THEORY OF COMPUTING, Volume 20 (3), 2024, pp. 1–87
www.theoryofcomputing.org

Verifier-on-a-Leash: New Schemes for Verifiable Delegated Quantum Computation, with Quasilinear Resources

Andrea Coladangelo* Alex B. Grilo† Stacey Jeffery‡
Thomas Vidick§

Received June 4, 2019; Revised February 15, 2022; Published September 3, 2024

Abstract. The problem of reliably certifying the outcome of a computation performed by a quantum device is rapidly gaining relevance. We present two protocols for a classical verifier to verifiably delegate a quantum computation to two non-communicating but entangled quantum provers, with statistical soundness. Our protocols have near-optimal complexity in terms of the total resources employed by the verifier and the honest provers, with the total number of operations of each party, including the number of entangled pairs of qubits required of the honest provers, scaling as $O(g \log g)$ for delegating a circuit of size g. This is in contrast to previous protocols, whose overhead in terms of resources employed, while polynomial, is far

A conference version of this paper appeared in the Proceedings of the 48th Ann. Internat. Conf. on Theory and Appl. of Cryptographic Techniques (EUROCRYPT 2019).

*Supported by AFOSR YIP award number FA9550-16-1-0495 and by the Simons Institute for the Theory of Computing under a Quantum Postdoctoral Fellowship.

†Part of this work was performed when AG was affiliated to IRIF, CNRS/University of Paris, where he was supported by ERC QCC and part of this work was performed when AG was affiliated to CWI and QuSoft, where we has partially supported by ERC Consolidator Grant 615307-QPROGRESS.

‡Supported by an NWO Veni Innovational Research Grant under project number 639.021.752; an NWO WISE Grant; an NWO Klein Grant under project number OCENW.KLEIN.061; and the CIFAR Quantum Information Science Program.

§Supported by NSF CAREER Grant CCF-1553477, MURI Grant FA9550-18-1-0161, AFOSR YIP award number FA9550-16-1-0495, and the IQIM, an NSF Physics Frontiers Center (NSF Grant PHY-1125565) with support of the Gordon and Betty Moore Foundation (GBMF-12500028).

 DOI: 10.4086/toc.2024.v020a003

beyond what is feasible in practice. Our first protocol requires a number of rounds that is linear in the depth of the circuit being delegated, and is blind, meaning neither prover can learn the circuit or its input. The second protocol is not blind, but requires only a constant number of rounds of interaction.

Our main technical innovation is an efficient rigidity theorem that allows a verifier to test that two entangled provers perform measurements specified by an arbitrary m-qubit tensor product of single-qubit Clifford observables on their respective halves of m shared EPR pairs, with a robustness that is independent of m. Our two-prover classical-verifier delegation protocols are obtained by combining this rigidity theorem with a single-prover quantum-verifier protocol for the verifiable delegation of a quantum computation, introduced by Broadbent (Theory of Computing, 2018).

ACM Classification: F.1.3, G.3

AMS Classification: 68Q15, 81P68

Key words and phrases: quantum computing, quantum interactive proofs, delegated computation, nonlocal games

1 Introduction

Quantum computers hold the potential to speed up a wide range of computational tasks (see, for example, [31]). Recent progress towards implementing limited quantum devices has added urgency to the already important question of how a classical verifier can test a quantum device. This verifier could be an experimentalist running a new experimental setup; a consumer who has purchased a purported quantum device; or a client who wishes to delegate some task to a quantum server. In all cases, the user would like to exert some form of control over the quantum device. For example, the experimentalist may think that she is testing that a particular experiment prepares a certain quantum state by performing a series of measurements, i. e., by state tomography, but this assumes some level of trust in the measurement apparatus being used. For a classical party to truly test a quantum system, that system should be modeled in a device-independent way, having classical inputs (e. g., measurement settings) and classical outputs (e. g., measurement results).

Tests of quantum mechanical properties of a system first appeared in the form of Bell tests [4, 10]. In a Bell test, a verifier asks classical questions to a quantum-device and receives classical answers. These tests make one crucial assumption on the system to be tested: that it consists of two spatially isolated components that are unable to communicate throughout the experiment. One can then upper bound the value of some statistical quantity of interest subject to the constraint that the two devices do not share any entanglement. Such a bound is referred to as a Bell inequality. While the violation of a Bell inequality can be seen as a certificate of entanglement, the area of self-testing, first introduced in [27], allows for the certification of much stronger statements, including which measurements are being performed, and on which state. Informally, a *robust rigidity theorem* is a statement about which kind of apparatus, quantum state and measurements, must be used by a pair of isolated devices in order to succeed in a given statistical test. Following a well-established tradition, we will refer to such tests as *games*, call the devices *players* (or *provers*), and the quantum state and measurements that they implement the *strategy* of the players. A rigidity theorem is a statement about the necessary structure of near-optimal strategies for a game.

In 2012, Reichardt, Unger and Vazirani proved a robust rigidity theorem for playing a sequence of n CHSH games [37]. Aside from its intrinsic interest, this rigidity theorem had two important consequences. One was the first device-independent protocol for quantum key distribution. The second was a protocol whereby a completely classical verifier can test a universal quantum computer consisting of two non-communicating devices. The resulting protocol for delegating quantum computations has received a lot of attention as the first classical-verifier delegation protocol. The task is well-motivated: for the foreseeable future, making use of a quantum computer will likely require delegating the computation to a potentially untrusted cloud service, such as that provided by IBM [8].

Unfortunately, the complexity overhead of the delegation protocol from [37], in terms of both the number of EPR pairs needed for the provers and the overall time complexity of the provers as well as the (classical) verifier, while polynomial, is prohibitively large. Although the authors of [37] do not provide an explicit value for the exponent, in [20] it is estimated that their protocol requires resources that scale like $\Omega(g^{8192})$, where g is the number of gates in the delegated circuit (notwithstanding the implicit constant, this already makes the approach thoroughly impractical for even a 2-gate circuit!). The large overhead is in part due to a very small (although still inverse polynomial) gap between the completeness and soundness parameters of the rigidity theorem; this requires the verifier to perform many more Bell tests than the actual number of EPR pairs needed to implement the computation, which would scale linearly with the circuit size.

Subsequent work has presented significantly more efficient protocols for achieving the same, or similar, functionality [28, 17, 20]. We refer to Table 1 for a summary of estimated lower bounds on the complexity of each of these results (these estimates were computed in [20]). Prior to our work, the best two-prover delegation protocol required resources scaling like g^{2048} for delegating a g-gate circuit. Things improve significantly if we allow for more than two provers, however, the most efficient multi-prover delegation protocols still required resources that scale as at least $\Omega(g^4 \log g)$ for delegating a g-gate circuit on n qubits. Since we expect that in the foreseeable future most quantum computations will be delegated to a third-party server, even such small polynomial overhead is unacceptable, as it already negates the quantum advantage for a number of problems, such as quantum search.

The most efficient classical-verifier delegation protocols known [13, 14, 35], with poly(n) and 7 provers, respectively, require resources that scale as $O(g^3)$, but this efficiency comes at the cost of a technique of “post-hoc” verification. In this technique, the provers must learn the verifier’s input even before they are separated, so that they can prepare the history state for the computation.[1] As a result, these protocols are not blind[2]. Other articles such as [21],

[1]Using results of Ji [24], this allows the protocol to be single-round. Alternatively, the state can be created by a single prover and teleported to the others with the help of the verifier, resulting in a two-round protocol.

[2]*Blindness* is a property of delegation protocols, which informally states that the prover learns nothing about the verifier’s private circuit.

	Provers	Rounds	Total Resources	Blind
RUV 2012 [37]	2	poly(n)	$\geq g^{8192}$	yes
McKague 2013 [28]	poly(n)	poly(n)	$\geq 2^{153} g^{22}$	yes
GKW 2015 [17]	2	poly(n)	$\geq g^{2048}$	yes
HPDF 2015 [20]	poly(n)	poly(n)	$\Theta(g^4 \log g)$	yes
Verifier-on-a-Leash Protocol (Section 4)	2	O(depth)	$\Theta(g \log g)$	yes
Dog-Walker Protocol (Section 5)	2	$O(1)$	$\Theta(g \log g)$	no

Table 1: Resource requirements of various delegation protocols in the multi-prover model. We use n to denote the number of qubits and g the number of gates in the delegated circuit. "depth" refers to the depth of the delegated circuit. "Total Resources" refers to the gate complexity of the provers, the number of EPR pairs of entanglement needed, and the number of bits of communication in the protocol. To ensure fair comparison, each protocol is required to produce the correct answer with probability 99%. For all protocols except our two new protocols, this requires a polynomial number of sequential repetitions, which is taken into account when computing the total resources.

achieve two-prover verifiable delegation with complexity that scales like $O(g^4 \log g)$, but in much weaker models; for example, in [21] the provers' private system is assumed a priori to be in tensor product form, with well-defined registers. General techniques are available to remove the strong assumption, but they would lead to similar large overhead as previous results.

In contrast, in the setting where the verifier is allowed to have some limited quantum power, such as the ability to generate single-qubit states and measure them with observables from a small finite set, efficient schemes for blind verifiable delegation do exist [2, 15, 32, 7, 22, 33, 14, 16, 34] (see also [12] for a recent survey). In this case, only a single prover is needed, and the most efficient *single-prover quantum-verifier* protocols can evaluate a quantum circuit with g gates with resources scaling as $O(g)$ (e. g., [7]). The main reason these protocols are much more efficient than the classical-verifier multi-prover protocols is that they avoid the need for directly testing any of the qubits used by the prover, instead requiring the trusted verifier to directly either prepare or measure the qubits used for the computation.

Recently, another model has been considered where the classical verifier delegates her quantum computation to a single quantum prover [25, 18]. The protocols proposed in this setting are *computationally secure*, i. e., the security of the protocol rests on the assumption that the prover cannot solve an (expected to be) hard problem for quantum computers (specifically, the Learning with Errors problem).

New delegation protocols. In this article, we propose verifiable two-prover delegation protocols that overcome the prohibitively large resource requirements of all previous multi-prover protocols. We describe two new two-prover classical-verifier protocols in which the complexity (in terms of number or EPR pairs used and time) of verifiably delegating a g-gate quantum circuit solving a BQP problem scales as $O(g \log g)$.[3]

We achieve our protocols by adapting the efficient single-prover quantum-verifier delegation protocol introduced by Broadbent [7] (we refer to this as the "EPR protocol"), which has the advantage of offering a direct implementation of the delegated circuit, in the circuit model of computation and with very little modification needed to ensure verifiability, as well as an elegantly simple and intuitive analysis.

Our first protocol is blind, and requires a number of rounds of interaction that scales linearly with the depth of the circuit being delegated. The second protocol is not blind, but only requires a constant number of rounds of interaction with the provers. Our result is the first multi-prover delegation protocol to require only a quasilinear amount of resources, in terms of number of EPR pairs and time. However, notwithstanding our improvements, a physical implementation of verifiable delegation protocols remains a challenging task for the available technology.

The idea at the heart of our protocols is that they provide methods to delegate the quantum computation performed by the quantum verifier in Broadbent's EPR protocol [7] to one of the two provers (call him PV for Prover V). This is achieved via new robust rigidity tests which are used to certify that the two provers share many EPR pairs, and indeed PV performs the same actions as the honest verifier on her half EPR pairs. These actions are sequences of single-qubit measurements of Clifford observables from the set $\Sigma = \{X, Y, Z, F, G\}$ (where F and G are defined in (2.2)). The other prover (which we call PP for Prover P) is then asked to play the role of Broadbent's prover. Soundness of our two-prover protocols is then the result of soundness of Broadbent's EPR protocol, together with our rigidity results. [4]

New rigidity results. We overcome existing efficiency limitations by introducing a new robust rigidity theorem. Our theorem allows a classical verifier to certify that two non-communicating provers apply a measurement associated with an arbitrary m-qubit tensor product of single-qubit Clifford observables on their respective halves of m shared EPR pairs. This is the first result to achieve self-testing for such a large class of measurements. The majority of previous articles in self-testing have been primarily concerned with certifying the state and were limited to simple single-qubit measurements in the X-Z plane. Prior self-testing results for multi-qubit measurements only allow one to test for tensor products of σ_X and σ_Z observables. While this is sufficient for verification in the post-hoc model of [13, 14], testing for σ_X and σ_Z observables does not directly allow for the verification of a general computation (unless one relies on techniques such as process tomography [37], which introduce substantial additional overhead).

Our first contribution is to extend the "Pauli braiding test" of [35] (which allows one to test tensor products of σ_X and σ_Z observables with constant robustness) to allow for σ_Y observables as well. This is somewhat subtle due to an ambiguity in the complex phase that cannot be

[3]The $\log g$ overhead is due to the complexity of sampling from the right distribution in rigidity tests, which are discussed next. We leave the possibility of removing this by derandomization for future work. Another source of overhead is in achieving blindness: in order to hide the circuit, we encode it as part of the input to a universal circuit, introducing a factor of $O(\log g)$ overhead.

[4]This idea can be understood more directly as employing rigidity tests to delegate to PV the preparation of the random eigenstates required in Broadbent's basic prepare-and-measure protocol in [7], thus enabling the classical part of that protocol to be executed between PP and the classical verifier.

detected by any classical two-player test; we formalize the ambiguity and show how it can be effectively accounted for. Our second contribution is to substantially increase the set of elementary gates that can be tested, to include arbitrary m-qubit tensor products of single-qubit Clifford observables. This is achieved by introducing a new "conjugation test", which tests how an observable applied by the provers acts on the Pauli group. The test is inspired by general results of Slofstra [39] which provide an approach to test that a set of observables satisfy some algebraic relations (when acting on EPR pairs), but is substantially more direct.

A key feature of our rigidity results is that their robustness scales independently of the number of EPR pairs tested, as in [35]. This is crucial for the efficiency of our delegation protocols. The robustness for previous results in parallel self-testing, other than [35], had a polynomial dependence on the number of EPR pairs tested. We give an informal statement of our robust rigidity theorem.

