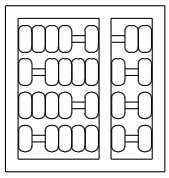

INSTITUTO DE COMPUTAÇÃO
UNIVERSIDADE ESTADUAL DE CAMPINAS

Classical Probabilistic Checkable Proof and Multi-Prover Quantum Merlin-Arthur

F. G. Jeronimo *A. V. Moura*

Technical Report - IC-14-16 - Relatório Técnico

October - 2014 - Outubro

Classical Probabilistic Checkable Proof and Multi-Prover Quantum Merlin-Arthur

Fernando Granha Jeronimo [*] Arnaldo Vieira Moura [†]

Abstract

Classically, extending the Merlin-Arthur complexity class to multiple provers does not increase its computational power since multiple Merlins can be simulated by a single one. However, in the quantum model an analogous result may no longer hold if the provers are assumed to be unentangled. Surprisingly, NP-complete problems admit quantum Multi-prover Merlin-Arthur protocols in which only two unentangled witnesses of logarithm size are used. In this work, we extend one protocol so that it can simulate generic classical Probabilistic Checkable Proofs (PCP) verifiers. By combining this new protocol with specific PCPs theorems, it is possible to recover known results in a simplified way. The first result is a Two-prover QMA protocol for $3SAT$ with logarithmic size witnesses and a completeness soundness gap of $\Omega(\frac{1}{n^{2+\varepsilon}})$ for any $\varepsilon > 0$. The second one is a known characterization of NEXP.

1 Introduction

Witness verification protocols have a relevant role in Computational Complexity since they capture several problems of practical interest [1]. Languages whose membership can not be even certified in polynomial time are beyond polynomial time solvability. The famous P vs. NP question asks the converse: can all efficient certifiable languages be efficiently solved? With the advent of quantum computing [2], witness verification protocols have been extended and adapted to this new quantum model. Unique quantum mechanical properties lead to models that bare no resemblance to classical ones. Classically, having multiple witnesses does not change the computational power. However, in the quantum case, can the lack of entanglement make the system more powerful?

This question was firstly studied by Kobayashi et al. who introduced the class QMA(k) [3]. It captures the notion of k unentangled quantum provers. An entanglement correlation is a unique quantum mechanical property that can not be described classically, as attested in practice by violations of Bell inequalities [4]. These super classical correlations can be an important resource in certain quantum information processing tasks such as superdense

[*]This work was supported in part by FAPESP 2013/20661-1. F. G. Jeronimo is with the Institute of Computing, University of Campinas, Campinas, SP Brazil (e-mail: fegranha@gmail.com).

[†]A. V. Moura is with the Institute of Computing, University of Campinas, Campinas, SP Brazil (e-mail: arnaldo@ic.unicamp.br).

coding and teleportation [5]. Nonetheless, in the context of Multi-prover proof systems entanglement shared among the provers might harm their soundness. Exploring the hypothesis that the proofs are not entangled may lead to distinctive features of theses systems. Understanding these features, creating methods to detect entanglement, or even to break it [6], are important research directions underlying the study of the complexity class QMA(k).

Blier and Tapp conceived a verifier protocol in $\mathrm{QMA}(2)_{\log(n)}$ for the vertex three-coloring problem on graphs ($3COL$) [7]. Since this is a NP-complete problem, it follows that $\mathrm{NP} \subseteq \mathrm{QMA}(2)_{\log(n)}$. This means that it suffices to have two unentangled quantum proofs of logarithm size to verify if a language is in NP. This type of protocol is an indication that unentanglement might increase the computational power of a proof system.

In this work, we extend Blier and Tapp's protocol to create a generic QMA(k) verifier capable of simulating classical PCP verifiers. With this generalization, several classical PCP results can benefit from an exponential proof size reduction in the quantum setting. On the other hand, this dramatic reduction comes at the cost of reducing the completeness-soundness gap. Furthermore, we show that it is possible to recover two known results in a simplified way. Firstly, a $\mathrm{QMA}(2)_{\log(n)}$ verifier for $3SAT$ with completeness-soundness gap of $\Omega(\frac{1}{n^{2+\varepsilon}})$ for any $\varepsilon > 0$, which lies between the Beigi [8] and the Le Gall et al. [9] results. Secondly, we also have a proof of $\mathrm{QMA}(2) = \mathrm{NEXP}$ in the context of small gap [10].

The organization of the article is as follows. In section 2, related results about Quantum Merlin-Arthur Multi-provers are discussed. In section 3, definitions and theorems used in this paper are stated. Our main result, the verifier protocol that simulates a generic PCP classical verifier, is presented in section 4, along with some implications for two concrete classical PCP theorems. Finally, in section 5 we conclude with some open questions. We assume familiarity with Quantum Computing [11] and Computational Complexity [12].

2 Related Work

The discovery of NP-complete verifier protocols in the context of unentangled Multi-prover Quantum Merlin-Arthur provers with logarithmic proof size attracted much attention to the complexity class QMA(k) and its variations. These variations may concern the number of provers, the proof size, and the type of measurements used by the verifier. Even though a large number of results are now known, tight bounds for this class remain a major open question. In this section, we briefly survey some of these results and we highlight some connections with our work.

What makes QMA(k) surprising is that if protocols such as the one of Blier and Tapp were true for the classical Multi-prover case, it would imply that P = NP. A brute force algorithm would just need to enumerate all possible proofs and check them. Given that the proof length is logarithmic, the total number of proofs is polynomial in the input size. As a result, this algorithm would require only polynomial time. However, in the quantum case we do not know how to search separable (not entangled) states efficiently [13]. In fact, the problem of deciding if a classical description of a density operator is close to a separable one was shown to be NP-hard when the distance depends on an inverse polynomial in the dimension [14].

Aaronson et al. showed that with $O(\sqrt{n}\log(n))$ proofs of logarithm size it is possible to verify a $3SAT$ instance with a constant completeness-soundness gap [6]. The original protocol of Blier and Tapp (BT) used only two proofs and achieved a gap of $\Omega(\frac{1}{n^6})$ for $3COL$ [7]. Subsequent works have improved this gap. Beigi devised a protocol for $3SAT$ with gap $\Omega(\frac{1}{n^{3+\epsilon}})$ [8]. Afterwards, Chiesa et al. using the same original ideas of BT improved the previous analysis for $3COL$ to a gap of $\Omega(\frac{1}{n^2})$ [10]. Finally, Le Gall et al. using the BT protocol improved the gap to $\Omega(\frac{1}{n\text{polylog}(n)})$ for $3SAT$, but now combined with a gapped Constraint Satisfaction instance from Dinur's PCP Theorem [15] [9].

