfloor Np \rfloor} \binom{N}{k} p^{k-1} (1 - p)^{N-k-1} (Np - k)
= \sum_{k=\lfloor Np \rfloor}^{N} \binom{N}{k} p^{k-1} (1 - p)^{N-k-1} (k - Np), \tag{56}
\]

where we note that all terms under summation signs are positive.
Now take the derivative of Eq. (52) with respect to $p$ to obtain

$$\frac{\partial P_g}{\partial p} = \sum_{k=0}^{N} \binom{N}{k} p^{k-1} (1 - p)^{N-k-1} (k - Np) g(k)$$

$$= -\sum_{k=0}^{\lfloor Np \rfloor} \binom{N}{k} p^{k-1} (1 - p)^{N-k-1} (Np - k) g(k)$$

$$+ \sum_{k=\lceil Np \rceil}^{N} \binom{N}{k} p^{k-1} (1 - p)^{N-k-1} (k - Np) g(k)$$

$$\geq -\sum_{k=0}^{\lfloor Np \rfloor} \binom{N}{k} p^{k-1} (1 - p)^{N-k-1} (Np - k) g(\lfloor Np \rfloor)$$

$$+ \sum_{k=\lceil Np \rceil}^{N} \binom{N}{k} p^{k-1} (1 - p)^{N-k-1} (k - Np) g(\lceil Np \rceil)$$

$$= \sum_{k=\lceil Np \rceil}^{N} \binom{N}{k} p^{k-1} (1 - p)^{N-k-1} (k - Np)$$

$$\times (g(\lceil Np \rceil) - g(\lfloor Np \rfloor))$$

$$\geq 0$$

where for the last equality we have used Eq. (56).

Now note that either $k_0 \in \{0, \ldots, \lfloor Np \rfloor - 1\}$, or $k_0 = \lfloor Np \rfloor$, or $k_0 \in \{\lceil Np \rceil, \ldots, N - 1\}$. In the second case, there is a strict inequality when going from Eqs. (59) to (60). In the first case or the third case, there is a strict inequality when going from Eqs. (57) to (58). Therefore, under the condition that $g$ is increasing and nonconstant, $\frac{\partial P_g}{\partial p} > 0$, i.e. $P_g$ is strictly increasing. \qed

This result shows that there are many e-maps. We now show that we have a lot of freedom in choosing the functions $\{f_n\}$ that define the e-map.

**Theorem 10** Let $Q = \{Q_n\}$ be a quantum verification procedures with witness Hilbert space dimension $m(n)$. Let $u, v, M \in \text{poly}$, and denote $\epsilon(n) = 1/u(n)$ and $\delta(n) = \exp(-v(n))$. Let $S$ and $T$ denote the following sets:

$$S = \{S_n : n \in \mathbb{N}\}$$

$$S_n = (s_0, s_1, \ldots, s_M, s_{M+1})$$

$$s_i \in [0, 1], s_0 = 0, s_{M+1} = 1$$

$$\forall i : s_i - s_{i-1} \geq \epsilon > 0$$

$$\forall i : s_i \text{ is polynomial time computable}$$


and

\[ T = \{ T_n : n \in \mathbb{N} \} \]

\[ T_n = (t_0, t_1, \ldots, t_M, t_{M+1}) \]

\[ t_i \in [0, 1], \quad t_0 = 0, \quad t_{M+1} = 1 \]

\[ \forall i : \quad t_i - t_{i-1} \geq \delta > 0 \]

\[ \forall i : \quad t_i \text{ is polynomial time computable} \quad (62) \]

where \( M = M(n) \). (Note that the definitions of \( S \) and \( T \) differ only by Eqs. (61) and (62) which ensure that \( s_i \) and \( t_i \) are ranked in increasing order, but with different gaps).

Then, there exists a quantum verification procedure \( Q' \) such that \( Q \) e-maps to \( Q' \) and the polynomial time computable strictly increasing functions \( f_n \) that define the e-map satisfy \( f_n(s_i) = t_i \) for all \( i \in \{0, \ldots, M+1\} \).

The fact that the \( s_i \)'s have inverse polynomial gaps, see Eq. (61), is the main remaining constraint on the choice of the functions \( f_n \). When we use Theorem 10, this will, however, not be a limitation, as typically the \( s_i \)'s will be taken to be soundness and/or completeness bounds, which always have inverse polynomial gaps. We do not expect that this condition can be lifted because the spectra of quantum verification procedures are related to their complexity. In particular, it seems unlikely that one could expand exponentially small intervals in the spectrum into inverse polynomial intervals. Indeed, it is known that when the gap between the largest and second largest eigenvalue of the quantum verification procedure and/or the gap between the completeness and soundness bounds is taken to be exponentially small, one has new, much larger, complexity classes such as PP and PSPACE, see [16] for details and exact definitions. If we could take the \( s_i \)'s to have exponentially small gaps, one could probably show that these complexity classes collapse with QMA.

**Proof** Outline of the proof. We will use Theorem 9. We will show that there exists \((N, G = \{ \tilde{g}_n \})\) as in Definition 29, with the functions \( \tilde{g}_n : \{0, \ldots, N\} \to [0, 1] \) polynomial time computable and strictly increasing, such that the \((N, G)\)-generalised amplification procedure \( Q' \) obtained from \( Q \) satisfies the conditions of Theorem 10. The polynomial time computable strictly increasing functions \( f_n \) that define the e-map will be given by \( P_{\tilde{g}_n} \).

It is convenient to extend the discrete functions \( \tilde{g}_n \) to continuous functions \( g_n : [0, N] \to [0, 1] \) such that \( \tilde{g}_n \) coincides with \( g_n \) on the integers. The functions \( g_n \) are taken to be continuous, piecewise linear and to satisfy \( g_n(Ns_i) = t_i + \lambda_i \) where \( \lambda_i \) are small parameters that we fix later in the proof. We then show that the conditions \( f_n(s_i) = t_i \) yield a set of \( M \) linear equations for \( \lambda_i \). We show that for large \( N \) the solutions \( \lambda_i \) of these equations are exponentially small. The smallness of the \( \lambda_i \) is also a sufficient condition for the functions \( g_n \) to be strictly increasing, which implies that the \( f_n \) are strictly increasing (see Theorem 9).

**Definition of \( \tilde{g}_n \)**

Choose a function \( N \in \text{poly} \). We will determine how large \( N \) must be at the end of the proof.
We denote by
\[
\Delta_i = \left[ N \left(s_i - \frac{\epsilon}{3}\right), N \left(s_i + \frac{\epsilon}{3}\right) \right],
\]
\[
\Delta_0 = \left[ 0, N \frac{\epsilon}{3}\right],
\]
\[
\Delta_{M+1} = \left[ 1 - N \frac{\epsilon}{3}, 1 \right],
\]
\[
\Xi_i = (N(s_i + \epsilon/3), N(s_{i+1} - \epsilon/3)),
\] (63)
where \(i = 1, \ldots, M\). And we denote by
\[
\tilde{\Delta}_i = \{n \in \mathbb{N} : n \in \Delta_i \},
\]
\[
\tilde{\Xi}_i = \{n \in \mathbb{N} : n \in \Xi_i \}
\] (64)
the integers belonging to these intervals.

Let \(X_i \sim B(N, s_i)\) be distributed as a binomial. For all \(s_i, i = 1, \ldots, M\), denote
\[
\Pr[X_i \in \tilde{\Delta}_i] = 1 - \mu_i.
\] (65)

Denote
\[
\mu = \max_i \{\mu_i\}.
\] (66)

Note that by taking \(N\) sufficiently large, we can ensure that \(\mu\) is exponentially small, and in particular smaller than \(\delta\).

Let \((\lambda_0, \lambda_1, \ldots, \lambda_M, \lambda_{M+1})\) be parameters we will fix later, except that we fix \(\lambda_0 = 0\) and \(\lambda_{M+1} = 0\). Denote
\[
\Lambda = \max_i \{||\lambda_i||\}.
\] (67)

Let
\[
\sigma = \frac{\delta}{2\epsilon}.
\] (68)

Consider the continuous, piecewise linear functions \(g_n : [0, N] \to \mathbb{R}\) which on \(\Delta_i\) are given by
\[
g_n(z) = (t_i + \lambda_i) + \sigma (t - Ns_i), \quad z \in \Delta_i,
\] (69)

\[\copyright \ Springer\]
and which are linear outside of the intervals $\Delta_i$. Continuity then implies that for $z \in \Xi_i$, $i = 0, \ldots, M$, one has the expression:

$$g_n(z) = \frac{(t_{i+1} + \lambda_{i+1}) - (t_i + \lambda_i) - 2\epsilon\sigma/3}{N(s_{i+1} - s_i - 2\epsilon/3)}(z - N(s_i + \epsilon/3)) + (t_i + \lambda_i + \frac{\sigma\epsilon}{3}).$$  \hspace{1cm} (70)

We denote by $\tilde{g}_n : \{0, \ldots, N\} \rightarrow [0, 1]$ the functions which coincide with the functions $g_n$ on the integers.

**Strategy for proving the existence of an e-map with the desired properties**

We wish to show that for $N$ large enough, one can choose the parameters $\lambda_i$ such that:

1. $Q$ e-maps to the $(N, G = \{g_n\})$ generalised amplification procedure obtained from $Q$;
2. and that for all $i$

$$t_i = \sum_{k=0}^{N} f(k; N, s_i)\tilde{g}_n(k).$$ \hspace{1cm} (71)

Note that if $\lambda_i = 0$, then $\tilde{g}_n(Ns_i) = t_i$. Hence, if the probability mass functions $f(k; N, s_i)$ are strongly peaked around $Ns_i$ (which is the case if $N$ is large enough), one expects that Eq. (71) can be satisfied for small $\lambda_i$. We show that this is indeed the case below.

**Boundary values**

The functions $g_n$ satisfy $g_n(0) = 0$ and $g_n(N) = 1$.

**Condition for strict increase**

Consider the slope of the functions $g_n$. Over the intervals $\Delta_i$, the slope is $\sigma$ which is strictly positive.

Between the intervals $\Delta_i$, the slope is equal to

$$\frac{(t_{i+1} + \lambda_{i+1}) - (t_i + \lambda_i) - 2\epsilon\sigma/3}{N(s_{i+1} - s_i - 2\epsilon/3)},$$  \hspace{1cm} (72)

see Eq. (70). This is strictly positive if $(t_{i+1} + \lambda_{i+1}) - (t_i + \lambda_i) - 2\epsilon\sigma/3$ is strictly positive. Now note that

$$(t_{i+1} + \lambda_{i+1}) - (t_i + \lambda_i) - 2\epsilon\sigma/3 > 2\delta/3 - 2\Lambda$$  \hspace{1cm} (73)

Hence, a sufficient condition for the functions $g_n$ being strictly increasing is

$$\Lambda < \delta/3.$$  \hspace{1cm} (74)

**Computing $\lambda_i$**
Equations (71) are a set of $M$ linear equations in the $\lambda_i$, with coefficients that can be efficiently computed. Hence, since $s_i$ and $t_i$ are polynomial time computable, the functions $g_n$ are polynomial time computable.

It remains to show that for $N$ large enough solving Eq. (71) for the $\lambda_i$ yields solutions that satisfy Eq. (74).

**Properties of invertible matrices**

Let $A \in \mathbb{R}^{M \times M}$ be an $M \times M$ matrix, and denote by $A_{ij}$ its elements. Denote by

$$
\|A\|_\infty = \max_{ij} |A_{ij}|
$$

(75)

the $\infty$-norm of $A$.

