Electronic Colloquium on Computational Complexity, Report No. 110 (2011)

Improved Soundness for QMA with Multiple Provers

Alessandro Chiesa*
MIT CSAIL

Michael Forbes†
MIT CSAIL

August 9, 2011

Abstract

We present three contributions to the understanding of QMA with multiple provers:

- We give a tight soundness analysis of the protocol of [Blier and Tapp, ICQNM '09], yielding a soundness gap $\Omega(N^{-2})$, which is the best-known soundness gap for two-prover QMA protocols with logarithmic proof size. Maybe surprisingly, our improvement is achieved *without* the use of an instance with a constant soundness gap (i.e., without using a "PCP"); this is unlike the previously best-known soundness gap of $\Omega(N^{-3-\varepsilon})$ given by [Beigi, QIC '10], which was achieved using a (balanced) 2-out-of-4 instance with constant soundness gap.
- We give a tight soundness analysis of the protocol of [Chen and Drucker, ArXiV '10], thereby improving their result from a "monolithic" protocol where $\Theta(\sqrt{N})$ provers are *needed* in order to have any soundness gap, to a protocol with a *smooth trade-off* between the number of provers κ and a soundness gap $\Omega(\kappa^2 N^{-1})$, as long as $\kappa \in \Omega(\log N)$. (And, when $\kappa \in \Theta(\sqrt{N})$, we recover the original parameters of Chen and Drucker.) Further, we explain why even our tight analysis cannot give any soundness gap for the "$\kappa \in O(1)$ regime", implying that new protocols are needed for any "sublinear" constant-prover LOCC QMA protocol with an inverse-polynomial soundness gap.
- We make partial progress towards an open question of [Aaronson et al., ToC '09] about what kinds of NP-complete problems are amenable to "sublinear" multiple-prover QMA protocols, by observing that a *large class* of such examples can easily be derived from results already in the PCP literature — namely, at least the languages recognized by a non-deterministic RAMs in quasilinear time. We also take the opportunity to give generic lemmas that allow for such results to be stated in a more general (and unified) way.

*Email: alexch@csail.mit.edu.
†Email: miforbes@mit.edu.

ISSN 1433-8092

1 Introduction

The class QMA is the natural quantum analogue of NP (and MA): with the help of a quantum proof (given by the all-powerful "Merlin"), a quantum polynomial-time verifier ("Arthur") attempts to decide whether an input string x is in a given language L or not; this class was first studied by Knill [Kni96], Kitaev [Kit99], and Watrous [Wat00]. For more details, see the survey of Aharonov and Naveh [AN02].

Kobayashi et al. [KMY03] first introduced and studied the class $\mathsf{QMA}(\kappa)$, where Arthur receives $\kappa \in [2, \mathsf{poly}(N)]$ quantum proofs that are *promised to be unentangled*. While multiple proofs in the classical case do not increase the power of the class (i.e., "$\mathsf{NP}(\kappa) = \mathsf{NP}$" and "$\mathsf{MA}(\kappa) = \mathsf{MA}$"), there is some evidence that multiple unentangled proofs in the quantum case are in fact more powerful that one (as currently conjectured): for example, Liu et al. [LCV07] have proposed a problem, pure state N-representability, that is known to lie in $\mathsf{QMA}(2)$ but is not known to lie in QMA; also, several works [BT09, Bei10, ABD+09, CD10] have proposed multi-prover QMA protocols for certain NP languages whose (soundness and proof length) parameters are not known to be achievable with only one prover. (See Table 1 for a summary of such results.)

Harrow and Montanaro [HM10] recently answered several important open problems regarding the class $\mathsf{QMA}(\kappa)$, by proving that amplification within $\mathsf{QMA}(\kappa)$ is possible and that $\mathsf{QMA}(\mathsf{poly}(N)) = \mathsf{QMA}(2)$; the "collapse" is achieved by giving an analysis of a *product test*, which allows a verifier to use the unentanglement promise of only two registers to ensure that states within a single register are close to a separable state.

Brandão et al. [BaCJ10, Corollary 4] prove (among other things) that two-prover QMA protocols where the verifier is restricted to LOCC measurements only can be simulated by a *single* prover QMA protocol, incurring only in a quadratic increase in total proof length. In particular, for example, this implies that a two-prover QMA protocol for $\mathsf{3SAT}$ with an LOCC verifier and total proof length of $o(N)$ is unlikely to exist (for, otherwise, $\mathsf{3SAT}$ could be solved in deterministic subexponential time).

Particularly interesting is the gap between the "lower bound" of Brandão et al. [BaCJ10] and the "upper bound" results that are known for multi-prover QMA protocols for certain NP languages. Specifically, Aaronson et al. [ABD+09] give a $\widetilde{\Theta}(\sqrt{N})$-prover QMA protocol for $\mathsf{3SAT}$, with perfect completeness and constant soundness gap, where each prover sends $\Theta(\log N)$ qubits; two improvements, in different directions, on this protocol are known:

- *Reducing the number of provers.* Harrow and Montanaro [HM10], through their product test, reduce the number of provers of [ABD+09] to only two, thereby obtaining a two-prover QMA protocol for $\mathsf{3SAT}$, with perfect completeness and constant soundness gap, where each prover sends $\widetilde{\Theta}(\sqrt{N})$ qubits.

- *Avoiding use of the swap test (and any entangling measurement).* Chen and Drucker [CD10] simplify the verifier of [ABD+09] by simply not using the swap test, thereby making the verifier perform only LOCC (in fact, Bell) measurements; along the way, they also manage to greatly simplify the soundness analysis too. (Also, but less relevant: they (i) use a coloring problem as a starting point instead of a "structured" SAT instance, and (ii) they lose perfect completeness.)

However, no result that improves on *both* directions is known; such a result, in light of the lower bound of Brandão et al. [BaCJ10], would be a tight upper bound (under plausible hardness assumptions). In this work, we are interested in studying this gap, and therefore address the following question:

Question 1. *Does there exist a two-prover* QMA *protocol for* $\mathsf{3SAT}$*, with a constant soundness gap and* $\sqrt{n}\mathsf{polylog}(n)$ *total number of qubits, where the verifier is only allowed to perform LOCC measurements?*

paper	language	PCP?	provers	$\frac{\text{qubits}}{\text{provers}}$	c	$c-s$	verifier test
[BT09]	$\mathsf{2CSP}(N, M, 3)$	no	2	$\Theta(\log N)$	1	$\Omega(N^{-6})$	SWAP, Bell
[Bei10]	$(2,4)\mathsf{SAT}^*(N)$	yes	2	$\Theta(\log N)$	$\frac{3}{4}+\frac{\sqrt{2(N-1)}}{6N^{1.5}}$	$\Omega(N^{-3-\varepsilon})$	SWAP, Bell
[ABD+09]	$(2,4)\mathsf{SAT}^*(N)$	yes	$\Theta(\sqrt{N})$	$\Theta(\log N)$	1	$\Omega(1)$	SWAP, Bell
[CD10]	$\mathsf{2CSP}(N, M, O(1))$	yes	$\Theta(\sqrt{N})$	$\Theta(\log N)$	$1-e^{-\Omega(\sqrt{N})}$	$\Omega(1)$	Bell
[HM10]	$(2,4)\mathsf{SAT}^*(N)$	yes	2	$\widetilde{\Theta}(\sqrt{N})$	1	$\Omega(1)$	SWAP, Bell
this work	$\mathsf{2CSP}(N, M, O(1))$	no	2	$\Theta(\log N)$	1	$\Omega(N^{-2})$	SWAP, Bell
this work	$\mathsf{2CSP}(N, M, O(1))$	yes	κ	$\Theta(\log N)$	$1-e^{-\Omega(\kappa)}$	$\Omega(\kappa^2 N^{-1})$	Bell

Table 1: A summary of the known multi-prover QMA protocols for languages in NP. The language $\mathsf{2CSP}(N, M, K)$ consists of satisfiable 2CSP instances on N vertices, with M (edge) constraints and an alphabet size of K; the language $(2,4)\mathsf{SAT}^*(N)$ consists of satisfiable 2-out-of-4 balanced SAT instances on N variables. See Section 2 for formal definitions of these languages.

1.1 Our Contributions

The goal of this research was (and still is) to answer, in the positive, Question 1. Unfortunately, we have not succeeded yet. Nonetheless, along the way we have collected observations that we believe to be of interest, as well as technical contributions to existing works.

Specifically,

- We address an open question of Aaronson et al. [ABD+09] about what kinds of NP-complete problems are amenable to "sublinear" multiple-prover QMA protocols, by observing that a *large class* of such examples can easily be derived from results already in the PCP literature. We also take the opportunity to give generic lemmas that allow for such results to be stated in a more general (and unified) way.

- We give a tight soundness analysis of the protocol of Chen and Drucker [CD10], thereby improving their result from a "monolithic" protocol where $\Theta(\sqrt{N})$ provers are *needed* in order to have any soundness gap, to a protocol with a *smooth trade-off* between the number of provers κ and a soundness gap $\Omega(\kappa^2 N^{-1})$, as long as $\kappa \in \Omega(\log N)$. (And, when $\kappa \in \Theta(\sqrt{N})$, we recover the original parameters of [CD10].) Further, we explain why even our tight analysis cannot give any soundness gap for the "$\kappa \in O(1)$ regime", implying that new protocols are needed for any "sublinear" constant-prover LOCC QMA protocol with an inverse-polynomial soundness gap.

- We give a tight soundness analysis of the protocol of Blier and Tapp [BT09], yielding a soundness gap $\Omega(N^{-2})$, which is the best-known soundness gap for two-prover QMA protocols with logarithmic proof size. Maybe surprisingly, our improvement is achieved *without* the use of an instance with a constant soundness gap (i.e., without using a "PCP"); this is unlike the previously best-known soundness gap of $\Omega(N^{-3-\varepsilon})$ given by Beigi [Bei10], which was achieved using a (balanced) 2-out-of-4 instance with constant soundness gap.

We now discuss each of the above contributions in some more detail, while all the details are left to subsequent sections. At the end of this section we also briefly discuss our ideas about possible approaches (as well as unlikely approaches) for progress towards answering Question 1.

1.1.1 Languages with sublinear quantum proofs

The main theorem of Aaronson et al. [ABD$^+$09] is:

Theorem 1.1 ([ABD$^+$09, Theorem 1]). *Let φ be a satisfiable* 3SAT *instance with N variables and M clauses (and $M \geq N$). Then one can prove satisfiability of φ, with perfect completeness and constant soundness, using $\widetilde{\Theta}(\sqrt{M})$ unentangled quantum proofs, each with $\Theta(\log N)$ qubits.*

What is surprising about the result is that, for $M \in O(N)$, the total number of qubits sent by all the provers to the verifier is *sublinear*; instead, the best known proof length in the case of only one prover (i.e., in the case of QMA) is linear (and we believe one cannot do better, by the Exponential-Time Hypothesis).

Aaronson et al. [ABD$^+$09] thus raised the following question:

Question 2. *For which* NP*-complete problems, other than* 3SAT*, an analogue of Theorem 1.1 holds?*

Clearly, an analogue of Theorem 1.1 holds for any language L that can be reduced to 3SAT with only a polylogarithmic blow-up in instance size. (Note that the computational efficiency of the reduction itself is irrelevant here.) However, can we say more? For example, can we say something about languages for which no such reduction to 3SAT is known?

We make the observation the existing PCP literature already yields a large class of languages for which an analogue of Theorem 1.1 does hold:

Claim 1.2 (Sublinear Multiple-Prover Quantum Proofs). *Let L be any language that can be recognized in non-deterministic quasilinear time by a random-access machine. Let x be an instance in L of size N. Then one can prove that x is in L, with perfect completeness and constant soundness, using $\widetilde{\Theta}(\sqrt{N})$ unentangled quantum proofs, each with $O(\log N)$ qubits.*

The starting point of Aaronson et al. [ABD$^+$09] was the existence of a reduction from 3SAT to 2CSP with *constant* soundness gap implied by combining the results on short PCPs by Ben-Sasson and Sudan [BSS08] and on gap amplification by Dinur [Din07]. We simply observe that a similar reduction holds for any language that can be recognized in non-deterministic quasilinear time by a multi-tape Turing machine (a class of languages which, by a result of Gurevich and Shelah [GS89], happens to equal the class of languages recognized in non-deterministic quasilinear time by random-access machines — which are easier to understand).