Chen and Drucker simplified the analysis of Aaronson et al. in [6], providing a BellQMA protocol for $3SAT$ [16]. The BellQMA is a restricted class of QMA protocols in which the verifier is neither allowed to make entangled measurements nor condition them to previous outcomes.

Harrow and Montanaro showed that $\text{QMA}(k) = \text{QMA}(2)$ for k a polynomial in the input size [17]. This result is a corollary of a method called "product test". Given the hypothesis of having two equal unentangled states, the product test succeeds with high probability if and only if these states are close to a product of k sub-states. In other words, given a bipartite unentanglement hypothesis, it is possible to verify k-partite entanglement. An important question is how difficult it is to verify k-partite entanglement without this hypothesis.

Chailloux and Sattath using the ideas of Harrow and Montanaro for $\text{QMA}(k) = \text{QMA}(2)$ showed that the Separable Sparse Hamiltonian problem is QMA(2)-complete whereas the Separable Local Hamiltonian problem is still only QMA-complete [18]. Moreover, two other problems were shown to be QMA(2)-complete namely QPROD-ISOMETRY and QSEP-ISOMETRY. These problems ask for an input to the isometry such that the output is close to a product and a separable state, respectively. Furthermore, an explicit algorithm for QMA(2) achieving better than a NEXP upper bound for special cases was given in [19].

Using a new quantum de Finetti Theorem, Brandão et al. showed that for the special case of parallel one-way LOCC ($\mathbf{LOCC}_1^{\|}$) verifiers, it holds that $\text{QMA}(k)_{\mathbf{LOCC}_1^{\|}} = \text{QMA}$ for $k \in O(1)$ [20]. In a k party system, the parallel one-way LOCC class of measurements operationally works as follows: the first $k-1$ parties apply each a POVM independently, and the the last system is measured conditioned on the previous outcomes. Latter, this result was extended to show that $\text{BellQMA}(k) = \text{QMA}$ for a polynomial k [21]. An analogous result was shown to the fully one way LOCC class ($\mathbf{LOCC}_1$) in which each party is measured sequentially with a POVM defined by previous outcomes [22]. This result led to a more general collapse in which $\text{QMA}(k)_{\mathbf{LOCC}_1} = \text{QMA}$ for a polynomial k.

Pereszlényi analyzed the case of QMA(2) with small gaps, in which small means at most inverse exponential in the input size [23]. Using the same ideas of Blier and Tapp [7] and a NEXP-complete problem, he devised a protocol to show that NEXP is equal to QMA(2) with a small gap. Assuming EXP $\neq$ NEXP and using the fact that QMA with small gap is contained in EXP, we have a separation between QMA and QMA(2) in this small gap context. Combining our generic QMA(2) protocol and the classical PCP verifier in the proof $\text{NEXP} \subseteq \text{PCP}(poly(n), O(1))$, we can achieve a similar result.

Apart from the collapse $\text{QMA}(k) = \text{QMA}(2)$, there are many open questions regarding the power of QMA(2). For the general case, a lower bound better than the trivial QMA

is not known. Neither is an upper bound better than the trivial NEXP one. Watrous and Marriott showed that $\mathrm{QMA}(1)_{\log(n)} \subseteq \mathrm{BQP}$ [24], but this proof is not enough to show $\mathrm{QMA}(2) = \mathrm{QMA}$.

3 Preliminaries

In this section, we define complexity classes and state a few theorems which are relevant to this work.

3.1 Classical Proof Verification

The complexity class NP captures the languages that can be efficiently *i.e*, in polynomial time, decided by a deterministic classical verifier.

Definition 3.1. *A language L is in* NP *if there exists a deterministic polynomial time verifier V and a polynomial p such that*

- *for all $x \in L$, there exists a witness $y \in \{0,1\}^{p(|x|)}$, such that $V(x,y)$ accepts;*
- *for all $x \notin L$ and $y \in \{0,1\}^{p(|x|)}$, $V(x,y)$ rejects.*

In the above statement, the string y is referred interchangeably as a proof, a witness or a certificate. It attests the membership of x in the language L and it can be thought of as being given to the verifier by a computationally unbounded prover.

If the deterministic verifier in the definition of NP was replaced by a probabilistic one, it might be possible to reduce the number of inspected positions in order to decide whether the input x belongs to the language, and with a low error probability. This notion of probabilistic verification is captured by the Probabilistic Checkable Proofs (PCP) class. This class is usually parameterized by the amount of randomness $r(n)$, the number of queried position $q(n)$, the proof alphabet size, and the completeness and the soundness of the verifier. It can be formally stated as follows.

Definition 3.2. *A language L is in* $\mathrm{PCP}_{1,1-\epsilon}(r(n), q(n))_{\Sigma}$ *if there exist a probabilistic verifier V and a polynomial p such that*

- ***Completeness**: for all $x \in L$, then there exists a witness $y \in \Sigma^{p(|x|)}$ such that $P[V(x,y)$ accepts$] = 1$.*
- ***Soundness**: for all $x \notin L$ and $y \in \Sigma^{p(|x|)}$ $P[V(x,y)$ accepts$] \leq 1 - \epsilon$.*

V uses at most $r(n)$ random bits, makes at most $q(n)$ queries to y.

What makes this probabilistic characterization so attractive is that it was shown that NP has an alternative characterization as $\mathrm{PCP}_{1,\frac{1}{2}}(O(\log(n), O(1))$. This means that its is possible to rewrite any witness of a NP instance in such a way that a probabilistic verifier only queries a constant number of positions [25] [26].

Many different characterization of NP have been proposed in terms of PCPs. The following is an specific characterization of the NP-complete problem $3SAT$.

Theorem 3.3 (Theorem 7 from [26]). *There exist a constant $\delta > 0$ and an alphabet Σ of constant size such that $3SAT \in \mathrm{PCP}_{1,1-\delta}(O(\log(n)), 2)$. Moreover, the PCP verifier makes two query projection tests and the proof size m is almost linear, that is $m = n^{1+o(1)}$.*

Note that there are equivalent formulations of PCPs in terms of constraint satisfaction problems and multi-player games [15] [12]. Here, we focus our attention on the verifier characterization.

There is also a similar result for the scaled up analogue of NP denoted NEXP. The NEXP class is defined as follows.

Definition 3.4. *A language L is in* NEXP *if there exists an exponential time deterministic verifier V and a polynomial p such that*

- *for all $x \in L$, there exists a witness $y \in \{0,1\}^{2^{p(|x|)}}$, such that $V(x,y)$ accepts;*
- *for all $x \notin L$ and $y \in \{0,1\}^{2^{p(|x|)}}$, $V(x,y)$ rejects.*

The PCP verifier for NEXP also queries only a constant number of bits as stated by the next Theorem.