Recall that if $A, A' \in \mathbb{R}^{M \times M}$, then the product matrix $AA'$ has norm $\|AA'\|_\infty \leq M\|A\|_\infty \|A'\|_\infty$. From this, it follows that if $\|A\|_\infty \leq \alpha$, then $\|A^k\|_\infty \leq M^{k-1}\alpha^k$.

From the identity

$$
(\mathbb{I} + A + A^2 + \cdots + A^k)(\mathbb{I} - A) = \mathbb{I} - A^{k-1},
$$

(76)

it follows that the matrix $(1 - A)$ is invertible if $\lim_{k \to \infty} A^k = 0$, in which case

$$
(\mathbb{I} - A)^{-1} = \lim_{k \to \infty} (\mathbb{I} + A + A^2 + \cdots + A^k).
$$

(77)

In particular, $(\mathbb{I} - A)$ is invertible if $\|A\|_\infty < 1/M$, and one has

$$
\|(\mathbb{I} - A)^{-1}\|_\infty \leq \frac{1}{1 - M\|A\|_\infty}.
$$

(78)

In particular, if $\|A\|_\infty < 1/(2M)$, then $\|(\mathbb{I} - A)^{-1}\|_\infty < 2$.

Let $B \in \mathbb{R}^M$ be an $M$ component vector. Denote by

$$
\|B\|_\infty = \max_i |B_i|
$$

(79)

its $\infty$-norm. If $A \in \mathbb{R}^{M \times M}$ and $B \in \mathbb{R}^M$, then the vector $AB$ has norm bounded by

$$
\|AB\|_\infty \leq M\|A\|_\infty \|B\|_\infty.
$$

(80)

As a consequence, if one needs to solve the system of $M$ linear equations for $\lambda_i$, with $A \in \mathbb{R}^{M \times M}$ and $B \in \mathbb{R}^M$,

$$
(\mathbb{I} - A)\lambda = B,
$$

(81)

and if $\|A\|_\infty < 1/(2M)$, then
\[ \max_i \lambda_i \leq 2M \max_i |B_i| \quad (82) \]

**System of equations for \( \lambda_i \)**

Equation (71), viewed as equations for the \( \lambda_i \), can be rewritten in the form (81). We will now bound the entry-wise 1-norm of the corresponding matrix \( A \) and vector \( B \).

Explicitly, Eq. (71) takes the form

\[
t_i = \sum_{k \in \tilde{\Delta}_i} f(k; N, s_i)(t_i + \lambda_i) \\
+ \sum_{k \in \tilde{\Delta}_i} f(k; N, s_i) \sigma (k - Ns_i) \\
+ \sum_{k \in \{0, \ldots, N\} \setminus \tilde{\Delta}_i} f(k; N, s_i) g_n(k) \quad (83)
\]

We now consider the contributions of the three terms in Eq. (83) to \( |A_{ij}| \) and \( |B_i| \).

**Left-hand side and first term** The first term on the right-hand side in Eq. (83) is

\[
\sum_{k \in \Delta_i} f(k; N, s_i)(t_i + \lambda_i) = (1 - \mu_i)(t_i + \lambda_i).
\]

(84)

Therefore, the contribution from Eq. (84) to \( |A_{ii}| \) is \( \mu_i \). And the joint contribution of Eq. (84) and the left-hand side of Eq. (83) to \( |B_i| \) is \( \mu_i t_i \).

**Second term**

\[
\sigma \left| \sum_{k \in \Delta_i} f(k; N, s_i)(k - Ns_i) \right| = \sigma \left| \sum_{k \in \{0, \ldots, N\} \setminus \Delta_i} f(k; N, s_i)(k - Ns_i) \right| \\
\leq \mu_i \sigma N \quad (85)
\]

where we have used Eq. (55). Therefore, the contribution from Eq. (85) to \( |B_i| \) is at most \( \mu_i \sigma N \).

**Third term** Note that when \( \lambda_i = 0 \) for all \( i \), then \( g_n(t) \in [0, 1] \). Hence, the parts of the third term that are independent of the \( \lambda \)’s are bounded by \( \mu_i \). Therefore, the third term contributes at most \( \mu_i \) to \( |B_i| \).
The parts of the third term proportional to \( \lambda \) are given by

\[
\sum_{i' = 0}^{M+1} \sum_{k \in \Delta_{i'}} f(k; N, s_i) \lambda_{i'} + \sum_{i' = 0}^{M} \sum_{k \in S_{i'}} f(k; N, s_i)(\lambda_{i' + 1} - \lambda_{i'}) \frac{k - N(s_{i'} + \epsilon/3)}{N(s_{i' + 1} - s_{i'} - 2\epsilon/3)} \tag{86}
\]

\[
+ \sum_{i' = 0}^{M} \sum_{k \in S_{i'}} f(k; N, s_i) \lambda_{i'} \tag{87}
\]

Note that the coefficient of each \( \lambda_{i'} \) in lines (86) and (88) is bounded by \( \mu \). Therefore, the contribution from (86) to \(|A_{ii'}|\) (with \( i' \neq i \)) is at most \( \mu \), and the contribution from (88) to \(|A_{ii'}|\) is at most \( \mu \).

Note that \( N(s_{i' + 1} - s_{i'} - 2\epsilon/3) \geq N\epsilon/3 \) and that \( k - N(s_{i'} + \epsilon/3) \leq N \); hence, the factor \( (k - N(s_{i'} + \epsilon/3))/(N(s_{i' + 1} - s_{i'} - 2\epsilon/3)) \) in line (87) is bounded by \( 3/\epsilon \). Hence, the coefficient of each \( \lambda_{i'} \) and \( \lambda_{i' + 1} \) in line (87) is bounded by \( 3\mu/\epsilon \). Therefore, the contribution from (87) to \(|A_{ii'}|\) is at most \( 6\mu/\epsilon \).

For large \( N \), \( \lambda \) are unique and small

Putting all together, the matrix \( A \) in Eq. (81) is bounded by

\[
\|A\|_{\infty} \leq \mu(2 + 6/\epsilon). \tag{89}
\]

And the right hand side of Eq. (81) is bounded by

\[
|B_i| \leq \mu_i(t_i + \sigma N + 1) \leq \mu(2 + \sigma N). \tag{90}
\]

Therefore, for large enough \( N \), i.e. \( \mu \) sufficiently small, \( \|A\|_{\infty} \leq 1/(2M) \). When this is the case, there is a unique solution for the \( \lambda \)'s, and

\[
|\lambda_i| \leq 2M(2 + \sigma N)\mu. \tag{91}
\]

Since \( \mu \) decreases exponentially with \( N \), and the other factors increase polynomially with \( N \), by taking \( N \) large enough one can ensure that Eq. (74) is satisfied. 

\[\square\]

12 Nondestructive procedures

As a first application of Theorem 10, we introduce the notion of nondestructive procedure.

Definition 30 (Nondestructive \((a, b)\)-Quantum Verification Procedure). Let \( a, b \) be functions as in Definition 3. An \((a, b)\)-quantum verification procedure \( Q = \{Q_n : n \in \mathbb{N}\} \) is nondestructive if it outputs both a classical bit (the outcome of the quantum
verification procedure) and a quantum state of \( m \) qubits (with \( m \) the dimension of the witness Hilbert space), such that if the input of the procedure is an eigenstate \(|\psi_i\rangle\) of \( Q_n \) for \( x \) then, conditional on the classical output bit being 1 (i.e. on the procedure accepting), the quantum output is the eigenstate \(|\psi_i\rangle\).

**Theorem 11** (Properties of nondestructive procedures). Let \( Q = \{Q_n: n \in \mathbb{N}\} \) be a nondestructive procedure as in Definition 30. Denote by \(|\psi_i\rangle\) the eigenbasis of \( Q_n \) for \( x \) and by \( p_i \) the acceptance probability of \(|\psi_i\rangle\). Then, the following hold:

(1) If the quantum input of \( Q_n \) is a pure state \(|\psi_{\text{in}}\rangle\) which we express in the eigenbasis of \( Q_n \) as

\[
|\psi_{\text{in}}\rangle = \sum_i \alpha_i |\psi_i\rangle,
\]

then, conditional on the classical output bit being 1, the quantum output will be the pure state

\[
|\psi_{\text{out}}\rangle = \frac{1}{\sqrt{\sum_i p_i |\alpha_i|^2}} \sum_i \sqrt{p_i} \alpha_i |\psi_i\rangle.
\]

(2) If one uses the state Eq. (93) as input to the procedure \( Q_n \), the probability of acceptance will be larger than the probability of acceptance on the original state Eq. (92):

\[
\Pr[Q_n(x, |\psi_{\text{out}}\rangle) = 1] \geq \Pr[Q_n(x, |\psi_{\text{in}}\rangle) = 1].
\]

**Proof** The expression Eq. (93) is immediate. We prove Eq. (94). To this end, we introduce the positive operator \( Q_x = \sum_i p_i |\psi_i\rangle\langle\psi_i| \), which is the POVM element corresponding to the classical output of the procedure being 1 (i.e. accepting). Then, we can write

\[
\Pr[Q_n(x, |\psi_{\text{in}}\rangle) = 1] = \langle\psi_{\text{in}}|Q_x|\psi_{\text{in}}\rangle
\]

and

\[
|\psi_{\text{out}}\rangle = \frac{\sqrt{Q_x}|\psi_{\text{in}}\rangle}{\sqrt{\langle\psi_{\text{in}}|Q_x|\psi_{\text{in}}\rangle}}.
\]

Consequently,

\[
\Pr[Q_n(x, |\psi_{\text{out}}\rangle) = 1] = \langle\psi_{\text{out}}|Q_x|\psi_{\text{out}}\rangle
\]

\[
= \frac{\langle\psi_{\text{in}}|Q_x^2|\psi_{\text{in}}\rangle}{\langle\psi_{\text{in}}|Q_x|\psi_{\text{in}}\rangle}
\]

\[
\geq \frac{\langle\psi_{\text{in}}|Q_x|\psi_{\text{in}}\rangle \langle\psi_{\text{in}}|Q_x|\psi_{\text{in}}\rangle}{\langle\psi_{\text{in}}|Q_x|\psi_{\text{in}}\rangle}
\]

\[
= \langle\psi_{\text{in}}|Q_x|\psi_{\text{in}}\rangle,
\]

\( \Box \) Springer
where we have used the fact that $I_m \geq |\psi_{in}\rangle\langle\psi_{in}|$ with $I_m$ the identity operator. □

We now show that without loss of generality we can take quantum verification procedures to be nondestructive.

**Theorem 12** (Existence of nondestructive procedures). Let $Q = \{Q_n\}$ be a quantum verification procedures, and let $S = \{S_n\}$, $S_n = (s_0, s_1, \ldots, s_M, s_{M+1})$, $T = \{T_n\}$, $T_n = (t_0, t_1, \ldots, t_M, t_{M+1})$ be as in Theorem 10. Then, there exists a nondestructive quantum verification procedure $Q^{ND}$ such that $Q$ e-maps to $Q^{ND}$ and the polynomial time computable strictly increasing functions $f_n$ that define the e-map satisfy $f_n(s_i) = t_i$ for all $s_i \in S_n$.

**Proof**  Step 1: procedure $Q^{(1)}$

Use Theorem 10 to construct a procedure $Q^{(1)}$ with the property that the polynomial time computable strictly increasing functions $f_n^{(1)}$ that define the e-map satisfy $f_n^{(1)}(s_i) = \sqrt{t_i}$.