In fact, we make a much more general observation:

Claim 1.3 (Sublinear Multiple-Prover Quantum Proofs for NTIME Languages). *Let $t\colon \mathbb{N} \to \mathbb{N}$ be any proper complexity function and let $\mathsf{NTIME}_{\mathsf{RAM}}(t)$ be the class of languages solvable in non-deterministic $t(n)$-time by a random-access machine (RAM). For any language $L \in \mathsf{NTIME}_{\mathsf{RAM}}(t)$, it is possible to prove membership in L, with perfect completeness and constant soundness, using $\widetilde{\Theta}\big(\sqrt{t(n)}\big)$ unentangled quantum proofs, each with $O\big(\log t(n)\big)$ qubits.*[1]

Again, the proof is simply the observation that any language $L \in \mathsf{NTIME}_{\mathsf{RAM}}(t)$ can be reduced to a 2CSP with constant soundness gap with $t\mathsf{polylog}(t)$ vertices and edges and a constant-size color alphabet, and then the protocol of Aaronson et al. [ABD$^+$09] can be applied to obtain the claimed parameters.

We also take the opportunity to clearly state the "size-efficient" reduction from $\mathsf{NTIME}_{\mathsf{RAM}}(t)$ to 2CSP with constant soundness, because the reduction not only generalizes the result of Aaronson et al. [ABD$^+$09] to all of $\mathsf{NTIME}_{\mathsf{RAM}}$, but also generalizes all the other results in multi-prover QMA protocols (namely, [CD10], [Bei10], and [BT09]), because they too are all based on 2CSP (or languages that can

[1] Of course, if t is superpolynomial, we should consider verifiers that are allowed to run in time $\mathsf{poly}(t(n))$.

be efficiently reduced to form 2CSP). For example, we state in this general form our improvements to [CD10] (in Claim 1.6) and to [BT09] (in Claim 1.8).

For details, see Section 3.

1.1.2 Technical improvements to [CD10]

Aaronson et al. [ABD+09] raised the question of whether it is possible to construct a (multi-prover) QMA protocol with constant soundness gap and sublinear proof size for an NP-complete language, but using *no entangled measurements*. Chen and Drucker [CD10] gave a positive answer:

Theorem 1.4 ([CD10])**.** *Let φ be a satisfiable* 3SAT *instance with N variables and M clauses (and $M \geq N$). Then one can prove satisfiability of φ, with almost-perfect completeness and constant soundness, using $\widetilde{\Theta}(\sqrt{M})$ unentangled quantum proofs, each with $\Theta(\log M)$ qubits, and by only making LOCC (in fact, Bell) measurements.*

The analysis of [CD10] does not give a smooth tradeoff between the number of provers and soundness, because their proof only shows a soundness gap when the number of provers is $\widetilde{\Theta}(\sqrt{M})$. We give a tight analysis of their protocol that yields a soundness gap for a number of provers $\kappa \in \Omega(\log N)$:

Claim 1.5 (Improved soundness for [CD10])**.** *Let φ be a satisfiable* 3SAT *instance with N variables and M clauses (and $M \geq N$). Then one can prove satisfiability of φ, with completeness $1-e^{-\Omega(\kappa)}$ and soundness $1-\Omega(\frac{\kappa^2}{N+\kappa^2})$, using κ unentangled quantum proofs, each with $\Theta(\log N)$ qubits, and by only making LOCC (in fact, Bell) measurements. Thus, for $\kappa \in \Omega(\log N)$ and $\kappa \in O(\sqrt{N})$, the soundness gap is $\Omega(\kappa^2 N^{-1})$. Moreover, our analysis is tight, in the sense of Remark 2.*

The improvement comes from the simple observation that the second-moment argument of [CD10] can be strengthened by using a one-sided Chebyshev inequality in place of the two-sided Chebyshev inequality. See Section 5 for more details.

We believe that our technical improvement to [CD10] is of interest because it helps us "push the barrier closer" to the best two-prover LOCC QMA protocols with logarithmic proof length. We believe they exist, but we have not discovered one yet.

More generally, using our observations about "size-efficient" reductions from $\mathsf{NTIME}_{\mathsf{RAM}}(t)$ to 2CSP instances of constant soundness gap (cf. Section 3), we obtain the immediate corollary:

Claim 1.6. *Let $t\colon \mathbb{N} \to \mathbb{N}$ be any proper complexity function and let $L \in \mathsf{NTIME}_{\mathsf{RAM}}(t)$. Then there exists a function $t'\colon \mathbb{N} \to \mathbb{N}$ with $t'(n) \in O\big(t(n)\mathsf{polylog}(t(n))\big)$ such that it is possible to prove membership in $L \cap \{0,1\}^n$, with completeness $1-e^{-\Omega(\kappa)}$ and soundness $1-\Omega(\frac{\kappa^2}{t(n)'+\kappa^2})$, using w unentangled quantum proofs, each with $O\big(\log t'(n)\big)$ qubits.*

1.1.3 Technical improvements to [BT09]

The known results for two-prover QMA protocols with a polylogarithmic proof size for NP-complete languages are the following:

- Blier and Tapp [BT09] give a protocol for instances of graph 3-coloring on N vertices and M edges that has completeness $c = 1$ and soundness $s = 1-\Omega(N^{-6})$; and
- Beigi [Bei10] gives a protocol for constant-gap instances of (balanced) 2-out-of-4 SAT with M clauses that has completeness $c = \frac{3}{4} + \frac{\sqrt{2}}{6M}\sqrt{1-\frac{1}{M}}$ and soundness $s = c - \Omega(M^{-3-\varepsilon})$ for every $\varepsilon > 0$.

We give a tight (and more general) soundness analysis of the protocol of Blier and Tapp [BT09], yielding the best known soundness gap for such protocols:

Claim 1.7 (Improved soundness for [BT09])**.** *The protocol of Blier and Tapp [BT09] for* 2CSP*'s on N vertices and M edge constraints over a K-size alphabet has soundness $s = 1 - \Omega(N^{-2})$, assuming $K \in O(1)$. Moreover, our analysis is tight, in the sense of Remark 3.*

Note that our analysis, just like the original one of Blier and Tapp [BT09], does not assume an instance with constant soundness gap, unlike the improvement by Beigi [Bei10] (and all other multi-prover QMA protocols for NP-complete languages). See Section 6 for details.

More generally, we can use our observations about reducing $\mathsf{NTIME}_{\mathsf{RAM}}(t)$ languages to 2CSP instances with a "quasilinear blowup in size" (cf. Section 3) to obtain the immediate corollary:[2]

Claim 1.8. *Let $t \colon \mathbb{N} \to \mathbb{N}$ be any proper complexity function and let $L \in \mathsf{NTIME}_{\mathsf{RAM}}(t)$. Then there exists a function $t' \colon \mathbb{N} \to \mathbb{N}$ with $t'(n) \in O\big(t(n)\mathsf{polylog}(t(n))\big)$ such that it is possible to prove membership in $L \cap \{0,1\}^n$, with perfect completeness and soundness $1 - \Omega(t'(n)^{-2})$, using 2 unentangled quantum proofs, each with $O\big(\log t'(n)\big)$ qubits.*

1.1.4 On the way to a solution

We can think of two ways of answering Question 1: an "indirect" construction and a "direct" construction.

Indirect construction. The first step is to construct two-prover LOCC QMA protocol for 3SAT with $\Omega(\frac{1}{\sqrt{N}\mathsf{polylog}(N)})$ soundness gap and logarithmic proof size; the second step is to directly amplify the protocol to constant soundness, thereby obtaining the required parameters of proof length and soundness. (Indeed, since LOCC QMA protocols amplify "naturally", there is no need to use a product test [HM10], which would have broken the LOCC property anyways, nor there is any need to invoke additional assumptions such as the Weak Additivity Conjecture [ABD+09, Theorem 35].)

Through Claim 1.7 we have made some progress in this direction by improving the best-known soundness gap of two-prover protocols for 3SAT with a polylogarithmic proof size to $\Omega(N^{-2})$. Unfortunately, the protocol is not LOCC and does achieve the required soundness gap of $\Omega(\frac{1}{\sqrt{N}\mathsf{polylog}(N)})$. On the bright side, the protocol does not exploit the power of PCPs. We believe that an improvement should be possible:

Conjecture 1. *There exists a two-prover LOCC* QMA *protocol for* 3SAT *with $\Omega(\frac{1}{N\mathsf{polylog}(N)})$ soundness gap and logarithmic proof size.*

While we believe that our understanding of two-prover protocols for NP-complete languages and logarithmic proof size is still far from complete, we also believe that an answer to Question 1 via an indirect construction is unlikely:

Conjecture 2. *There is no two-prover LOCC* QMA *protocol (or even a* QMA *protocol) for* 3SAT *with $\omega(\frac{1}{N\mathsf{polylog}(N)})$ soundness gap and logarithmic proof size.*

We are not aware of any unlikely complexity consequences if Conjecture 2 turns out to be false. (Aaronson et al. [ABD+09, Footnote 2] did observe that if a weaker conjecture, where $\omega(\frac{1}{N\mathsf{polylog}(N)})$ is replaced by $\Omega(1)$, were to be true, then it would imply that $\mathsf{QMA}(2) = \mathsf{NEXP}$, which is believed to be unlikely.)

[2]Specifically, the corollary directly follows from invoking Claim 3.1; in this case, we happen not to exploit the constant soundness gap of the 2CSP instance so obtained.

Direct construction. A protocol with the required parameters is constructed "directly" in the sense of proposing an LOCC verifier test that acts on all the provided qubits at the same time, possibly in a much more complicated way than just repeating a simpler verifier protocol (as in the indirect construction).

The main difficulty, unsurprisingly, is indeed the LOCC requirement, which, in particular, forbids us any use of the swap test across the two registers. Unfortunately, the swap test forms the basis of almost every result on properties of multiple-prover QMA, including:

- the fact that any $\mathsf{QMA}(\kappa)$ protocol with constant soundness can be simulated by a $\mathsf{QMA}(2)$ protocol with $\Omega(1/\kappa)$ soundness [ABD+09, Theorem 36];
- the fact that symmetric $\mathsf{QMA}(\kappa)$ with almost perfect completeness and constant soundness is contained in $\mathsf{QMA}(\kappa)$ [ABD+09, Lemma 38];
- the fact that $\mathsf{QMA}(\kappa)$ is contained in "$\mathsf{QMA}(\frac{2}{3}\kappa)$" with constant losses in completeness and soundness [KMY03, Lemma 8];
- the protocols of [BT09], [Bei10], [ABD+09], and [HM10].

Most importantly, the swap test is at the basis of the product test of Harrow and Montanaro [HM10]. In particular, the (natural) approach that attempts to construct a "product test type result" out of LOCC measurements (and apply it to, say, the protocol of [CD10]) runs into the risk of implying that $\mathsf{QMA}(\kappa) = \mathsf{QMA}_{\mathsf{LOCC}}(2)$, which, through the result of Brandão et al. [BaCJ10], would have the unlikely consequence of $\mathsf{QMA}(k) = \mathsf{QMA}$. Thus, any such approach must make essential "non-black-box" use of the structure of the language at hand (e.g., that of 2-out-of-4 SAT) to avoid being a "generic" test.

We do not have conjectures about how a direct construction might look like.

1.2 Open Problems

The basic Question 1 remains unanswered. We have proposed two concrete conjectures, Conjecture 1 and Conjecture 2; we believe that any proof or disproof of these conjectures, while it might not directly answer Question 1, should definitely greatly contribute towards our understanding of multiple-prover QMA protocols for NP languages.

We also take the opportunity to informally conjecture that 2CSP instances with constant soundness gap are the "right" instances to consider for further progress, and that we only need to become better LOCC QMA protocol designers.

2 Preliminaries

Two languages and non-deterministic time. First, we define two NP languages that we will be working with. The first language is constraint-satisfaction problems on graphs:

Definition 2.1 (Graph Constraint Satisfaction)**.** *Let $G, = (V, E)$ be a graph (possibly with self-loops) and an alphabet Σ. A* graph constraint-satisfaction problem *is a pair $\mathcal{C} = (G, \{R_e\}_{e\in E})$ where $R_e \colon \Sigma\times\Sigma \to \{0,1\}$ for each $e \in E$. We say that $\mathcal{C}$ is satisfiable if there is a labeling $C \colon V \to \Sigma$ such that every edge predicate evaluates to 1. We say that $\mathcal{C}$ is δ-satisfiable if, for every possibly labeling of the vertices, at most a δ fraction of the edge predicates evaluate to 1.*

Fix positive integers N, M, and K. The class $\mathsf{2CSP}(N, M, K)$ consists of satisfiable graph constraint-satisfaction problems over K-size alphabets on graphs of N vertices and M edges.