Theorem 1.1 (Informal)**.** *Let $m \in \mathbb{Z}_{>0}$. Let $\mathcal{G}$ be a fixed, finite set of single-qubit Clifford observables. Then there exists an efficient two-prover test* $\textsc{rigid}(\mathcal{G}, m)$ *with $O(m)$-bit questions (a constant fraction of which are of the form $W \in \mathcal{G}^m$) and answers such that the following properties hold:*

- *(Completeness) There is a strategy for the provers that uses $m+1$ EPR pairs and succeeds with probability at least $1 - e^{-\Omega(m)}$ in the test.*
- *(Soundness) For any $\varepsilon > 0$, any strategy for the provers that succeeds with probability $1-\varepsilon$ in the test must be* $\mathrm{poly}(\varepsilon)$*-close, up to local isometries, to a strategy in which the provers begin with $(m+1)$ EPR pairs and is such that upon receipt of a question of the form $W \in \mathcal{G}^m$ the prover measures the "correct" observable W.*

Although we do not strive to obtain the best dependence on ε, we believe it should be possible to obtain a scaling of the form $C\sqrt{\varepsilon}$ for a reasonable constant C. We discuss the test in Section 3. Next, we describe the two delegation protocols in a little more detail.

Verifier-on-a-Leash protocol. The first protocol, which we call *Verifier-on-a-Leash Protocol*, or "Leash Protocol" for short, is divided into two subgames; which game is played is chosen by the verifier by flipping a biased coin with appropriately chosen probabilities.

- The first game is a sequential version of the rigidity game $\textsc{rigid}(\Sigma, m)$, from Theorem 1.1 (this is described in detail in Figure 11). This aims to enforce that PV performs precisely the right measurements;
- The second game is the *delegation game* (this is described in detail in Figures 12, 13, and 14, and its structure is summarized in Figure 9). Here the verifier guides PP through the computation in a similar way as in Broadbent's EPR Protocol [7].

In the delegation game, the questions to PV are of all of the form $W \in \Sigma^m$, where $\Sigma = \{X, Y, Z, F, G\}$. The latter is the set of measurements performed by the verifier in Broadbent's EPR protocol. On the other hand, PP is asked to perform the same measurements as a prover in Broadbent's EPR protocol.

In the rigidity game, instead, the questions for PV come from a slightly larger set (which also includes Bell basis measurements). However, crucially, a *subset* of these questions are of the form $W \in \Sigma^m$, with the same distribution as in the *delegation game*. This ensures that, upon receiving a question of the form $W \in \Sigma^m$, PV is not able to tell which of the two games is being played. Hence, we can apply the rigidity result of Theorem 1.1 to guarantee the honest behavior of PV in the delegation game. With the latter guarantee in hand, we can deduce that in the delegation game, PP is constrained to behaving like an honest prover in Broadbent's EPR protocol.

Overall, PV (who plays the role of the verifier in Broadbent's EPR protocol) only needs to perform products of single-qubit Clifford observables and Bell-basis measurements (universal quantum computational power is not needed for this prover), while PP needs to behave like the honest prover in Broadbent's EPR protocol (this requires universal quantum computation).

The protocol requires $2d + 1$ rounds of interaction, where d is the T-depth of the circuit being delegated (this is the number of layers of T gates in the circuit - see Section 4.1 for a precise definition). The protocol requires $O(n + g)$ EPR pairs to delegate a g-gate circuit on n qubits, and the overall time complexity of the protocol is $O(g \log g)$. The input to the circuit is hidden from the provers, meaning that the protocol can be made blind by encoding the circuit in the input, and delegating a universal circuit. However, blindness holds only as long as PV and PP stay separated after the execution of the protocol. We note that using universal circuits incurs a $\log n$ factor increase in the depth of the circuit [5].

The completeness of the protocol follows directly from the completeness of Broadbent's EPR protocol and of the rigidity game $\textsc{rigid}(\Sigma, m)$. Once we ensure the correct behavior of PV using our rigidity test, soundness follows from soundness of Broadbent's protocol as well, since the combined behavior of our verifier and an honest PV in the delegation game is nearly identical to that of the verifier in Broadbent's protocol.

Dog-Walker protocol. The second protocol, which we refer to as the *Dog-Walker Protocol*, also starts from Broadbent's protocol but modifies it in a different way to achieve a protocol that only requires a constant number of rounds of interaction. The latter property is achieved by leveraging the fact that, when the prover in Broadbent's EPR protocol is honest, his actions can be performed *before* the actions of the verifier. Thus the main difference between the Leash Protocol and the Dog-Walker Protocol is that, in the latter, the classical verifier first obtains all of PP's measurement outcomes via one round of interaction. Then these outcomes are sent by the verifier to PV, together with the input x of the computation (which is now communicated in the clear). With these, PV is able to perform the required adaptive measurements without the need to interact with the verifier any further. An additional rigidity test, which we refer to as the Tomography test is necessary to enforce that PV performs the adaptive measurements honestly. We skip for now the details on this new test, and we defer its presentation to the beginning of Section 3 and its precise description to Section 3.6.

The proof of security is slightly more involved, but the key ideas are the same: we use a combination of our new rigidity results and the techniques of Broadbent's protocol to control the two provers, one of which plays the role of Broadbent's verifier, and the other the role of the prover. Because of the more complicated "leash" structure in this protocol we call it the *Dog-Walker Protocol*. Like the Leash Protocol, the Dog-Walker Protocol has overall time complexity $O(g \log g)$. Unlike the leash protocol, the Dog-Walker protocol is not blind, since PV simply receives the input in the clear.

Based on the Dog-Walker Protocol, it is possible to design a classical-verifier two-prover protocol for all languages in QMA. This is achieved along the same lines as the proof that QMIP = MIP* from [37]. PV, given the input, creates the QMA witness and teleports it to PP with the help of the verifier. The verifier then delegates the QMA verification circuit to the second prover, as in the Dog-Walker Protocol. PV can then be re-used to verify the operations of PP. The Dog-Walker Protocol enables this extension in a straightforward manner, since it can be adapted to have PV decide the input to the computation. We notice that such a transformation is not possible with the Leash protocol given that PP must know the input x in order to be able to create the corresponding QMA witness.

We remark that the soundness of both the Leash Protocol and the Dog-Walker Protocol can be amplified by sequential repetition. In particular, an arbitrarily low, but constant, soundness error can be achieved in the Dog-Walker Protocol by repeating the protocol a constant number of times, thus maintaining constant round-complexity (we refer to Section 6 for the details).

Subsequent work. Bowles et al. [6] have independently derived a variant of our rigidity test for multi-qubit σ_X, σ_Y and σ_Z observables in the context of entanglement certification protocols in quantum networks. Their self-test result has a slightly smaller set of questions but significantly weaker robustness bounds.

Grilo [19] presented a protocol for verifiable two-prover delegation of quantum computation by a classical client with a single round of communication. Because of this single-round structure, space-like separation can replace the non-communication assumption. The latter protocol is not blind, and requires resources scaling as $\Omega(ng^2)$ to delegate a circuit of g gates on n qubits.

Open questions and directions for future work. We have introduced a new rigidity theorem and shown how it can be used to transform a specific quantum-verifier delegation protocol, due to Broadbent, into a classical-verifier protocol with an additional prover, while suffering very little overhead in terms of the efficiency of the protocol. We believe that a similar transformation could be performed starting from delegation protocols based on other models of computation, such as the protocol in the measurement-based model of [15] or the protocol based on computation by teleportation considered in [37], and would lead to similar efficiency improvements.

Recently, [23] provided an experimental demonstration of a two-prover delegation protocol based on [37] for a 3-qubit quantum circuit based on Shor's algorithm to factor the number 15; in order to obtain an actual implementation, necessitating "only" on the order of 6000 CHSH tests, the authors had to make the strong assumption that the devices behave in an independent and identically distributed (i. i. d.) manner at each use, and therefore the authors could not use the most general testing results from [37]. We believe that our improved rigidity theorem could lead to an implementation that does not require any additional assumptions. We also leave as an open problem investigating whether (a variant of) our protocol can be made fault-tolerant, making it more suitable for future implementation.

We note that our protocols require the verifier to communicate with one prover after at least one round of communication with the other has been completed. Therefore, the requirement that the provers do not communicate throughout the protocol cannot be enforced through space-like separation, and must be taken as an a priori assumption. The single-round protocol of [19], for which non-communication can be enforced through space-like separation, is not blind. Hence, it is an open question whether there exists a two-prover delegation protocol that consists of a single round of simultaneous communication with each prover, and is both blind and verifiable. We also wonder if the fact that blindness is compromised after the provers collude is unavoidable in this model. A different avenue to achieve this is to rely on computational assumptions on the power of the provers to achieve protocols with more properties (non-interactive, blind, verifiable) [11, 3, 26, 25]. Unfortunately at the moment all such protocols suffer from a significant overhead due to the use of the computational assumption; namely, a number of qubits that scales at least as $\min(n, g)$ *times* a polynomial in the security parameter.

Regarding blindness of the Leash protocol, our current proof does not say anything about the possibility of the provers being able to *increase* their knowledge on the input given prior side-information. This would be particularly important if the Leash protocol is composed with other protocols. We leave as an open question if the blindness of the Leash protocol could be proven using simulation-based security definitions, which would imply its composability.

Finally, due to its efficiency and robustness, our ridigity theorem is a potentially useful tool in many other cryptographic protocols. For instance, an interesting direction to explore is the possibility of exploiting our theorem to achieve more efficient protocols for device-independent quantum key distribution, entanglement certification or other cryptographic protocols involving more complex untrusted computation of the users.

Organization. In Section 2, we give the necessary preliminaries, including outlining Broadbent's EPR Protocol (Section 2.4). In Section 3, we introduce our new rigidity theorems. In Section 4, we present our first protocol, the leash protocol, and in Section 5, we discuss our second protocol, the Dog-Walker Protocol (including the extension to a two-prover protocol for QMA). In Section 6, we discuss the sequential repetition of our protocols.

Acknowledgments. We thank Anne Broadbent for useful discussions in the early stages of this work. All authors acknowledge the IQIM, an NSF Physics Frontiers Center at the California Institute of Technology, where this research was initiated. We also thank the anonymous reviewers that helped us to improve the presentation of this manuscript.

2 Preliminaries

2.1 Notation

We often write $\vec{x} = (x_1, \dots, x_n) \in \{0,1\}^n$ for a string of bits, and $W = W_1 \cdots W_m \in \Sigma^m$ for a string, where Σ is a finite alphabet. If $S \subseteq \{1, \dots, m\}$ we write W_S for the substring of W indexed by S. For an event E, we use 1_E to denote the indicator variable for that event, so $1_E = 1$ if E is true, and otherwise $1_E = 0$. We write $\mathrm{poly}(\varepsilon)$ for $O(\varepsilon^c)$, where c is a universal constant that may change each time the notation is used.

$\mathcal{H}$ is a finite-dimensional Hilbert space. We denote by $\mathrm{U}(\mathcal{H})$ the set of unitary operators, $\mathrm{Obs}(\mathcal{H})$ the set of binary observables (we omit the term "binary" from here on; in this paper all observables are binary) and $\mathrm{Proj}(\mathcal{H})$ the set of projective measurements on $\mathcal{H}$. We let $|\mathrm{EPR}\rangle$ denote an EPR pair:

$$|\mathrm{EPR}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Observables. We use capital letters $X, Z, W, \ldots$ to denote observables. We use greek letters σ, τ with a subscript σ_W, τ_W, to emphasize that the observable W specified as subscript acts in a particular basis. For example, X is an arbitrary observable but σ_X is specifically the Pauli X matrix defined in (2.1).

For $a \in \{0,1\}^n$ and commuting observables $\sigma_{W_1}, \ldots, \sigma_{W_n}$, we write $\sigma_W(a) = \prod_{i=1}^n (\sigma_{W_i})^{a_i}$. The associated projective measurements are $\{\sigma_{W_i}^0, \sigma_{W_i}^1\}$ where $\sigma_{W_i} = \sigma_{W_i}^0 - \sigma_{W_i}^1$ and $\{\sigma_W^u\}_{u\in\{0,1\}^n}$ where $\sigma_W^u = \mathrm{E}_a(-1)^{u\cdot a}\sigma_W(a)$. Often the σ_{W_i} will be single-qubit observables acting on distinct qubits, in which case each is implicitly tensored with the identity outside of the qubit on which it acts.

We recall the commutator notation $[A, B]$ for $AB + BA$ and anti-commutator notation $\{A, B\}$ for $AB + BA$, where A, B are linear operators on the same Hilbert space.

Pauli and Clifford groups. Let

$$\sigma_I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \text{and} \quad \sigma_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{2.1}$$

denote the standard Pauli matrices acting on a qubit. The single-qubit Weyl-Heisenberg group

$$\mathcal{H}^{(1)} = H(\mathbb{Z}_2) = \Big\{(-1)^c \sigma_X(a)\sigma_Z(b) \;:\; a, b, c \in \{0,1\}\Big\}$$

is the matrix group generated by the Pauli σ_X and σ_Z. We let $\mathcal{H}^{(n)} = H(\mathbb{Z}_2^n)$ be the direct product of n copies of $\mathcal{H}^{(1)}$. The n-qubit Clifford group is the normalizer of $\mathcal{H}^{(n)}$ in the unitary group, up to phase:

$$G_C^{(n)} = \big\{G \in \mathrm{U}((\mathbb{C}^2)^{\otimes n}) : G\sigma G^\dagger \in \mathcal{H}^{(n)} \quad \forall \sigma \in \mathcal{H}^{(n)}\big\}.$$

Some Clifford observables we will use include

$$\sigma_H = \frac{\sigma_X + \sigma_Z}{\sqrt{2}}, \quad \sigma_{H'} = \frac{\sigma_X - \sigma_Z}{\sqrt{2}}, \quad \sigma_F = \frac{-\sigma_X + \sigma_Y}{\sqrt{2}}, \quad \sigma_G = \frac{\sigma_X + \sigma_Y}{\sqrt{2}}. \tag{2.2}$$

Note that σ_H and $\sigma_{H'}$ satisgy $\sigma_X\sigma_H\sigma_X = \sigma_{H'}$ and $\sigma_Z\sigma_H\sigma_Z = -\sigma_{H'}$. Similarly, σ_F and σ_G satisfy $\sigma_X\sigma_F\sigma_X = -\sigma_G$ and $\sigma_Y\sigma_F\sigma_Y = \sigma_G$.