Theorem 3.5 (Adapted from Theorem 2.7 of [27]).

$$\mathrm{NEXP} \subseteq \mathrm{PCP}_{1,\frac{1}{2}}(O(poly(n), O(1))_{\Sigma}$$

where $\Sigma = \{0,1\}$ and the verifier runs in $poly(n)$ time.

3.2 Quantum Proof Verification

The concept of proof verification was also extended to the quantum model,leading to the class QMA. This class extends NP by allowing the witness and the verification procedure to be quantum ones. In fact, since quantum computation is inherently probabilistic its closest classical analogue is MA.

Definition 3.6. *A language L is in* $\mathrm{QMA}(c(n), s(n))$ *if there are polynomial time computable functions $c, s : \mathbb{N} \to [0,1]$, such that for every $x \in \{0,1\}^n$ there is a polynomial time quantum verifier V_x satisfying*

- ***Completeness**: if $x \in L$, there is a witness $|\psi\rangle$ with $\Pr[V_x|\psi\rangle$ accepts$] \geq c(n)$.*
- ***Soundness**: if $x \notin L$, then for all $|\psi\rangle$ $\Pr[V_x|\psi\rangle$ accepts$] \leq s(n)$.*

Moreover, the witness has $p(n)$ qubits for some polynomial p and the completeness soundness gap $c(n) - s(n)$ is at least $\frac{1}{g(n)}$ for some polynomial $g(n)$.

In the previous definition, given that the fraction $\frac{1}{g(n)}$ is an inverse polynomial, it is possible to amplify a QMA protocol to achieve an exponentially small completeness and soundness errors without changing the witness size [24]. In this case, even tough completeness and soundness can be arbitrary, it is common to define QMA as $\mathrm{QMA}(\frac{2}{3}, \frac{1}{3})$.

In this work, we are particularly interested in the extension of QMA that uses multiple unentangled provers, denoted QMA(k). Observe that the study of multi-prover MA is non-trivial only in the quantum model, where the unentanglement promise plays a crucial role. This distinctive quantum class is formally defined next.

Definition 3.7. *A language L is in* $\mathrm{QMA}(k, c(n), s(n))_{l(n)}$ *if there are polynomial time computable functions $c, s : \mathbb{N} \to [0,1]$, $l : \mathbb{N} \to \mathbb{N}$, such that for every $x \in \{0,1\}^n$ there is a polynomial time quantum verifier V_x satisfying*

- ***Completeness**: if $x \in L$, there is a witness $|\psi_1\rangle \otimes \cdots \otimes |\psi_k\rangle$ with $\Pr[V_x|\psi_1\rangle \otimes \cdots \otimes |\psi_k\rangle$ accepts$] \geq c(n)$.*
- ***Soundness**: if $x \notin L$, then for all $|\psi_1\rangle \otimes \cdots \otimes |\psi_k\rangle$ $\Pr[V_x|\psi_1\rangle \otimes \cdots \otimes |\psi_k\rangle$ accepts$] \leq s(n)$.*

Moreover, for each $i \in [k]$ the witness size is bounded by $O(l(n))$ qubits and the completeness soundness gap $c(n) - s(n)$ is at least $\frac{1}{g(n)}$, for some polynomial $g(n)$.

Here, $[k]$ is short for the interval $[1, \ldots, k]$. Using the product test of Harrow and Montanaro it is possible to show that a polynomial number of unentangled proofs is not more powerful than just two. This result is stated in the following collapse Lemma which is a corollary of the product test.

Lemma 3.8 (From [17])**.** *For any m, k, $0 \leq s < c \leq 1$,*

$$\mathrm{QMA}(k, c, s)_m \subseteq \mathrm{QMA}(2, c', s')_{km}$$

where $c' = \frac{1+c}{2}$ and $s' = 1 - \frac{(1-s)^2}{100}$

3.3 Trace Distance

The trace distance is one of the standard ways of measuring distance between quantum states. It is based on the trace norm which, for an Hermitian operator Δ, is denoted by $\|\Delta\|_1$ and it is equal to the sum of the absolute values of its eigenvalues. The trace distance between two density operators ρ and σ is $D(\rho, \sigma) = \frac{1}{2}\|\rho - \sigma\|_1$. For the special case of two pure states this distance becomes $D(|\psi\rangle, |\phi\rangle) = \sqrt{1 - |\langle\psi|\phi\rangle|^2}$.

In the following, we make use of an operational property of the trace distance. This distance is equal to the optimal bias in distinguishing two quantum states with a promise that we are given one of them uniformly at random. For instance, let P and Q be the probability distribution when measuring theses states in the computational basis, then the statistical distance $D(P, Q)$ can be used as a lower bound for the trace distance.

3.4 Swap Test

The swap test of two unentangled states ρ and σ, denoted $\mathrm{SWAP}(\rho, \sigma)$, accepts with high probability if and only if they are close with respect to the trace distance and if they are close to pure states. The acceptance probability is given by $\frac{1}{2} + \frac{1}{2}\mathrm{Tr}(\rho\sigma)$. For pure states $|\psi\rangle$ and $|\phi\rangle$, it is simply $\frac{1}{2} + \frac{1}{2}|\langle\psi|\phi\rangle|^2$.

3.5 Quantum Fourier Transform

We denote the unitary Quantum Fourier Transform (QFT) acting on $\mathcal{H}_m$ as F_m. Let $\omega = e^{\frac{2\pi i}{m}}$. In matrix form

$$F_m = \frac{1}{\sqrt{m}} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{m-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(m-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{(m-1)} & \omega^{2(m-1)} & \cdots & \omega^{m(m-1)} \end{pmatrix}.$$

The Fourier transform can be considered as a representation change from the temporal domain to the frequency domain. With this interpretation, the input vector corresponds to samples of the input signal taken at a uniform rate and the output vector corresponds to its frequency decomposition.

The uniform superposition on m base states is referred to as $|\overline{0}_m\rangle = F_m|0\rangle = \sum_i \frac{1}{\sqrt{m}}|i\rangle$. For simplicity, the index m is suppressed when it is clear from the context. Additionally, F_{2^m} admits an efficient implementation using $O(m^2)$ elementary gates [11].

4 Quantum multiprover protocol for PCPs

In this section, we show a QMA($q(n)$) protocol that simulates a classical $\mathrm{PCP}_{1,1-\epsilon_0}(r(n), q(n))_\Sigma$ verifier. The protocol is presented in detail next, followed by the proof of its completeness and soundness. It is an extension of Blier and Tapp's protocol [7]. Part of our analysis is similar to theirs, but it is also tighter and more general.