**Step 2: procedure $Q^{ND}$**

Procedure $Q^{ND}$ is obtained as follows: Run the iterative procedure of Definition 29 with parameter $N = 2$ on procedure $Q^{(1)}$, obtaining 2 bits $z_1$ and $z_2$. Accept if $z_1 = z_2 = 1$. Otherwise reject.

**Step 3: proof that $Q^{ND}$ is a nondestructive procedure with the desired properties**

1. $Q$ e-maps to $Q^{(1)}$ and $Q^{(1)}$ e-maps to $Q^{ND}$, hence $Q$ e-maps to $Q^{ND}$. Therefore, the eigenbasis $\{|\psi_i\rangle\}$ of $Q$ for $x$ is also an eigenbasis $Q^{(1)}$ and of $Q^{ND}$ for $x$.
2. The polynomial time computable strictly increasing functions $f_n$ that defines the e-map satisfies $f_n(p) = \left(f_n^{(1)}(p)\right)^2$; hence, it satisfies $f_n(s_i) = t_i$.
3. If $Q^{ND}$ accepts, then the procedure has ended with a measurement of $\{\Pi_0, 1 - \Pi_0\}$ with outcome 1. Therefore, by property 2c of Theorem 8, if the original state of the witness space was an eigenstate $|\psi_i\rangle$ of $Q$, then conditional on $Q^{ND}$ accepting, the state of the witness space is $|\psi_i\rangle$.

□

**13 Equivalent definitions of QMA ∩ coQMA**

Definition 5 is our starting point for studying $QMA \cap coQMA$. It is, however, not very satisfactory for defining functional $QMA \cap coQMA$. Indeed, recall that functional QMA is based on the existence of a quantum verification procedure, of witnesses (i.e. of states that are accepted with high probability by the quantum verification procedure and certify that $x \in L$) and of the eigenbasis of the quantum verification procedure. However, it does not seem possible to introduce these notions starting from Definition 5. The difficulty stems from the fact that the two quantum verification procedures $Q$ and $Q'$ do not commute.

To circumvent this, we introduce two alternative definitions of $QMA \cap coQMA$, the first is based on a 3-outcome quantum verification procedure and the second is based
on a 2-outcome quantum verification procedure. The later is particularly useful, as it allows us to apply the notions of eigenbasis, spectrum, eigenspaces and amplification in the context of QMA ∩ coQMA.

The inspiration for the following definition comes from the fact that a quantum verification procedure for a language \( L \subseteq QMA \) has two outcomes, but these two outcomes play different roles. Outcome 1 certifies that \( x \in L \) (up to some uncertainty, since outcomes are probabilistic), while outcome 0 does not provide information whether \( x \in L \) or \( x \notin L \). In the case of QMA ∩ coQMA, we need one outcome to certify that \( x \in L \), one outcome to certify that \( x \notin L \) and one outcome that does not provide information.

**Definition 31** \((a_3, b_3; a'_3, b'_3)\)-Three outcome quantum verification procedure). Let \( a_3, b_3 \) and \( a'_3, b'_3 \) be functions as in Definition 3. An \((a_3, b_3; a'_3, b'_3)\)-Three Outcome Quantum Verification Procedure is a 3-outcome procedure \( Q^3 = \{Q_n^3 : n \in \mathbb{N}\} \) whose outcomes are denoted \( \{0, L, \overline{L}\} \), and such that for every \( x \) of length \( n \), either both of the following hold:

\[
\exists |\psi\rangle, \Pr[Q_n^3(x, |\psi\rangle) = L] \geq a_3, \quad (98)
\]

\[
\forall |\psi\rangle, \Pr[Q_n^3(x, |\psi\rangle) = \overline{L}] \leq b_3; \quad (99)
\]

or both the following hold:

\[
\exists |\psi\rangle, \Pr[Q_n^3(x, |\psi\rangle) = \overline{L}] \geq a'_3, \quad (100)
\]

\[
\forall |\psi\rangle, \Pr[Q_n^3(x, |\psi\rangle) = L] \leq b_3. \quad (101)
\]

**Definition 32** (The language class L3). Let \( a_3, b_3 \) and \( a'_3, b'_3 \) be functions as in Definition 3. Let \( L3(a_3, b_3; a'_3, b'_3) \) be the set of languages \( L \subseteq \{0, 1\}^n \) such that there exists an \((a_3, b_3; a'_3, b'_3)\)-three outcome quantum verification procedure \( Q^3 = \{Q_n^3 : n \in \mathbb{N}\} \), where for every \( x \), we have \( x \in L \) if and only if Eqs. (98) and (99) hold (and consequently we have \( x \notin L \) if and only if Eqs. (100) and (101) hold).

The following definitions will enable us to provide a definition of QMA ∩ coQMA based on a quantum verification procedure that only has two outcomes. The idea behind this definition is that if outcome 1 occurs with high probability this certifies that \( x \in L \), if outcome 0 occurs with high probability this certifies that \( x \notin L \), while if outcomes 1 and 0 occur with approximately the same probability, then no information is obtained.

**Definition 33** \((a_2, b_2; a'_2, b'_2)\)-Quantum verification procedure). Let \( a_2, b_2 \) and \( a'_2, b'_2 \) be pairs of functions as in Definition 3.

An \((a_2, b_2; a'_2, b'_2)\)-Quantum Verification Procedure is a quantum verification procedure \( Q^2 = \{Q_n^2 : n \in \mathbb{N}\} \) such that for every \( x \) of length \( n \), either both of the following hold:

\[
\exists |\psi\rangle, \Pr[Q_n^2(x, |\psi\rangle) = 1] \geq \frac{1}{2} + \frac{a_2}{2}, \quad (102)
\]

\[
\forall |\psi\rangle, \Pr[Q_n^2(x, |\psi\rangle) = 1] \geq \frac{1}{2} - \frac{b'_2}{2}; \quad (103)
\]
or both the following hold:

\[ \exists |\psi\rangle, \Pr[Q_n^2(x, |\psi\rangle) = 0] \geq \frac{1}{2} + \frac{a_1'}{2}, \quad (104) \]

\[ \forall |\psi\rangle, \Pr[Q_n^2(x, |\psi\rangle) = 0] \geq \frac{1}{2} - \frac{b_2}{2}. \quad (105) \]

**Definition 34** *(The language class L2)*. Let \( a_2, b_2 \) and \( a_2', b_2' \) be pairs of functions as in Definition 3. Let \( L_2(a_2, b_2; a_2', b_2') \) be the set of languages \( L \subseteq \{0, 1\}^* \) such that there exists an \( (a_2, b_2; a_2', b_2') \)-quantum verification procedure \( Q^2 = \{Q_n^2 : n \in \mathbb{N}\} \), where for every \( x \), we have \( x \in L \) if and only if Eqs. (102) and (103) hold (and consequently, we have \( x \notin L \) if and only if Eqs. (104) and (105) hold).

We note that the language class \( L2 \) is independent of the bounds used to define it.

**Theorem 13** *(L2(a2, b2; a2', b2') is independent of the completeness and soundness probabilities)*. Let \( a_2, b_2 \) and, \( a_2', b_2' \) be pairs of functions as in Definition 3. For any \( r \in \text{poly} \), for any \( \tilde{a}_2, \tilde{b}_2, \tilde{a}_2', \tilde{b}_2' \) pairs of functions as in Definition 3 with \( \tilde{a}_2, \tilde{a}_2' < 1 - 2^{-r} \) and \( \tilde{b}_2, \tilde{b}_2' > 2^{-r} \), it holds that \( L_2(a_2, b_2; a_2', b_2') \subseteq L_2(\tilde{a}_2, \tilde{b}_2; \tilde{a}_2', \tilde{b}_2') \).

**Proof** *Step 1: e-map from Q2 to \( \tilde{Q}_2 \)*

Let \( L \) be a language in \( L_2(a_2, b_2; a_2', b_2') \). Let \( Q^2 = \{Q_n^2 : n \in \mathbb{N}\} \) be the quantum verification procedure associated with language \( L \), i.e. such that for every \( x \), we have \( x \in L \) if and only if Eqs. (102) and (103) hold (and consequently we have \( x \notin L \) if and only if Eqs. (104) and (105) hold).

If we rewrite the four bound Eqs. (102), (103), (104),(105) in terms of \( \Pr[Q_n^2(x, |\psi\rangle) = 1] \), then the corresponding right-hand sides, ranked in increasing order, are

\[ 0 < \frac{1}{2} - \frac{a_2'}{2} < \frac{1}{2} - \frac{b_2'}{2} < \frac{1}{2} + \frac{b_2}{2} < \frac{1}{2} + \frac{a_2}{2} < 1. \quad (106) \]

We would like to apply Theorem 10 to the values in Eq. (106). However, we cannot do this directly, because some of the differences between two consecutive terms in Eq. (106) may be exponentially small (in fact the ones corresponding to the first, third, and fifth inequalities). We note, however, that language \( L \) does not change if we keep the procedure \( Q^2 \) unchanged, but change the bounds according to

\[ (a_2, b_2; a_2', b_2') \rightarrow (\tilde{a}_2, \tilde{b}_2; \tilde{a}_2', \tilde{b}_2') ; \]

\[ \tilde{a}_2 = a_2 - \frac{1}{3q}, \]

\[ \tilde{b}_2 = b_2 + \frac{1}{3q}, \]

\[ \tilde{a}_2' = a_2' - \frac{1}{3q}, \]

\[ \tilde{b}_2' = b_2' + \frac{1}{3q} \quad (107) \]
where \( q \) is a polynomial such that \( a_2 - b_2 \geq 1/q \) and \( a'_2 - b'_2 \geq 1/q \) (which necessarily exists, given the definition of \((a_2, b_2; a'_2, b'_2)\)).

We thus apply Theorem 10 to the procedure \( Q_2 \) and the sets

\[
S = \{S_n : n \in \mathbb{N}\}
\]

\[
S_n = \left(0, \frac{1}{2} - \frac{\tilde{a}'_2}{2}, \frac{1}{2} - \frac{\tilde{b}'_2}{2}, \frac{1}{2} + \frac{\tilde{b}'_2}{2}, \frac{1}{2} + \frac{\tilde{a}'_2}{2}, 1\right)
\]

and

\[
T = \{T_n : n \in \mathbb{N}\}
\]

\[
T_n = \left(0, \frac{1}{2} - \frac{\tilde{a}'_2}{2}, \frac{1}{2} - \frac{\tilde{b}'_2}{2}, \frac{1}{2} + \frac{\tilde{b}'_2}{2}, \frac{1}{2} + \frac{\tilde{a}'_2}{2}, 1\right)
\]

yielding a new procedure \( \tilde{Q}_2 \).

**Step 2:** \( L_2(a_2, b_2; a'_2, b'_2) \subseteq L_2(\tilde{a}_2, \tilde{b}_2; \tilde{a}'_2, \tilde{b}'_2) \)

We now can show that for the language \( \tilde{L} \in L_2(a_2, b_2; a'_2, b'_2) \) introduced at the beginning of Step 1, it also holds that \( L \in L_2(\tilde{a}_2, \tilde{b}_2; \tilde{a}'_2, \tilde{b}'_2) \).