2.2 Concentration inequality

A *supermartingale* is a sequence of random variables $\{X_k\}_{k\geq 0}$ such that for all $k \geq 0$, $X_k \geq \mathbb{E}[X_{k+1}|X_1, \ldots, X_k]$. We make use of the following formulation of the Azuma–Hoeffding inequality. See, for example, [9, Section 6] and [30, Theorem 12.4]. The latter gives a proof for martingales that also applies to supermartingales.

Theorem 2.1. *Let $\{X_k\}_{k\geq 0}$ be a real-valued supermartingale such that for every $k \in \mathbb{N}$, the condition $|X_k - X_{k-1}| \leq d_k$ holds almost surely, for some $d_k \geq 0$. Then for any $n \geq 1$ and $\lambda \geq 0$,*

$$\Pr(X_n \geq X_0 + \lambda) \leq \exp\left(-\frac{\lambda^2}{2\sum_{k=1}^{n} d_k^2}\right).$$

2.3 Quantum circuits

We use capital letters in sans-serif font to denote gates. We work with the universal quantum gate set $\{\mathsf{CNOT}, \mathsf{H}, \mathsf{T}\}$, where the controlled-not gate is the two-qubit gate with the unitary action

$$\mathsf{CNOT}|b_1, b_2\rangle = |b_1, b_1 \oplus b_2\rangle,$$

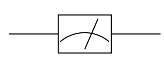
and the Hadamard and T gates are single-qubit gates with actions

$$\mathsf{H}|b\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle + (-1)^b|1\rangle\Big) \quad \text{and} \quad \mathsf{T}|b\rangle = \mathrm{e}^{ib\pi/4}|b\rangle,$$

respectively. We will also use the following gates:

$$\mathsf{X}|b\rangle = |b \oplus 1\rangle, \quad \mathsf{Z}|b\rangle = (-1)^b|b\rangle, \quad \text{and} \quad \mathsf{P}|b\rangle = i^b|b\rangle.$$

Measurements in the Z basis (or computational basis) will be denoted by the standard measurement symbol:



To measure another observable, W, we can perform a unitary change of basis U_W before the measurement in the computational basis.

We assume that every circuit has a specified output wire, which is measured at the end of the computation to obtain the output bit. Without loss of generality, we can assume this is always the first wire. For an n-qubit system, we let Π_b, for $b \in \{0, 1\}$, denote the orthogonal projector onto states with $|b\rangle$ in the output wire: $|b\rangle\langle b| \otimes \mathrm{Id}$. For example, the probability that a circuit Q outputs 0 on input $|\vec{x}\rangle$ is $\left\|\Pi_0 Q|\vec{x}\rangle\right\|^2$.

We can always decompose a quantum circuit into layers such that each layer contains at most one T gate applied to each wire. The minimum number of layers for which this is possible is called the T *depth* of the circuit. We note that throughout this paper we will assume circuits are compiled in a specific form that introduces extra T gates (see the paragraph on the H gadget in Section 2.4). The T depth of the resulting circuit is proportional to the depth of the original circuit.

2.4 Broadbent's EPR protocol

In this section we summarize the main features of a delegation protocol introduced in [7], highlighting the aspects that will be relevant to understanding our subsequent adaptation into two-prover protocols. The "EPR Protocol" from [7] involves the interaction between a verifier V_{EPR} and a prover P^*_{EPR}. We write P_{EPR} for the "honest" behavior of the prover. The verifier V_{EPR} has limited quantum powers. Her goal is to delegate a BQP computation to the prover P^*_{EPR} in a verifiable way. Specifically, the verifier has as input a quantum circuit Q on n qubits and an input string $\vec{x} \in \{0,1\}^n$, and the prover gets as input Q. The verifier and prover interact. At the end of the protocol, the verifier outputs either accept or reject. The protocol is such that there exist values p_{sound} and p_{compl} with $p_{\text{sound}} < p_{\text{compl}}$ such that $p_{\text{compl}} - p_{\text{sound}}$, called the *soundness-completeness gap*, is a constant independent of input size, and moreover:

Completeness: If the prover is honest and $\left\|\Pi_0 Q|\vec{x}\rangle\right\|^2 \geq 2/3$, then the verifier outputs accept with probability at least p_{compl};

Soundness: If $\left\|\Pi_0 Q|\vec{x}\rangle\right\|^2 \leq 1/3$, then the probability the verifier outputs accept is at most p_{sound}.

In the EPR protocol, V_{EPR} and P_{EPR} are assumed to share $(n+t)$ EPR pairs at the start of the protocol, where t is the number of T gates in Q and n the number of input bits. The first n EPR pairs correspond to the input to the computation; they are indexed by $N = \{1,\ldots,n\}$. The remaining pairs are indexed by $T = \{n+1,\ldots,n+t\}$; they will be used as ancilla qubits to implement each of the T gates in the delegated circuit. In [7] the EPR protocol is only considered in the analysis, and it is assumed that the EPR pairs are prepared by the verifier.

The behavior of V_{EPR} depends on a *run type* randomly chosen by V_{EPR} *after* her interaction with P_{EPR}. There are three possible run types:

- Computation run ($r=0$): the verifier delegates the computation to P_{EPR}, and at the end of the run can recover its output if P_{EPR} behaves honestly;
- X-test run ($r=1$) and Z-test run ($r=2$): the verifier tests that P_{EPR} behaves honestly, and rejects if malicious behavior is detected.

For some constant p, V chooses $r=0$ with probability p, and otherwise chooses $r \in \{1,2\}$ with equal probability. Since the choice of run type is made after the interaction with P_{EPR}, P_{EPR}'s behavior cannot depend on the run type. In particular, any deviating behavior in a computation run is reproduced in both types of test runs. The analysis amounts to showing that any deviating behavior that affects the outcome of the computation will be detected in at least one of the test runs.

In slightly more detail, the high-level structure of the protocol is the following. V_{EPR} measures her halves of the n qubits in N in order to prepare the input state on P_{EPR}'s system. As a result the input is quantum one-time padded with keys that depend on V_{EPR}'s measurement results. For example, in a computation run, V_{EPR} measures each input qubit in the Z basis, and gets some result $\vec{d} \in \{0,1\}^n$, meaning the input on P_{EPR}'s side has been prepared as $\mathsf{X}^{\vec{d}}|0\rangle^{\otimes n}$. In [7], the input is always considered to be $\vec{0}$, but we can also prepare an arbitrary classical input

$\vec{x} \in \{0,1\}^n$ by reinterpreting the one-time pad key as $\vec{a} = \vec{d} \oplus \vec{x}$ so that the input state on P_{EPR}'s side is $\mathsf{X}^{\vec{a}}|\vec{x}\rangle$. In a test run, on the other hand, the input is prepared as the one-time pad of either $|0\rangle^{\otimes n}$ or $|+\rangle^{\otimes n}$. Note that as indicated in Figure 2 this choice of measurements will be made after the interaction with P_{EPR} has taken place.

The honest prover P_{EPR} applies the circuit Q, which we assume is compiled in the universal gate set $\{\mathsf{H}, \mathsf{T}, \mathsf{CNOT}\}$, to his one-time padded input. We will shortly describe gadgets that P_{EPR} can apply in order to implement each of the three gate types. The gadgets are designed in a way that in a test run each gadget amounts to an application of an identity gate; this is what enables V_{EPR} to perform certain tests in those runs that are meant to identify deviating behavior of a dishonest prover. After each gadget, the one-time padded keys can be updated by V_{EPR}, who is able to keep track of the keys at any point in the circuit using the *update rules* in Table 2.

		Key Update Rule
CNOT		$(a_j, b_j, a_{j'}, b_{j'}) \leftarrow (a_j, b_j + b_{j'}, a_j + a_{j'}, b_{j'})$
H		$(a_j, b_j) \leftarrow (b_j, a_j)$
T	Computation Run	$(a_j, b_j) \leftarrow (a_j + c_i, b_j + e_i + a_j + c_i + (a_j + c_i)z_i)$
	X-test, even parity; or Z-test, odd parity	$(a_j, b_j) \leftarrow (e_i, 0)$
	Z-test, even parity; or X-test, odd parity	$(a_j, b_j) \leftarrow (0, b_j + e_i + z_i)$

Table 2: Rules for updating the one-time-pad keys after applying each type of gate in the EPR Protocol, in particular: after applying a CNOT gate controlled on the j-th wire and targeting the j'-th wire; applying an H gate to the j-th wire; or applying the i-th T gate to the j-th wire.

We now describe the three gadgets, before giving a complete description of the protocol.

CNOT Gadget To implement a CNOT gate on wires j and j', P_{EPR} simply performs the CNOT gate on those wires of his input qubits. The one-time pad keys are changed by the update rule in Table 2, because $\mathsf{CNOT} \cdot \mathsf{X}^{a_j}\mathsf{Z}^{b_j} \otimes \mathsf{X}^{a_{j'}}\mathsf{Z}^{b_{j'}} = \mathsf{X}^{a_j}\mathsf{Z}^{b_j+b_{j'}} \otimes \mathsf{X}^{a_j+a_{j'}}\mathsf{Z}^{b_{j'}} \cdot \mathsf{CNOT}$. Note that $\mathsf{CNOT}|0\rangle|0\rangle = |0\rangle|0\rangle$ and $\mathsf{CNOT}|+\rangle|+\rangle = |+\rangle|+\rangle$, so in the test runs, P_{EPR} is applying the identity.

H Gadget To implement an H gate on wire j, P_{EPR} simply performs the H on wire j, and the one-time-pad keys are changed as in Table 2. Unlike CNOT, H does not act as the identity on $|0\rangle$ and $|+\rangle$, so it is not the identity in a test run. To remedy this, assume that Q is compiled so that every H gate appears in a pattern $\mathsf{H}(\mathsf{TTH})^k$, where k is odd. This can be accomplished by replacing each H by HTTHTTHTTH, which implements the same unitary. In test runs, the T gadget, described shortly, implements the identity, and since $\mathsf{H}(\mathsf{Id}\,\mathsf{H})^k$ for odd k implements the identity, $\mathsf{H}(\mathsf{TTH})^k$ will also have no effect in test runs.

Parity of a T Gate Within a pattern $\mathsf{H}(\mathsf{TTH})^k$, the H has the effect of switching between an X-test run scenario (the state $|0\rangle$) and a Z-test run scenario (the state $|+\rangle$). In order to consistently talk about the type of a run while evaluating the circuit, we can associate a parity with each T gate in the circuit. The parity of the T gates that are not part of the pattern $\mathsf{H}(\mathsf{TTH})^k$ will be defined to be even. An H will always flip the parity, so that within such a pattern, the first two T gates will be odd, the next two will be even, etc., until the last two T gates will be odd again.

T Gadget The gadget for implementing the i-th T gate on the j-th wire is performed on P_{EPR}'s j-th input qubit, and his i-th auxiliary qubit (indexed by $n+i$), which we can think of as being prepared in a particular auxiliary state by V_{EPR} measuring her half of the corresponding EPR pair, as shown in Figure 1. The gadget depends on a uniformly random bit z_i that is chosen by V_{EPR} and sent to the prover.

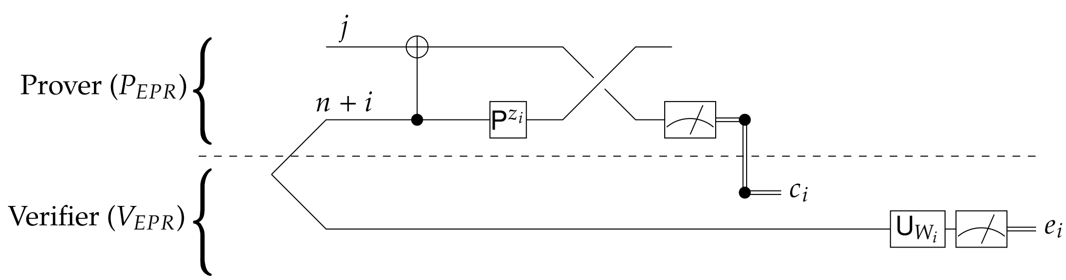


Figure 1: The gadget for implementing the i-th T gate on the j-th wire. The gate U_{W_i} implementing the change of basis associated with observable W_i is applied as part of the procedure V^r_{EPR} (see Figure 3b) and is determined by the run type r, the parity of the i-th T gate, z_i, c_i, and a'_i (the X-key going into the i-th T gate), as in Table 3.

The EPR protocol. We show how the gadgets just described are used in the complete protocol. We first describe the protocol for V_{EPR} below. For later convenience we have divided the action of V_{EPR} into classical actions and a single quantum subroutine V^r_{EPR} depending on the run type r.

The procedure V^r_{EPR} measures each of the $n+t$ EPR halves according to some observable that depends on r, $\vec{c}$, and $\vec{z}$. In the case of a computation run, V^0_{EPR} measures the qubits in T adaptively. We describe the steps of V_{EPR}, V^r_{EPR} and the honest behavior of P_{EPR} in Fig. 3.

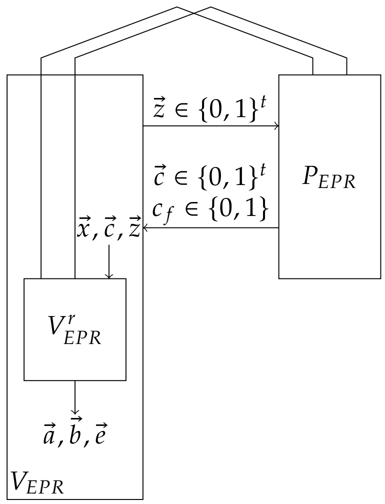


Figure 2: This figure describes how different pieces of the protocol fit together. V_{EPR} and P_{EPR} share $n+t$ EPR pairs. The honest prover P_{EPR} can be seen as a procedure that acts on $n+t$ qubits — the EPR pair halves — depending on a t-bit string $\vec{z}$. We have separated the quantum part of V_{EPR} into its own procedure, called V^r_{EPR}, where $r \in \{0,1,2\}$ indicates the *run type*, which V_{EPR} runs on her $n+t$ EPR halves, and the $2t$ bits $\vec{c}$ and $\vec{z}$. Aside from running V^r_{EPR}, V_{EPR} is classical.