4.1 Protocol

The idea of our protocol is to encode the classical witness as a uniform superposition of indexes and their corresponding values. The quantum verifier expects a state in the form:

$$\sum_{i=1}^{m} \frac{1}{\sqrt{m}}|i\rangle|y_i\rangle, \tag{1}$$

where $y = y_1 \dots y_m$ is the original classical witness. The first and second parts of the quantum register are referred to as position and value registers, respectively. This witness is in the $\mathcal{H}_m \otimes \mathcal{H}_{|\Sigma|}$ Hilbert space, with total dimension $m|\Sigma|$.

The quantum verifier V is responsible for two tasks: verifying that the received proofs are close to a proper state of the form 1, and simulating the classical verifier for $\mathrm{PCP}_{1,1-\epsilon_0}(r(n), q(n))_\Sigma$. We refer to this verifier as V_0. Note that using $r(n)$ random bits and making $q(n)$ queries, it is not possible to query more than $q(n)2^{r(n)}$ different positions in a witness. Therefore, the proof size can be bounded by $\lceil \log(|\Sigma|) \rceil q(n)2^{r(n)}$. Since this proof is represented as a uniform superposition in the quantum case, its size has an upper bound of $O(\lceil \log(|\Sigma|) \rceil + \log(q(n)2^{r(n)}))$, if represented by qubits. Moreover, it is possible to assume that $q(n)$ is at least two as additional queries can be ignored.

The quantum verifier conducts four tests in which the first three check if the state is close to a proper state, and the last one checks if the encoded classical witness is valid. More specifically, the first one is an equality test that ensures that the quantum states are close using the swap test. The second test certifies that all positions are present in the quantum proof. The third one ensures that the value of a given position is consistent in all proofs. Finally, the last test simulates V_0. Each time V_0 tries to read a position in y, V measures one of its unmeasured quantum proofs and the simulation continues if and only if the measured and queried positions are the same. Otherwise, V accepts the input in order to avoid losing perfect completeness.

A precise description of V is given next. With equal probability, one of the four tests is performed.

- **Test 1:** (equality of certificates) Choose randomly two out of the $q(n)$ proofs, and denote them by $|\phi\rangle$ and $|\psi\rangle$. Accept if and only if SWAP($|\phi\rangle$,$|\psi\rangle$) accepts.
- **Test 2:** (all nodes are present) For each quantum proof $|\psi\rangle$:
  - Apply the QFT to the value portion of $|\psi\rangle$, and measure it.
  - If the outcome is frequency zero, measure the position register in the Fourier basis. If the outcome is not $|\overline{0}\rangle$, then reject.

  If all quantum proofs pass the previous test, then accept.
- **Test 3:** (positions have consistent values) Choose randomly two out of the $q(n)$ proofs, denote them by $|\phi\rangle$ and $|\psi\rangle$. Measure these proofs. If the same position was retrieved in both, accept if and only if both have the same value.
- **Test 4:** (check using V_0) Simulate V_0. Each time V_0 attempts to query a position, measure an unmeasured quantum proof. If the queried position and the measured position are the same, continue the simulation with the associated value. Otherwise accept, in order to ensure perfect completeness. Suppose V_0 successfully retrieved the values of all queried positions. In this case, accept if and only if V_0 accepts.

4.2 Completeness

We will now prove that the protocol described in the last subsection accepts with probability 1.

Let $y = y_1 y_2 \dots y_m$ be the classical $\mathrm{PCP}_{1,1-\epsilon}(r(n), q(n))_\Sigma$ proof. The $q(n)$ optimal $\mathrm{QMA}(q(n))_{\log(m)}$ proofs will be equal and encoded in a proper state of the form 1. We will now prove that each test accepts with probability 1.

Since all proofs are identical pure states, when we apply the swap test its failure probability is zero. Therefore, test 1 always accepts.

Each position has a well defined value $|y_i\rangle$ that is $\beta_{ij} = 1$ for some $j \in [|\Sigma|]$. In this case, after a QFT on the value register is performed, if a frequency of zero is measured, we know that the position register is in the superposition $\frac{1}{\sqrt{m}} \sum_{i=1}^{m} |i\rangle$. Consequently, test 2

accepts with probability 1. Furthermore, test 3 never rejects these certificates as values are consistent in all proofs.

Finally, if test 4 fails to retrieve a queried position, it accepts to ensure perfect completeness. Otherwise, if all positions were correctly retrieved, it can rely on the simulation of the classical PCP verifier that itself has perfect completeness.

4.3 Soundness

To prove the soundness of V, a series of lemmas are required. Despite the fact that the classical PCP verifier is robust for instances not in the language, the main concern in the quantum case is to ensure that it will be able to query the desired positions with non zero probability. Otherwise, our protocol would always accept.

Now, we briefly outline a sequence of lemmas and their respective goals. Firstly, in Lemma 4.1, by establishing a maximum failure probability in test 1, it is possible to conclude that the amplitudes in the proofs are component-wise close. Lemma 4.2 uses the previous Lemma and a probability bound of test 3, to conclude that, for positions with high amplitude, their values are well defined, *i.e*, have a high amplitude. Using some positions with well defined values, the QFT in the value register succeeds with non zero probability, as shown by Lemma 4.3.

In a generic way, Lemma 4.4 shows that a quantum state cannot differ much from a uniform superposition, if we require state $|\overline{0}\rangle$ to be measured in the Fourier basis. Combining Lemmas 4.3 and 4.4, Lemma 4.5 establishes a minimum amplitude for all positions. Finally, assuming tests 1 to 3 succeed with at least the probability stated in the previous Lemmas, it is possible to determine the total rejecting probability of test 4, which uses the classical PCP verifier.

As some of the lemmas depend on the assumptions of previous lemmas, to simplify their description we just mention this dependency where necessary. Further, we establish a common notation when writing quantum proofs. In tests 1 to 3, out of the $q(n)$ proofs, we work with at most two of them. These two proofs denoted by $|\psi\rangle$ and $|\phi\rangle$ are defined as follows in terms of their amplitudes:

$$|\psi\rangle = \sum_i \alpha_i |i\rangle \sum_j \beta_{ij} |j\rangle, \quad \text{and}$$
$$|\phi\rangle = \sum_i \alpha'_i |i\rangle \sum_j \beta'_{ij} |j\rangle,$$

where $\sum_i |\alpha_i|^2 = \sum_i |\alpha'_i|^2 = 1$ and for all i, it holds that $\sum_j |\beta_{ij}|^2 = \sum_j |\beta'_{ij}|^2 = 1$.