The second language is SAT formulae with some additional structure:

Definition 2.2 (2-Out-Of-4 SAT)**.** *The class* $(2,4)\mathsf{SAT}$ *consists of* 2*-out-of-*4 *satisfiable* 4*-CNF formulae. (A* 4*-CNF formula is* 2*-out-of-*4 *satisfiable if there is an assignment to the variables such that for every clause in the* 4*-CNF exactly two of the four variables are satisfied.)*

For brevity, we will denote $(2,4)\mathsf{SAT}^*$ *the gap-version*[3] *of* $(2,4)\mathsf{SAT}$ *such that every variable appears in* $\Theta(1)$ *number of clauses.*

Next, we recall the definition of a proper complexity function:

Definition 2.3 (Proper Complexity Function)**.** *A monotonically increasing function* $f\colon \mathbb{N} \to \mathbb{N}$ *is a* proper complexity function *if a multi-tape Turing machine can compute* $1^n \mapsto 1^{f(n)}$ *in time and space* $O(f(n))$*. See [Pap94, Definition 7.1] for more details.*

Finally, we recall non-deterministic time complexity classes with respect to multi-tape Turing machines and random-access machines:

Definition 2.4 ($\mathsf{NTIME_{mTM}}$)**.** *A multi-tape Turing machine is a finite state machine attached to multiple tapes, with one head per tape. The tapes are infinite in one direction. The machine can read and write to each tape, moving one cell per time step. See [Pap94] for more details.*

That the machine is non-deterministic means that the finite state control of the Turing machine can non-deterministically decide its next move, such that the machine accepts if and only if there is some non-deterministic choice that allows it to accept.

For a proper complexity function t*,* $\mathsf{NTIME_{mTM}}(t)$ *denotes the class of languages that can be recognized by a* t*-time non-deterministic multi-tape Turing machine.*

Definition 2.5 ($\mathsf{NTIME_{RAM}}$)**.** *A random-access machine (RAM) is a list of commands that includes a finite number of control registers as well as an unbounded number of indexable registers. Each register holds an integer. Commands include addition, multiplication (with a log-cost penalty), branching on register contents, and indexing the registers with the contents of other registers. See [GS89] for more details.*

That the machine is non-deterministic means that the finite list of commands of the random-access machine allow non-deterministic branching to its next move, such that the machine accepts if and only if there is some non-deterministic choice that allows it to accept.

For a proper complexity function t*,* $\mathsf{NTIME_{RAM}}(t)$ *denotes the class of languages that can be recognized by a* t*-time non-deterministic random-access machine.*

Information theory. First, we recall the classical information-theoretic notion of statistical distance between two probability distributions [NC00, Sec. 9.1]:

Definition 2.6 (Statistical Distance)**.** *Let* P *and* Q *be two probability distributions over the same finite set* S*. The* statistical distance *between* P *and* Q*, denoted* $|P - Q|_1$*, is defined as the quantity*

$$\frac{1}{2} \sum_{s \in S} \left| P(s) - Q(s) \right| \ .$$

Next, we recall its quantum analogue of trace distance [NC00, Sec. 9.2.1]:

[3]That is, the problem of distinguishing 4-CNF formulas that are perfectly 2-out-of-4 satisfiable versus those that are only $1 - \Omega(1)$ 2-out-of-4 satisfiable

Definition 2.7 (Trace Distance)**.** *The* trace distance *between two quantum states ρ and σ, denoted $|\rho - \sigma|_{\mathrm{Tr}}$, is defined as the quantity:*

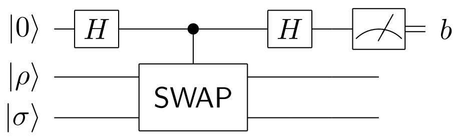
$$\frac{1}{2}\,\mathrm{Tr}\left(\sqrt{(\rho-\sigma)^{\dagger}(\rho-\sigma)}\right) \quad .$$

If ρ and σ commute, then they can be simultaneously diagonalized, and the trace distance between ρ and σ reduces to the statistical distance between the two probability distributions induced by the two sets of eigenvalues of ρ and σ.

If ρ and σ are two pure states $|\phi\rangle\langle\phi|$ and $|\psi\rangle\langle\psi|$, then the trace distance between $|\phi\rangle\langle\phi|$ and $|\psi\rangle\langle\psi|$ simplifies [NC00, Sec. 9.2.3] to the quantity $\sqrt{1 - |\langle\phi|\psi\rangle|^2}$.

Also, we recall that, given a projective measurement (i.e., a Hermitian operator) M, if P and Q are the probability distributions describing the outcomes obtained when measuring M on $|\phi\rangle$ and $|\psi\rangle$ respectively, then $|P - Q|_1 \leq ||\phi\rangle\langle\phi| - |\psi\rangle\langle\psi||_{\mathrm{Tr}}$. For convenience, we will denote by $\mathsf{dstr}_M(|\phi\rangle)$ the distribution P, and simply $\mathsf{dstr}(|\phi\rangle)$ when M is assumed to be a full computational basis measurement.

Swap test. Buhrman et al. [BCWdW01] introduced the *swap-test on two quantum states ρ and σ*, given by the following quantum circuit:



Essentially, the swap-test measures the overlap between two quantum states, because

$$\Pr\left[b = 0\right] = \frac{1 + \mathrm{Tr}(\rho\sigma)}{2} \quad ,$$

i.e., if $\rho = \sigma$, then the swap-test always yields the outcome 0, if instead $\rho \neq \sigma$, then the probability of measuring 0 is directly proportional to the overlap between ρ and σ. In particular, if one wishes to use the swap test in order to check whether two quantum states are equal or not, then the probability of discovering that they are in fact not equal (i.e., the test "rejects") is equal to $(1 - \mathrm{Tr}(\rho\sigma))/2$. Note that if ρ and σ are two pure states $|\phi\rangle\langle\phi|$ and $|\psi\rangle\langle\psi|$, then the probability above is equal to $(1 - |\langle\phi|\psi\rangle|^2)/2$; for convenience, we denote this probability by $\mathsf{REJ}\big(\textsc{Swap}(|\phi\rangle, |\psi\rangle)\big)$.

If the probability that the swap test rejects two quantum states is bounded above, then the statistical distance between the two probability distributions arising when measuring the two quantum states (in any basis) is also bounded above:

Lemma 2.1. *Let $|\phi\rangle$ and $|\psi\rangle$ be quantum states and δ a number in $[0, 1]$. If $\mathsf{REJ}\big(\textsc{Swap}(|\phi\rangle, |\psi\rangle)\big) \leq \delta$, then $|\mathsf{dstr}(|\phi\rangle) - \mathsf{dstr}(|\psi\rangle)|_1 \leq \sqrt{2\delta}$.*

Proof. Recall that $\mathsf{REJ}\big(\textsc{Swap}(|\phi\rangle, |\psi\rangle)\big) = \frac{1}{2} - \frac{|\langle\phi|\psi\rangle|^2}{2}$, so that

$$|\mathsf{dstr}(|\phi\rangle) - \mathsf{dstr}(|\psi\rangle)|_1 \leq ||\phi\rangle\langle\phi| - |\psi\rangle\langle\psi||_{\mathrm{Tr}} = \sqrt{1 - |\langle\phi|\psi\rangle|^2} \leq \sqrt{2\delta} \quad .$$

□

Quantum Fourier transform. Finally, we recall the quantum Fourier transform:

Definition 2.8 (Quantum Fourier Transform)**.** *Let $\mathcal{H}_n$ be an n-dimensional Hilbert space with orthonormal basis $\{|0\rangle, \ldots, |n-1\rangle\}$. The* n-dimensional quantum Fourier transform*, denoted F_n, is the linear operator whose action on the basis vector $|j\rangle$, $j \in \{0, 1 \ldots, n-1\}$, is given by*

$$|j\rangle \mapsto \frac{1}{\sqrt{n}} \cdot \sum_{k=0}^{n-1} e^{2\pi\sqrt{-1}(jkN^{-1})}|k\rangle \quad .$$

We recall that F_n is a unitary operator. Also, we will denote by $|0_{F_n}\rangle$ the image of $|0\rangle$ under F_n, and it satisfies the following equation:

$$|0_{F_n}\rangle = \frac{|0\rangle + |1\rangle + \cdots + |n-1\rangle}{\sqrt{n}} .$$

For more details on the quantum Fourier transform, see [NC00, Ch. 5].

Quantum proofs. In an κ-prover QMA protocol, the BQP verifier (Arthur) receives a classical input $x \in \{0,1\}^*$ together with κ quantum proofs $|\Psi^{(1)}\rangle, \ldots, |\Psi^{(\kappa)}\rangle$ sent by the κ provers (Merlins); the provers (and thus the quantum proofs they send) are promised to be *unentangled*. The verifier will then decide whether to accept x or not, based on all the quantum proofs he received.

Definition 2.9 (Multi-Prover QMA). *Fix a set of admissible Hermitian operators $\mathcal{M}$ (i.e., each $M \in \mathcal{M}$ satisfies $0 \preceq M \preceq I$), polynomially-bounded functions $\kappa, \ell \colon \mathbb{N} \to \mathbb{N}$, and arbitrary functions $s, c \colon \mathbb{N} \to [0,1]$.*

A language $L \subseteq \{0,1\}^*$ is in $\mathsf{QMA}_\ell^{\mathcal{M}}(\kappa, c, s)$ if there exists a polynomial-time quantum algorithm V_L restricted to performing measurements from $\mathcal{M}$ such that, for all inputs $x \in \{0,1\}^n$, the following conditions hold:

- Completeness: *If $x \in L$, there exist $\kappa(n)$ quantum proofs $|\Psi^{(1)}\rangle, \ldots, |\Psi^{(\kappa(n))}\rangle$, each a state of at most $\ell(n)$ qubits, such that V_L accepts with probability at least $c(n)$ on input $|x\rangle|\Psi^{(1)}\rangle \cdots |\Psi^{(\kappa(n))}\rangle$; and*

- Soundness: *If $x \notin L$, for every $\kappa(n)$ quantum proofs $|\Psi^{(1)}\rangle, \ldots, |\Psi^{(\kappa(n))}\rangle$, each a state of at most $\ell(n)$ qubits, V_L rejects with probability at least $s(n)$ on input $|x\rangle|\Psi^{(1)}\rangle \cdots |\Psi^{(\kappa(n))}\rangle$.*

The class $\mathsf{QMA}_\ell(\kappa, c, s)$ is defined to be the class $\mathsf{QMA}_\ell^{\mathcal{M}}(\kappa, c, s)$ where $\mathcal{M}$ is the set of all Hermitian operators. The class $\mathsf{QMA}(\kappa, c, s)$ is defined to be the class $\mathsf{QMA}_{\mathsf{poly}(\cdot)}(\kappa, c, s)$. The class $\mathsf{QMA}(\kappa)$ is defined to be the class $\mathsf{QMA}(\kappa, 2/3, 2/3)$.

Note that any set of admissible Hermitian operators $\mathcal{M}$ induces a set of binary measurements, where each $M \in \mathcal{M}$ means "accept" and $I - M$ means "reject". For example, if we let $\mathcal{M} = \mathsf{Bell}$ is the set of Bell measurements (non-adaptive, unentangled measurements), $\mathcal{M} = \mathsf{LOCC}$ is the set of LOCC measurements (adaptive, unentangled measurements), and $\mathcal{M} = \mathsf{SEP}$ is the set of separable admissible Hermitian operators (which includes the swap test and product test).

3 Quasilinear PCPs

In this section, we show how a few simple observations suffice to generalize the known positive results on multi-prover QMA protocols for NP languages (i.e., [BT09], [Bei10], [ABD+09], [CD10], and [HM10]). Doing so allows us to exhibit a large class of problems that qualify as positive examples to Question 2 raised by Aaronson et al. [ABD+09].