			U_{W_i} (observable W_i)
Computation Run	$a'_i \oplus c_i \oplus z_i = 0$		HT (observable G)
	$a'_i \oplus c_i \oplus z_i = 1$		HPT (observable F)
X-test Run	even T gate		Id (observable Z)
	odd T gate	$z_i = 0$	H (observable X)
		$z_i = 1$	HP (observable Y)
Z-test Run	odd T gate		Id (observable Z)
	even T gate	$z_i = 0$	H (observable X)
		$z_i = 1$	HP (observable Y)

Table 3: The choice of U_{W_i} in the T gadget. We also indicate the observable W_i associated with the final measurement $W_i = \mathsf{U}^\dagger_{W_i} Z \mathsf{U}_{W_i}$.

Completeness and soundness. We summarize the relevant part of the analysis of the EPR protocol from [7]. First suppose P_{EPR} behaves honestly. If $\left\|\Pi_0 Q|\vec{x}\rangle\right\|^2 = p$, then in a computation run, V_{EPR} outputs accept with probability p, whereas in a test run, V_{EPR} outputs accept with probability 1. This establishes completeness of the protocol:

Theorem 2.2 (Completeness)**.** *Suppose the verifier executes the EPR Protocol, choosing $r = 0$ with probability p, on an input $(Q, |\vec{x}\rangle)$ such that $\left\|\Pi_0 Q|\vec{x}\rangle\right\|^2 \geq 1-\delta$. Then the probability that V_{EPR} accepts when interacting with the honest prover P_{EPR} is at least $(1-p) + p(1-\delta)$.*

The following theorem is implicit in [7, Section 7.6], but we include a brief proof sketch:

Theorem 2.3 (Soundness)**.** *Suppose the verifier executes the EPR Protocol, choosing $r = 0$ with probability p, on an input $(Q, |\vec{x}\rangle)$ such that $\left\|\Pi_0 Q|\vec{x}\rangle\right\|^2 \leq \delta$. Let P^*_{EPR} be an arbitrary prover such that*

P^*_{EPR} is accepted by V_{EPR} with probability q_t conditioned on $r \neq 0$, and q_c conditioned on $r = 0$. Then the prover's overall acceptance probability is $pq_c + (1-p)q_t$, and

$$q_c \;\leq\; 2\,(q_t\,\delta + (1-q_t)) - \delta.$$

Proof sketch. Using the notation of [7], let $E(\rho) = \sum_k K_k \rho K_k^\dagger$ be the Kraus decomposition of an arbitrary attack performed by a malicious prover on the m-qubit state resulting from an honest run of the protocol.[5] We write the k-th Kraus operator of E as a sum of Paulis $K_k = \sum_{Q \in \mathcal{P}^{(m)}} \alpha_{k,Q} Q$. Finally, we define the set of benign attacks $B_{t,m} \subseteq \mathcal{P}^{(m)}$ as the subset of Paulis containing I or Z in the positions that are measured (in the computational basis) during the protocol.

Notice that the benign attacks do not affect the the acceptance of the protocol, and therefore the value $A = \sum_k \sum_{Q \notin B_{t,m}} |\alpha_{k,Q}|^2$ can be interpreted then as the total weight on attacks that could change the outcome of the computation. By [7], the probability of rejecting in a computation run is $1 - q_c \geq (1-\delta)(1-A)$, whereas the probability of rejecting in a test run is $1 - q_t \geq \frac{1}{2}A$. Combining these gives $q_c \leq 2(q_t\delta + (1-q_t)) - \delta$. □

3 Rigidity

In this section we describe the main rigidity tests used in our delegation protocols. To present the tests we adopt the terminology of "players" instead of "provers" and "referee" instead of "verifier", as this terminology is the standard one in the area of self-testing from which the section borrows. Each of the tests consists of a two-message interaction between the referee and the two players: first, a pair of questions is selected by the referee and each player is sent one element of the pair. Second, each player responds to its question with an answer. Finally, the referee decides to accept or reject the player's answers in the test.

Our main test is called RIGID(Σ, m) and it is described in Section 3.5. Here Σ denotes the five-element set $\Sigma = \{X, Y, Z, F, G\}$. Each element of Σ is a label for the corresponding single-qubit observable introduced in Section 2.1. The test is parametrized by an integer m which denotes the number m of EPR pairs used by the players in the honest strategy. In the test, with some constant probability either player is sent as question a string W chosen uniformly at random from Σ^m. In these cases the honest player is expected to measure each qubit in the basis indicated by W and return the m-bit string of outcomes obtained. In other cases, the player may be asked to perform measurements in other bases, such as a measurement of pairs of qubits in the Bell basis. These measurements are required to test that the player indeed performs the right measurement when sent a basis from Σ^m (up to an isometry, as explained in Section 3.1 below).

In general a strategy for the players in any of the tests presented in this section consists of an arbitrary entangled state $|\psi\rangle \in \mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B}$ (which we take to be pure), and measurements (which

[5] Note that we can assume such behavior by the malicious prover without loss of generality since all measurements can be performed coherently, with the first step of the attack undoing all honest operations.

1. V_{EPR} sends $\vec{z} \in_R \{0,1\}^t$ to P_{EPR}, and receives back $\vec{c} \in \{0,1\}^t$ and $c_f \in \{0,1\}$.

2. V_{EPR} chooses a random run type $r \in \{0,1,2\}$ and runs V^r_{EPR} (see Figure 3b) on $\vec{x}, \vec{c}, \vec{z}$ and on her EPR halves, to obtain bits $\vec{a}, \vec{b} \in \{0,1\}^n$ and $\vec{e} \in \{0,1\}^t$.

3. V_{EPR} applies the update rules from Table 2 on the initial keys $(\vec{a}, \vec{b})$, gate-by-gate, to obtain, for every $i \in [t]$, the X-key before the i-th T gate is applied, a'_i, and the final X key for the output wire, a'_f. If $r = 1$ (X-test run) and there exists an i such that the i-th T gate is even and $c_i \neq a'_i \oplus e_i$, output reject. If $r = 2$ (Z-test run) and there exists an i such that the i-th T gate is odd and $c_i \neq a'_i \oplus e_i$, output reject. If $r \in \{0,1\}$ (computation or X-test run) and $c_f \oplus a'_f \neq 0$, output reject. Otherwise, output accept.

(a) V_{EPR}'s point of view.

Input: A circuit Q with t T gates, $\vec{x} \in \{0,1\}^n$, $\vec{c}, \vec{z} \in \{0,1\}^t$, an n-qubit system indexed by N, and a t-qubit system indexed by T.

1. If $r \in \{0,1\}$, measure each qubit in N in the Z basis, and otherwise measure in the X basis, to get results $\vec{d} \in \{0,1\}^n$. If $r = 0$, set $(\vec{a}, \vec{b}) = (\vec{d} \oplus \vec{x}, 0^n)$; if $r = 1$, set $(\vec{a}, \vec{b}) = (\vec{d}, 0^n)$; and if $r = 2$ set $(\vec{a}, \vec{b}) = (0^n, \vec{d})$.

2. Going through Q gate-by-gate, use the update rules in Table 2 to update the one-time-pad keys. For every $i \in [t]$, when the i-th T gate is reached, let a'_i be the X key before the i-th T gate is applied. Choose an observable W_i according to Table 3 in which to measure the i-th qubit in T, corresponding to the i-th T gate, obtaining result e_i.

(b) The procedure V^r_{EPR}, employed by V_{EPR}.

1. Receive $\vec{z} \in \{0,1\}^t$ from V_{EPR}.

2. Evaluate Q gate-by-gate using the appropriate gadget for each gate. In particular, use z_i to implement the i-th T gadget, and obtain measurement result c_i.

3. Measure the output qubit to obtain c_f, and return $\vec{c}$ and c_f to V_{EPR}.

(c) Honest prover strategy P_{EPR}

Figure 3: The EPR Protocol.

we take to be projective) for each possible question.[6] This includes an m-bit outcome projective measurement $\{W^u\}_{u\in\{0,1\}^m}$ for each of the queries $W \in \Sigma^m$, which we take to be identical for both players (in Section 3.2 we justify why this is without loss of generality). Our rigidity result states that for any strategy that succeeds with probability $1-\varepsilon$ in the test, the measurements associated with questions in Σ^m are within $\mathrm{poly}(\varepsilon)$ of the honest strategy, up to local isometries and in the appropriate norm, which depends on the state shared by the players (see Theorem 3.1 for a precise statement). This is almost true, but for an irreconcilable ambiguity in the definition of the complex phase $\sqrt{-1}$. The fact that complex conjugation of observables leaves correlations invariant implies that no classical test can distinguish between the two nontrivial inequivalent irreducible representations of the Pauli group, which are given by the Pauli matrices $\sigma_X, \sigma_Y, \sigma_Z$ and their complex conjugates $\overline{\sigma_X} = \sigma_X$, $\overline{\sigma_Z} = \sigma_Z$, $\overline{\sigma_Y} = -\sigma_Y$, respectively. In particular, the players may use a strategy that uses a combination of both representations; as long as they do so consistently, no test will be able to detect this behavior.[7] The formulation of our result accommodates this irreducible degree of freedom by forcing the players to use a single qubit, the $(m+1)$-st, to make their choice of representation (so honest players require the use of $(m+1)$ EPR pairs to test the operation of m-fold tensor products of observables from Σs).

Theorem 3.1 below summarizes the guarantees of our main test, RIGID(Σ, m). Informally, Theorem 3.1 establishes that a strategy that succeeds in RIGID(Σ, m) with probability at least $1-\epsilon$ must be such that (up to local isometries):

- The players' joint state is close to a tensor product of m EPR pairs, together with an arbitrary ancilla register;
- The projective measurements performed by either player upon receipt of a query of the form $W \in \Sigma^m$ are, on average over the uniformly random choice of $W \in \Sigma^m$, close to a measurement that consists of first, measuring an ancilla register $\hat{\mathsf{A}}$ or $\hat{\mathsf{B}}$ to extract a single bit that specifies whether to perform the ideal measurements or their conjugated counterparts, respectively, and second, measuring the player's m half-EPR pairs in either the bases indicated by W, or their complex conjugates, depending on the bit obtained from the ancilla register.

For an observable $W \in \Sigma$, let $\sigma_W = \sigma_W^{+1} - \sigma_W^{-1}$ be its eigendecomposition, where σ_W are the "honest" Pauli matrices defined in (2.1) and (2.2). For $u \in \{\pm 1\}$ let $\sigma_{W,+}^u = \sigma_W^u$ for $W \in \Sigma$, and

$$\sigma_{X,-}^u = \sigma_X^u, \quad \sigma_{Z,-}^u = \sigma_Z^u, \quad \sigma_{Y,-}^u = \sigma_Y^{-u}, \quad \sigma_{F,-}^u = \sigma_G^{-u}, \quad \sigma_{G,-}^u = \sigma_F^{-u} .$$

(In words, $\sigma_{W,-}^u$ is just the complex conjugate of σ_W^u.) We note that for the purpose of our delegation protocols, we made a particular choice of the set Σ. The result generalizes to any constant-sized set of single-qubit Clifford observables, yielding a test for m-fold tensor products of single-qubit Clifford observables from Σ.

[6]We make the assumption that the players employ a pure-state strategy for convenience, but it is easy to check that all proofs extend to the case of a mixed strategy. Moreover, it is always possible to consider (as we do) projective strategies only by applying Naimark's dilation theorem, and adding an auxiliary local system to each player as necessary, since no bound is assumed on the dimension of their systems.

[7]See [38, Appendix A] for an extended discussion of this issue, with a similar resolution to ours.