The first part of the quantum register is used to store the position and the second part stores the value in the alphabet Σ. Moreover, the probability of choosing a specific pair of proofs is $\frac{1}{\binom{q(n)}{2}}$. Since the latter appears in several of the following lemmas, we will denote it simply by p_{pair}.

The following Lemma states that if test 1 (swap test) succeeds with high probability, then the quantum proofs are component-wise close.

Lemma 4.1. *If there exists k and l such that $||\alpha_k\beta_{kl}|^2 - |\alpha'_k\beta'_{kl}|^2| \geq \frac{1}{f_{swap}(m)}$, where $f_{swap}(m) \in \Omega(m)$, then test 1 fails with probability at least $\frac{p_{pair}}{8f_{swap}(m)^2}$.*

Proof. Let $P_{i,j} = |\alpha_i\beta_{ij}|^2$ and $Q_{i,j} = |\alpha'_i\beta'_{ij}|^2$ be the probability distributions when $|\psi\rangle$ and $|\phi\rangle$ are measured in the computational basis. Using the properties of the trace distance $D(|\psi\rangle, |\phi\rangle)$, it is possible to find an upper bound on $|\langle\psi|\phi\rangle|^2$ as shown below:

$$\begin{aligned}
\sqrt{1 - |\langle\psi|\phi\rangle|^2} &= D(|\psi\rangle, |\phi\rangle) \\
&\geq D(P, Q) \\
&= \frac{1}{2}\sum_{ij} ||\alpha_i\beta_{ij}|^2 - |\alpha'_i\beta'_{ij}|^2| \\
&\geq \frac{1}{2}||\alpha_k\beta_{kl}|^2 - |\alpha'_k\beta'_{kl}|^2| \\
&= \frac{1}{2}\frac{1}{f_{swap}(m)}.
\end{aligned}$$

With the bound $|\langle\psi|\phi\rangle|^2 \leq 1 - \frac{1}{4f_{swap}(m)^2}$, we can obtain a lower bound on the swap test failure probability, that is

$$\frac{1}{2} - \frac{|\langle\psi|\phi\rangle|^2}{2} \geq \frac{1}{8f_{swap}(m)^2}.$$

Since the probability of selecting a specific pair of proofs is p_{pair}, the total failure probability of test 1 is at least

$$\frac{p_{pair}}{8f_{swap}(m)^2}.$$

□

The next Lemma states that positions with high amplitude have well defined values. One important difference from Blier and Tapp's work is the extension to arbitrary alphabets [7].

Lemma 4.2. *If test 1 fails with probability $p_{fail_1} < \frac{p_{pair}}{8f_{swap}(m)^2}$ with $f_{swap}(m) = 4m|\Sigma|$, and test 3 fails with probability $p_{fail_3} < p_0 p_{pair} p_r^2$, then for any position l such that $|\alpha_l|^2 \geq \frac{1}{2m}$ the following hold:*

(i) position l in $|\phi\rangle$ has $|\alpha'_l|^2 > \frac{1}{4m|\Sigma|}$;

(ii) position l can be measured in $|\psi\rangle$ or $|\phi\rangle$ with probability at least $p_r = \frac{1}{4m|\Sigma|}$;

(iii) for any $K \in]0.5, 1[$, there is a value j in $[|\Sigma|]$ such that both $|\beta_{lj}|^2, |\beta'_{lj}|^2 \geq K$, given the right choice of $p_0 \in]0, 0.5[$.

Proof.

(i) From Lemma 4.1, test 1 guarantees that $||\alpha_l\beta_{lj}|^2 - |\alpha'_l\beta'_{lj}|^2| < \frac{1}{f_{swap}(m)}$ when $p_{fail_1} < \frac{p_{pair}}{8f_{swap}(m)^2}$. Further, there is a j such that $|\beta_{lj}|^2 \geq \frac{1}{|\Sigma|}$ since $\sum_j |\beta_{lj}|^2 = 1$. For this j, the term $|\alpha_l\beta_{lj}|^2$ can be bounded below by $\frac{1}{2m|\Sigma|}$, giving

$$|\frac{1}{2m|\Sigma|} - |\alpha'_l|^2|\beta'_{lj}|^2| < \frac{1}{f_{swap}(m)}.$$

Since $|\beta'_{lj}|^2$ is at most 1, we have $|\alpha'_l|^2 > \frac{1}{2m|\Sigma|} - \frac{1}{f_{swap}(m)}$. Taking $f_{swap}(m)$ as $4m|\Sigma|$, a lower bound for $|\alpha'_l|^2$ becomes

$$|\alpha'_l|^2 > \frac{1}{2m|\Sigma|} - \frac{1}{f_{swap}(m)} > \frac{1}{2m|\Sigma|} - \frac{1}{4m|\Sigma|} = \frac{1}{4m|\Sigma|}.$$

(ii) To retrieve position l in a quantum proof, it is possible to measure this proof directly. From item (i), this measurement succeeds with probability at least $p_r = \frac{1}{4m|\Sigma|}$, for both proofs $|\psi\rangle$ and $|\phi\rangle$.

(iii) By adjusting p_0 in the upper bound of the failure probability of test 3, given by $p_{fail_3} < p_0 p_{pair} p_r^2$, it is possible to enforce that position l has one value with high amplitude.

Let $x = [|\beta_{l1}|^2, \ldots, |\beta_{l|\Sigma|}|^2]$ and $y = [|\beta'_{l1}|^2, \ldots, |\beta'_{l|\Sigma|}|^2]$ denote two vectors containing the squared amplitudes of the register values for positions l of $|\psi\rangle$ and $|\phi\rangle$, respectively. Suppose that position l was measured in both proofs. We denote by p_0 the probability of detecting if the content of register values disagree in which case test 3 rejects. This probability can be written as

$$p_0 = \sum_{j \neq k} |\beta_{lj}|^2 |\beta'_{lk}|^2.$$

If $p_{fail_3} < p_0 p_{pair} p_r^2$, we have $\sum_{j \neq k} |\beta_{lj}|^2 |\beta'_{lk}|^2 < p_0$, or conversely

$$\sum_j |\beta_{lj}|^2 |\beta'_{lj}|^2 \geq 1 - p_0.$$

The previous sum can be rewritten as the inner product

$$\langle x|y\rangle \geq 1 - p_0,$$

where the two vectors are in $\mathbb{R}^{|\Sigma|}$, $\|x\|_1 = \|y\|_1 = 1$, and their components are non-negative.

For $p_0 < 0.5$, Lemma A.1 can be applied showing the existence of a j such that $|\beta_{lj}|^2$ and $|\beta'_{lj}|^2$ are greater or equal than any fixed $K \in]0.5, 1[$ given the appropriate choice of p_0. □

By bounding the success probability of tests 1 and 3, it is possible to bound the probability of retrieving a zero frequency in the register value after a QFT is performed.