Suppose \( x \in L \). We need to show that

\[
\exists \langle \psi \rangle, \Pr[\tilde{Q}^2_n(x, |\psi\rangle) = 1] \geq \frac{1}{2} + \frac{\tilde{a}'_2}{2}
\]

and that

\[
\forall \langle \psi \rangle, \Pr[\tilde{Q}^2_n(x, |\psi\rangle) = 0] \geq \frac{1}{2} - \frac{\tilde{b}'_2}{2}.
\]

We know that \( \exists \langle \psi \rangle, \Pr[Q^2_n(x, |\psi\rangle) = 1] \geq \frac{1}{2} + \frac{a'_2}{2} \). Consequently, there exists an eigenstate \( |\psi_i\rangle \) of \( Q^2_n \) with acceptance probability \( p_i = \Pr[Q^2_n(x, |\psi_i\rangle) = 1] \geq \frac{1}{2} + \frac{a'_2}{2} \). The state \( |\psi_i\rangle \) is also an eigenstate of \( \tilde{Q}^2_n \) with acceptance probability \( \tilde{p}_i = \Pr[\tilde{Q}^2_n(x, |\psi_i\rangle) = 1] \geq \frac{1}{2} + \frac{\tilde{a}'_2}{2} \). Hence, Eq. (110) holds.

We also know that \( \forall \langle \psi \rangle, \Pr[Q^2_n(x, |\psi\rangle) = 1] \geq \frac{1}{2} - \frac{b'_2}{2} \). Consequently for all eigenstates \( |\psi_i\rangle \) of \( Q^2_n \), it holds that their acceptance probability satisfies \( p_i \geq \frac{1}{2} - \frac{b'_2}{2} \). Therefore, all eigenstates of \( \tilde{Q}^2_n \) have acceptance probability that satisfies \( \tilde{p}_i \geq \frac{1}{2} - \frac{\tilde{b}'_2}{2} \). Hence, Eq. (111) holds.

A similar reasoning applies when \( x \notin L \).

Therefore, \( L \in L_2(\tilde{a}_2, \tilde{b}_2; \tilde{a}'_2, \tilde{b}'_2) \), and consequently, \( L_2(a_2, b_2; a'_2, b'_2) \subseteq L_2(\tilde{a}_2, \tilde{b}_2; \tilde{a}'_2, \tilde{b}'_2) \). \( \square \)

We now show that all the above definitions are equivalent.
Theorem 14 (QMA ∩ coQMA = L3 = L2). For all a, b, a', b', pairs of functions as in Definition 3, the following equalities hold

\[ \text{QMA} \cap \text{coQMA} = L3(a, b; a', b') = L2(a, b; a', b'). \]  

(112)

Proof Step 1: QMA ∩ coQMA(a, b; a', b') ⊆ L3(a, b; a', b')

Let a, b and a', b' functions as in Definition 3. Let \( L \in \text{QMA} \cap \text{coQMA}(a, b; a', b') \). Then, there exist a, b and a', b' functions as in Definition 3, and there exist two quantum verification procedures \( Q = \{ Q_n : n \in \mathbb{N} \} \) and \( Q' = \{ Q'_n : n \in \mathbb{N} \} \) such that Eqs. (11) to (14) hold. We now show that \( L \in L3(a, b; a', b') \).

Recall that \( Q_n \) takes as input \((x, |\psi\rangle \otimes |0^{k}\rangle)\) where \(|x| = n\) is a state of \( m \) qubits, and both \( m = m(n) \) and \(|k| = m(n) \) are polynomial functions of \( n \), and that \( Q'_n \) takes as input \((x, |\psi'\rangle \otimes |0^{k'}\rangle)\) where \(|x| = n\) is a state of \( m' \) qubits, and both \( m' = m'(n) \) and \(|k'| = m'(n) \) are polynomial functions of \( n \).

Define \( m_3 = \max\{m, m'\} + 1 \), and \( k_3 = \max\{k, k'\} \). Define the circuit \( Q_3^3 \) which on input \((x, |\psi\rangle \otimes |0^{k}\rangle)\) with \(|x| = n\) and \(|\tilde{\psi}\rangle\) a state of \( m_3 \) qubits, acts as follows:

1. Measure the first qubit of \(|\tilde{\psi}\rangle\) in the standard basis.
2. If the result of the first measurement is 1, then carry out the procedure \( Q_n \) on input \((x, |\psi\rangle \otimes |0^{k}\rangle)\) where the second register contains qubits 2, \ldots, \( m + 1 \) of \(|\psi\rangle\) and the third register contains the first \( k \) ancilla qubits. If the outcome of \( Q_n \) is 1, then output \( L \); while if the outcome of \( Q_n \) is 0, then output 0.
3. If the result of the first measurement is 0, then carry out the procedure \( Q'_n \) on input \((x, |\psi\rangle \otimes |0^{k}\rangle)\) where the second register contains qubits 2, \ldots, \( m' + 1 \) of \(|\psi\rangle\) and the third register contains the first \( k' \) ancilla qubits. If the outcome of \( Q'_n \) is 1, then output \( L \); while if the outcome of \( Q_n \) is 0, then output 0.

One easily checks that the family of circuits \( Q_3^3 = \{ Q_3^3 : n \in \mathbb{N} \} \) thus defined satisfy Eqs. (98) and (99) when \( x \in L \), and satisfy Eqs. (100) and (101) when \( x \notin L \), with \( a_3 = a, b_3 = b, a'_3 = a', b'_3 = b' \).

Step 2: L3(a, b; a', b') ⊆ QMA ∩ coQMA(a, b; a', b')

Let \( a_3, b_3 \) and \( a'_3, b'_3 \) be pairs of functions as in Definition 3. Let \( L \in L3(a, b; a', b') \). Then, there exists a three outcome quantum verification procedure \( Q_3^3 = \{ Q_3^3 : n \in \mathbb{N} \} \) that satisfies Eqs. (98) and (99) when \( x \in L \), and satisfies Eqs. (100) and (101) when \( x \notin L \). We now show that \( L \in \text{QMA} \cap \text{coQMA}(a, b; a', b') \).

Note that \( Q_3^3 \) takes as input \((x, |\psi\rangle \otimes |0^{k}\rangle)\) where \(|x| = n\) is a state of \( m_3 \) qubits, and both \( m_3 = m_3(n) \) and \( k_3 = k_3(n) \) belong to poly.

Define two quantum verification procedures \( Q = \{ Q_n : n \in \mathbb{N} \} \) and \( Q' = \{ Q'_n : n \in \mathbb{N} \} \) as follows:

\( Q_n \) and \( Q'_n \) take as input \((x, |\psi\rangle \otimes |0^{k}\rangle)\), with \(|\psi\rangle\) a state of \( m_3 \) qubits.

On input \((x, |\psi\rangle \otimes |0^{k}\rangle)\), run \( Q_3^3(x, |\psi\rangle \otimes |0^{k}\rangle) \).

In the case of \( Q_n \):
if \( Q_3^3(x, |\psi\rangle \otimes |0^{k}\rangle) = L \) output 1,
if \( Q_3^3(x, |\psi\rangle \otimes |0^{k}\rangle) = 0 \) output 0,
if \( Q_3^3(x, |\psi\rangle \otimes |0^{k}\rangle) = \overline{L} \) output 0.

In the case of \( Q'_n \):

if $Q_n^3(x, |\psi_\rangle \otimes |0^{k_3}\rangle) = L$ output 0,
if $Q_n^3(x, |\psi_\rangle \otimes |0^{k_3}\rangle) = 0$ output 0,
if $Q_n^3(x, |\psi_\rangle \otimes |0^{k_3}\rangle) = \overline{L}$ output 1.

One easily checks that the family of circuits $Q = \{Q_n : n \in \mathbb{N}\}$ and $Q' = \{Q_n' : n \in \mathbb{N}\}$ thus defined satisfy Eqs. (11) and (12) when $x \in L$, and satisfy Eqs. (13) and (14) when $x \notin L$, with $a = a_3, b = b'_3$ and $a' = a'_3, b' = b_3$.

Summary of steps 1 and 2
Since $QMA \cap \text{coQMA}(a, b; a', b')$ is independent of the bounds $a, b; a', b'$, see Definition 7, we have proven the first equality in Eq. (112), including the fact that $L_3(a, b; a', b')$ is independent of the bounds $a, b; a', b'$.

Step 3: $L_3 \subseteq L_2$
Let $L \in L_3(3/4, 1/4; 3/4, 1/4)$, and let $Q^3 = \{Q_n^3 : n \in \mathbb{N}\}, n, m_3, k_3$ be defined as in the first two paragraphs of Step 2. We show that $L \in L_2(1/2, 1/4; 1/2, 1/4)$.

Define the quantum verification procedures $Q^2 = \{Q_n^2 : n \in \mathbb{N}\}$ as follows:
Run $Q_n^3(x, |\psi_\rangle \otimes |0^{k_3}\rangle)$ and

- if $Q_n^3(x, |\psi_\rangle) = L$ then output 1;
- if $Q_n^3(x, |\psi_\rangle) = 0$, then output a random bit drawn uniformly at random from the set $\{0, 1\}$;
- if $Q_n^3(x, |\psi_\rangle) = \overline{L}$ then output 0.

Let us consider the case $x \in L$. For brevity in what follows we omit the arguments of $Q^3$. For all input states $|\psi_\rangle$, we have

$$
\Pr[Q^2 = 1] = \Pr[Q^3 = L] + \frac{1}{2} \Pr[Q^3 = 0] = \Pr[Q^3 = L] + \frac{1}{2} \left(1 - \Pr[Q^3 = L] - \Pr[Q^3 = \overline{L}]\right) = \frac{1}{2} + \frac{1}{2} \Pr[Q^3 = L] - \frac{1}{2} \Pr[Q^3 = \overline{L}].
$$

(113)

Since $x \in L$, we have that for all $|\psi_\rangle$, $\Pr[Q^3 = \overline{L}] \leq 1/4$. Furthermore, we trivially have $\Pr[Q^3 = L] \geq 0$. Therefore, Eq. (113) implies that for all $|\psi_\rangle$ the following holds:

$$
\Pr[Q^2 = 1] \geq \frac{1}{2} - \frac{1}{2} \cdot \frac{1}{4} = \frac{3}{8}.
$$

(114)

Since $x \in L$, there exists a $|\psi_\rangle$ such that $\Pr[Q^3 = L] \geq 3/4$. Therefore, Eq. (113) implies that for this $|\psi_\rangle$ we have

$$
\Pr[Q^2 = 1] \geq \frac{1}{2} + \frac{3}{2} \cdot \frac{1}{4} = \frac{3}{4}.
$$

(115)

Therefore, the family of circuits $Q^2 = \{Q_n^2 : n \in \mathbb{N}\}$ satisfy Eqs. (102) and (103) when $x \in L$ with $a_2 = 1/2$ and $b'_2 = 1/4$. 

Springer
Similar reasoning shows that when \( x \notin L \), the family of circuits \( Q^2 = \{ Q^2_n : n \in \mathbb{N} \} \) satisfy Eqs. (104) and (105) with \( a'_2 = 1/2 \) and \( b_2 = 1/4 \).

As a consequence,

\[
L3(3/4, 1/4; 3/4, 1/4) \subseteq L2(1/2, 1/4; 1/2, 1/4). \tag{116}
\]

**Step 4: \( L2 \subseteq L3 \)**

Let \( a_2, b_2 \) and \( a'_2, b'_2 \) be functions as in Definition 3. Let \( L \in L2(a_2, b_2; a'_2, b'_2) \). Then there exists a \( (a_2, b_2; a'_2, b'_2) \)-procedure \( Q^2 = \{ Q^2_n : n \in \mathbb{N} \} \) that satisfies Eqs. (102) and (103) when \( x \in L \), and satisfies Eqs. (104) and (105) when \( x \notin L \). We now show that

\[
L \in L3 \left( \left( \frac{1}{2} + \frac{a_2}{2} \right)^2, \left( \frac{1}{2} + \frac{b_2}{2} \right)^2, \left( \frac{1}{2} + \frac{a'_2}{2} \right)^2, \left( \frac{1}{2} + \frac{b'_2}{2} \right)^2 \right). \tag{117}
\]

Note that \( Q^2_n \) takes as input \( (x, |\psi\rangle \otimes |0^{k_2}\rangle) \) where \( |x| = n \), \( |\psi\rangle \) is a state of \( m_2 \) qubits, and both \( m_2 = m_2(n) \) and \( k_2 = k_2(n) \) are in \( \text{poly} \).