Theorem 3.1. *Let $\varepsilon > 0$ and m an integer. Suppose that a strategy for the players succeeds with probability $1-\varepsilon$ in the test* RIGID(Σ, m)*. For $W \in \Sigma^m$ and $D \in \{A, B\}$ let $\{W_D^u\}_u$ be the measurement performed by player D on question W. Let also $|\psi\rangle$ be the state shared by the players. Then for $D \in \{A, B\}$ there exists an isometry*

$$V_D : \mathcal{H}_D \to (\mathbb{C}^2)^{\otimes m}_{D'} \otimes \mathcal{H}_{\widehat{D}}$$

and a state $|\textsc{aux}\rangle_{\widehat{A}\widehat{B}} \in \mathcal{H}_{\widehat{A}} \otimes \mathcal{H}_{\widehat{B}}$ such that

$$\left\|(V_A \otimes V_B)|\psi\rangle_{AB} - |\mathrm{EPR}\rangle^{\otimes m} \otimes |\textsc{aux}\rangle_{\widehat{A}\widehat{B}}\right\|^2 = O(\sqrt{\varepsilon}) , \tag{3.1}$$

and positive semidefinite matrices τ_λ on $\widehat{A}$ with orthogonal support, for $\lambda \in \{+,-\}$, such that $\mathrm{Tr}(\tau_+) + \mathrm{Tr}(\tau_-) = 1$ and

$$\begin{aligned} \mathop{E}_{W\in\Sigma^m} \sum_{u\in\{0,1\}^m} \Big\| V_A \mathrm{Tr}_B\big((\mathrm{Id}_A \otimes W_B^u)|\psi\rangle\langle\psi|_{AB}(\mathrm{Id}_A \otimes W_B^u)^\dagger\big) V_A^\dagger \\ - \sum_{\lambda\in\{\pm\}} \Big(\bigotimes_{i=1}^m \frac{\sigma^{u_i}_{W_i,\lambda}}{2}\Big) \otimes \tau_\lambda \Big\|_1 \\ = O(\mathrm{poly}(\varepsilon)). \end{aligned} \tag{3.2}$$

A symmetric relation holds with the roles of A and B exchanged. Moreover, players employing the honest strategy succeed with probability $1 - \mathrm{e}^{-\Omega(m)}$ in RIGID(Σ, m)*.*

We give some intuition for (3.2). In the honest strategy for RIGID(Σ, m), for any $W \in \Sigma^m$ the $\{W_\mathsf{B}^u\}_{u\in\{0,1\}^m}$ form a projective measurement on m qubits that consists in measuring the i-th qubit in the eigenbasis of the observable σ_W, for $i \in \{1, \dots, m\}$. Moreover, in the honest strategy the state $|\psi\rangle_\mathsf{AB}$ consists of m EPR pairs shared between the players. Therefore, the post-measurement state on $\mathcal{H}_\mathsf{A}$ associated with the outcome u when $\{W_\mathsf{B}^u\}_{u\in\{0,1\}^m}$ is performed on $\mathcal{H}_\mathsf{B}$ is (without renormalization) $\otimes_i(\frac{1}{2}\sigma^{u_i}_{W_i})$. In case the system $\hat{\mathsf{A}}$ is trivial (1-dimensional) and $\tau_+ = 1$, $\tau_- = 0$, (3.2) states that the post-measurement state for any successful strategy is close to the "ideal" post-measurement state. Informally the density matrices τ_λ, which live on $\mathcal{H}_{\hat{\mathsf{A}}}$, represent a "phase ambiguity" already discussed prior to the theorem statement: the malicious player B is allowed to use a strategy that is a mixture of two strategies, resulting in the post-measurement state being a mixture of two post-measurement states, the "ideal" one ($\lambda = 1$) and the "phase-flipped" one ($\lambda = -1$). Here it is important that τ_+ and τ_- have orthogonal, so that there is no overlap between the two components. This ambiguity is unavoidable since no test of the form considered here (that takes the form of a two-player one-round interaction) can distinguish between Y and Y^T, whose eigenvectors are swapped.

The statement of the theorem differs from more standard rigidity statements in providing guarantees on the initial shared state as well as certain post-measurement states that can be created by the players, as opposed to guarantees on the player's observables. The motivation for this is to write the theorem in a way that is easily usable in the other sections and in particular the analysis of the leash protocol from Section 4.

Before proceeding with the details we give an outline for the proof of Theorem 3.1. As already mentioned the test to which Theorem 3.1 applies is denoted $\textsc{rigid}(\Sigma, m)$. The goal of this test is to rigidly enforce that each players measures m qubits in a basis indicated by a string $W \in \Sigma^m$ when asked to do so, and reports the m-bit outcome.

The first ingredient to design the test $\textsc{rigid}(\Sigma, m)$ is an extension of the "Pauli braiding test" from [35] to handle tensor products of not only σ_X and σ_Z, but also σ_Y Pauli observables. This test is denoted $\textsc{pbt}(X, Y, Z)$ and described in Appendix A.4.3. The test would allow us to conclude if we had $\Sigma = \{X, Y, Z\}$. It remains to develop the ability to test for the single-qubit Clifford observables F and G as well as tensor products of them and X, Y, Z. Our strategy to do this is the following.

- First we introduce a test for a player making use of a unitary R that conjugates Paulis to Paulis in a prescribed way; for example we may test that $RXR = -Y$. Here we wrote "makes use of" because the test does not directly access the unitary R, which need not be a measurement observable (such as a binary observable). Instead the player is asked to measure according to the observable $X_R = \begin{pmatrix} 0 & R^\dagger \\ R & 0 \end{pmatrix}$. As a consequence the honest strategy for this test makes use of one more qubit than the number of qubits required to implement R. Our test for conjugation is called $\textsc{conj-cliff}(R)$ and described in Section 3.3. This test is based on a more general conjugation test introduced in Section 3.2, which is not restricted to Cliffords. Note that the test $\textsc{conj-cliff}(R)$ directly tests for m-qubit Clifford observables through their action on the m-qubit Clifford group, which can be tested using $\textsc{pbt}(X, Y, Z)$.

- The test $\textsc{conj-cliff}(R)$ allows us to test that a unitary respects the requisite conjugation relations. However, this is not sufficient in general, as for example F and $(-F)$ both have the same action on the Pauli group. When testing for observables that are associated with strings $W \in \Sigma^m$ we need to make sure that every time the symbol F appears it is the "same" observable that is used, and not sometimes its opposite (which would correspond to exchanging eigenvectors).[8] In Section 3.4 we introduce a test $\textsc{cliff}(\Sigma, m)$ which removes such inconsistencies by implementing a swap test between the (supposedly) same observable acting on different qubits. The swap test is realized by asking one player to measure in the Bell basis and the other, for instance, to measure FF, and the results are checked for consistency.

- Finally in Section 3.5 the test $\textsc{rigid}(\Sigma, m)$ is introduced. The only missing ingredient is to test that all the F observables are indeed F as intended, and not all $-F$. For this we perform tomography against the X and Z observables, which allows us to distinguish between the two eigenstates of F, thereby lifting the remaining ambiguity (and similarly for G).

We start by introducing the language required to formulate our testing results.

[8]Here "same" is in quotes because the observables act on different qubits"

3.1 Testing

In this section we recall the standard formalisms from self-testing, including state-dependent distance measure, local isometries, etc. We also introduce a framework of "tests for relations" that will be convenient to formulate our results.

3.1.1 Distance measures

Ultimately our goal is to test that a player implements a certain tensor product of single-qubit or two-qubit measurements defined by observables such as σ_X, σ_Y, or σ_G. Since it is impossible to detect whether a player applies a certain operation X on state $|\psi\rangle$, or $VXV^\dagger$ on state $V|\psi\rangle$, for any isometry $V : \mathrm{L}(\mathcal{H}) \to \mathrm{L}(\mathcal{H}')$ such that $V^\dagger V = \mathrm{Id}$, we will (as is standard in testing) focus on testing identity up to *local isometries*. Towards this, we introduce the following important piece of notation:

Definition 3.2. For finite-dimensional Hilbert spaces $\mathcal{H}_\mathsf{A}$ and $\mathcal{H}_{\mathsf{A}'}$, $\delta > 0$, and operators $R \in \mathrm{L}(\mathcal{H}_\mathsf{A})$ and $S \in \mathrm{L}(\mathcal{H}_{\mathsf{A}'})$ we say that R and S are δ-isometric with respect to $|\psi\rangle \in \mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B}$, and write $R \simeq_\delta S$, if there exists an isometry $V : \mathcal{H}_\mathsf{A} \to \mathcal{H}_{\mathsf{A}'}$ such that

$$\left\|(R - V^\dagger S V) \otimes \mathrm{Id}_\mathsf{B} \, |\psi\rangle\right\|^2 = O(\delta).$$

When $R = \{R_a\}$ and $S = \{S_a\}$ are POVM with the same set of outcomes we write $R_a \simeq_\delta S_a$ to mean

$$\sum_a \left\|(R_a - V^\dagger S_a V) \otimes \mathrm{Id}_\mathsf{B} \, |\psi\rangle\right\|^2 = O(\delta).$$

If V is the identity, then we further say that R and S are δ-equivalent, and write $R \approx_\delta S$ for $\|(R - S) \otimes \mathrm{Id}_\mathsf{B} \, |\psi\rangle\|^2 = O(\delta)$.

The notation $R \simeq_\delta S$ carries some ambiguity, as it does not specify the state $|\psi\rangle$. The latter should always be clear from context: we will often simply write that R and S are δ-isometric, without explicitly specifying $|\psi\rangle$ or the isometry. The relation is transitive, but not reflexive: the operator on the right will always act on a space of dimension at least as large as that on which the operator on the left acts. The notion of δ-equivalence is both transitive (its square root obeys the triangle inequality) and reflexive, and we will use it as our main notion of distance.

3.1.2 Strategies

Given a two-player game, or test, a strategy for the players consists of a bipartite entangled state $|\psi\rangle \in \mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B}$ together with families of projective measurements $\{W_\mathsf{A}^a\}$ for Alice and $\{W_\mathsf{B}^a\}$ for Bob, one for each question W that can be sent to either player in the test. (We often use the same symbol, a capital letter $X, Z, W, \ldots$, to denote a question in the game and the associated projective measurement $\{W^a\}$ applied by the player upon reception of that question.) Recall that to a projective measurement with outcomes in $\{0,1\}^n$ we associate a family of observables $W(u)$ parametrized by n-bit strings $u \in \{0,1\}^n$, defined by $W(u) = \sum_a (-1)^{u \cdot a} W^a$. If $n = 1$ we simply write $W = W(1) = W^0 - W^1$; note that $W(0) = \mathrm{Id}$.

As already mentioned, for convenience we restrict our attention to pure-state strategies employing projective measurements. We will loosely refer to a strategy for the players as $(W, |\psi\rangle)$, with the symbol W referring to the complete set of projective measurements used by the players in the game.

3.1.3 Consistency tests

We formulate our tests as two-player games in which both players are treated symmetrically. Specifically, when in a test we write "send one player the question X and the other the question Y" we implicitly mean that the role of "first player" and "second player" have been assigned at random, and moreover a player only gets told its question, not its "role" as assigned by the referee. Taking advantage of this symmetry we often omit the subscript A or B, as all statements involving observables for one player hold verbatim with the other player's observables as well.

With the exception of the Tomography Test TOM presented in Section 3.6, all the games we consider implicitly include a "consistency test" which is meant to enforce that whenever both players are sent identical questions, they produce matching answers.[9] More precisely, let T be any of the two-player tests described in the paper. Let $\Pr_T(W, W')$ be the distribution on questions (W, W') to the players that is specified by T. Since the players are always treated symmetrically, $\Pr_T(\cdot, \cdot)$ is permutation-invariant. Let $\Pr_T(\cdot)$ denote the marginal on either player. Then, instead of executing the test T as described, the verifier performs the following:

(i) With probability $1/2$, execute T.

(ii) With probability $1/2$, select a random question W according to $\Pr_T(W)$. Send W to both players. Accept if and only if the players' answers are equal.

Then, success with probability at least $1 - \varepsilon$ in the modified test implies success with probability at least $1 - 2\varepsilon$ in the original test, as well as in the consistency test. If $\{W_{\mathsf{A}}^a\}$ and $\{W_{\mathsf{B}}^b\}$ are the players' corresponding projective measurements and $|\psi\rangle_{\mathsf{AB}}$ their shared state, the latter condition implies

$$\begin{aligned}\sum_a \|(W_{\mathsf{A}}^a \otimes \mathrm{Id} - \mathrm{Id} \otimes W_{\mathsf{B}}^a)|\psi\rangle_{\mathsf{AB}}\|^2 &= 2 - 2\sum_a \langle\psi|_{\mathsf{AB}} W_{\mathsf{A}}^a \otimes W_{\mathsf{B}}^a |\psi\rangle_{\mathsf{AB}} \\ &\leq 4\varepsilon, \end{aligned} \tag{3.3}$$

so that $W_{\mathsf{A}}^a \otimes \mathrm{Id} \approx_\varepsilon \mathrm{Id} \otimes W_{\mathsf{B}}^a$ (where the condition should be interpreted on average over the choice of a question W distributed as in the test). Similarly, if W_{A}, W_{B} are observables for the players that succeed in the consistency test with probability $1-2\varepsilon$ we obtain $W_{\mathsf{A}} \otimes \mathrm{Id} \approx_\varepsilon \mathrm{Id} \otimes W_{\mathsf{B}}$. We will often use both relations to "switch" operators from one player's space to the other's; as a result we will also often omit an explicit specification of which player's space an observable is applied to.

[9] Here by a "test" we mean a named test, such as CONJ(A, B, R) or AC(X, Z). Since CONJ(A, B, R) uses AC(X, Z) as a subroutine, both the named subtest AC(X, Z) and the named test CONJ(A, B, R) are endowed with an additional consistency test.

3.1.4 Relations

We use $\mathcal{R}$ to denote a set of relations over matrix variables $X, Z, W, \ldots$, such as

$$\mathcal{R} = \{XZXZ = -\mathrm{Id},\ HX = ZH,\ \{X, Z, H\} \in \mathrm{Obs}\}.$$

Here the notation $\{X, Z, H\} \in \mathrm{Obs}$ means that each of the symbols in $\{X, Z, H\}$ satisfies the pair of relations, $\{X = X^\dagger, X^2 = \mathrm{Id}\}$ (since we consider only binary observables) and similarly for Z, H. Each relation implicitly imposes that the variables that appear in it have compatible dimension, e. g., $XZXZ = -\mathrm{Id}$ imposes that X, Z have the same dimension. We only consider relations that can be expressed in the form of one of the following equations:

- $(-1)^a W_1 \cdots W_k = \mathrm{Id}$, where the W_i are (not necessarily distinct) unitary variables and $a \in \mathbb{Z}_2$, or
- $W_1 \cdot (\sum_a \omega_a W_2^a) = \mathrm{Id}$, where W_1 is a unitary variable, $\{W_2^a\}$ a projective measurement with s possible outcomes, and ω_a are (arbitrary) s-th roots of unity.

Here what we mean by "unitary variable" and "projective measurement" is that when saying that a collection of matrices satisfies the relation, we always require that the matrices be unitary and a projective measurement), resp.; if they are not then by definition they do not satisfy the relation.