Lemma 4.3. *Given the assumptions of Lemma 4.2, the probability of measuring a zero frequency in the register value, after a QFT is applied to it, is greater than* $\frac{1}{3|\Sigma|}$.

Proof. If position i was measured, the probability of measuring frequency zero in the register value is

$$\frac{1}{|\Sigma|}|\beta_{i0} + \cdots + \beta_{i|\Sigma|}|^2.$$

From Lemma 4.2, we know that there is an i (we renamed l to i) and a j such that $|\alpha_i|^2 \geq \frac{1}{2m}$ and $|\beta_{ij}|^2 \geq K$. Without loss of generality let $j = 1$. We have

$$\frac{1}{|\Sigma|}|\beta_{i1} + \cdots + \beta_{i|\Sigma|}|^2 \geq \frac{1}{|\Sigma|}(|\beta_{i1}| - |\sum_{j=2}^{|\Sigma|}\beta_{ij}|)^2.$$

By appropriately choosing K, the factor $\frac{2}{3|\Sigma|}$ can be used as a lower bound for the previous expression.

At most $m-1$ positions may satisfy $|\alpha_i|^2 \leq \frac{1}{2m}$. As a result, the probability of obtaining frequency zero is at least

$$(1 - (m-1)\frac{1}{2m})\frac{2}{3|\Sigma|} \geq \frac{1}{3|\Sigma|}.$$

This completes the proof. □

For a generic quantum state, if we intend to measure $|\overline{0}\rangle$ in the Fourier basis with high probability, then Lemma 4.4 gives a minimum amplitude for each position.

Lemma 4.4. *Given a state $|\psi\rangle = \sum_i \gamma_i|i\rangle$, and a l such that $|\gamma_l|^2 < \frac{1}{2m}$, the probability of not getting $|\overline{0}\rangle = F_m|0\rangle$ when $|\psi\rangle$ is measured in the Fourier basis is at least $\frac{1}{16m^2}$.*

Proof. Let P and Q be the probability distributions when measuring $|\psi\rangle$ and $|\overline{0}\rangle$ in the computational basis, respectively. Using the properties of the trace distance, we have

$$\begin{aligned}
\sqrt{1 - |\langle\psi|\overline{0}\rangle|^2} &= D(|\psi\rangle, |\overline{0}\rangle) \\
&\geq D(P, Q) \\
&= \frac{1}{2}\sum_i ||\gamma_i|^2 - \frac{1}{m}| \\
&\geq \frac{1}{2}||\gamma_l|^2 - \frac{1}{m}| \\
&\geq \frac{1}{4m}.
\end{aligned}$$

The value $1 - |\langle\psi|\overline{0}\rangle|^2$ is the probability of not getting $|\overline{0}\rangle$ when measuring in the Fourier basis. In this case, it is at least $\frac{1}{16m^2}$. □

Lemma 4.5. *If the assumption of Lemma 4.3 is met, and test 2 fails with probability $p_{fail_2} < \frac{1}{48|\Sigma|m^2}$, then $|\alpha_i|^2 \geq \frac{1}{2m}$, for all i.*

Proof. With the assumption of Lemma 4.3, there is a $\frac{1}{3|\Sigma|}$ probability of measuring frequency zero for the register value. In that case, Lemma 4.4 implies that, for all i, $|\alpha_i|^2 \geq \frac{1}{2m}$, or otherwise $p_{fail_2} \geq \frac{1}{3|\Sigma|}\frac{1}{16m^2} = \frac{1}{48|\Sigma|m^2}$. □

Lemma 4.6. *Let V_0 be the classical* PCP *verifier, and let $1-\epsilon_0$ be its soundness. If the assumptions of Lemma 4.5 are met, then test 4 rejects the input x with probability at least $\epsilon_0(K\frac{1}{2m})^{q(n)}$ when x is not in the language of V_0.*

Proof. When the hypothesis of Lemma 4.5 are met, each position has probability at least $\frac{1}{2m}$. In this case, item (iii) of Lemma 4.2 also applies. Thus each position has a well defined value with probability K. The encoded classical witness is considered to be composed of these values.

The probability of correctly measuring each of the $q(n)$ positions desired by the verifier V_0, is at least

$$(K\frac{1}{2m})^{q(n)}.$$

Consequently, the total probability of detecting a no-instance is at least

$$\epsilon_0(K\frac{1}{2m})^{q(n)}.$$

The proof is complete. □

Now we are ready to state our main result showing the relationship of a generic classical PCP verifier and the complexity class QMA(k).

Theorem 4.7.

$$\mathrm{PCP}_{1,1-\epsilon_0}(r(n),q(n))_\Sigma \subseteq \mathrm{QMA}(q(n),1,1-\epsilon)_{l(n,\Sigma)},$$

where

- *the classical witness size m is a function of n;*
- $l(n,\Sigma) = O(\lceil\log(|\Sigma|)\rceil + \log(m))$*;*
- $\epsilon = \min\{\frac{p_{pair}}{km^2}, \epsilon_0(K\frac{1}{2m})^{q(n)}\}$*;*
- $k = \frac{48|\Sigma|^2}{p_0}$*;*
- $p_0 \in]0, 0.5[$*;*
- $K \in]0.5, 1[$ *is a function of* p_0*;*
- $p_{pair} = \frac{1}{\binom{q(n)}{2}}$.

Proof. Firstly, we observe that claim A.2 allows the encoding of the classical $\mathrm{PCP}_{1,1-\epsilon_0}(r(n), q(n))_\Sigma$ witness using qubits instead of qudits. The conversion process at most doubles the witness and alphabet sizes, while all other parameters remain the same. This observation is important because the Fourier unitary operator will always admit an efficient implementation since the position and register values have at most polynomially many qubits in n.

To prove the current Theorem we use the protocol described at the beginning of section 4.1. A proof of its perfect completeness was already given in 4.2, and it is only left to show its soundness, which also follows by combining the previous lemmas.

Tests 1 to 3 of the quantum verifier V ensure that the proofs are well formed in the sense that they have a minimum amplitude for all positions, and the associated values are consistent in all proofs. Assuming the probability of failure in each of these tests are smaller than $\frac{p_{pair}}{km^2}$ for $k = \frac{48|\Sigma|^2}{p_0}$, we have a series of implications that makes the hypothesis of Lemma 4.6 hold. Lemma 4.2 implies the statement in Lemma 4.4, which in turn implies the statement in Lemma 4.5. Since the hypothesis of Lemma 4.6 is met, test 4 fails with probability at least $\epsilon_0(K\frac{1}{2m})^{q(n)}$. As each test is selected with equal probability, the soundness is at most $1 - \min\{\frac{p_{pair}}{km^2}, \epsilon_0(K\frac{1}{2m})^{q(n)}\}$. □

As a corollary, PCP verifiers can be simulated with two uentangled provers.