Note that since \( Q^2 \) is a quantum verification procedure, there exists an eigenbasis of \( Q^2 \) for \( x \), denoted \( B_{Q^2}(x) = \{|\psi_i^2\rangle : 1 \leq i \leq 2^{m_2}\} \). We denote by \( p_i = \text{Pr}[Q^2_n(x, |\psi_i^2\rangle) = 1] \) the acceptance probability of \( |\psi_i^2\rangle \).

Define the polynomial time uniform family of quantum circuits \( Q^3 = \{ Q^3_n : n \in \mathbb{N} \} \) as follows:

\( Q^3_n \) takes as input \( (x, |\psi\rangle \otimes |0^{k_3}\rangle) \) where \( |x| = n \), \( |\psi\rangle \) is a state of \( m_2 \) qubits, and \( k_3 = k_3(n) \) is a polynomial function of \( n \).

On input \( (x, |\psi\rangle) \), carry out a slight modification of the Iterative Procedure of Definition 29 (see note Definition 29) applied to \( Q^2 \) as follows.

The parameter \( N \) takes the value \( N = 2 \).

The functions \( g_{|x|} = g \) are taken as probability distributions over the alphabet \( \{L, 0, \overline{L}\} \). They are independent of \( |x| \) and take the deterministic form:

\[
g : \{0, 1, 2\} \to \{L, 0, \overline{L}\}, \quad g(2) = L, \quad g(1) = 0, \quad g(0) = \overline{L} \tag{118}
\]

Let us bound the probabilities of the outcomes \( L, 0, \overline{L} \). We can restrict our discussion to the eigenstates of \( Q^2 \) (because of the absence of interferences, see Equation (21)).

One finds

\[
\text{Pr}[Q^3_n(x, |\psi_i^2\rangle) = L] = p_i^2, \\
\text{Pr}[Q^3_n(x, |\psi_i^2\rangle) = 0] = 2p_i(1 - p_i), \\
\text{Pr}[Q^3_n(x, |\psi_i^2\rangle) = \overline{L}] = (1 - p_i)^2. \tag{119}
\]
One then easily checks that the family of circuits $Q^3 = \{ Q^3_n : n \in \mathbb{N} \}$ thus defined satisfy Eqs. (98) and (99) when $x \in L$ and satisfy Eqs. (100) and (101) when $x \notin L$, with $a_3 = (\frac{1}{2} + \frac{a_2}{2})^2$, $b_3 = (\frac{1}{2} + \frac{b_2}{2})^2$ and $a_3' = (\frac{1}{2} + \frac{a_2'}{2})^2$, $b_3' = (\frac{1}{2} + \frac{b_2'}{2})^2$.

Summary of Steps 3 and 4
Since $L_2(a, b; a', b')$ and $L_3(a, b; a', b')$ are independent of the bounds $a, b; a', b'$ (see Theorem 13 and remark in paragraph “Summary of steps 1 and 2”), steps 3 and 4 show that $L_2 = L_3$. Combining with steps 1 and 2, we have the second equality in Eq. (112). □

14 Functional QMA $\cap$ coQMA

14.1 Definitions

We first generalise Definition 19 as follows:

Definition 35 (Accepting and rejecting subspaces). Let $Q = \{ Q_n \}$ be a quantum verification procedure and fix $a, a' \in [0, 1]$.

We define the following binary relations over binary strings and quantum states:

$$\mathcal{H}_Q^{[1-a', 1+a]}(x, |\psi\rangle) = 1 \text{ if } |\psi\rangle \in \text{Span}(\mathcal{H}_Q^{\geq \frac{1+a}{2}}(x) \cup \mathcal{H}_Q^{\leq \frac{1-a'}{2}}(x))$$

and

$$\mathcal{H}_Q^{[\frac{1-a'}{2}, \frac{1+a}{2}]}(x, |\psi\rangle) = 1 \text{ if } |\psi\rangle \in \text{Span} \left( \left\{ \mathcal{H}_Q(x, p) : \frac{1-a'}{2} \leq p \leq \frac{1+a}{2} \right\} \right).$$

and to simplify notation, we denote

$$\mathcal{H}_Q^{[1-a', 1+a]}(x) = \left\{ |\psi\rangle : \mathcal{H}_Q^{[1-a', 1+a]}(x, |\psi\rangle) = 1 \right\},$$

$$\mathcal{H}_Q^{[\frac{1-a'}{2}, \frac{1+a}{2}]}(x) = \left\{ |\psi\rangle : \mathcal{H}_Q^{[\frac{1-a'}{2}, \frac{1+a}{2}]}(x, |\psi\rangle) = 1 \right\}. \tag{120}$$

We base our definition of functional QMA $\cap$ coQMA on $(a_2, b_2; a'_2, b'_2)$-Quantum Verification Procedures because these have an eigenbasis which allows the definition of accepting and rejecting subspaces.

Definition 36 (Functional QMA $\cap$ coQMA (F(QMA $\cap$ coQMA))). Let $a_2, b_2$ and $a'_2, b'_2$ be functions as in Definition 3. The class $F(QMA \cap coQMA) (a_2, b_2; a'_2, b'_2)$ is the set $\{ (\mathcal{H}_Q^{[1-a_2', 1+a_2]}(x), \mathcal{H}_Q^{[1-b_2', 1+b_2]}(x)) \}$ of pairs of relations, where $Q^2$ is an $(a_2, b_2; a'_2, b'_2)$-quantum verification procedure.

We already showed in Theorem 13 that the language $L_2$ is independent of the completeness and soundness bounds used to define it. We now show, using the same
Theorem 15 F(QMA ∩ coQMA) is independent of the bounds \((a_2, b_2; a'_2, b'_2)\). Let \(Q^2\) be an \((a_2, b_2; a'_2, b'_2)\)-quantum verification procedure, with \(a_2, b_2\) and \(a'_2, b'_2\) functions as in Definition 3.

Let \(\tilde{a}_2, \tilde{b}_2\) and \(\tilde{a}'_2, \tilde{b}'_2\) be functions as in Definition 3 with \(\tilde{a}_2, \tilde{a}'_2 < 1 - 2^{-r}\) and \(\tilde{b}_2, \tilde{b}'_2 > 2^{-r}\), for some \(r \in \text{poly}\).

Then, there exists an \((\tilde{a}_2, \tilde{b}_2; \tilde{a}'_2, \tilde{b}'_2)\)-quantum verification procedure \(\tilde{Q}^2\), such that there exists an e-map from \(Q^2\) to \(\tilde{Q}^2\) and the strictly increasing functions \(\{f_n\}\) that define the e-map (see Definition 28) satisfy \(f_n(a_2) = \tilde{a}_2, f_n(b_2) = \tilde{b}_2, f_n(a'_2) = \tilde{a}'_2, f_n(b'_2) = \tilde{b}'_2\). Consequently, for all \(x\)

\[
\mathcal{H}^{L}_{\tilde{Q}^2} \left[ \left\{ 0, \frac{1-\tilde{a}'_2}{2} \right\} \cup \left\{ \frac{1+\tilde{a}_2}{2}, 1 \right\} \right](x) = \mathcal{H}^{L}_{\tilde{Q}^2} \left[ \left\{ 0, \frac{1-\tilde{a}'_2}{2} \right\} \cup \left\{ \frac{1+\tilde{a}_2}{2}, 1 \right\} \right](x) \quad (121)
\]

and

\[
\mathcal{H}^{L}_{\tilde{Q}^2} \left[ \left\{ \frac{1-\tilde{b}'_2}{2}, \frac{1+\tilde{b}_2}{2} \right\} \right](x) = \mathcal{H}^{L}_{\tilde{Q}^2} \left[ \left\{ \frac{1-\tilde{b}'_2}{2}, \frac{1+\tilde{b}_2}{2} \right\} \right](x). \quad (122)
\]

Proof The proof of Theorem 13 also proves Theorem 15. \(\square\)

As a consequence, the precise values of the bounds \((a_2, b_2; a'_2, b'_2)\) are irrelevant. We therefore define \(F(\text{QMA} \cap \text{coQMA})\) using standard values for \(a_2, a'_2\) and \(b_2; b'_2\).

Definition 37 We define the class \(F(\text{QMA} \cap \text{coQMA})\) as \(F(\text{QMA} \cap \text{coQMA})\) \((2/3, 1/3; 2/3, 1/3)\).

Since the definition of Functional QMA \(\cap\) coQMA is in terms of Definition 33, what about Functional QMA \(\cap\) coQMA if one uses the original Definition 5? The proof of Theorem 14 provides a natural mapping from the pair of quantum verification procedures \(Q\) and \(Q'\) used in Definition 5 to the single quantum verification procedure \(Q^2\) used in Definition 33. Using this mapping leads to the following definition.

Definition 38 \((\text{Canonical definition of functional QMA} \cap \text{coQMA})\). Let \(a, b\) and \(a', b'\) be pairs of functions as in Definition 3. Let \(Q\) and \(Q'\) be two quantum verification procedures as in Definition 5. These procedures define a language \(L \in \text{QMA} \cap \text{coQMA}\).

Let \(|\psi_i\rangle\) be an eigenbasis of \(Q\) for \(x\), and \(p_i\) the corresponding acceptance probability, and let \(|\psi'_i\rangle\) be an eigenbasis of \(Q'\) for \(x\) and \(p'_i\) the corresponding acceptance probability.

For all \(x\), denote by

\[
\mathcal{H}^+(x) = \{|0\otimes|\psi_i\rangle : p_i > a\} \cup \{|1\otimes|\psi'_i\rangle : p'_i > a'\} \quad (123)
\]
and by
\[
\mathcal{H}^- (x) = \{|0\}\otimes |\psi_i\rangle : p_i < b\} \cup \{|1\} \otimes |\psi'_i\rangle : p'_i < b'\}
\quad (124)
\]

Then, the pair of relations
\[
(\mathcal{H}^+ (x), \mathcal{H}^- (x)) \in \text{F}(\text{QMA} \cap \text{coQMA})(a, b; a', b')
\quad (125)
\]
are the canonical relations associated with the pair of procedures \(Q\) and \(Q'\) with completeness and soundness probabilities \(a, b\) and \(a', b'\).

From this definition, we see that one of the original problems we were confronted with, namely that \(Q\) and \(Q'\) do not commute has been circumvented by appending to the witnesses a single qubit whose state, \(|0\rangle\) or \(|1\rangle\), indicates whether this is a witness for \(Q\) or for \(Q'\).

15 Total functional QMA equals functional QMA \& coQMA

We now prove that Total Functional QMA equals Functional QMA \& coQMA.

**Theorem 16** \(F(\text{QMA} \cap \text{coQMA}) = \text{TFQMA}\)

**Proof** Step 1: \(F(\text{QMA} \cap \text{coQMA}) \subseteq \text{TFQMA}\)

Let \(Q^2 = \{Q^2_n : n \in \mathbb{N}\}\) be an \((2/3, 1/3; 2/3, 1/3)\)-quantum verification procedure. For brevity, we denote in what follows \(a = 2/3 \) and \(b = 1/3\).