Definition 3.3 (Rigid self-test)**.** We say that a set $\mathcal{R}$ of relations is $(c, \delta(\varepsilon))$-testable, on average under the distribution $\mathcal{D} : \mathcal{R} \to [0, 1]$, if there exists a game (or test) G with question set $\mathcal{Q}$ such that the following holds. The set $\mathcal{Q}$ includes (at least) a symbol for each variable in $\mathcal{R}$ that is either an observable or a POVM. Moreover,

- (*Completeness*) There exists a set of operators which exactly satisfy all relations in $\mathcal{R}$ and a strategy for the players which uses these operators for the questions in $\mathcal{Q}$ that correspond to symbols appearing in the relations in $\mathcal{R}$ (together possibly with others for the additional questions) that has success probability at least c;
- (*Soundness*) For any $\varepsilon > 0$ and any strategy $(W, |\psi\rangle_{AB})$ that succeeds in the game with probability at least $c - \varepsilon$, the associated measurement operators satisfy the relations in $\mathcal{R}$ up to $\delta(\varepsilon)$. More precisely, on average over the choice of a relation $f(W) = \mathrm{Id}$ from $\mathcal{R}$ chosen according to $\mathcal{D}$, it holds that $\|(f(W) - \mathrm{Id}) \otimes \mathrm{Id}\, |\psi\rangle_{\mathsf{AB}}\|^2 \leq \delta(\varepsilon)$.

If both conditions hold, we also say that the game G is a robust $(c, \delta(\varepsilon))$ self-test for the set $\mathcal{R}$ of relations.

Most of the games we consider have perfect completeness, $c = 1$, in which case we omit explicitly mentioning the parameter. The distribution $\mathcal{D}$ will often be implicit from context, and we do not always specify it explicitly (e. g., in case we only measure $\delta(\varepsilon)$ up to multiplicative factors of order $|\mathcal{R}|$ the exact distribution $\mathcal{D}$ does not matter as long as it has complete support).

Definition 3.4 (Stable relations)**.** We say that a set of relations $\mathcal{R}$ is $\delta(\varepsilon)$-stable, on average under the distribution $\mathcal{D} : \mathcal{R} \to [0, 1]$, if for any state $|\psi\rangle \in \mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B}$ and families of operators $W_A \in \mathrm{L}(\mathcal{H}_\mathsf{A})$ and $W_B \in \mathrm{L}(\mathcal{H}_\mathsf{B})$ that are consistent on average, i. e.,

$$\mathop{\mathrm{E}}_{f\sim\mathcal{D}} \mathop{\mathrm{E}}_{W\in_U f} \left\|(\mathrm{Id} \otimes W_B - W_A \otimes \mathrm{Id})|\psi\rangle\right\|^2 \leq \varepsilon,$$

where $W \in_U f$ is shorthand for W being a uniformly random operator among those appearing in the relation specified by f, and satisfy the relations on average, i. e.,

$$\mathop{\mathrm{E}}_{\substack{f\sim\mathcal{D}:\\ f(W)=\mathrm{Id}\in\mathcal{R}}} \left\|(f(W_A) - \mathrm{Id}) \otimes \mathrm{Id}\,|\psi\rangle\right\|^2 \leq \varepsilon,$$

there exists operators $\hat{W}$ which satisfy the same relations exactly and are $\delta(\varepsilon)$-isometric to the W with respect to $|\psi\rangle$, on average over the choice of a random relation in $\mathcal{R}$ and a uniformly random W appearing in the relation, i. e., there exists an isometry V_A such that

$$\mathop{\mathrm{E}}_{f\sim\mathcal{D}} \mathop{\mathrm{E}}_{W\in_U f} \left\|(\hat{W}_A - V_A W_A) \otimes \mathrm{Id}\,|\psi\rangle\right\|^2 = O(\delta(\varepsilon)).$$

3.2 The conjugation test

We give a test which certifies that a unitary (not necessarily an observable) conjugates one observable to another. More precisely, let A, B be observables and R a unitary acting on the same space $\mathcal{H}$. The test $\textsc{conj}(A, B, R)$ certifies that the players implement observables of the form

$$X_R = \begin{pmatrix} 0 & R^\dagger \\ R & 0 \end{pmatrix} \qquad \text{and} \qquad C = C_{A,B} = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}, \tag{3.4}$$

such that moreover X_R and C commute. The fact that X_R is an observable implies that R is unitary,[10] while the commutation condition is equivalent to the relation $RAR^\dagger = B$. The test thus tests for the relations

$$\mathcal{C}\{R, C\} = \left\{\{X_R, C, X, Z\} \in \mathrm{Obs}\right\} \cup \left\{XZ = -ZX\right\} \cup \left\{X_R C = C X_R,\ X_R Z = -Z X_R,\ CZ = ZC\right\}.$$

Here the anti-commuting observables X and Z are used to specify a basis in which X_R and C can be block-diagonalized. The anti-commutation and commutation relations with Z enforce that X_R and C have the form described in (3.4). These relations are enforced using commutation and anti-commutation tests that are standard in the literature on self-testing. For convenience, we state those tests, $\textsc{com}$ and $\textsc{ac}$, in Appendix A. The conjugation test, which uses them as subtests, is given in Figure 4. Here, "Inputs" refers to a subset of designated questions in the test; "Relation" indicates a relation that the test aims to certify; "Test" describes the certification protocol. (Recall that all our protocols implicitly include a "consistency test", not specified on

[10]Note that R will not be directly accessed in the test, since by itself it does not necessarily correspond to a measurement.

the figure, in which a question is chosen uniformly at random from the marginal distribution and sent to both players, whose answers are accepted if and only if they are equal. We use this consistency test implicitly by analyzing only strategies that are symmetric, i. e., both provers' Hilbert spaces and measurement operators are identical.)

Test CONJ(A,B,R)

- Inputs: A, B, X, Z, X_R and C observables.
- Relations: $\mathcal{C}\{R, C\}$, with R defined from X_R, and C related to A and B, as in (3.4).
- Test: execute each of the following with equal probability

  (a) With probability $1/8$ each, execute tests $\textsc{ac}(X, Z)$, $\textsc{com}(C, Z)$, $\textsc{com}(X_R, C)$, $\textsc{ac}(X_R, Z)$ and $\textsc{com}(A, X)$, $\textsc{com}(B, X)$, $\textsc{com}(A, Z)$, $\textsc{com}(B, Z)$.

  (b) Ask one player to measure A, B, C or Z (with probability $1/4$ each), and the other to jointly measure A or B (with probability $1/2$ each) and Z. The first player returns one bit, and the second two bits. Make an acceptance decision as follows:

  – If the first player was asked C and the second player was asked (A, Z) then accept *unless* the second player's second answer bit is 0 and his first answer bit does not match the first player's;

  – If the first player was asked C and the second player was asked (B, Z) then accept *unless* the second player's second answer bit is 1 and his first answer bit does not match the first player's;

  – If the first player was asked A, B, or Z then accept if and only if his answer bit matches the corresponding answer from the second player.

  In all other cases, accept.

Figure 4: The conjugation test, $\textsc{conj}(A, B, R)$.

Lemma 3.5. *The test $\textsc{conj}(A, B, R)$ is a $(1, \delta)$ self-test for the set of relations $\mathcal{C}\{R, C\}$, for some $\delta = O(\sqrt{\varepsilon})$. Moreover, for any strategy that succeeds with probability at least $1 - \varepsilon$ in the test it holds that $C \approx_\delta A(\mathrm{Id} + Z)/2 + B(\mathrm{Id} - Z)/2$, where A, B, C and Z are the observables applied by the player on receipt of a question with the same label.*

Proof. Completeness is clear, as players making measurements on a maximally entangled state on $\mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}}$, tensored with an EPR pair on $\mathbb{C}^2_{\mathsf{A}'} \otimes \mathbb{C}^2_{\mathsf{B}'}$ for the X and Z observables, and using X_R and C defined in (3.4) (with the blocks specified by the space associated with each player's half-EPR pair) succeed in each test with probability 1.

We now consider soundness. Success in $\textsc{ac}(X, Z)$ in part (a) of the test implies the existence of local isometries V_A, V_B such that $V_A : \mathcal{H}_{\mathsf{A}} \to \mathcal{H}_{\hat{\mathsf{A}}} \otimes \mathbb{C}^2_{\mathsf{A}'}$, with $X \simeq_{\sqrt{\varepsilon}} \mathrm{Id}_{\hat{\mathsf{A}}} \otimes \sigma_X$ and $Z \simeq_{\sqrt{\varepsilon}} \mathrm{Id}_{\hat{\mathsf{A}}} \otimes \sigma_Z$. By Lemma A.3, approximate commutation with both X and Z enforced by the tests $\textsc{com}(A, X)$, $\textsc{com}(A, Z)$, $\textsc{com}(B, X)$ and $\textsc{com}(B, Z)$ implies that under the same isometry,

$$A \simeq_{\sqrt{\varepsilon}} A_I \otimes \mathrm{Id} \qquad \text{and} \qquad B \simeq_{\sqrt{\varepsilon}} B_I \otimes \mathrm{Id} \,, \tag{3.5}$$

for observables A_I, B_I on $\mathcal{H}_{\hat{\mathsf{A}}}$. Similarly, the parts of the test involving C and X_R imply that they each have the block decomposition specified in (3.4). In particular, using the second part of Lemma A.6 (with $n = 1$ and $c = 1$, exchanging the roles of Z and X) anti-commutation of X_R with Z certifies that X_R has a decomposition of the form

$$X_R \simeq_{\sqrt{\varepsilon}} R_X \otimes \sigma_X + R_Y \otimes \sigma_Y \,. \tag{3.6}$$

Let $R = (R_X + iR_Y)|R_X + iR_Y|^{-1}$, so that R is unitary. Note that since X_R is an observable, $X_R^2 = \mathrm{Id}$.

and so it follows from (3.6) that $(R_X + iR_Y)(R_X + iR_Y)^\dagger \otimes \mathrm{Id} \simeq_{\sqrt{\varepsilon}} \mathrm{Id}$. Thus $R \simeq_{\sqrt{\varepsilon}} R_X + iR_Y$. Similarly, using the first part of Lemma A.6 commutation of C with Z implies that

$$C \simeq_{\sqrt{\varepsilon}} C_I \otimes \sigma_I + C_Z \otimes \sigma_Z \,, \tag{3.7}$$

for Hermitian C_I, C_Z such that $C_I \pm C_Z$ are observables because C is an observable.

Next we analyze part (b) of the test. Let $\{W_{AZ}^{a,z}\}$ be the projective measurement applied by the second player upon query (A, Z). Success with probability $1 - O(\varepsilon)$ conditioned on the questions being C and (A, Z) item ensures that

$$\left|\langle\psi| C^0 \otimes (W_{AZ}^{00} + W_{AZ}^{01} + W_{AZ}^{11}) + C^1 \otimes (W_{AZ}^{10} + W_{AZ}^{01} + W_{AZ}^{11})|\psi\rangle\right| \geq 1 - O(\varepsilon), \tag{3.8}$$

and a similar condition holds for the case C and (B, Z), with W_{BZ} instead of W_{AZ}.

Success with probability $1 - O(\varepsilon)$ in the case of questions A, B or Z and (A, Z) or (B, Z) ensures consistency of $\{W_{AZ}^{a,z}\}$ and $\{W_{BZ}^{b,z}\}$, resp., with the observable A and B, resp., when marginalizing over the second outcome, and Z when marginalizing over the first outcome. Since A and B approximately commute with Z, using the decompositions for A and B derived in (3.5) it follows that $W_{AZ} \simeq_{\sqrt{\varepsilon}} A_I \otimes \sigma_Z$ and $W_{BZ} \simeq_{\sqrt{\varepsilon}} B_I \otimes \sigma_Z$.

Similarly regarding the observable C, using that we already showed in (3.7) that C is block-diagonal in the basis specified by X and Z, (3.8) and $W_{AZ} \simeq_{\sqrt{\varepsilon}} A_I \otimes \sigma_Z$ gives $(C_I^0 + C_Z^0) \simeq_{\sqrt{\varepsilon}} A_I^0$ and $(C_I^1 + C_Z^1) \simeq_{\sqrt{\varepsilon}} A_I^1$. Using the analogous relations for W_{BZ} we get $(C_I - C_Z) \simeq_{\sqrt{\varepsilon}} B_I$. Thus $C_I \simeq_{\sqrt{\varepsilon}} (A + B)/2$ and $C_Z \simeq_{\sqrt{\varepsilon}} (A - B)/2$. This shows the "Moreover" part of the lemma.

Finally, success in test COM(X_R, C) certifies the approximate commutation relation $[X_R, C] \simeq_{\sqrt{\varepsilon}} 0$, which, given the decomposition of X_R and C obtained so far, implies $RA \simeq_{\sqrt{\varepsilon}} BR$, as desired. □

3.3 Testing Clifford unitaries

Let $m \geq 1$ be an integer, and R an m-qubit Clifford unitary. R is characterized, up to phase, by its action by conjugation on the m-qubit Weyl-Heisenberg group. This action is described by linear functions $h_S : \{0,1\}^m \times \{0,1\}^m \to \{0,1\}$ and $h_X, h_Z : \{0,1\}^m \times \{0,1\}^m \to \{0,1\}^m$ such that

$$R\sigma_X(a)\sigma_Z(b)R^\dagger = (-1)^{h_S(a,b)}\sigma_X(h_X(a,b))\sigma_Z(h_Z(a,b)), \qquad \forall a, b \in \{0,1\}^m. \tag{3.9}$$

Using that $(\sigma_X(a)\sigma_Z(b))^\dagger = (-1)^{a\cdot b}\sigma_X(a)\sigma_Z(b)$, the same condition must hold of the right-hand side of (3.9), thus $h_X(a,b) \cdot h_Z(a,b) = a \cdot b \mod 2$. To any family of observables

$\{X(a), Z(b),\ a, b \in \{0,1\}^m\}$ satisfying the Pauli anti-commutation relations we associate, for $a, b \in \{0,1\}^m$,

$$A(a,b) = i^{a\cdot b} X(a)Z(b), \qquad B(a,b) = i^{a\cdot b} X(h_X(a,b))Z(h_Z(a,b)), \tag{3.10}$$

where the phase $i^{a\cdot b}$ is introduced to ensure that $A(a,b)$ and $B(a,b)$ are observables. Define X_R in terms of R, and $C(a,b)$ in terms of $A(a,b)$ and $B(a,b)$, as in (3.4). The Clifford conjugation test aims to test for the conjugation relation $X_R A(a,b) X_R^\dagger = B(a,b)$, for all (in fact, on average over a randomly chosen) (a,b). For this, we first need a test that ensures $A(a,b)$ and $B(a,b)$ themselves have the correct form, in terms of a tensor product of Pauli observables. Such a test was introduced in [35], where it is called "Pauli braiding test". The test certifies the Pauli relations

$$\begin{aligned}
\mathcal{P}^{(m)}\{X,Y,Z\} &= \Big\{W(a) \in \mathrm{Obs} \,:\, W \in \{X,Y,Z\}^m,\ a \in \{0,1\}^m\Big\} \\
&\cup \Big\{W(a)W'(a') = (-1)^{|\{i:\, W_i \neq W'_i \wedge a_i a'_i = 1\}|} W'(a')W(a) \,:\, W, W' \in \{X,Y,Z\}^n,\ a, a' \in \{0,1\}^m\Big\} \\
&\cup \Big\{W(a)W(a') = W(a+a') \,:\, W \in \{X,Y,Z\}^n,\ a, a' \in \{0,1\}^m\Big\}.
\end{aligned}$$

The Pauli braiding test, which is due to [35], allows to test for tensor products of σ_X and σ_Z Pauli observables. We recall the test in Appendix A.4.1. In Appendix A.4.3 we extend the test to include Pauli σ_Y. We refer to the extended test as PBT(X,Y,Z). For the extended test we can show the following; see Appendix A.4.3 for the proof.