Corollary 4.8.

$$\mathrm{PCP}_{1,1-\epsilon_0}(r(n), q(n))_\Sigma \subseteq \mathrm{QMA}(2, 1, 1-\epsilon')_{l'(n,\Sigma)}.$$

Proof. Follows directly from Theorem 4.7, and from $\mathrm{QMA}(k) = \mathrm{QMA}(2)$ in Lemma 3.8. The parameters are the same as in the previous theorem, and we let $\epsilon' = \frac{\epsilon^2}{100}$. □

For the specific case of the language $3SAT$, we have the following corollary.

Corollary 4.9. *Language* $3SAT$ *is in* $\mathrm{QMA}(2, 1, 1 - \Omega(\frac{1}{n^{2+\varepsilon}}))_{\log(n)}$ *for any* $\varepsilon > 0$.

Proof. Theorem 3.3 states that $3SAT$ is in $\mathrm{PCP}_{1,1-\delta}(O(\log(n)), 2)_\Sigma$ for constants δ and $|\Sigma|$. Also, the proof size is $m = n^{1+o(1)}$. From Theorem 4.7, we conclude that $3SAT$ is in $\mathrm{QMA}(2, 1, 1 - \Omega(\frac{1}{n^{2+\varepsilon}}))_{\log(n)}$ for any $\varepsilon > 0$. □

With our generalization, it is possible to obtain again the known result NEXP = QMA(2) with a small gap[23]. But now without the need of going into the details of a specific complete problem for NEXP.

Corollary 4.10.

$$\mathrm{NEXP} = \mathrm{QMA}(2, 1, 1 - \Omega(\frac{1}{2^{poly(n)}}))_{poly(n)}.$$

Proof. The containment $\mathrm{QMA}(2, 1, 1 - \Omega(\frac{1}{2^{poly(n)}}))_{poly(n)} \subseteq \mathrm{NEXP}$ is straightforward. An EXP time classical verifier receives the two exponential size quantum witnesses (up to a doubly exponential precision) from a prover and then it simulates the quantum verifier.

The other containment $\mathrm{NEXP} \subseteq \mathrm{QMA}(2, 1, 1 - \Omega(\frac{1}{2^{poly(n)}}))_{poly(n)}$ follows by combining Theorem 3.5 and Corollary 4.8 in a similar way, as in the previous proof. □

Remark 4.11. *From this last corollary, it is possible to conclude a known result, namely, optimizing the function* $\mathrm{Tr}(M\rho^{AB})$ *over the separable states is* NP*-hard up to an inverse polynomial error in the dimension, where* $0 \leq M \leq I$ *[13]. This is one of the reasons why it is challenging to find an upper bound for* QMA(2) *better than* NEXP*.*

5 Conclusions

In this work, we generalized the Blier and Tapp protocol to simulate any classical PCP verifier. The quantum setting allows an exponential reduction in the proof size, while also reducing the completeness-soundness gap of the system. With our generalization and two concrete classical PCP Theorems, we recover two known results. Firstly, using a PCP Theorem for $3SAT$, we find a completeness-soundness gap of $\Omega(\frac{1}{n^{2+\varepsilon}})$ for any $\varepsilon > 0$ which lies between the Beigi and the Le Gall et al. results. Moreover, with a PCP Theorem for NEXP, we recover that QMA(2) is equal to NEXP in the context of small gaps, as in Pereszlényi [23].

We ask if it is possible to adapt a classical PCP verifier to take advantaged of the probability distribution naturally associated with quantum amplitudes. That is, instead of looking for specific positions in the proof, the verifier maight enforce some minimum amplitude for each position, or some other distribution, in an attempt to increase the completeness-soundness gap. Another question is if it is possible to use the quantum setting developed here to derive classical PCP hardness results. For instance, it might be possible to obtain a lower bound for the number of queries, given a certain alphabet size, based on the assumption that $\mathrm{P} \neq \mathrm{NP}$.

References

[1] M. R. Garey and D. S. Johnson (1990), *Computers and Intractability; A Guide to the Theory of NP-Completeness* (W. H. Freeman & Co., New York, NY, USA). ISBN 0716710455.

[2] R. P. Feynman (1982), *Simulating physics with computers.* International Journal of Theoretical Physics, Vol. 21(6-7), pp. 467–488.

[3] H. Kobayashi, K. Matsumoto and T. Yamakami (2003), *Quantum merlin-arthur proof systems: Are multiple merlins more helpful to arthur?* In T. Ibaraki, N. Katoh and H. Ono, eds., *ISAAC*, Vol. 2906 of *Lecture Notes in Computer Science*, pp. 189–198 (Springer).

[4] M. A. Rowe, D. Kielpinski, V. Meyer, C. A. Sackett, W. M. Itano, C. Monroe and D. J. Wineland (2001), *Experimental violation of a bell's inequality with efficient detection.* Nature, Vol. 409, pp. 791–794.

[5] M. M. Wilde (2013), *Quantum Information Theory* (Cambridge University Press, New York, NY, USA), 1st edition.

[6] S. Aaronson, S. Beigi, A. Drucker, B. Fefferman and P. W. Shor (2008), *The power of unentanglement.* Electronic Colloquium on Computational Complexity (ECCC), Vol. 15(051).

[7] H. Blier and A. Tapp (2009), *All languages in np have very short quantum proofs.* Quantum, Nano, and Micro Technologies, First International Conference on, Vol. 0, pp. 34–37.

[8] S. Beigi (2010), *NP vs qma_log(2).* Quantum Information & Computation, Vol. 10(1&2), p. 2.

[9] F. Gall, S. Nakagawa and H. Nishimura (2012), *On qma protocols with two short quantum proofs.* Quantum Information and Computation, Vol. 12(7-8), pp. 589–600.

[10] A. Chiesa and M. A. Forbes (2011), *Improved soundness for qma with multiple provers.* CoRR, Vol. abs/1108.2098.

[11] M. Nielsen and I. Chuang (2000), *Quantum computation and quantum information.* Cambridge Series on Information and the Natural Sciences (Cambridge University Press). ISBN 9780521635035.

[12] S. Arora and B. Barak (2009), *Computational Complexity: A Modern Approach* (Cambridge University Press, New York, NY, USA), 1st edition. ISBN 0521424267, 9780521424264.