The main observation is the fact that "short" PCPs exist not only for 3SAT but, more generally, for every NTIME language:

Claim 3.1 (Quasilinear PCPs for NTIME Languages). *Let $t \colon \mathbb{N} \to \mathbb{N}$ be any proper complexity function and let L be a language in $\mathsf{NTIME}_{\mathsf{RAM}}(t)$. Then, there exist*

- *a* size function $S_L \colon \mathbb{N} \to \mathbb{N}$ *with* $S_L(n) \in t(n)\mathsf{polylog}(t(n))$,
- *a* density function $D_L \colon \mathbb{N} \to \mathbb{N}$ *with* $D_L(n) \in t(n)\mathsf{polylog}(t(n))$,
- *a* color constant $K_L \in \mathbb{N}$,
- *a* reduction complexity function $C_L \colon \mathbb{N} \to \mathbb{N}$ *with* $C_L \in \mathsf{poly}(t(n))$,

- *a* C_L*-time reduction* $R_L\colon \{0,1\}^* \to \{0,1\}^*$ *from* L *to* 2CSP*,*
- *a* gap constant $\eta_L \in (0,1)$*, and*
- *a* regularity constant $d_L \in \mathbb{N}$*,*

such that, for every instance $x \in \{0,1\}^n$*, the following properties hold:*

- Efficiency: $R_L(x)$ *is a* $\mathsf{2CSP}(N,M,K)$ *instance with* $N = S_L(n)$*,* $M = D_L(n)$*, and* $K = K_L$*;*
- Completeness: *if* $x \in L$*, then* $R_L(x) \in \mathsf{2CSP}(N,M,K)$*;*
- Soundness: *if* $x \notin L$*, then* $R_L(x)$ *is* $(1-\eta_L)$*-satisfiable; and*
- Regularity: $R_L(x)$ *is* d_L*-regular (with self-loops).*

The claim is simply a statement about the short PCPs that are obtained by combing the works of Ben-Sasson and Sudan [BSS08] and Dinur [Din07], together with some simple observations about the generality of their results.

Proof. Ben-Sasson and Sudan proved [BSS08, Theorem 2.2] that

$$\mathsf{NTIME}_{\mathsf{mTM}}(t(n)) \subseteq \mathsf{PCP}_{1,\frac{1}{2}}\left[\log\left(t(n)\mathsf{polylog}(t(n))\right), \mathsf{polylog}(t(n))\right] .$$

In order to construct "short" PCPs for 3SAT, Dinur:

(i) observes [Din07, Lemma 8.3] that the result of Ben-Sasson and Sudan implies that 3SAT can be reduced to 2CSP instances that satisfy all the properties of the claim, with the exception that the soundness gap is is only $1/\mathsf{polylog}(n)$; and

(ii) then she applies her main technical result of gap amplification [Din07, Theorem 1.5] to bring the soundness gap to a constant η.

Then, (i) and (ii) together easily imply "short" PCPs for 3SAT [Din07, Theorem 8.1].

We note that Dinur's first observation, (i), only relies on the fact that $\mathsf{3SAT} \in \mathsf{NTIME}_{\mathsf{mTM}}(t(n))$ for some $t(n) \in n\mathsf{polylog}(n)$, and a similar observation can be made for a general language $L \in \mathsf{NTIME}_{\mathsf{mTM}}(t(n))$, which, again combined with her gap amplification result, yields the claim for languages in $\mathsf{NTIME}_{\mathsf{mTM}}(t(n))$.

We choose to not state the claim for languages in $\mathsf{NTIME}_{\mathsf{mTM}}(t(n))$, because it is not as illuminating; it seems quite tedious (and difficult) to check whether a given language L can be recognized in non-deterministic $t(n)$-time by some multi-tape Turing machine. Instead, we observe that, by using a result of Gurevich and Shelah [GS89, Theorem 2], which implies that $\mathsf{NTIME}_{\mathsf{RAM}}(t) \subseteq \mathsf{NTIME}_{\mathsf{mTM}}(t'(n))$ for some $t'(n) \in t(n)\mathsf{polylog}(t(n))$, we obtain the claim as stated;[4] this way, the task of checking whether a given language is in L is in $\mathsf{NTIME}_{\mathsf{RAM}}(t)$ is much simpler: one only needs to write "pseudocode" for the non-deterministic verifier, and prove that it halts in time $t(n)$. □

Remark 1 (Other Non-Deterministic Models of Computation)**.** On the one hand, the deterministic time complexity of different models of computation is not always "tightly related". For example, it is believed that a deterministic multi-tape Turing machine cannot simulate a generic deterministic t-time random-access machine in time $t\mathsf{polylog}(t)$. Similar beliefs (and sometimes proofs) exist between supposedly "weak" models of computation (such as Turing machines) and "strong" models of computation (such as random-access machines).

On the other hand, surprisingly, the situation is quite different for *non*-deterministic models of computation, where, instead, it turns out that their time complexities *are* tightly related. For example, the result of [GS89] shows that, "up to polylogarithmic factors", $\mathsf{NTIME}_{\mathsf{RAM}}(t) = \mathsf{NTIME}_{\mathsf{mTM}}(t)$. In the same paper, similar results are shown for other models, such as Kolmogorov-Uspensky machines

[4]The result of Gurevich and Shelah [GS89, Theorem 2] in fact states that $\mathsf{NTIME}_{\mathsf{RAM}}(n) \subseteq \mathsf{NTIME}_{\mathsf{mTM}}(n\mathsf{polylog}(n))$, but the proof can easily be extended to show that $\mathsf{NTIME}_{\mathsf{RAM}}(t) \subseteq \mathsf{NTIME}_{\mathsf{mTM}}(t'(n))$ for some $t'(n) \in t(n)\mathsf{polylog}(t(n))$.

and Schönhage machines. In other words, the class $\mathsf{NTIME}(t)$, unlike $\mathsf{TIME}(t)$, is quite robust (again, up to polylogarithmic factors) to a choice of model of computation, so that Claim 3.1 could indeed be stated relative to many other models of computation.

However, we believe the result is most useful when stated relative to random-access machines, because they are closest to our notion of a computer, and we can easily test our intuition about whether a given language L can be put in $\mathsf{NTIME}(t)$ for some t.

The $\mathsf{2CSP}$ instance guaranteed by Claim 3.1 is already a "nice" instance for which multiple-prover QMA results have been proved. For example, a $\mathsf{2CSP}$ instance is the starting point of Blier and Tapp [BT09] and Chen and Drucker [CD10], so that we obtain generic results for both protocols.[5] See Claim 1.8 and Claim 1.5 for generic statements (of our improvement) of both results.

Other works, instead, such as [ABD+09] and [Bei10] "process the $\mathsf{2CSP}$ instance further", in order to give it additional structure (that is exploited in their protocols). Thus, these additional processings also inherit the more general reduction guaranteed by Claim 3.1 for all of the languages in $\mathsf{NTIME}_{\mathsf{RAM}}(t)$:

Corollary 1 (Constant-Gap Boolean Formulae for NTIME Languages)**.** *Let $t\colon \mathbb{N} \to \mathbb{N}$ be any proper complexity function and let L be a language in $\mathsf{NTIME}_{\mathsf{RAM}}(t)$. Then,*

(i) $\mathsf{3SAT}$ **Formulae:** *there exist*

- *a* size function $S_L\colon \mathbb{N} \to \mathbb{N}$ *with* $S_L(n) \in t(n)\mathsf{polylog}(t(n))$,
- *a* density function $D_L\colon \mathbb{N} \to \mathbb{N}$ *with* $D_L(n) \in t(n)\mathsf{polylog}(t(n))$,
- *a* reduction complexity function $C_L\colon \mathbb{N} \to \mathbb{N}$ *with* $C_L \in \mathsf{poly}(t(n))$,
- *a C_L-time reduction $R_L\colon \{0,1\}^* \to \{0,1\}^*$ from L to* $\mathsf{3SAT}$*, and*
- *a* gap constant $\eta_L \in (0, 1)$,

such that, for ever instance $x \in \{0,1\}^n$, the following properties hold:

- Efficiency: *$R_L(x)$ is a* $\mathsf{3SAT}$ *instance with $N = S_L(n)$ variables and $M = D_L(n)$ clauses;*
- Completeness: *if $x \in L$, then $R_L(x) \in$* $\mathsf{3SAT}$*; and*
- Soundness: *if $x \notin L$, then $R_L(x)$ is $(1 - \eta_L)$-satisfiable.*

(ii) $(2,4)\mathsf{SAT}^*$ **Formulae:** *there exist*

- *a* size function $S_L\colon \mathbb{N} \to \mathbb{N}$ *with* $S_L(n) \in t(n)\mathsf{polylog}(t(n))$,
- *a* density function $D_L\colon \mathbb{N} \to \mathbb{N}$ *with* $D_L(n) \in t(n)\mathsf{polylog}(t(n))$,
- *a* reduction complexity function $C_L\colon \mathbb{N} \to \mathbb{N}$ *with* $C_L \in \mathsf{poly}(t(n))$,
- *a C_L-time reduction $R_L\colon \{0,1\}^* \to \{0,1\}^*$ from L to* $(2,4)\mathsf{SAT}$*, and*
- *a* gap constant $\eta_L \in (0, 1)$,
- *a* balance constant $b_L \in \mathbb{N}$,

such that, for ever instance $x \in \{0,1\}^n$, the following properties hold:

- Efficiency: *$R_L(x)$ is a* $\mathsf{3SAT}$ *instance with $N = S_L(n)$ variables and $M = D_L(n)$ clauses;*
- Completeness: *if $x \in L$, then $R_L(x) \in$* $\mathsf{3SAT}$*;*
- Soundness: *if $x \notin L$, then $R_L(x)$ is $(1 - \eta_L)$-satisfiable;*
- Balance: *each variable of $R_L(x)$ appears in at most d_L clauses.*

Of course, one could add more items to the above corollary, other than $\mathsf{3SAT}$ and $(2,4)\mathsf{SAT}$, if other languages that can be efficiently reduced to from $\mathsf{2CSP}$ are found to be useful. We chose to mention only $\mathsf{3SAT}$ because of its general importance and $(2,4)\mathsf{SAT}^*$ because it was successfully used by [ABD+09] and [Bei10].

[5] Blier and Tapp, though, do not exploit the constant soundness gap, so simply start from the classical NP-complete problem of graph 3-colorability.

The proof of the corollary was party sketched, in the particular case of $t(n) = n$ in [ABD+09, Lemma 12]. We give here the more general proof:

Proof. To obtain (i), we argue as follows. To prove the first item, it suffices to convert the instance guaranteed by Claim 3.1, which is a 2CSP instance over a constant-size alphabet, into a 3SAT instance, in a way that preserves perfect completeness and degrades the soundness gap by at most a constant factor.

First, consider a 2CSP instance over a constant-size alphabet. Observe that we can transform this into a CSP over a binary alphabet by allowing constraints to restrict multiple variables. As the original alphabet was of constant-size, this only increase the arity, number of variables, and number of constraints in the CSP by a constant factor. Further, the soundness gap is preserved.

So consider now a constraint C in the CSP over variables $\vec{x}$. By the Cook-Levin Theorem, there exist a 3SAT formula φ_C and additional variables $\vec{y}$ such that $C(\vec{x})$ if and only if there exists $\vec{y}$ such that $\varphi_C(\vec{x}, \vec{y})$. Observe that the size of φ_C is at most some constant g, because the original CSP is over a constant-size alphabet and has arity 2. Define the output of this reduction to be the 3SAT formula $\varphi := \bigwedge_C \varphi_C$.

We now analyze the properties of φ. First, observe that the number of clauses in φ is at most g times the number of constraints in the original CSP, and the number of variables is also a constant-factor more than the number of variables in the original CSP. Further, if the original CSP was satisfiable, then so must be φ_C, so perfect completeness is preserved. To analyze soundness, suppose that the original CSP was at most δ satisfiable. Then, in any assignment to φ, at least $(1 - \delta) \cdot E$ clauses must be unsatisfied, where E is the number of constraints in the original CSP. At there are at most gE clauses in φ, this means that φ can have at most $1 - \frac{1-\delta}{g}$ satisfied clauses. Thus, there is still a constant soundness gap.

To obtain (ii), we first invoke (i) so to obtain a reduction to 3SAT, and then follow the outline of Aaronson et al. [ABD+09, Lemma 12]. Specifically, the instance output by the reduction guaranteed by (i) can first be further modified using a reduction of Papadimitriou and Yannakakis [PY91] from 3SAT to 3SAT that makes each variable appear in at most $b_L = 29$ (in fact, exactly) clauses (and this reduction preserves the constant soundness gap); then, we apply a reduction of Khanna et al. [KSTW01] (that preserves both the constant soundness gap and the balanced property of the formula) from 3SAT to (2, 4)SAT. The reason that the outline of Aaronson et al. [ABD+09, Lemma 12] also works in the general case considered in this corollary is that the number of variables and clauses increases only a by a constant through these two additional reductions. □

4 Graph States

Let $G = (V, E)$ be a graph with N vertices and M edges, and let Σ be a finite color alphabet of size K. The graph G and the color alphabet Σ will be fixed throughout the rest of the paper.