Lemma 3.6. *Suppose $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ and $W(a) \in \mathrm{Obs}(\mathcal{H}_A)$, for $W \in \{X,Y,Z\}^m$ and $a \in \{0,1\}^m$, specify a strategy for the players that has success probability at least $1-\varepsilon$ in the extended Pauli braiding test* PBT(X,Y,Z) *described in Figure 32. Then there exist a state $|\textsc{aux}\rangle_{\hat{A}\hat{B}}$ and isometries $V_D : \mathcal{H}_D \to ((\mathbb{C}^2)^{\otimes m})_{D'} \otimes \hat{\mathcal{H}}_{\hat{D}}$, for $D \in \{A,B\}$, such that*

$$\Big\|(V_A \otimes V_B)|\psi\rangle_{AB} - |\mathrm{EPR}\rangle_{A'B'}^{\otimes m} |\textsc{aux}\rangle_{\hat{A}\hat{B}}\Big\|^2 = O(\sqrt{\varepsilon}),$$

and on expectation over $W \in \{X,Y,Z\}^m$,

$$\mathop{E}_{a\in\{0,1\}^m} \Big\|\big(W(a) - V_A^\dagger(\sigma_W(a) \otimes \Delta_W(a))V_A\big) \otimes \mathrm{Id}_B\, |\psi\rangle\Big\|^2 = O(\sqrt{\varepsilon}), \tag{3.11}$$

where $\Delta_W(a) = \prod_i \Delta_{W_i}^{a_i} \in \mathrm{Obs}(\mathcal{H}_{\hat{A}})$ are observables with $\Delta_X = \Delta_Z = \mathrm{Id}$ and Δ_Y an arbitrary observable on $\hat{\mathcal{H}}_{\hat{A}}$. Moreover, similar conditions hold on the B systems and

$$\Big\|\Delta_Y \otimes \Delta_Y |\textsc{aux}\rangle - |\textsc{aux}\rangle\Big\|^2 = O(\sqrt{\varepsilon}),$$

where as usual we use the same label for an observable acting on registers A or B.

Building on the Pauli braiding test and the conjugation test from the previous section, the Clifford conjugation test CONJ-CLIFF(R) described in Figure 5 provides a test for the set of relations

$$\begin{aligned}\mathcal{J}_{h_S,h_X,h_Z}\{R\} = \mathcal{P}^{(m)}\{X,Y,Z\} &\cup \{R \in \mathrm{U}\} \cup \{\Delta_Y \in \mathrm{Obs}\} \\ &\cup \left\{RX(a)Z(b)R^\dagger = \Delta_Y^{h_S(a,b)} X(h_X(a,b))Z(h_Z(a,b)) \,:\, a,b \in \{0,1\}^m\right\} \\ &\cup \left\{\Delta_Y X(a) = X(a)\Delta_Y,\ \Delta_Y Z(b) = Z(b)\Delta_Y \,:\, a,b \in \{0,1\}^m\right\}. \end{aligned} \tag{3.12}$$

Note the presence of the observable Δ_Y, which arises from the conjugation ambiguity in the definition of Y (see Lemma 3.6).

Test CONJ-CLIFF(R):

- Input: R an m-qubit Clifford unitary. Let h_S, h_X, h_Z be such that (3.9) holds, and $A(a,b), B(a,b)$ the observables defined in (3.10).
- Relations: $\mathcal{J}_{h_S,h_X,h_Z}\{R\}$ defined in (3.12).
- Test: execute each of the following with equal probability
  - (a) Execute test PBT(X,Y,Z) on $(m+1)$ qubits, where the last qubit is called the "control" qubit;
  - (b) Select $a,b \in \{0,1\}^m$ uniformly at random. Let $C(a,b)$ be the observable defined from $A(a,b)$ and $B(a,b)$ in (3.4), with the block structure specified by the control qubit. Execute test CONJ$\{A(a,b),B(a,b),R\}$. In the test, to specify query $A(a,b)$ or $B(a,b)$, represent each as a string in $\{I,X,Y,Z\}^m$ (omitting the additional phase i, which is applied by the prover but not specified explicitly on the query label) and use the same label as for the same query when it is used in part (a).

Figure 5: The Clifford conjugation test, CONJ-CLIFF(R).

Lemma 3.7. *Let R be an m-qubit Clifford unitary and h_S, h_X, h_Z such that (3.9) holds. Suppose a strategy for the players succeeds with probability at least $1-\varepsilon$ in test CONJ-CLIFF(R). Let $V_A : \mathcal{H}_A \to ((\mathbb{C}^2)^{\otimes(m+1)})_{A'} \otimes \mathcal{H}_{\hat{A}}$ be the isometry whose existence follows from part (a) of the test, and Δ_Y the observable on $\mathcal{H}_{\hat{A}}$, that represents the phase ambiguity (see Lemma 3.6). Then there exists a unitary Λ_R on $\mathcal{H}_{\hat{A}}$ and another unitary Λ_R on $\mathcal{H}_{\hat{B}}$, such that each commutes with Δ_Y on the same system and*

$$\left\|\Lambda_R \otimes \Lambda_R |\textsc{aux}\rangle - |\textsc{aux}\rangle\right\|^2 = O(\mathrm{poly}(\varepsilon)), \tag{3.13}$$

where $|\textsc{aux}\rangle$ is the state defined in Lemma 3.6. Moreover, let $\hat{\tau}_R$ be any m-qubit Clifford unitary, acting on the space $(\mathbb{C}^2)^{\otimes m}$ into which the isometry V_A maps, which satisfies the relations specified in (3.9), where for any location $i \in \{1,\dots,m\}$ such that $a_i = b_i = 1$ we replace $\sigma_X\sigma_Z$ by $\tau_Y = \sigma_Y \otimes (i\Delta_Y)$.[11]

[11]Note that $\hat{\tau}_R$ is uniquely defined up to phase.

Then, letting $\tau_R = \hat{\tau}_R(\mathrm{Id}_{A'} \otimes \Lambda_R)$ *we have that under the same isometry,*

$$R \simeq_{\mathrm{poly}(\varepsilon)} \tau_R.$$

In the lemma, the unitary Λ_R is necessary because whenever a unitary R satisfies the relations (3.9) the unitary $R \otimes \Lambda_R$ satisfies them as well, where Λ_R is any unitary acting on an ancilla system. In Section 3.5 we show that these unitaries can be ignored when looking at post-measurement states in the protocol, which is what will ultimately be important for us.

Note that $\hat{\tau}_R$ is only defined up to phase in the lemma. Any representative will do, as the phase ambiguity can be absorbed in Λ_R. As an example, in this notation we have

$$\hat{\tau}_F = \frac{1}{\sqrt{2}}\big(-\sigma_X + \sigma_Y \otimes \Delta_Y\big), \qquad \hat{\tau}_G = \frac{1}{\sqrt{2}}\big(\sigma_X + \sigma_Y \otimes \Delta_Y\big), \tag{3.14}$$

where the "honest" single-qubit Clifford observables σ_F and σ_G are defined in (2.2).

Completeness of the test is clear, as players making measurements on $(m+1)$ shared EPR pairs using standard Pauli observables, R, and $C(a,b)$ defined in (3.4) with $A(a,b)$ and $B(a,b)$ as in (3.10) will pass all tests with probability 1.

Proof sketch. For $D \in \{A, B\}$ let V_D be the isometries that follow from part (a) of the test and Lemma 3.6. According to (3.10), $A(a,b)$ and $B(a,b)$ can each be expressed (up to phase) as a tensor product of X, Y, Z operators, where the number of occurrences of Y modulo 2 is $a \cdot b$ for $A(a,b)$ and $h_X(a,b) \cdot h_Z(a,b) = a \cdot b \mod 2$ for $B(a,b)$. Thus the labels used to specify the observables in $A(a,b)$ and $B(a,b)$ in part (b), together with the analysis of part (a) and Lemma 3.6, imply that under the same isometry we have

$$A(a,b) \simeq_{\sqrt{\varepsilon}} \sigma_X(a)\sigma_Z(b) \otimes (i\Delta_Y)^{a\cdot b} \text{ and } B(a,b) \simeq_{\sqrt{\varepsilon}} \sigma_X(h_X(a,b))\sigma_Z(h_Z(a,b)) \otimes (i\Delta_Y)^{a\cdot b + h_S(a,b)},$$

where the imaginary phase comes from (3.10). Applying the analysis of the conjugation test given in Lemma 3.5 shows that X_R must have the form in (3.4), for some R that approximately conjugates $A(a,b)$ to $B(a,b)$, on average over uniformly random $a, b \in \{0,1\}^m$.

Let $\hat{\tau}_R$ be as defined in the lemma. Note that $\hat{\tau}_R$ acts on $\mathcal{H}_{\mathsf{A}'}$ and $\mathcal{H}_{\hat{\mathsf{A}}}$. After application of the isometry, R has an expansion

$$R \simeq \hat{\tau}_R \cdot \Big(\sum_{a,b} \sigma_X(a)\sigma_Z(b) \otimes \Lambda_R(a,b)\Big), \tag{3.15}$$

for arbitrary $\Lambda_R(a,b)$ on $\mathcal{H}_{\hat{\mathsf{A}}}$; since $\hat{\tau}_R$ is invertible such an expansion exists for any operator. Using the approximate version of (3.9) certified by the conjugation test (Lemma 3.5),

$$RV_A^\dagger\big(\sigma_X(a)\sigma_Z(b) \otimes \Delta_Y^{a\cdot b}\big)V_A \approx V_A^\dagger\big(\sigma_X(h_X(a,b))\sigma_Z(h_Z(a,b)) \otimes \Delta_Y^{a\cdot b + h_S(a,b)}\big)V_A R,$$

where the approximation holds on average over a uniformly random choice of (a,b) and up to error that is polynomial in ε but independent of m. Expanding out R and using the consistency relations between the two players,

$$\sum_{c,d} \hat{\tau}_R\Big(\sigma_X(c)\sigma_Z(d) \otimes \Lambda_R(c,d)\Big) \otimes \Big((-1)^{a\cdot b}\sigma_X(a)\sigma_Z(b) \otimes \Delta_Y^{a\cdot b}\Big)$$
$$\approx \sum_{c,d} \Big(\sigma_X(h_X(a,b))\sigma_Z(h_Z(a,b)) \otimes \Delta_Y^{a\cdot b+h_S(a,b)}\Big)\, \hat{\tau}_R\,\Big(\sigma_X(c)\sigma_Z(d) \otimes \Lambda_R(c,d)\Big) \otimes \mathrm{Id}\,, \tag{3.16}$$

where the factor $(-1)^{a\cdot b}$ comes from using

$$\big(\sigma_X(a)\sigma_Z(b) \otimes \mathrm{Id}\,\big)|\mathrm{EPR}\rangle^{\otimes m} \;=\; \big(\,\mathrm{Id} \otimes \big(\sigma_X(a)\sigma_Z(b)\big)^T\big)|\mathrm{EPR}\rangle^{\otimes m}\;.$$

The approximation in (3.16) and the following equations are meant on average over uniformly random $a,b \in \{0,1\}^n$. Using the conjugation relations satisfied, by definition, by $\hat{\tau}_R$, the right-hand side of (3.16) simplifies to

$$\sum_{c,d} \hat{\tau}_R\Big(\sigma_X(a)\sigma_Z(b)\sigma_X(c)\sigma_Z(d) \otimes \Delta_Y^{a\cdot b}\Lambda_R(c,d)\Big) \otimes \mathrm{Id}\,. \tag{3.17}$$

Next using the fact that the state on which the approximations are measured is maximally entangled across registers A and B together with the Pauli (anti-)commutation relations to simplify the left-hand side of (3.16), together with (3.17) we arrive at the approximation

$$\sum_{c,d} \Big((-1)^{a\cdot d+b\cdot c}\sigma_X(a+c)\sigma_Z(b+d) \otimes \Lambda_R(c,d)\Big) \otimes \Big(\,\mathrm{Id} \otimes \Delta_Y^{a\cdot b}\Big)$$
$$\approx \sum_{c,d} \Big(\sigma_X(a+c)\sigma_Z(b+d) \otimes \Delta_Y^{a\cdot b}\Lambda_R(c,d)\Big) \otimes \mathrm{Id}\,.$$

If $(c,d) \neq (0,0)$ a fraction about half of all (a,b) such that $a\cdot b = 0$ satisfy $a\cdot d + b\cdot c = 1$. Using that $\{\sigma_X(a)\sigma_Z(b) \otimes \mathrm{Id}\,|\mathrm{EPR}\rangle\}$ are orthogonal for different (a,b), the above then implies that $\Lambda_R(c,d) \approx -\Lambda_R(c,d)$, on average over $(c,d) \neq (0,0)$. Hence $\Lambda_R(c,d) \approx 0$, on average over $(c,d) \neq (0,0)$. Considering (a,b) such that $a\cdot b = 1$ implies that $\Lambda_R(0,0)$ approximately commutes with Δ_Y. Finally, the relation (3.13) follows from consistency of X_R with itself implicitly enforced in the test (see Section 3.1.3). □

3.4 Tensor products of single-qubit Clifford observables

We turn to testing observables in the m-fold direct product of the Clifford group. Although the test can be formulated more generally, for our purposes it will be sufficient to specialize it to the case where each element in the direct product is an observable taken from the set $\Sigma = \{X,Y,Z,F,G\}$ associated with the single-qubit Pauli observables defined in Section 2.1. Recall that the associated operators satisfy the conjugation relation $\sigma_Y\sigma_F\sigma_Y = \sigma_G$, which will be tested as part of our procedures (specifically, item (c) in Figure 6).