The corresponding accepting and rejecting subspaces are \(\mathcal{H}_{Q^2}^{0, \frac{1-a}{2}}\cup\frac{1+a}{2}, 1\} (x)\) and \(\mathcal{H}_{Q^2}^{\frac{1-b}{2}, \frac{1+b}{2}} (x)\). Note that \(\mathcal{H}_{Q^2}^{0, \frac{1-a}{2}}\cup\frac{1+a}{2}, 1\} (x)\) is nonempty for all \(x\). Denote by \(B_{Q^2}(x) = \{|\psi^2_i\rangle\}\) the eigenbasis of \(Q^2\) for \(x\) and by \(p_i = \Pr\left[Q^2_n(x, |\psi^2_i\rangle) = 1\right]\) the acceptance probability of \(|\psi^2_i\rangle\).

We will show that there exists a \(\frac{1+a^2}{2}\)-total quantum verification procedure \(Q^T = \{Q^T_n : n \in \mathbb{N}\}\) such that

\[
\mathcal{H}_{Q^T}^{\geq \frac{1+a^2}{2}} (x) = \mathcal{H}_{Q^2}^{0, \frac{1-a}{2}}\cup\frac{1+a}{2}, 1\} (x)
\quad (126)
\]

and

\[
\mathcal{H}_{Q^T}^{\leq \frac{1+b^2}{2}} (x) = \mathcal{H}_{Q^2}^{\frac{1-b}{2}, \frac{1+b}{2}} (x).
\quad (127)
\]

We define \(Q^T\) as follows:

On input \((x, |\psi\rangle)\) run the iterative procedure of Definition 29 on \(Q^2_n\) on input \((x, |\psi\rangle)\), for parameter \(N = 2\), thereby producing a 2 bit output \(z_1, z_2\) and functions
$G = \{ g_{|x|} \}$ independent of $|x|$ given by:

\begin{align*}
g(0) &= g(2) = 1 \\
g(1) &= 0.
\end{align*}

(128)

One easily checks that

\begin{align*}
\Pr[Q_n^T(x, |\psi_i^2\rangle) = 1] &= p_i^2 + (1 - p_i)^2 \\
\Pr[Q_n^T(x, |\psi_i^2\rangle) = 0] &= 2p_i(1 - p_i).
\end{align*}

(129) (130)

Equations (126) and (127) then follow from Eq. (129).

The completeness and soundness thresholds of procedure $Q^T$ are $\frac{1 + a^2}{2} = \frac{13}{18}$ and $\frac{1 + b^2}{2} = \frac{10}{18}$. They can be changed to $\frac{2}{3}$ and $\frac{1}{3}$, see Theorem 5, which proves the result.

**Step 2:** TFQMA $\subseteq F(QMA \cap coQMA)$

Let $Q = \{ Q_n : n \in \mathbb{N} \}$ be an $a$-total quantum verification procedure. Choose any $b$ such that $a$, $b$ is a pair of functions as in Definition 3. The corresponding accepting and rejecting subspaces are $\mathcal{H}^a_Q(x)$ and $\mathcal{H}^\leq b_Q(x)$.

Denote by $B_Q(x) = \{|\psi_i\rangle\}$ the eigenbasis of $Q$ for $x$ and by $p_i = \Pr[Q_n(x, |\psi_i\rangle) = 1]$ the acceptance probability of $|\psi_i\rangle$.

We show that there exists an $(a, b; a, b)$-quantum verification procedure $Q^2 = \{ Q^2_n : n \in \mathbb{N} \}$ such that

\begin{align*}
\mathcal{H}^{\frac{1-a}{2}, \frac{1+a}{2}}_Q(x) &= \mathcal{H}^a_Q(x) \\
\mathcal{H}^{\frac{1-b}{2}, \frac{1+b}{2}}_Q(x) &= \mathcal{H}^\leq b_Q(x).
\end{align*}

(131) (132)

We define $Q^2(x, |\psi\rangle)$ as follows:

Let $c$ be a bit drawn uniformly at random from the distribution $\{0, 1\}$.
If $c = 0$, accept
If $c = 1$, carry out the procedure $Q$ on input $(x, |\psi\rangle)$. Output $Q_n(x, |\psi\rangle)$.

One easily checks that

\begin{align*}
\Pr[Q^2_n(x, |\psi_i\rangle) = 1] &= \frac{1 + p_i}{2}
\end{align*}

(133)

from which Eqs. (131) and (132) follow. (Note that we in fact have that $\mathcal{H}^{<1/2}_Q(x) = \emptyset$, and consequently $\mathcal{H}^{\frac{1-a}{2}, \frac{1+a}{2}}_Q(x) = \mathcal{H}^{\leq \frac{1+a}{2}}_Q(x)$ and $\mathcal{H}^{\frac{1-b}{2}, \frac{1+b}{2}}_Q(x) = \mathcal{H}^{\frac{1+b}{2}}_Q(x)$.)
If $\text{TFQMA}_W \subseteq \text{FBQP}_W$ then $\text{QMA} \cap \text{coQMA} = \text{BQP}$

We show that if the functional $\text{TFQMA}$ class is trivial, in the sense that one can always efficiently produce a witness, then $\text{QMA} \cap \text{coQMA} = \text{BQP}$.

**Theorem 17** If $\text{TFQMA}_W$ is included in $\text{FBQP}_W$ then $\text{QMA} \cap \text{coQMA}$ equals $\text{BQP}$.

**Proof**  

Step 1: Trivial direction It follows from Definition 11 that $\text{BQP} = \text{coBQP}$. Therefore, $\text{BQP} \subseteq \text{QMA} \cap \text{coQMA}$.

Step 2: Procedure $Q^2$ We will show that under the condition $\text{TFQMA}_W(a) \subseteq \text{FBQP}_W(a)$, it holds that $\text{QMA} \cap \text{coQMA} \subseteq \text{BQP}$.

Let $L \in \text{QMA} \cap \text{coQMA}$. Then, there exists an $(2/3, 1/3; 2/3, 1/3)$-Quantum Verification Procedure $Q^2 = \{Q^2_n : n \in \mathbb{N}\}$ such that for every $x$ of length $n$, either both Eqs. (102) and (103), or both Eqs. (104) and (105) hold.

Denote by $B_{Q^2}(x) = \{|\psi_i^2\rangle\}$ the eigenbasis of $Q^2$ for $x$ and by $p_i = \Pr[Q^2_n(x, |\psi_i^2\rangle) = 1]$ the acceptance probability of $|\psi_i^2\rangle$.

Note that the definition of $(2/3, 1/3; 2/3, 1/3)$-procedures implies that

\[
\begin{align*}
\text{if } x \in L & \text{ then } \frac{1}{3} \leq p_i \leq 1 \forall i, \\
& \text{ and } \exists p_i > \frac{5}{6}; \\
\text{if } x \notin L & \text{ then } 0 \leq p_i \leq \frac{2}{3} \forall i, \\
& \text{ and } \exists p_i < \frac{1}{6}.
\end{align*}
\]

Step 3: $\frac{13}{18}$-total procedure $Q^T$ The next step of the proof is to construct from $Q^2$ a total procedure $Q^T$ which has the same eigenbasis $B_{Q^2}(x)$ as $Q^2$. This will allow us to use the hypothesis that $\text{TFQMA}_W(a) \subseteq \text{FBQP}_W(a)$.

For simplicity, we construct $Q^T$ exactly as in Step 1 of the proof of Theorem 16 (using the construction in the paragraph surrounding Eqs. (128), (129), (130)). This yields a $\frac{13}{18}$-total procedure $Q^T = \{Q^T_n : n \in \mathbb{N}\}$ which has the same eigenbasis $B_{Q^2}(x)$ as $Q^2$. We denote by $p^T_i = \Pr[Q^T_n(x, |\psi_i^2\rangle) = 1]$ the acceptance probability of $|\psi_i^2\rangle$ by procedure $Q^T$. We have that $p^T_i = \beta(p_i)$ with

\[
\beta(p_i) = p^2_i + (1 - p_i)^2,
\]

see Eq. (129).

The hypothesis $\text{TFQMA}_W(a) \subseteq \text{FBQP}_W(a)$ implies that there exists an efficiently preparable family of density matrices $\{\rho(x)\}$ such that for all $x$

\[
\Pr[Q^T_n(x, \rho(x)) = 1] \geq \beta \left(\frac{5}{6}\right) = \frac{13}{18}.
\]
However, Eq. (139) does not tell us about the overlap of $\rho$ with the accepting space $H_{Q^T}^{13/18}(x) = H_{Q^2}^{[0,1/6]}[5/6,1](x)$. In fact, this overlap could be exponentially small (see Example 1 for an explanation). But if we consider a slightly large space, for instance $H_{Q^2}^{[0,1/4]}[3/4,1](x)$, then the overlap of $\rho$ with this larger space can be lower bounded. We proceed to compute such a lower bound.

In what follows, we take $x \in L$. In this case, $H_{Q^2}^{13/18}(x) = H_{Q^2}^{[5/6,1]}(x)$ (the accepting probabilities are all larger than $1/3$, see Eq. (134)), and we will lower bound the overlap of $\rho$ with $H_{Q^2}^{[3/4,1]}(x)$.

We denote $\rho_{ij} = \langle \psi^2_i | \rho | \psi^2_j \rangle$ the matrix elements of $\rho$ in the eigenbasis of $Q^2$. Because there is no interferences between eigenbasis states, we have

$$\Pr[Q^2_n(x, \rho(x))] = \sum_i p_i \rho_{ii},$$
$$\Pr[Q^T_n(x, \rho(x))] = \sum_i \beta(p_i) \rho_{ii}. \quad (140)$$

Hence, for $x \in L$, we have

$$\beta\left(\frac{5}{6}\right) \leq \Pr[Q^T_n(x, \rho(x)) = 1]$$
$$= \sum_{i: \frac{1}{3} \leq p_i < \frac{3}{4}} \beta(p_i) \rho_{ii} + \sum_{i: \frac{3}{4} \leq p_i \leq 1} \beta(p_i) \rho_{ii}$$
$$\leq \sum_{i: \frac{1}{3} \leq p_i < \frac{3}{4}} \beta\left(\frac{3}{4}\right) \rho_{ii} + \sum_{i: \frac{3}{4} \leq p_i \leq 1} \beta(1) \rho_{ii}$$
$$= \beta\left(\frac{3}{4}\right) + \left(1 - \beta\left(\frac{3}{4}\right)\right) \sum_{i: \frac{3}{4} \leq p_i \leq 1} \rho_{ii}$$

where we have used Eq. (134), $\beta(1) = 1$, and the fact that over the interval $[1/3, 3/4]$, $\beta(p)$ has its maximum at $3/4$: $\max_{p \in [1/3, 3/4]} \beta(p) = \beta(3/4)$.

It then follows that

$$\sum_{i: \frac{3}{4} \leq p_i \leq 1} \rho_{ii} \geq \frac{\beta\left(\frac{5}{6}\right) - \beta\left(\frac{3}{4}\right)}{1 - \beta\left(\frac{3}{4}\right)} = \frac{7}{27} \quad (141)$$

This is the desired lower bound on the overlap of $\rho$ with $H_{Q^2}^{[3/4,1]}(x)$.

**Step 4: Procedure $Q^P$**

Unfortunately Eq. (141) cannot be used to directly prove that procedure $Q^2$ belongs to BQP. We therefore introduce an amplified version of $Q^2$ for which Eq. (141) will be sufficient.
We use Theorem 10 which implies that there exists a quantum verification procedure $Q^P$ such that $Q^2$ e-maps to $Q^P$ and such that the polynomial time computable strictly increasing functions $\{f_n\}$ that define the reduction satisfy

\[
\begin{align*}
  f_n(3/4) &= \frac{6}{7}, \\
  f_n(2/3) &= \frac{1}{7}.
\end{align*}
\]

Note that $Q^P$ has the same eigenbasis $B_{Q^2}(x)$ as $Q^2$ (and thus as $Q^T$). We denote by $p_i^P = \Pr[Q^P_n(x, |\psi_i^2\rangle) = 1]$ the acceptance probability of $|\psi_i^2\rangle$ by procedure $Q^P$. We have that $p_i^P = f_n(p_i)$.