We say that a quantum state $|\Psi\rangle$ is a *graph state* (for G and Σ) if it is a quantum state over a Hilbert space $\mathcal{H} = (\mathcal{H}_2)^{\otimes \log N} \otimes (\mathcal{H}_2)^{\otimes \log K}$. Thus, any graph state $|\Psi\rangle$ can be written as

$$|\Psi\rangle = \sum_{v=0}^{N-1} \alpha_v |v\rangle \sum_{j=0}^{K-1} \beta_{v,j} |j\rangle \ ,$$

where $\sum_{v=0}^{N-1} |\alpha_v|^2 = 1$ and $\sum_{j=0}^{K-1} |\beta_{v,j}|^2$ for each $v \in \{0, \ldots, N-1\}$ and $j \in \{0, \ldots, K-1\}$. (Note that the definition of a graph state is independent of the edge set E.)

We believe that developing strong tools for *graph-state property testing* is essential for making improvement towards better multi-prover QMA protocols.[6] As a first move in that direction, we give in the next subsection two lemmas for graph states, which were implicitly used in both [BT09] and [CD10] with very different parameters, and present them in a generic form. After that, we summarize the tests for graph states that have been used in previous protocols.

4.1 Two Lemmas on Graph States

Let us first introduce some simple notation: given any graph state $|\Psi\rangle$,

- for $c \in (0, 1]$, $R_c(|\Psi\rangle)$ is the subset of V consisting of those vertices v for which $|\alpha_v|^2 < c$;
- for $c \in (0, 1]$, $S_c(|\Psi\rangle)$ is equal to $V - R_c(|\Psi\rangle)$;
- for $j = 0, \dots, K-1$, $p_j(|\Psi\rangle)$ is equal to the probability of measuring j in the color register of the quantum state $(I_N \times F_K)|\Psi\rangle$; and
- for $j = 0, \dots, K-1$, $|\gamma(j)\rangle = \sum_{v=0}^{N-1} \gamma_v(j)|v\rangle$ is the reduced quantum state obtained when we measure j in the color register of $(I_N \otimes F_K)|\Psi\rangle$.

First, we prove that, as long as a color j has a large-enough probability of being measured in the color register of $(I_N \times F_K)|\Psi\rangle$, if a vertex v has small amplitude then it will also have a small amplitude in the reduced state conditioned on measuring j.

Lemma 4.1 (modified [CD10, Lemma 3], which was implicit in [BT09, Lemma 3.7])**.** *Fix a vertex $v \in \{0, \dots, N-1\}$, a color $j \in \{0, \dots, K-1\}$, and two positive numbers c_1 and c_2. Then:*

$$\left(p_j(|\Psi\rangle) \geq \frac{1}{c_2} \text{ and } |\alpha_v|^2 < \frac{1}{c_1 N}\right) \longrightarrow \left(|\gamma_v(j)|^2 < \frac{c_2}{c_1 N}\right) .$$

Proof. Let $|X\rangle$ be the quantum state obtained from $|\Psi\rangle$ after performing the quantum Fourier transform on the color register of $|\Psi\rangle$, i.e.,

$$\begin{aligned} |X\rangle &= (I_N \otimes F_K)|\Psi\rangle \\ &= (I_N \otimes F_K) \sum_{v=0}^{N-1} \alpha_v |v\rangle \sum_{j=0}^{K-1} \beta_{v,j} |j\rangle \\ &= \sum_{v=0}^{N-1} \alpha_v |v\rangle \sum_{j=0}^{K-1} \beta_{v,j} \frac{1}{\sqrt{K}} \sum_{k=0}^{K} e^{\frac{2\pi\sqrt{-1}jk}{K}} |k\rangle \\ &= \frac{1}{\sqrt{K}} \sum_{k=0}^{K} \left(\sum_{v=0}^{N-1} \alpha_v \left(\sum_{j=0}^{K-1} \beta_{v,j} e^{\frac{2\pi\sqrt{-1}jk}{K}} \right) |v\rangle \right) |k\rangle . \end{aligned}$$

For each $v \in \{0, \dots, n\}$, let $P_{v,j}(|\Psi\rangle)$ be the probability that the color register of $|X\rangle$ is measured j and the vertex register is measured v. Recalling that $|\gamma(j)\rangle = \sum_{v=0}^{N-1} \gamma_v(j)|v\rangle$ is the reduced quantum state when outcome j occurs, we have that

$$P_{v,j}(|\Psi\rangle) = p_j(|\Psi\rangle) \cdot |\gamma_v(j)|^2 .$$

[6] For example, we believe that a two-prover $\mathsf{QMA}_{\mathsf{LOCC}}$ protocol for $\mathsf{2CSP}(N, \widetilde{O}(N), O(1))$ with $\Omega(1/N)$ soundness gap and polylogarithmic proof length exists (cf. Conjecture 1), but we do not know of one yet. Our improved soundness analysis of [CD10] almost achieves that, and it seems that a somewhat smarter LOCC verifier should suffice. Developing a theory of graph-state property testing should shed some light on how to design such a verifier.

On the other hand, it is also the case that

$$
\begin{aligned}
P_{v,j}(|\Psi\rangle) &= \left| \frac{\alpha_v}{\sqrt{K}} \sum_{j=0}^{K-1} \beta_{v,j} e^{\frac{2\pi\sqrt{-1}jk}{K}} \right|^2 \\
&= \frac{|\alpha_v|^2}{K} \cdot \left| \sum_{j=0}^{K-1} \beta_{v,j} e^{\frac{2\pi\sqrt{-1}jk}{K}} \right|^2 \\
&\leq \frac{|\alpha_v|^2}{K} \cdot K \sum_{j=0}^{K-1} \left| \beta_{v,j} e^{\frac{2\pi\sqrt{-1}jk}{K}} \right|^2 \qquad \text{(by Cauchy-Schwarz)} \\
&= |\alpha_v|^2 \quad .
\end{aligned}
$$

We deduce that $p_j(|\Psi\rangle) \cdot |\gamma_v(j)|^2 \leq |\alpha_v|^2$ or, equivalently, that

$$
|\gamma_v(j)|^2 \leq \frac{|\alpha_v|^2}{p_j(|\Psi\rangle)} \quad .
$$

By assumption, the probability of measuring j in the color register of $|X\rangle = (I_N \otimes F_K)|\Psi\rangle$, which is $p_j\big(|\Psi\rangle\big)$, is at least $\frac{1}{c_2}$. Also by assumption, $|\alpha_v|^2 < \frac{1}{c_1 N}$. Therefore,

$$
|\gamma_v(j)|^2 \leq \frac{|\alpha_v|^2}{p_j(|\Psi\rangle)} < \frac{c_2}{c_1 N} \quad ,
$$

as desired. ∎

Next, we prove that if a quantum state has at least one amplitude that is "far" from uniform, then the probability of measuring any given outcome in the Fourier basis can be upper bounded.

Lemma 4.2. *Let $|\gamma\rangle = \sum_{w=0}^{N-1} \gamma_w |v\rangle$ be a quantum state. For every $v \in \{0, \ldots, N-1\}$, the probability of measuring v in the (only) register of $F_N|\gamma\rangle$ is at most*

$$
1 - \frac{1}{4}\left(\sum_{w=0}^{N-1} \left| |\gamma_w|^2 - \frac{1}{N} \right| \right)^2 \quad .
$$

Proof. The probability of measuring v in the (only) register of $F_N|\gamma\rangle$ is given by

$$
\left|\langle \gamma | F_N^{-1} | v \rangle\right|^2 \quad .
$$

Observe that

$$
\left|\mathsf{dstr}\big(|\gamma\rangle\big) - \mathsf{dstr}\big(F_N^{-1}|v\rangle\big)\right|_1 = \frac{1}{2} \sum_{w=0}^{N-1} \left| |\gamma_w|^2 - \left| \frac{e^{\frac{2\pi\sqrt{-1}wv}{N}}}{\sqrt{N}} \right|^2 \right| = \frac{1}{2} \sum_{w=0}^{N-1} \left| |\gamma_w|^2 - \frac{1}{N} \right| \quad .
$$

Recalling that $|\mathsf{dstr}(|\phi\rangle) - \mathsf{dstr}(|\psi\rangle)|_1 \leq \sqrt{1 - |\langle \phi | \psi \rangle|^2}$, we obtain that

$$
\left|\langle \gamma | F_N^{-1} | v \rangle\right|^2 \leq 1 - \frac{1}{4}\left(\sum_{w=0}^{N-1} \left| |\gamma_w|^2 - \frac{1}{N} \right| \right)^2 \quad ,
$$

as desired. ∎

4.2 Summary of Tests for Graph States

We give a brief summary and description of the tests that have been used successfully in protocols with graph states. The first one is the **swap test**, which checks whether two states are close to each other:

$\textsc{Swap}\big(|\Psi\rangle, |\Phi\rangle\big) \equiv$

1. Perform the swap test on the two quantum (graph) states $|\psi\rangle$ and $|\phi\rangle$.
2. Accept if and only if the swap test accepts.

See Section 2 for properties of the swap test. Another test that is often useful is the **uniformity test**:

$\textsc{Unif}\big(|\Psi\rangle\big) \equiv$

1. Compute $|\Phi\rangle = (F_N \otimes F_K)|\Psi\rangle$.
2. Measure the vertex and color register of $|\Phi\rangle$ in the computational basis to get outcome (v, j).
3. If $j = 0$ but $v \neq 0$, then reject.
4. Accept.

A variant of the above test is the **conditional uniformity test**: for any $z \in [0, K]$,

$\textsc{CondUnif}_z\big(|\Psi^{(1)}\rangle, \ldots, |\Psi^{(\kappa)}\rangle\big) \equiv$

1. For $i = 1, \ldots, \kappa$, compute $|\Phi^{(i)}\rangle = (F_N \otimes F_K)|\Psi^{(i)}\rangle$.
2. For $i = 1, \ldots, \kappa$, measure the vertex and color register of $|\Phi^{(i)}\rangle$ in the computational basis to get outcome (v_i, j_i).
3. If $z < |\{i \in \{1, \ldots, \kappa\} : j_i = 0\}|$, then reject.
4. For $i = 1, \ldots, \kappa$, if $j_i = 0$ but $v_i \neq 0$, then reject.
5. Accept.

Intuitively, the conditional uniformity test also makes sure that a significant fraction of the graph states are such that, when their color register is measured in the Fourier basis, the color 0 has a not too small probability of occurring. Finally, the **consistency test** with respect to a given 2CSP instance $\mathcal{C} = (G, \{R_e\}_{e\in E})$ is:

$\textsc{Cons}_{\mathcal{C}}\big(|\Psi^{(1)}\rangle, \ldots, |\Psi^{(\kappa)}\rangle\big) \equiv$

1. For $i = 1, \ldots, \kappa$, measure the graph state $|\Psi^{(i)}\rangle$ in the standard basis to get outcome (v_i, j_i).
2. If there exist distinct $i, i' \in \{1, \ldots, \kappa\}$ such that $v_i = v_{i'}$ but $j_i \neq j_{i'}$, then reject.
3. If there exist distinct $i, i' \in \{1, \ldots, \kappa\}$ such that $(v_i, v_{i'}) \in E$ but $R_{(v_i, v_{i'})}(j_i, j_{i'}) = 0$, reject.
4. Accept.

Throughout, we will denote by $\mathsf{REJ}(\cdot)$ the rejection probability of a given test; e.g., $\mathsf{REJ}\big(\textsc{Swap}\big(|\Psi\rangle, |\Phi\rangle\big)\big)$ denotes the rejection probability of the swap test on the two quantum states $|\Psi\rangle$ and $|\Phi\rangle$.

5 An Improvement on the Soundness Analysis of [CD10]

In this section, we give the details for our tight soundness analysis of the two-prover QMA protocol of Chen and Drucker [CD10]. Specifically, we prove:

Claim (1.5, restated)**.** *The κ-prover QMA protocol for $\mathsf{2CSP}(N, M, K)$ given by Algorithm 1 has completeness $1 - e^{-\Omega(\kappa)}$ and soundness $1 - \Omega\left(\frac{\kappa^2}{N+\kappa^2}\right)$, assuming $K \in O(1)$; thus, for $\kappa \in \Omega(\log N)$ and $\kappa \in O(\sqrt{N})$, the soundness gap is $\Omega(\kappa^2 N^{-1})$. Moreover, the analysis of the soundness of the protocol cannot be improved, in the sense of Remark 2.*

The claim improves the status quo by giving a smooth trade-off between the number of provers κ and the soundness gap as a function of κ, whereas the soundness analysis of [CD10] only gave a soundness gap for $\kappa \in \Theta(\sqrt{N})$.