[13] F. G. S. L. Brandão, M. Christandl and J. Yard (2011), *A quasipolynomial-time algorithm for the quantum separability problem.* In *STOC*, pp. 343–352.

[14] S. Gharibian (2010), *Strong np-hardness of the quantum separability problem.* Quantum Info. Comput., Vol. 10(3), pp. 343–360.

[15] I. Dinur (2007), *The pcp theorem by gap amplification.* J. ACM, Vol. 54(3).

[16] J. Chen and A. Drucker (2010), *Short multi-prover quantum proofs for sat without entangled measurements.* CoRR, Vol. abs/1011.0716.

[17] A. W. Harrow and A. Montanaro (2013), *Testing product states, quantum merlin-arthur games and tensor optimization.* J. ACM, Vol. 60(1), p. 3.

[18] A. Chailloux and O. Sattath (2012), *The complexity of the separable hamiltonian problem.* In *IEEE Conference on Computational Complexity*, pp. 32–41 (IEEE).

[19] Y. Shi and X. Wu (2012), *Epsilon-net method for optimizations over separable states.* In *Proceedings of the 39th International Colloquium Conference on Automata, Languages, and Programming - Volume Part I*, ICALP'12, pp. 798–809 (Springer-Verlag).

[20] F. Brandão, M. Christandl and J. Yard (2011), *Faithful squashed entanglement.* Communications in Mathematical Physics, Vol. 306(3), pp. 805–830.

[21] F. G. Brandão and A. W. Harrow (2013), *Quantum de finetti theorems under local measurements with applications.* STOC '13, pp. 861–870 (ACM, New York, NY, USA).

[22] K. Li and G. Smith (2014), *Quantum de finetti theorem measured with fully one-way locc norm.* CoRR, Vol. abs/1408.6829.

[23] A. Pereszlényi (2012), *Multi-prover quantum merlin-arthur proof systems with small gap.* CoRR, Vol. abs/1205.2761.

[24] C. Marriott and J. Watrous (2005), *Quantum arthur-merlin games.* Computational Complexity, Vol. 14(2), pp. 122–152.

[25] S. Arora, C. Lund, R. Motwani, M. Sudan and M. Szegedy (1998), *Proof verification and the hardness of approximation problems.* J. ACM, Vol. 45(3), pp. 501–555.

[26] D. Moshkovitz and R. Raz (2008), *Two query pcp with sub-constant error.* Electronic Colloquium on Computational Complexity (ECCC), Vol. 15(071).

[27] O. Meir (2009), *Combinatorial pcps with efficient verifiers.* In *FOCS*, pp. 463–471 (IEEE Computer Society).

A Mathematical Lemmas

We present a simple mathematical lemma used in the proof of 4.2. This lemma states that if it is possible to control the lower bound of the inner product of two unity length L_1 norm vectors, then there is a component in both vectors that can be made arbitrarily close to 1. This result is useful when enforcing that the value of a position in the quantum proof is consistent with respect to other proofs.

Lemma A.1. *Let $x = [x_1, \ldots, x_n]$ and $y = [y_1, \ldots, y_n]$ be vectors in $\Re^n$ where $x_i, y_i \geq 0$, for all i, and assume $\|x\|_1 = 1$ and $\|y\|_1 = 1$. Let $\langle x|y\rangle \geq k_1 > \frac{1}{2}$. For every $k_2 \in]0.5, 1[$, by adjusting k_1 it is possible to obtain a $j \in [n]$ such that $|x_j|$ and $|y_j|$ are greater than k_2.*

Proof. Let θ be the smallest angle between x and y. From the hypothesis, their inner product is at least k_1 resulting in

$$\cos\theta \|x\|_2 \|y\|_2 = \langle x|y\rangle \geq k_1.$$

Without loss generality, assume that $\|x\|_2$ is greater than $\|y\|_2$. Then we have

$$\|x\|_2^2 \geq \cos\theta \|x\|_2 \|y\|_2 = \langle x|y\rangle \geq k_1.$$

Let x_1 be the greatest component of x. Since each component of x is non negative and $\|x\|_1 = 1$, the following inequality holds

$$(1 - x_1)^2 = (\sum_{i=2}^{n} x_i)^2 \geq \sum_{i=2}^{n} x_i^2.$$

Then, $\|x\|_2^2$ can be upper bounded by:

$$x_1^2 + (1-x_1)^2 \geq \|x\|_2^2 \geq \cos\theta \, \|x\|_2 \, \|y\|_2 = \langle x|y\rangle \geq k_1.$$

Solving this simple quadratic equation yields the roots $\frac{2\pm\sqrt{4-8(1-k_1)}}{4}$. For $k_1 \in]0.5, 1[$, we note that the minimum value of $x_1 \geq 0$ satisfying the previous inequality is monotonically increasing in k_1 and varies in the range $]0.5, 1[$ as desired.

For vector y, we have

$$\|y\|_2 \geq \cos\theta \, \|x\|_2 \, \|y\|_2 = \langle x|y\rangle \geq k_1,$$

and a similar reasoning applies by squaring both sides. Moreover, vectors x and y can be made arbitrarily close to parallel ones since $k_1 \leq \cos\theta \, \|x\|_2 \, \|y\|_2 \leq \cos\theta$. Therefore, the same greatest component of x and y can be made arbitrarily large by controlling k_1.

Note that this Lemma could also have been proved using the Hölder inequality, which states that

$$|\langle x|y\rangle| \leq \|x\|_p \, \|y\|_q$$

where p and q satisfy $\frac{1}{p} + \frac{1}{q} = 1$. By taking $p = 1$ and q unbounded, it is easy to see that the result follows. □

If we intend to work with qubits instead of qudits, there is one simple technicality that we need to address. The PCP witness and the alphabet size should be a power of two. The next claim shows how to make the appropriate conversion.

Claim A.2. *Let V be a $\mathrm{PCP}_{1,1-\epsilon_0}(r(n), q(n))_\Sigma$ verifier. It is possible to convert V to a $\mathrm{PCP}_{1,1-\epsilon_0}(r(n), q(n))_{\Sigma'}$ verifier in which the new witness size m' and the new alphabet size $|\Sigma'|$ are a power of two. Further, if m is the witness size of V, then $m' \leq 2m$ and $|\Sigma'| \leq 2|\Sigma|$.*

Proof. It is possible to add positions to the witness $y = y_1 \dots y_m$ until its size becomes a power of two. Note that this process at most doubles its size. A similar reasoning applies to the original alphabet Σ.

The verifier can always ignore extra positions in the proof by not querying them, thus $r(n)$, $q(n)$ and the completeness remain the same. Also, if the new verifier reads a symbol that was not in the alphabet Σ it can readily reject. Therefore, soundness also remains the same. □