We bound the success probability of $Q^P_n(x, \rho(x))$ when $x \in L$ and $\rho(x)$ is the efficiently preparable state that satisfies Eq. (139):

\[
\Pr[Q^P_n(x, \rho(x)) = 1] = \sum_i f_n(p_i) \rho_{ii} \geq \sum_{i : \frac{3}{4} \leq p_i \leq 1} f_n(p_i) \rho_{ii} \geq \sum_{i : \frac{3}{4} \leq p_i \leq 1} \frac{6}{7} \rho_{ii} \geq \frac{7 \cdot 6}{27} \cdot \frac{2}{9} = \frac{1}{7}
\]

where we have used Eqs. (141), (142), and the fact that $f_n$ is strictly increasing.

Let us bound the success probability of $Q^P_n(x, \rho)$ when $x \notin L$ and $\rho$ is an arbitrary state:

\[
\Pr[Q^P_n(x, \rho) = 1] = \sum_i f_n(p_i) \rho_{ii} = \sum_{i : 0 \leq p_i \leq \frac{2}{3}} f_n(p_i) \rho_{ii} \leq \sum_{i : 0 \leq p_i \leq \frac{2}{3}} f_n \left( \frac{2}{3} \right) \rho_{ii} = \frac{1}{7}
\]

where we have used Eq. (136), Eq. (143), and the fact that $f_n$ is strictly increasing.

Therefore $Q^P$ is a $(2/9, 1/7)$-procedure that defines the same language $L$ as $Q^2$. Furthermore, when $x \in L$, there exists an efficiently preparable witness. Thus, $Q^P$ satisfies the conditions of Definition 13, and $L \in BQP'\left(\frac{2}{9}, \frac{1}{7}\right) = BQP$. 

\[\Box\]
17 If there exists a QMA complete problem that robustly reduces to a problem in TFQMA, then QMA = QMA \cap \text{coQMA}

**Theorem 18** Let \( a' : \mathbb{N} \rightarrow [0, 1] \) be a polynomially time computable function. Let \(a, b\) be functions as in Definition 3. Suppose that there exists 1) an \((a, b)\)-quantum verification procedure \( Q = \{Q_n : n \in \mathbb{N}\} \) for a QMA-complete language \( L \), and 2) an \( a'\)-total quantum verification procedure \( Q^{(T)} = \{Q_n^{(T)} : n \in \mathbb{N}\} \), and 3) \( \epsilon \in 1/\text{poly} \) such that there exists a robust reduction from \( Q \) to \( Q^{(T)} \) with parameter \( \epsilon \in 1/\text{poly} \), then \( \text{QMA} = \text{QMA} \cap \text{coQMA} \).

**Proof** Step 0: idea of the proof

We denote by \((f, \Phi)\) the pair of a polynomial time computable function and an efficiently implementable channel that define the robust reduction in \( Q \) to \( Q^{(T)} \), and denote by \( \epsilon \in 1/\text{poly} \) the parameter of the robust reduction, see Definition 27.

We denote by \( L \) the language associated with \( Q \). We denote by \( \bar{L} \) the complement of \( L \). We will show that under the hypothesis of Theorem 18, \( L \in \text{QMA} \). To this end, we will construct a procedure \( Q^{CO} \) which rejects on all states when \( x \in L \), but which accepts on some states when \( x \in \bar{L} \).

The basic idea behind the construction of \( Q^{CO} \) is similar to the proof in the classical case given in [1]. Namely, given \( x \) and given an input state \( |\psi\rangle \), we first check whether \( |\psi\rangle \) is a witness for \( Q^{(T)}(f(x)) \). If this check is successful, we check if \( Q(x, \Phi(|\psi\rangle)) \) rejects in which case we accept, while if \( Q(x, \Phi(|\psi\rangle)) \) accepts we reject.

That \( Q^{CO} \) thus constructed should have the desired properties follows from the following reasoning. If \( x \in L \) then either \( |\psi\rangle \) is not a witness for \( Q^{(T)}(f(x)) \) and consequently \( Q^{CO} \) rejects, or \( |\psi\rangle \) is a witness for \( Q^{(T)}(f(x)) \), in which case \( Q(x, \Phi(|\psi\rangle)) \) will accept, and therefore, \( Q^{CO} \) again rejects. On the other hand, if \( x \in \bar{L} \), then the second step (testing whether one has a witness for \( Q \)) will always fail, and in this case \( Q^{CO} \) accepts. Because \( Q^{(T)} \) is a total procedure, one can always find a state on which the first step accepts. Therefore, for \( x \in \bar{L} \) there exists at least one a state on which \( Q^{CO} \) accepts.

However, there are several complications in the quantum case. We have prepared for these complications by our earlier theorems and definitions. First, it is not obvious that we can use the input state twice. We solve this by replacing \( Q^{(T)} \) by a nondestructive version of \( Q^{(T)} \) (Theorem 12).

Second, we need to be able to amplify the completeness and soundness probabilities without distorting the structure of the witness states. This is achieved through e-maps (Theorems 10 and 12). The amplified nondestructive version of \( Q^{(T)} \) is denoted \( \tilde{Q}^{(T)} \). We also introduce an amplified version of \( Q \), which we denote \( \tilde{Q} \).

Thirdly, we need to deal with the eigenstates of \( Q^{(T)} \) which have acceptance probability equal to \( a' - \delta \), with \( \delta \) exponentially small (see Example 1). This is addressed by requiring in the statement of the theorem that the reduction from \( Q \) to \( Q^{(T)} \) is a robust reduction (Definition 27). This ensures that eigenstates with acceptance probability equal to \( a' - \delta \) (if they exist) can be treated in the same way as the real witnesses (i.e. the eigenstates that have acceptance probability greater or equal to \( a' \)).

**Step 1: preliminary definitions**
Procedure $Q_n$ has as input a classical bit string of length $n$, a witness state of $m(n)$ qubits, and ancilla state of $k(n)$ qubits. We denote

$$\eta = 2^{-m-2}. \quad (146)$$

Using Theorem 12, we construct a $(1-\eta)$-total nondestructive procedure $\tilde{Q}^{(T)}$ such that $Q^{(T)}$ e-maps to $\tilde{Q}^{(T)}$ and such that the polynomial time computable strictly increasing functions $f_n^{(T)}$ that define the e-map satisfy $f_n^{(T)}(a') = 1 - \eta$, $f_n^{(T)}(a' - \epsilon) = \eta$.

Using Theorem 10, we construct a $(1 - \eta, \eta)$-procedure $\tilde{Q}$ such that $Q$ e-maps to $\tilde{Q}$, and such that the polynomial time computable strictly increasing functions $\tilde{f}_n$ that define the e-map satisfy $\tilde{f}_n(a) = 1 - \eta$, $\tilde{f}_n(b) = \eta$.

**Step 2: procedure $Q^{CO}$**

We define procedure $Q^{CO}$ as follows:

1. Denote by $(x, |\psi\rangle)$ the input to $Q^{CO}$.
2. Run $\tilde{Q}^{(T)}$ on input $(f(x), |\psi\rangle)$.
3. If $\tilde{Q}^{(T)}(f(x), |\psi\rangle) = 0$ (i.e. $\tilde{Q}^{(T)}$ rejects), output 0 (i.e. $Q^{CO}$ rejects).
4. If $\tilde{Q}^{(T)}(f(x), |\psi\rangle) = 1$, then apply $\Phi$ to the quantum output of $\tilde{Q}^{(T)}$. Denote by $|\tilde{\psi}\rangle$ the state so obtained.
5. Run $\tilde{Q}$ on input $(x, |\tilde{\psi}\rangle)$.
6. If $\tilde{Q}_n(x, |\tilde{\psi}\rangle) = 1$ (i.e. $\tilde{Q}$ accepts), output 0 (i.e. $Q^{CO}$ rejects).
7. If $\tilde{Q}_n(x, |\tilde{\psi}\rangle) = 0$ (i.e. $\tilde{Q}$ rejects), output 1 (i.e. $Q^{CO}$ accepts).

We now show that $Q^{CO}$ is a $((1 - \eta)^2, 1/4)$-procedure, and that the language associated with $Q^{CO}$ is $\bar{L}$, which proves the result.

**Step 3: Existence of a witness when $x \in \bar{L}$**

Take any $x \in \bar{L}$. Let $|\psi_i\rangle$ be an eigenstate of $Q^{(T)}$ with acceptance probability $p_i \geq a'$. Such an eigenstate exists, since $Q^{(T)}$ is an $a'$-total procedure. We will show that $Q^{CO}$ accepts on input $(x, |\psi_i\rangle)$ with probability $\geq (1 - \eta)^2$.

To this end note that on this input, step 4 of procedure $Q^{CO}$ succeeds with probability $\geq 1 - \eta$ and that the quantum output at step 4 is $|\psi_i\rangle$, i.e. it is not affected running $\tilde{Q}^{(T)}$ in step 2. This is where the nondestructiveness of $\tilde{Q}^{(T)}$ is used.

However, $x \in \bar{L}$. Therefore, in step 7, $\tilde{Q}$ outputs 0 with probability at least $1 - \eta$. Hence, the overall probability that $Q^{CO}$ accepts on input $(x, |\psi_i\rangle)$ is at least $(1 - \eta)^2$.

**Step 4: soundness probability of $Q^{CO}$ on eigenstates of $Q^{(T)}$**

Take any $x \in L$. Let $|\psi_i\rangle$ be an eigenstate of $Q^{(T)}$ with acceptance probability $p_i$. Consider the acceptance probability of $Q^{CO}$ on input $(x, |\psi_i\rangle)$.

- If $p_i < a' - \epsilon$, then $Q^{CO}$ rejects with probability at least $1 - \eta$ at step 3.
- If $p_i \geq a' - \epsilon$, then $Q^{CO}$ either rejects at step 3, or passes to step 5. In the latter case, the input of $\tilde{Q}$ is $(x, \Phi(x, |\psi_i\rangle))$, where $\Phi(x, |\psi_i\rangle)$ is a witness for $\tilde{Q}$ for $x$ (see definition of robust reductions). That is, $\tilde{Q}$ will accept on input $(x, \Phi(x, |\psi_i\rangle))$ with probability at least $1 - \eta$. Hence, the probability that $Q^{CO}$ rejects at step 6 is $\geq 1 - \eta$.

Thus, on all eigenstates $|\psi_i\rangle$ of $Q^{(T)}$, $Q^{CO}$ rejects with probability at least $1 - \eta$.

Note that this is the step where we use that the reduction from $Q$ to $Q^{(T)}$ is robust with parameter $\epsilon = 1/poly$. If we set $\epsilon$ to zero, then in step 4 we have no control.
over how the reduction acts on eigenstates of $Q^{(T)}$ which have acceptance probability equal to $a' - \delta$ with $\delta$ exponentially small.

**Step 5: soundness probability of $Q^{CO}$ on arbitrary states**

Take any $x \in L$. Let us now consider the probability that $Q^{CO}$ rejects on an arbitrary input state $\rho$. The acceptance probability of $Q^{CO}$ can be written as

$$\Pr[Q_n^{CO}(x, \rho) = 1] = \text{Tr}(M_1 \rho)$$  \hspace{1cm} (147)

where $M_1$ is the POVM element corresponding to $Q^{CO}$ accepting. Note that $M_1$ is a positive matrix of size $2^m \times 2^m$.