Algorithm 1: Verifier of [CD10]

---

inputs: a $\mathsf{2CSP}(N, M, K)$ instance $\mathcal{C} = (G, \{R_e\}_{e \in E})$

proofs: κ unentangled graph states $|\Psi^{(1)}\rangle, \ldots, |\Psi^{(\kappa)}\rangle$

verifier: draw $r \in \{1, 2\}$ at random, and perform the r-th test below:

1. $\textsc{CondUnif}_{\frac{99}{100}\kappa}\big(|\Psi^{(1)}\rangle, \ldots, |\Psi^{(\kappa)}\rangle\big)$
2. $\textsc{Cons}_{\mathcal{C}}\big(|\Psi^{(1)}\rangle, \ldots, |\Psi^{(\kappa)}\rangle\big)$

Remark 2 ("Tightness" of Our Analysis)**.** Consider a $\mathsf{2CSP}(N, M, K)$ instance $\mathcal{C} = (G, \{R_e\}_{e \in E})$; suppose that $\mathcal{C}$ is *not* satisfiable, and suppose also that $\mathcal{C}$ has constant soundness gap η. Hence, for any coloring $C \colon V \to \Sigma$, at least $\eta|E|$ of the edge constraints $\{R_e\}_{e \in E}$ are *not* satisfied. So fix any coloring C.

Now suppose that the κ graph states $|\Psi^{(1)}\rangle, \ldots, |\Psi^{(\kappa)}\rangle$ given to the verifier are all equal and indeed are a uniform superposition of all vertices with a unique color determined by C. If so, the test $\textsc{Cons}_{\mathcal{C}}\big(|\Psi^{(1)}\rangle, \ldots, |\Psi^{(\kappa)}\rangle\big)$ rejects with probability $O(\frac{\kappa^2}{N})$ by the Birthday Problem (indeed, we only have κ^2 chances to see a particular edge in the constraint graph, and a constrained edge is seen with only probability $\Theta(N^{-1})$ because the graph is sparse). Thus, our analysis is "tight" in the sense that the assumptions we made could indeed really be the case, so one cannot hope to exhibit an even better soundness analysis that proves a soundness gap of $\omega(\kappa^2/N)$.

Furthermore, if instead $\mathcal{C}$ is satisfiable (and the verifier receives uniform and equal κ graph states $|\Psi^{(1)}\rangle, \ldots, |\Psi^{(\kappa)}\rangle$ with a satisfying coloring), then completeness would be only $1 - e^{-\Theta(\kappa)}$ (due to the imperfect completeness of the conditional uniformity test). Thus, we are forced to take $\kappa \in \Omega(\log N)$ in order for there to be any inverse-polynomial soundness gap. (In other words, the protocol of [CD10] has no soundness gap in the "constant regime" $\kappa \in O(1)$; to breach the constant regime, it seems that one would have to strengthen the verifier with additional LOCC measurements to increase the soundness gap, or, at the very least, to endow the protocol with perfect completeness.)

We now proceed to the proof of Claim 1.5, which follows closely the proof of Chen and Drucker [CD10]. Throughout, we use notation for graph states, which was introduced in Section 4.

Observe that the completeness in Claim 1.5 follows exactly as in the analysis of Chen and Drucker. Thus, it remains to examine the soundness. Chen and Drucker [CD10, Lemma 3] gave sufficient conditions for an arbitrary graph state $|\Psi\rangle$ to be accepted by the uniformity test $\textsc{Unif}(|\Psi\rangle)$ with constant probability. We first show how to use the generic lemmas of Section 4 to prove the same result (and these same lemmas are used with very different parameters in our soundness analysis of the protocol of Blier and Tapp [BT09] in Section 6).

Lemma 5.1. *Fix $\varepsilon \in [0, 1]$. If $p_0(|\Psi\rangle) \geq \frac{1}{4K}$ and $\left|R_{\frac{1}{8KN}}(|\Psi\rangle)\right| \geq \varepsilon N$, then $\mathsf{REJ}\big(\textsc{Unif}(|\Psi\rangle)\big) \leq 1 - \frac{\varepsilon^2}{16}$.*

Proof. For each $v \in R_{\frac{1}{8KN}}\big(|\Psi\rangle\big)$, by invoking Lemma 4.1 with j, v, $c_1 = 4K$, and $c_2 = 8K$, we get that $|\gamma_v(j)|^2 < \frac{1}{2N}$. In particular, we deduce that

$$\sum_{w=0}^{N-1} \left| |\gamma_w|^2 - \frac{1}{N} \right| \geq \sum_{w \in R_{\frac{1}{8KN}}(|\Psi\rangle)} \left| |\gamma_w|^2 - \frac{1}{N} \right| \geq \left| R_{\frac{1}{8KN}}(|\Psi\rangle) \right| \cdot \frac{1}{2N} \geq \varepsilon N \cdot \frac{1}{2N} = \frac{\varepsilon}{2} \ .$$

Next, by invoking Lemma 4.2 with $|\gamma\rangle = |\gamma(j)\rangle$, we get that the probability of measuring v in the (only) register of $F_N|\gamma(j)\rangle$ is at most

$$1 - \frac{1}{4}\left(\sum_{w=0}^{N-1}\left||\gamma_w|^2 - \frac{1}{N}\right|\right)^2 .$$

We deduce that the probability of measuring v in the (only) register of $F_N|\gamma(j)\rangle$ is at most $1 - \frac{\varepsilon^2}{16}$, as desired. □

After establishing results of the above form, Chen and Drucker setup the hypothesis for the following lemma, which is analogous to their Lemma 4. We only repeat the hypothesis, and give our improvements. See [CD10] for how this fits into their overall proof strategy.

Lemma 5.2 (modified [CD10, Lemma 4]). *Let $G = (V, E)$ be a d-regular graph (possibly with self-loops) with N vertices, M edges, and $d > 1$. Let $\mathcal{C} = (G, \{R_e\}_e)$ be a 2CSP on the graph G with color alphabet Σ, and suppose that $\mathcal{C}$ is $(1-\eta)$-unsatisfiable. Let $D_1, \ldots, D_\kappa$ be independent distributions on $V \times \Sigma$, where (v_i, c_i) denotes the output of D_i.*

Suppose that for each $i \in \{1, \ldots, \kappa\}$ there exists $S_i \subseteq V$ with $|S_i| \geq (1-\varepsilon)N$ such that v_i is uniformly distributed over S_i, and $\varepsilon < \eta/20$. Then, there is a probability of at most $1 - \Omega_{\varepsilon,d}(\frac{\kappa^2}{N+\kappa^2})$ such that: either $e = (v_i, v_j)$ is an edge of G and $R_e(c_i, c_j) = 0$, or $v_i = v_j$ and $c_i \neq c_j$.

Proof. We follow the proof of Chen and Drucker [CD10]. For $i, j \in \{1, \ldots, \kappa\}$, define $V_{i,j}$ to be an indicator for the event that $e = (v_i, v_j)$ is an edge of G and either $R_e(c_i, c_j) = 0$, or $v_i = v_j$ and $c_i \neq c_j$. Denote $V = \sum_{i=1}^{\kappa-1}\sum_{j=i+1}^{\kappa} V_{i,j}$. Observe that the result follows from bounding $\Pr[V = 0]$. To bound this probability, we use Cantelli's inequality (also known as the one-sided Chebyschev inequality, cf [Ros84]): for a random variable X and $a > 0$, $\Pr[X \leq \mathbb{E}[X] - a] \leq \frac{\mathrm{Var}(X)}{\mathrm{Var}(X)+a^2}$. Thus, taking $X = V$ and $a = \mathbb{E}(V)$, and using the fact that V is a non-negative random variable, we have

$$\Pr[V = 0] \leq \frac{\mathrm{Var}(V)}{\mathrm{Var}(V) + \mathbb{E}[V]^2} = 1 - \frac{1}{\frac{\mathrm{Var}(V)}{\mathbb{E}[V]^2} + 1} .$$

The result will then follow from an upper bound on $\mathrm{Var}(V)$ and a lower bound on $\mathbb{E}[V]^2$.

We now invoke the following facts from the analysis of [CD10]:

(i) $\mathbb{E}[V_{i,j}] \geq \varepsilon/N$, and

(ii) $\mathrm{Var}(V) = O_{\varepsilon,d}(\kappa^2/N + \kappa^3/N^2)$.

Hence, the upper bound for $\mathrm{Var}(V)$ is already given. As for the lower bound on $\mathbb{E}[V]^2$: by linearity of expectation and (i) above, we see that $\mathbb{E}[V] = \binom{\kappa}{2}\mathbb{E}[V_{i,j}] = \Omega_\varepsilon(\kappa^2/N)$; thus, $\mathbb{E}[V]^2 \geq \Omega_\varepsilon(\kappa^4/N^2)$. Therefore,

$$\frac{\mathrm{Var}(V)}{\mathbb{E}[V]^2} \leq O_{\varepsilon,d}\left(\frac{\kappa^2/N + \kappa^3/N^2}{\kappa^4/N^2}\right) \leq O_{\varepsilon,d}\left(\frac{N+\kappa}{\kappa^2}\right) .$$

Combining with the above, we conclude that

$$\Pr\left[V = 0\right] \leq 1 - \frac{1}{\frac{\mathrm{Var}(V)}{\mathbb{E}[V]^2} + 1} \leq 1 - \frac{1}{O_{\varepsilon,d}\left(\frac{N+\kappa}{\kappa^2}\right) + 1} \leq 1 - \Omega_{\varepsilon,d}\left(\frac{\kappa^2}{N+\kappa^2}\right) ,$$

where the big-O and big-Ω notation hide constants depending on ε and d. □

6 An Improvement on the Soundness Analysis of [BT09]

In this section, we give the details for our tight soundness analysis of the two-prover QMA protocol of Blier and Tapp [BT09]. Specifically, we prove:

Claim (1.7, restated)**.** *The two-prover* QMA *protocol for* $\mathsf{2CSP}(N, M, K)$ *given in Algorithm 2 has (perfect completeness and) soundness* $1 - \Omega(N^{-2})$*, assuming* $K \in O(1)$*. Moreover, the analysis of the soundness of the protocol cannot be improved, in the sense of Remark 3.*

The claim improves the status quo for two-prover QMA protocols with polylogarithmic proof length in three ways:

(i) Previously, the best known soundness gap was $\Omega(N^{-3-\varepsilon})$, for every $\varepsilon > 0$, proved by Beigi [Bei10];

(ii) The result of Beigi [Bei10] did not enjoy perfect completeness; and

(iii) Our result does not exploit the power of PCPs, unlike the result of Beigi [Bei10].[7]

Algorithm 2: Verifier of [BT09]

---

inputs: a $\mathsf{2CSP}(N, M, K)$ instance $\mathcal{C} = (G, \{R_e\}_{e\in E})$

proofs: two unentangled graph states $|\Psi^{(1)}\rangle$ and $|\Psi^{(2)}\rangle$

verifier: draw $r \in \{1, 2, 3\}$ at random, and perform the r-th test below:

1. $\textsc{Swap}\big(|\Psi^{(1)}\rangle, |\Psi^{(2)}\rangle\big)$
2. $\textsc{Cons}_{\mathcal{C}}\big(|\Psi^{(1)}\rangle, |\Psi^{(2)}\rangle\big)$
3. $\textsc{Unif}\big(|\Psi^{(1)}\rangle\big) \wedge \textsc{Unif}\big(|\Psi^{(2)}\rangle\big)$

Remark 3 ("Tightness" of Our Analysis)**.** Consider a $\mathsf{2CSP}(N, M, K)$ instance $\mathcal{C} = (G, \{R_e\}_{e\in E})$; suppose that $\mathcal{C}$ is *not* satisfiable, and suppose further that there exists a coloring of the vertices $C \colon V \to \Sigma$ for which there exists exactly one edge $(\tilde{v}, \tilde{w}) \in E$ such that $R_{(\tilde{v},\tilde{w})}(C(\tilde{v}), C(\tilde{w})) = 0$.[8]

Now suppose that the two graph states $|\Psi^{(1)}\rangle$ and $|\Psi^{(2)}\rangle$ given to the verifier are equal and that they indeed are a uniform superposition of all vertices, colored with C. If so, both the first test (i.e., the swap test) and the third test (i.e., the two uniformity tests) accept with probability 1; however, the second test (i.e., the consistency test) accepts with probability that is exactly $1 - N^{-2}$.

In other words, our analysis is "tight" in the sense that the assumptions we made could indeed really be the case, thus implying that one cannot hope to exhibit an even better soundness analysis that proves a soundness of $1 - \omega(N^{-2})$.