We have established at Step 4 that for all $i$

$$0 \leq \langle \psi_i | M_1 | \psi_i \rangle \leq \eta. \hspace{1cm} (148)$$

It then follows that for all $i, j$

$$|\langle \psi_i | M_1 | \psi_j \rangle| \leq \eta. \hspace{1cm} (149)$$

(To see this, consider the restriction of $M_1$ to the 2-dimensional space spanned by $\{ |\psi_i \rangle, |\psi_j \rangle \}$. Restricted to this space, $M_1$ is a $2 \times 2$ positive matrix with diagonal elements bounded by $\eta$. The positivity of this $2 \times 2$ matrix implies that its determinant is positive, which implies Eq. (149)).

As a consequence, $\text{Tr}M_1^2 \leq \eta^2 2^{2m} \leq 2^{-4}$.

Using the Cauchy–Schwarz inequality, we have

$$\Pr[Q_n^{CO}(x, \rho) = 1]^2 = |\text{Tr}[M_1 \rho]|^2 \leq \text{Tr}[M_1^2] \text{Tr}[\rho^2] \leq \text{Tr}[M_1^2] \leq 2^{-4}. \hspace{1cm} (150)$$

Consequently, $\Pr[Q_n^{CO}(x, \rho) = 1] \leq 1/4.$ \hspace{1cm} $\Box$

**18 Conclusion**

In the present work, we have shown that $\text{TFQMA} = \text{F}(\text{QMA} \cap \text{coQMA})$; that if $\text{FBQP} = \text{TFQMA}$, then $\text{BQP} = \text{QMA} \cap \text{coQMA}$; and that if there is a QMA complete problem that strongly reduces to a problem in TFQMA, then $\text{QMA} \cap \text{coQMA} = \text{QMA}$.

These results are not very surprising, as they are immediate generalisations of the analog classical results. However, they are significantly more complicated to prove than the classical results.

In appendix, we sketch how similar results can be obtained for the classical probabilistic classes $\text{MA}$ and $\text{coMA}$. However, since one can always take $\text{MA}$ to have one sided error $[17]$, slightly stronger results should hold in this case. We leave the detailed results to further work.
It would be interesting to better understand the inclusions

\[ BQP \subseteq QMA \cap \text{coQMA} \subseteq QMA. \]  

(151)

In one direction, exhibiting problems in \( QMA \cap \text{coQMA} \) that do not seem to be in \( BQP \), and problems in \( QMA \) that do not seem to be in \( QMA \cap \text{coQMA} \), would provide evidence that the inclusions are strict.

In the statement of Theorem 18 we use the notion of robust reduction, see Definition 27. It may be that the theorem can be proved using the weaker notion of reduction given in Definition 25, but this probably requires new proof techniques. Alternatively, it is possible that the notion of robust reduction is the natural notion. Some evidence for this is given at the end of Sect. 8.2.

Acknowledgements Research at CQT is funded by the National Research Foundation, the Prime Minister’s Office, and the Ministry of Education, Singapore under the Research Centres of Excellence programme’s research grant R-710-000-012-135.

Appendix: MA and coMA

The questions we ask and answer in the present work concerning TFQMA and QMA \( \cap \) coQMA can also be asked about the analog probabilistic classical classes TFMA and MA \( \cap \) coMA.

However, in [17] it was shown that one can always take MA to have one sided error only. As a consequence, the results we obtain for TFQMA and QMA \( \cap \) coQMA can certainly be strengthened in the case of TFMA and MA \( \cap \) coMA. Investigating this would require further work and is not reported in the present paper.

Nevertheless, most of our proof techniques are in fact classical and can be easily be adapted to the probabilistic classical classes TFMA and MA \( \cap \) coMA. In the following paragraphs, we provide a dictionary allowing to pass from the classical to the quantum case. We also point out what parts of our arguments are classical, and what parts are intrinsically quantum. The aim of this qualitative appendix is to help to the reader with the main text, as the arguments concerning the quantum classes will be easier to follow when comparing with the corresponding probabilistic classical classes.

Definition 39 (Probabilistic verification procedure). A probabilistic verification procedure is a polynomial time uniform family of classical circuits \( C = \{C_n : n \in \mathbb{N}\} \) with \( C_n \) taking as input \( (x, y, z) \), where \( x \in \{0, 1\}^n \) is a binary string of length \( n \), \( y \) is a binary string of length \( m(n) \) with \( m = m(n) \), \( z \) is a string of random bits (identically independently distributed with bias \( 1/2 \)) of length \( l(n) \) with \( l = l(n) \in \text{poly} \). For fixed value of \( z \), the output of the circuit of \( C_n \) is a bit which we denote by \( C_n(x, y, z) \). We denote by \( p_y = \Pr_z[C_n(x, y, z) = 1] \).

Using this definition of probabilistic verification procedures, classes MA, coMA, MA \( \cap \) coMA are readily defined. Thus, for instance, languages \( L \in \text{MA} \) are those for which there exists \( C \) such that if \( x \in L \), then \( \exists y \) such that \( p_y \geq 2/3 \), and if \( x \notin L \), then \( \forall y \) we have \( p_y \leq 1/3 \).
For fixed $x$, the quantum analog of the couples $(y, p_y)$ are the eigenstates and their acceptance probabilities $(|\psi_i\rangle, p_i)$. Inputing an arbitrary pure state $|\psi\rangle$ or mixed state to a quantum verification procedure is analogous in the classical case to inputing a probabilistic distribution over $y$, see Theorem 3.

The analog of the accepting and rejecting subspaces, see Definition 19, are the following sets

$$S^a_C(x) = \left\{ y : \Pr_{z}[C_n(x, y, z) = 1] \geq a \right\},$$

$$S^b_C(x) = \left\{ y : \Pr_{z}[C_n(x, y, z) = 1] \leq b \right\}. \tag{152}$$

The class Functional MA (FMA) can be defined in terms of these sets, as well as the class Total Functional MA (TFMA). (Note that functional classes based on witnesses are not relevant in the classical case, as they would correspond to probabilistic distribution over $y$’s).

In the classical case, for fixed $x$ and $y$, one can sample repeatedly from the distribution $p_y$. Remarkably in the quantum case this is also possible, even though cloning of quantum states is impossible [13].

For fixed $x$ and $y$, if one wants to modify the acceptance probability $p_y$, a simple and natural procedure is to sample $N$ times from the distribution $p_y$, yielding a Binomial distribution $B(N, p_y)$. If one obtains $k$ heads, one tosses a new coin with bias $g(k)$. This yields a new acceptance probability $p_y' = P_g(p_y)$ (where the function $P_g$ depends on $N$ and the choice of function $g(k)$). This classical procedure can be implemented quantumly, in which case we call it an iterative procedure, see Definition 29.

We show in Theorem 9 that if $g$ is increasing and nonconstant, the function relating the new and old acceptance probabilities $p_y' (p_y)$ is strictly increasing. We then show in Theorem 10 that by taking $N$ sufficiently large, and appropriate $g$, the strictly increasing function $p_y' (p_y)$ can be made to pass through a finite number of points. These two results are purely classical, and apply both the classical and quantum iterative procedures.

The notion of nondestructive procedure, Definition 30, is nontrivial in the quantum case. In the classical case it is trivial, as one can copy at will the input.

In Sect. 13, we give three definitions of $\text{QMA} \cap \text{coQMA}$ and show that they are equivalent. Exactly the same definitions can be given for $\text{MA} \cap \text{coMA}$, and the proofs of equivalence also holds in the classical case. In particular, $\text{MA} \cap \text{coMA}$ can be defined in terms of a single probabilistic verification procedure. The class Functional $\text{MA} \cap \text{coMA}$ can then be defined in terms of the sets

$$S^a_C &= \left[ 0, \frac{1-a}{2} \right] \cup \left[ \frac{1+a}{2}, 1 \right] \tag{153}$$

as in Definition 36.
One can then prove analogs of the key results of Sects. 15, 16, and 17, namely that TFMA equals Functional MA ∩ coMA, that if TFMA is included in FBPP, then MA ∩ coMA equals BPP, and that if there exists a MA complete problem that robustly reduces to a problem in TFMA, then MA = MA ∩ coMA. Indeed, the proofs of all these results are in fact classical.

References

1. Megiddo, N., Papadimitriou, C.H.: On total functions, existence theorems and computational complexity. Theor. Comput. Sci. 81, 317–324 (1991)
2. Johnson, D.S., Papadimitriou, C.H., Yannakakis, M.: How easy is local search? J. Comput. Syst. Sci. 37(1), 79–100 (1988)
3. Papadimitriou, C.H., Schaefer, A.A., Yannakakis, M.: On the complexity of local search. In: Proceedings of the ACM 22nd Annual Symposium on Theory of Computing, pp. 438–445 (1990)
4. Krentel, M.W.: Structure in locally optimal solutions. In: Proceedings of the IEEE 30th Annual Symposium on Foundations of Computer Science, pp. 216–221 (1989)
5. Papadimitriou, C.H.: On the complexity of the parity argument and other inefficient proofs of existence. J. Comput. Syst. Sci. 48(3), 498–532 (1994)
6. Daskalakis, C., Goldberg, P.W., Papadimitriou, C.H.: The complexity of computing a Nash equilibrium. SIAM J. Comput. 39(1), 195–259 (2009)
7. Chen, X., Deng, X., Teng, S.H.: Settling the complexity of computing two-player Nash equilibria. J. ACM 56(3), 14–57 (2009)
8. Goldberg, P.W., Papadimitriou, C.: Towards a unified complexity theory of total functions. J. Comput. Syst. Sci. 94, 167–192 (2018)
9. Kitaev, A.Y., Shen, A.H., Vyalyi, M.N.: Classical and quantum computation. Graduate Studies in Mathematics, vol. 47 (AMS, Providence, RI) (2002)
10. Bookatz, A.D.: QMA-complete problems. Quantum Information and Computation, vol. 14, pp. 361–383. arXiv preprint arXiv:1212.6312 (2014)
11. Janzing, D., Wocjan, P., Beth, T.: Cooling and low energy state preparation for 3-local Hamiltonians are FQMA-complete. arXiv preprint arXiv:quant-ph/0303186 (2003)
12. Massar, S., Santha, M.: Total functions in QMA. Quantum Information Processing, vol. 20, pp. 35. arXiv preprint arXiv:1805.00670 (2021)
13. Marriott, C., Watrous, J.: Quantum Arthur–Merlin games. Comput. Complex. 14(2), 122–152 (2005)
14. Nagaji, D., Wocjan, P., Zhang, Y.: Fast amplification of QMA. Quantum Inf. Comput. 9(11), 1053–1068 (2009)
15. Aharonov, D., Ben-Or, M., Brandão, F.G.S.L., Sattath, O.: The pursuit for uniqueness: extending Valiant–Vazirani theorem to the probabilistic and quantum settings. arXiv preprint arXiv:0810.4840 (2008)
16. Deshpande, A., Gorshkov, A.V., Fefferman, B.: The importance of the spectral gap in estimating ground-state energies. arXiv preprint arXiv:2007.11582 (2020)
17. Fürer, M., Goldreich, O., Mansour, Y., Sipser, M., Zachos, S.: On completeness and soundness in interactive proof systems. In: Micali, S. (ed.) Advances in Computing Research: A Research Annual (Randomness and Computation), vol. 5, pp. 429–442 (1989)

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.