We now proceed to the proof of Claim 1.7, which we tackle in several lemmas, whose overall structure follows the approach taken by [BT09]. Throughout, we use notation for graph states introduced in Section 4. Also, given a $\mathsf{2CSP}$ instance $\mathcal{C}$, $\textsc{ColCons}_{\mathcal{C}}\big(|\Psi^{(1)}\rangle, |\Psi^{(2)}\rangle\big)$ denotes only the color consistency subtest of the test $\textsc{Cons}_{\mathcal{C}}\big(|\Psi^{(1)}\rangle, |\Psi^{(2)}\rangle\big)$ and $\textsc{EdgeCons}_{\mathcal{C}}\big(|\Psi^{(1)}\rangle, |\Psi^{(2)}\rangle\big)$ denotes only the edge consistency subtest of the test $\textsc{Cons}_{\mathcal{C}}\big(|\Psi^{(1)}\rangle, |\Psi^{(2)}\rangle\big)$.

First, we show that, as long as two graph states $|\Psi^{(1)}\rangle$ and $|\Psi^{(2)}\rangle$ are "close enough" and the colors of the vertices are "consistent enough", then a definite color can be chosen for vertices with

[7] And, unlike the results of [ABD+09] and [CD10].

[8] At most a constant number of unsatisfiable edges would also suffice.

large enough amplitude. (Indeed, if vertices with large enough amplitude were to be colored very inconsistently, then we would be able to catch them, through the second test.)

Lemma 6.1 (modified [BT09, Lemma 3.4])**.** *Fix any* 2CSP *instance* $\mathcal{C}$*. Define*

$$\delta = \frac{1}{2 \cdot 1600^2 K^4 N^2} \quad \textit{and} \quad \mu = \frac{1}{1600^2 K^4 N^2} \ .$$

Suppose that:

(i) $\mathsf{REJ}\big(\textsc{Swap}\big(|\Psi^{(1)}\rangle, |\Psi^{(2)}\rangle\big)\big) \leq \delta$*, and*

(ii) $\mathsf{REJ}\big(\textsc{ColCons}_{\mathcal{C}}\big(|\Psi^{(1)}\rangle, |\Psi^{(2)}\rangle\big)\big) \leq \mu$*.*

Then, for every vertex $v \in S_{\frac{1}{8N}}\big(|\Psi^{(1)}\rangle\big)$*, there exists a (unique)* $j \in \{0, \ldots, K-1\}$ *such that* $|\beta^{(1)}_{v,j}|^2 \geq \frac{100K-1}{100K}$*. (And, similarly, for every vertex* $v \in S_{\frac{1}{8N}}\big(|\Psi^{(2)}\rangle\big)$*, there exists a (unique)* $j \in \{0, \ldots, K-1\}$ *such that* $|\beta^{(2)}_{v,j}|^2 \geq \frac{100K-1}{100K}$*.)*

Proof. First, if such a j exists, it is unique, because $\frac{100K-1}{100K} > \frac{1}{2}$. Next suppose for the sake of contradiction that there exists some vertex $\tilde{v} \in S_{\frac{1}{8N}}\big(|\Psi^{(1)}\rangle\big)$ for which there is no such j, so that there exist distinct $j_1, j_2 \in \{0, \ldots, K-1\}$ such that $|\beta^{(1)}_{\tilde{v},j_1}|^2, |\beta^{(1)}_{\tilde{v},j_2}|^2 > \frac{1}{100K^2}$.[9] Then, the probability that the color-consistency test rejects the two graph states $|\Psi^{(1)}\rangle$ and $|\Psi^{(2)}\rangle$, is

$$\begin{aligned}
&\sum_{v=0}^{N-1} \sum_{j=0}^{K-1} \sum_{j' \neq j} \left|\alpha^{(1)}_v \beta^{(1)}_{v,j}\right|^2 \cdot \left|\alpha^{(2)}_v \beta^{(2)}_{v,j'}\right|^2 \\
&\geq \sum_{v=0}^{N-1} \sum_{j=0}^{K-1} \sum_{j' \neq j} \left|\alpha^{(1)}_v \beta^{(1)}_{v,j}\right|^2 \cdot \left(\left|\alpha^{(1)}_v \beta^{(1)}_{v,j'}\right|^2 - \sqrt{2\delta}\right) \qquad \text{(by Lemma 2.1)} \\
&\geq \sum_{v \in S_{\frac{1}{8N}}(|\Psi^{(1)}\rangle)} \sum_{j=0}^{K-1} \sum_{j' \neq j} \frac{\left|\beta^{(1)}_{v,j}\right|^2}{8N} \cdot \left(\frac{\left|\beta^{(1)}_{v,j'}\right|^2}{8N} - \sqrt{2\delta}\right) \\
&\geq \sum_{j=0}^{K-1} \sum_{j' \neq j} \frac{\left|\beta^{(1)}_{\tilde{v},j}\right|^2}{8N} \cdot \left(\frac{\left|\beta^{(1)}_{\tilde{v},j'}\right|^2}{8N} - \sqrt{2\delta}\right) \\
&\geq \frac{\left|\beta^{(1)}_{\tilde{v},j_1}\right|^2}{8N} \cdot \left(\frac{\left|\beta^{(1)}_{\tilde{v},j_2}\right|^2}{8N} - \sqrt{2\delta}\right) \\
&> \frac{1}{800K^2N} \cdot \left(\frac{1}{800K^2N} - \sqrt{2\delta}\right) \\
&\geq \frac{1}{800K^2N} \cdot \left(\frac{1}{800K^2N} - \sqrt{2 \cdot \frac{1}{2 \cdot 1600^2 K^4 N^2}}\right) \\
&\geq \frac{1}{1600^2 K^4 N^2} \ ,
\end{aligned}$$

[9] Indeed, from $|\beta^{(1)}_{\tilde{v},0}|^2, \ldots, |\beta^{(1)}_{\tilde{v},K-1}|^2 < \frac{100K-1}{100K}$ and $\sum_{j=0}^{K-1} |\beta^{(1)}_{\tilde{v},j}|^2 = 1$, we deduce that there exists some $j_1 \in \{0, \ldots, K-1\}$ such that $|\beta^{(1)}_{\tilde{v},j_1}|^2 \geq \frac{1}{K}$ and, from $|\beta^{(1)}_{\tilde{v},0}|^2, \ldots, |\beta^{(1)}_{\tilde{v},K-1}|^2 < \frac{100K-1}{100K}$ and $\sum_{j \neq j_1} |\beta^{(1)}_{\tilde{v},j}|^2 > \frac{1}{100K}$, we deduce that there exists some $j_2 \in \{0, \ldots, K-1\} - \{j_1\}$ such that $|\beta^{(1)}_{\tilde{v},j_2}|^2 \geq \frac{1}{100K(K-1)} > \frac{1}{100K^2}$. Overall, $|\beta^{(1)}_{\tilde{v},j_1}|^2, |\beta^{(1)}_{\tilde{v},j_2}|^2 > \frac{1}{100K^2}$.

which contradicts the assumption that $\mathsf{REJ}\big(\textsc{ColCons}_{\mathcal{C}}\big(|\Psi^{(1)}\rangle, |\Psi^{(2)}\rangle\big)\big) \leq \mu$. An analogous argument holds for $|\Psi^{(2)}\rangle$. $\square$

Next, we show that, under the same assumptions as Lemma 6.1, the probability of measuring j in the color register of $(I_N \otimes F_K)|\Psi^{(1)}\rangle$ is at least $\frac{1}{4K}$ for every color $j \in \{0, \ldots, K-1\}$.

Lemma 6.2 (modified [BT09, Lemma 3.5])**.** *Fix any* 2CSP *instance* $\mathcal{C}$*. Define*

$$\delta = \frac{1}{2 \cdot 1600^2 K^4 N^2} \quad \text{and} \quad \mu = \frac{1}{1600^2 K^4 N^2} \ .$$

Suppose that:

(i) $\mathsf{REJ}\big(\textsc{Swap}\big(|\Psi^{(1)}\rangle, |\Psi^{(2)}\rangle\big)\big) \leq \delta$*, and*

(ii) $\mathsf{REJ}\big(\textsc{ColCons}_{\mathcal{C}}\big(|\Psi^{(1)}\rangle, |\Psi^{(2)}\rangle\big)\big) \leq \mu$*.*

Then, $p_j\big(|\Psi^{(1)}\rangle\big) \geq \frac{1}{4K}$ *for every* $j \in \{0, \ldots, K-1\}$*. (And, similarly,* $p_j\big(|\Psi^{(2)}\rangle\big) \geq \frac{1}{4K}$ *for every* $j \in \{0, \ldots, K-1\}$*.)*

Proof. Suppose that the vertex register of the graph state $|\Psi^{(1)}\rangle$ is measured and that the outcome is some vertex $v \in \{0, \ldots, N-1\}$. If $v \in S_{\frac{1}{8N}}\big(|\Psi^{(1)}\rangle\big)$, from Lemma 6.1 we deduce that there exists a (unique) color $\tilde{j} \in \{0, \ldots, K-1\}$ such that $|\beta^{(1)}_{v,\tilde{j}}|^2 \geq \frac{100K-1}{100K}$; in particular, we also deduce that $\sum_{j \neq \tilde{j}} |\beta^{(1)}_{v,j}|^2 < \frac{1}{100K}$. Therefore, (conditioned on getting outcome v in the vertex register) the probability of measuring j in the color register of $(I_N \otimes F_K)|\Psi^{(1)}\rangle$ is

$$\begin{aligned}
&\frac{1}{K}\left|\sum_{j=1}^{K-1} \beta^{(1)}_{v,j} e^{\frac{2\pi\sqrt{-1}jv}{K}}\right|^2 \\
&\geq \frac{1}{K}\left|\left|\beta^{(1)}_{v,\tilde{j}} e^{\frac{2\pi\sqrt{-1}jv}{K}}\right| - \left|\sum_{j\neq\tilde{j}} \beta^{(1)}_{v,j} e^{\frac{2\pi\sqrt{-1}jv}{K}}\right|\right|^2 \\
&\geq \frac{1}{K}\left|\left|\beta^{(1)}_{v,\tilde{j}} e^{\frac{2\pi\sqrt{-1}jv}{K}}\right| - \sqrt{K\sum_{j\neq\tilde{j}} \left|\beta^{(1)}_{v,j} e^{\frac{2\pi\sqrt{-1}jv}{K}}\right|^2}\right|^2 && \text{(by Cauchy-Schwarz)} \\
&= \frac{1}{K}\left|\left|\beta^{(1)}_{v,\tilde{j}}\right| - \sqrt{K\sum_{j\neq\tilde{j}} \left|\beta^{(1)}_{v,j}\right|^2}\right|^2 \\
&\geq \frac{1}{K}\left|\sqrt{\frac{100K-1}{100K}} - \sqrt{K\frac{1}{100K}}\right|^2 \\
&\geq \frac{1}{K}\left(1 - \frac{1}{100K} + \frac{1}{100} - \frac{1}{5}\cdot\frac{100K-1}{100K}\right) \\
&= \frac{4}{5K} \ .
\end{aligned}$$

Now observe that $S_{\frac{1}{8N}}\big(|\Psi^{(1)}\rangle\big)$ cannot be empty, for otherwise $\sum_{v=0}^{N-1} |\alpha^{(1)}_v|^2 < N \cdot \frac{1}{8N} < 1$. Hence, there is at least one vertex $\tilde{v}$ in $S_{\frac{1}{8N}}(|\Psi^{(1)}\rangle)$. Thus, the probability of measuring j (with no conditioning) in the color register of $(I_N \otimes F_K)|\Psi^{(1)}\rangle$ is

$$
\begin{aligned}
p_j\big(|\Psi^{(1)}\rangle\big) &= \sum_{v=0}^{N-1} \left|\alpha_v^{(1)}\right|^2 \frac{1}{K} \left|\sum_{j=1}^{K-1} \beta_{v,j}^{(1)} e^{\frac{2\pi\sqrt{-1}jv}{K}}\right|^2 \\
&\geq \sum_{v\in S_{\frac{1}{8N}}(|\Psi^{(1)}\rangle)} \left|\alpha_v^{(1)}\right|^2 \frac{1}{K} \left|\sum_{j=1}^{K-1} \beta_{v,j}^{(1)} e^{\frac{2\pi\sqrt{-1}jv}{K}}\right|^2 \\
&\geq \frac{4}{5K} \sum_{v\in S_{\frac{1}{8N}}(|\Psi^{(1)}\rangle)} \left|\alpha_v^{(1)}\right|^2 \\
&\geq \frac{4}{5K}\left(1-(N-1)\cdot\frac{1}{8N}\right) \\
&\geq \frac{4}{5K}\cdot\frac{7}{8} \\
&\geq \frac{1}{4K} \quad ,
\end{aligned}
$$

as desired. An analogous argument holds for $|\Psi^{(2)}\rangle$. □

Next we prove that, under the same assumptions of Lemma 6.1 and Lemma 6.2, if we further require that the uniform test does not reject with high probability, then we can be sure that all the vertices have a somewhat large amplitude.

Lemma 6.3 (modified [BT09, Lemma 3.7]). *Fix any* 2CSP *instance* $\mathcal{C}$. *Define*

$$
\delta = \frac{1}{2\cdot 1600^2K^4N^2} \quad \text{and} \quad \mu = \frac{1}{1600^2K^4N^2} \quad \text{and} \quad \nu = \frac{1}{64KN^2} \quad .
$$

Suppose that:

(i) $\mathsf{REJ}\big(\textsc{Swap}\big(|\Psi^{(1)}\rangle, |\Psi^{(2)}\rangle\big)\big) \leq \delta$,

(ii) $\mathsf{REJ}\big(\textsc{ColCons}_{\mathcal{C}}\big(|\Psi^{(1)}\rangle, |\Psi^{(2)}\rangle\big)\big) \leq \mu$, *and*

(iii) $\mathsf{REJ}\big(\textsc{Unif}\big(|\Psi^{(1)}\rangle\big)\big) \leq \nu$.

Then, $V(G) = S_{\frac{1}{8KN}}\big(|\Psi^{(1)}\rangle\big)$. *(And, similarly,* $V(G) = S_{\frac{1}{8KN}}\big(|\Psi^{(2)}\rangle\big)$ *under the alternative assumption* $\mathsf{REJ}\big(\textsc{Unif}\big(|\Psi^{(2)}\rangle\big)\big) \leq \nu$ *instead.)*

Proof. Recall that:

- $p_j\big(|\Psi^{(1)}\rangle\big)$ is the probability of measuring j in the color register of $(I_N \otimes F_K)|\Psi^{(1)}\rangle$, and
- $|\gamma(j)^{(1)}\rangle = \sum_{v=0}^{N-1} \gamma_v(j)^{(1)}|v\rangle$ is the reduced quantum state obtained when we measure j in the color register of $(I_N \otimes F_K)|\Psi^{(1)}\rangle$.

By invoking Lemma 4.2 with $|\gamma\rangle = |\gamma(j)^{(1)}\rangle$, the probability of measuring v in the vertex register of $F_N|\gamma(j)^{(1)}\rangle$ is at most

$$
1 - \frac{1}{4}\left(\sum_{w=0}^{N-1}\left|\left|\gamma_w(j)^{(1)}\right|^2 - \frac{1}{N}\right|\right)^2 \quad .
$$

Also, by Lemma 6.2, $p_j\big(|\Psi^{(1)}\rangle\big) \geq \frac{1}{4K}$ for every $j \in \{0, \ldots, K-1\}$.

Suppose now by way of contradiction that there exists some vertex $\tilde{v} \in R_{\frac{1}{8KN}}\big(|\Psi^{(1)}\rangle\big)$, so that $|\alpha_v^{(1)}|^2 < \frac{1}{8KN}$. We can now invoke Lemma 4.1 with $c_1 = 4K$ and $c_2 = 8K$ to get that $|\gamma_{\tilde{v}}(j)^{(1)}|^2 < \frac{1}{2N}$. Therefore,

$$\sum_{w=0}^{N-1} \left| \left|\gamma_w(j)^{(1)}\right|^2 - \frac{1}{N} \right| \geq \left| \left|\gamma_{\tilde{v}}(j)^{(1)}\right|^2 - \frac{1}{N} \right| > \frac{1}{2N} \ ,$$

and we obtain that the probability of measuring v in the vertex register of $F_N|\gamma(j)^{(1)}\rangle$ is less than $1 - \frac{1}{16N^2}$. Thus, the probability of measuring j in the color register but not measuring v in the vertex register of $(F_N \otimes F_K)|\Psi^{(1)}\rangle$ is greater than

$$\frac{1}{4K} \cdot \frac{1}{16N^2} = \frac{1}{64KN^2} = \nu \ .$$

Taking $j = 0$ and $v = 0$, this contradicts the assumption that $\mathsf{REJ}\big(\textsc{Unif}\big(|\Psi^{(1)}\rangle\big)\big) \leq \nu$. An analogous argument holds for $|\Psi^{(2)}\rangle$. ☐

Finally, we can now lower bound the soundness of the protocol:

Lemma 6.4. *Define*

$$\delta = \frac{1}{2 \cdot 1600^2 K^4 N^2} \quad \textit{and} \quad \mu = \frac{1}{1600^2 K^4 N^2} \quad \textit{and} \quad \nu = \frac{1}{64KN^2} \quad \textit{and} \quad \xi = \frac{(100K-1)^2}{2 \cdot 800^2 K^4 N^2} \ .$$

and

$$s = \frac{1}{3} \min\left\{\delta\,,\, \mu\,,\, \nu\,,\, \xi\right\} \ .$$

Then the overall probability of rejecting an unsatisfiable graph G is greater than s.

Proof. If any of

(i) $\mathsf{REJ}\big(\textsc{Swap}\big(|\Psi^{(1)}\rangle, |\Psi^{(2)}\rangle\big)\big) \leq \delta$,

(ii) $\mathsf{REJ}\big(\textsc{ColCons}_{\mathcal{C}}\big(|\Psi^{(1)}\rangle, |\Psi^{(2)}\rangle\big)\big) \leq \mu$, and

(iii) $\mathsf{REJ}\big(\textsc{Unif}\big(|\Psi^{(1)}\rangle\big)\big) \leq \nu$ and $\mathsf{REJ}\big(\textsc{Unif}\big(|\Psi^{(2)}\rangle\big)\big) \leq \nu$

does not hold, then we are done. So suppose that (i)–(iii) hold. Define a coloring $C\colon V(G) \to \Sigma$ of the graph G by the rule

$$C(v) := \arg \max_{j \in \{0,\ldots,K-1\}} \left|\beta_{v,j}^{(1)}\right|^2 \ ,$$

for every vertex v. By Lemma 6.1, the coloring C is well-defined (i.e., is unique).

Let $U(G) \subseteq E(G)$ be the set of unsatisfied edges in G by the coloring C. Since G is unsatisfiable, $|U(G)| \geq 1$. Therefore, $\mathsf{REJ}\big(\textsc{EdgeCons}_{\mathcal{C}}\big(|\Psi^{(1)}\rangle, |\Psi^{(2)}\rangle\big)\big)$, which is the probability that the edge-consistency subtest rejects $|\Psi^{(1)}\rangle$ and $|\Psi^{(2)}\rangle$, is

$$\begin{aligned}
&\sum_{(v,w)\in U(G)} \left|\alpha_v^{(1)}\beta_{v,C(v)}^{(1)}\right|^2 \cdot \left|\alpha_w^{(2)}\beta_{w,C(w)}^{(2)}\right|^2 \\
&\geq \sum_{(v,w)\in U(G)} \left(\frac{1}{8KN}\cdot\frac{100K-1}{100K}\right)\cdot\left(\frac{1}{8KN}\cdot\frac{100K-1}{100K}\right) \\
&= |U(G)|\cdot\frac{(100K-1)^2}{800^2K^4N^2} \\
&\geq 1\cdot\frac{(100K-1)^2}{800^2K^4N^2} \\
&> s \ .
\end{aligned}$$

This concludes the proof of the lemma, as well as the proof of Claim 1.7. □

Acknowledgements

The authors would like to thank Scott Aaronson for his great lectures in quantum complexity theory and his suggestions while working on this note.

References

[ABD+09] Scott Aaronson, Salman Beigi, Andrew Drucker, Bill Fefferman, and Peter Shor. The power of unentanglement. *Theory of Computing*, 5(1):1–42, 2009. Earlier version appeared in CCC '08. arXiv:0804.0802v2. 2, 3, 4, 5, 6, 7, 10, 12, 13, 19

[AN02] Dorit Aharonov and Tomer Naveh. Quantum NP - a survey. Technical Report quant-ph/0210077, October 2002. arXiv:quant-ph/0210077v1. 2

[BaCJ10] Fernando Brandão, Matthias Christiandl, and Yard Jon. Faithful squashed entanglement. *ArXiv e-prints*, October 2010. arXiv:1010.1750v1. 2, 7

[BCWdW01] Harry Buhrman, Richard Cleve, John Watrous, and Ronald de Wolf. Quantum fingerprinting. *Physical Review Letters*, 87(16):167902, September 2001. arXiv:quant-ph/0102001v1. 9

[Bei10] Salman Beigi. NP vs. $\mathrm{QMA}_{\log}(2)$. *Quantum Information and Computation*, 54(1&2):0141–0151, 2010. arXiv:0810.5109v2. 2, 3, 4, 5, 6, 7, 10, 12, 19

[BSS08] Eli Ben-Sasson and Madhu Sudan. Short PCPs with polylog query complexity. *SIAM Journal on Computing*, 38(2):551–607, 2008. 4, 11

[BT09] Hugue Blier and Alain Tapp. All languages in NP have very short quantum proofs. In *ICQNM '09: Proceedings of the 3rd International Conference on Quantum, Nano and Micro Technologies*, pages 34–37, Los Alamitos, CA, USA, 2009. IEEE Computer Society. arXiv:0709.0738v1. Revised version: arXiv:0709.0738v2. 2, 3, 4, 5, 6, 7, 10, 12, 14, 17, 19, 20, 21, 22

[CD10] Jing Chen and Andrew Drucker. Short multi-prover quantum proofs for SAT without entangled measurements. *ArXiv e-prints*, November 2010. arXiv:1011.0716v2. 2, 3, 4, 5, 7, 10, 12, 14, 16, 17, 18, 19

[Din07] Irit Dinur. The PCP theorem by gap amplification. *Journal of the ACM*, 54, June 2007. Earlier version appeared in STOC '06. 4, 11

[GS89] Yuri Gurevich and Saharon Shelah. Nearly linear time. In Albert R. Meyer and Michael A. Taitslin, editors, *Logic at Botik'89: Symposium on Logical Foundations of Computer Science*, pages 108–118. Springer-Verlag New York, Inc., New York, NY, USA, 1989. 4, 8, 11

[HM10] Aram Harrow and Ashley Montanaro. An efficient test for product states, with applications to quantum merlin-arthur games. In *FOCS '10: Proceedings of the 51st Annual IEEE Symposium on Foundations of Computer Science*, page ???, Washington, DC, USA, 2010. IEEE Computer Society. arXiv:1001.0017v3. 2, 3, 6, 7, 10

[Kit99] Alexei Yu. Kitaev. Quantum NP. Talk at AQIP '99: Second Workshop on Algorithms in Quantum Information Processing, 1999. 2

[KMY03] Hirotada Kobayashi, Keiji Matsumoto, and Tomoyuki Yamakami. Quantum Merlin-Arthur proof systems: Are multiple Merlins more helpful to Arthur? In Toshihide Ibaraki, Naoki Katoh, and Hirotaka Ono, editors, *Algorithms and Computation*, volume 2906 of *Lecture Notes in Computer Science*, pages 189–198. Springer Berlin / Heidelberg, 2003. arXiv:quant-ph/0306051v2. 2, 7

[Kni96] Emanuel H. Knill. Quantum randomness and nondeterminism. Technical Report quant-ph/9610012, Oct 1996. arXiv:quant-ph/9610012v1. 2

[KSTW01] Sanjeev Khanna, Madhu Sudan, Luca Trevisan, and David P. Williamson. The approximability of constraint satisfaction problems. *SIAM Journal on Computing*, 30:1863–1920, December 2001. 13

[LCV07] Yi-Kai Liu, Matthias Christandl, and Frank Verstraete. Quantum computational complexity of the n-representability problem: QMA complete. *Physical Review Letters*, 98(11):110503, March 2007. arXiv:quant-ph/0609125v1. 2

[NC00] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, New York, NY, USA, 2000. 8, 9, 10

[Pap94] Christos H. Papadimitriou. *Computational Complexity*. Addison-Wesley, Reading, MA, USA, 1994. 8

[PY91] Christos H. Papadimitriou and Mihalis Yannakakis. Optimization, approximation, and complexity classes. *Journal of Computer and System Sciences*, 43(3):425–440, 1991. Earlier version appeared in STOC '88. 13

[Ros84] Sheldon Ross. *A first course in probability*. Macmillan Co., New York, second edition, 1984. 18

[Wat00] John Watrous. Succinct quantum proofs for properties of finite groups. In *FOCS '00: Proceedings of the 41st Annual IEEE Symposium on Foundations of Computer Science*, pages 537–546, Washington, DC, USA, 2000. IEEE Computer Society. arXiv:cs/0009002v1. 2

ECCC ISSN 1433-8092

http://eccc.hpi-web.de