The test is described in Figure 6. It is divided in five parts. Part (a) of the test executes CONJ-CLIFF(W) to verify that an observable $W \in \Sigma^m$ satisfies the appropriate Pauli conjugation relations (3.9). Note that a priori test CONJ-CLIFF(W) only tests for the observable X_W obtained from W in blocks as X_R from R in (3.4) (indeed, in that test W need not be an observable). Thus part (b) of the test is introduced to verify that $X_W \approx WX(e_{m+1})$, where the $(m+1)$-st qubit is the one used to specify the block decomposition relating X_W to W. The result of parts (a) and (b) is that, under the same isometry as used to specify the Pauli X and Z, $W \simeq \hat{\tau}_W \cdot (\mathrm{Id} \otimes \Lambda_W)$, according to the same decomposition as shown in Lemma 3.7. The goal of the remaining three parts of the test is to verify that $\Lambda_W = \Lambda_F^{|\{i: W_i \in \{F,G\}\}|}$, for a single observable Λ_F. For this, part (c) of the test verifies that Λ_W only depends on the locations at which $W_i \in \{F, G\}$, but not on the specific observables at those locations. Part (d) verifies that $\Lambda_W \approx \prod_{i: W_i \in \{F,G\}} \Lambda_i$ for commuting observables Λ_i. Finally, part (e) checks that Λ_i is (approximately) independent of i.

Test $\textsc{cliff}(\Sigma, m)$:

- Input: An integer m and a subset $\Sigma = \{X, Y, Z, F, G\}$ of the single-qubit Clifford group.
- Test: Select $W \in \Sigma^m$ uniformly at random. Execute each of the following with equal probability:
  (a) Execute the test $\textsc{conj-cliff}(W)$;
  (b) Send one player either the query W, or X_W and the other $(W, X(e_{m+1}))$, where e_{m+1} indicates the control qubit used for part (a). Receive one bit from the first player, and two from the second. If the query to the first player was W, check that the first player's answer is consistent with the second player's first answer bit. If the query to the first player was X_W, then: If the second player's second bit is 0, check that his first bit is consistent with the first player's; If the second player's second bit is 1, check that his first bit is different than the first player's.
  (c) Let S and T be subsets of the positions in which $W_i = F$ and $W_i = G$, respectively, are chosen uniformly at random. Let W' equal W except $W'_i = G$ for $i \in S$, and $W'_i = F$ for $i \in T$. Let $R = Y(\sum_{i \in S \cup T} e_i)$. Execute test $\textsc{conj}(W, W', R)$.
  (d) Set $W'_i = X, Y, F, G_i$ whenever $W_i = Y, X, G_i, F$, respectively. Set $W'_i = X$ whenever $W_i = Z$. Execute test $\textsc{pbt}(W, W')$ on m qubits.
  (e) Let S and T be subsets of (non-overlapping) pairs of positions in which $W_i = F$ and $W_i = G$, respectively, chosen uniformly at random. Send one player the query W, with entries $(i, j) \in S \cup T$ removed and replaced by $\Phi_{i,j}$ (indicating a measurement in the Bell basis).
    - With probability $1/2$, send the other player the query W. Check consistency of outcomes associated with positions not in $S \cup T$. For outcomes in $S \cup T$, check the natural consistency as well. E. g., if the Bell measurement indicated the outcome Φ_{00}, then the two outcomes reported by the other player at those locations should be identical.
    - With probability $1/2$, execute an independent copy of the Bell measurement test BELL (Figure 29) between the first and second players in each of the pair of qubits in $S \cup T$.

Figure 6: The m-qubit Clifford test, $\textsc{cliff}(\Sigma, m)$.

Theorem 3.8. *Suppose a strategy for the players succeeds in test* CLIFF(Σ, m) *(Figure 6) with probability at least* $1 - \varepsilon$*. Then for* $D \in \{A, B\}$ *there exists an isometry*

$$V_D : \mathcal{H}_D \to (\mathbb{C}^2)^{\otimes m}_{D'} \otimes \mathcal{H}_{\hat{D}}$$

such that

$$\left\| (V_A \otimes V_B)|\psi\rangle_{AB} - |\mathrm{EPR}\rangle^{\otimes m}_{A'B'} |\textsc{aux}\rangle_{\hat{A}\hat{B}} \right\|^2 = O(\sqrt{\varepsilon}), \tag{3.18}$$

and

$$\mathop{E}_{W \in \Sigma^m,\, c \in \{0,1\}^m} \left\| \mathrm{Id}_A \otimes \big(V_B W(c) - \tau_W(c) V_B\big) |\psi\rangle_{AB} \right\|^2 = O(\mathrm{poly}(\varepsilon)). \tag{3.19}$$

Here τ_W *is defined from* W *as in Lemma 3.7, with* $\Lambda_{W_i} = \mathrm{Id}$ *if* $W_i \in \{X, Y, Z\}$ *and* $\Lambda_{W_i} = \Lambda_F$ *if* $W_i \in \{F, G\}$*, where* Λ_F *is an observable on* $\mathcal{H}_{\hat{B}}$ *that commutes with* Δ_Y*.*

Proof sketch. We indicate all steps of the proof, but omit some of the more routine calculations for legibility. The existence of the isometry, as well as (3.18) and (3.19) for $W \in \{I, X, Y, Z\}^m$, follows from the test PBT(X, Y, Z), executed as part of the Clifford conjugation test from part (a), and Lemma 3.6. Using part (a) of the test and Lemma 3.7 it follows that every $W \in \Sigma^m$ is mapped under the same isometry to

$$W \simeq_{\sqrt{\varepsilon}} \tau_W = \hat{\tau}_W (\mathrm{Id} \otimes \Lambda_W), \tag{3.20}$$

where $\hat{\tau}_W$ is as defined in the lemma and Λ_W is an observable on $\mathcal{H}_{\hat{A}}$ which may depend on the whole string W; here we also use the consistency check in part (b) to relate the observable X_W used in the Clifford conjugation test with the observable W used in part (c). Note that from the definition we can write $\hat{\tau}_W = \otimes_i \hat{\tau}_{W_i}$, where in particular $\hat{\tau}_X = \sigma_X$, $\hat{\tau}_Z = \sigma_Z$ and $\hat{\tau}_Y = \sigma_Y \otimes \Delta_Y$.

The analysis of the conjugation test given in Lemma 3.5 shows that success with probability $1 - O(\varepsilon)$ in part (c) of the test implies the relations

$$\begin{aligned} \hat{\tau}_W \tau_R (\mathrm{Id} \otimes \Lambda_W) &= \tau_R \hat{\tau}_W (\mathrm{Id} \otimes \Lambda_W) \\ &\approx_{\sqrt{\varepsilon}} \hat{\tau}_{W'} \tau_R (\mathrm{Id} \otimes \Lambda_{W'}), \end{aligned}$$

where the first equality is by definition of τ_R, and uses that $\tau_Y = \sigma_Y \otimes \Delta_Y$ and Δ_Y commutes with Λ_W; the approximation holds as a consequence of the conjugation test and should be understood on average over a uniformly random choice of $W \in \Sigma^m$. Thus Λ_W depends only on the locations at which $W_i \in \{F, G\}$, but not on the particular values of the observables at those locations.

Part (d) of the test and Lemma 3.6 imply that the observables $W(a)$ satisfy approximate linearity conditions $W(a)W(a') \approx W(a + a')$, on average over a uniformly random choice of $W \in \Sigma^n$ and $a, a' \in \{0,1\}^n$. Using the form (3.20) for W and the fact that the $\hat{\tau}_W(a)$ satisfy the linearity relations by definition, we deduce that $\Lambda_{W(a)} \Lambda_{W(a')} \approx \Lambda_{W(a+a')}$ as well. Using the analysis of the Pauli braiding test (Lemma 3.6), this implies that for each i and W_i there is an observable Λ_{i,W_i} such that the Λ_{i,W_i} pairwise commute and $\Lambda_W \approx \prod_i \Lambda_{i,W_i}$. Using the preceding observations, $\Lambda_{i,W_i} \approx \Lambda_i$ if $W_i \in \{F, G\}$, and $\Lambda_{i,W_i} \approx \mathrm{Id}$ if $W_i \in \{X, Y, Z\}$.

Success in part (e) of the test implies the condition $\mathrm{E}_W \langle \psi | W \otimes W_\Phi | \psi \rangle \geq 1 - O(\varepsilon)$, where W is distributed as in the test, and W_Φ is the observable applied by the second player upon a query W, with some locations, indexed by pairs in S and T, have been replaced by the Φ symbol (as described in the test). Let U be the set of i such that $W_i \in \{F, G\}$. Since Δ_Y commutes with all observables in play, for clarity let us assume in the following that $\Delta_Y = \mathrm{Id}$. From the decomposition of the observables W obtained so far and the analysis of the test BELL given in Lemma A.4 it follows that

$$W \simeq \Big(\otimes_i \hat{\tau}_{W_i}\Big) \otimes \Big(\prod_{i\in U} \Lambda_i\Big), \quad \text{and} \quad W_\Phi \simeq \Big(\otimes_{i\notin S\cup T} \hat{\tau}_{W_i}\Big) \otimes \Big(\otimes_{(i,j)\in S\cup T} \mathrm{SW}_{i,j}\Big) \otimes \Big(\prod_{i\in U\setminus S\cup T} \Lambda_i\Big),$$

where the ordering of tensor products does not respect the ordering of qubits, but it should be clear which registers each operator acts on. Using that for any operators A, B and Δ,

$$\langle \mathrm{EPR}|^{\otimes 2}\big(A \otimes B \otimes |\Phi_{00}\rangle\langle\Phi_{00}|\big)|\mathrm{EPR}\rangle^{\otimes 2} = \frac{1}{8}\,\mathrm{Tr}\big(AB^T\big),$$

the above conditions imply

$$\mathop{\mathrm{E}}_{S=\{(s_i,s_i')\}}\ \mathop{\mathrm{E}}_{T=\{(t_i,t_i')\}} \Lambda_{s_i}\Lambda_{s_i'}\Lambda_{t_i}\Lambda_{t_i'} \approx \mathrm{Id},$$

where the expectation is taken over sets S and T specified as in part (e), for a given W, and on average over the choice of W. Let $\Lambda = \mathrm{E}_i\,\Lambda_i$. By an averaging argument it follows that for U the set of locations such that $W_i \in \{F, G\}$, $\prod_{i\in U}\Lambda_i \approx \Lambda^{|S|}$, again on average over the choice of W. To conclude we let $\Lambda_F = \Lambda/|\Lambda|$, which is an observable and satisfies the required conditions. □

3.5 Post-measurement states

We prove Theorem 3.1. The remaining work consists in "lifting" the phase ambiguity Λ_W which remains in the statement of Theorem 3.8 (in contrast to the ambiguity Δ_Y, which itself cannot be lifted solely by examining correlations). This ambiguity means that the players have the liberty of choosing to report opposite outcomes whenever they apply an F or G observable, but they have to be consistent between themselves and across all of their qubits in doing so. To verify that the provers use the "right" labeling for their outcomes we incorporate a small tomography test. Our final test RIGID(Σ, m), which builds on all tests developed in this section, is described in Figure 7. Note that a drawback of the tomography is that the test no longer achieves perfect completeness (although completeness remains exponentially close to 1).

Test $\textsc{rigid}(\Sigma, m)$:

- Input: An integer m and a subset $\Sigma = \{X, Y, Z, F, G\}$ of the single-qubit Clifford group.
- Test: execute each of the following with equal probability:
  - (a) Execute the test $\textsc{cliff}(\Sigma, m)$;
  - (b) Send each player a uniformly random query $W, W' \in \Sigma^m$. Let $T \subseteq \{1, \dots, m\}$ be the subset of positions i such that $W_i \in \{X, Y\}$ and $W'_i \in \{F, G\}$. Reject if the fraction of answers (a_i, b_i), for $i \in T$, from the players that satisfy the CHSH correlations (i. e., $a_i \neq b_i$ if and only if $(W_i, W'_i) = (X, F)$) is not at least $\cos^2 \frac{\pi}{8} - 0.1$.

Figure 7: The n-qubit rigidity test, $\textsc{rigid}(\Sigma, m)$.

Proof of Theorem 3.1. From Theorem 3.8 and part (a) we get isometries V_A, V_B and commuting observables Δ_Y, Λ_F on $\mathcal{H}_{\hat{\mathsf{A}}}$ such that the conclusions of the theorem hold. Write the eigendecomposition $\Delta_Y = \Delta_Y^+ - \Delta_Y^-$ and $\Lambda_F = \Lambda_F^+ - \Lambda_F^-$. For $\lambda \in \{+, -\}^2$ let

$$\tau_\lambda = \mathrm{Tr}_{\hat{\mathsf{B}}}\Big(\big(\mathrm{Id}_{\hat{\mathsf{A}}} \otimes \Delta_Y^{\lambda_1} \Lambda_F^{\lambda_2}\big) |\textsc{aux}\rangle\langle\textsc{aux}| \big(\mathrm{Id}_{\hat{\mathsf{A}}} \otimes \Delta_Y^{\lambda_1} \Lambda_F^{\lambda_2}\big)\Big).$$

Using that Δ_Y and Λ_F commute and satisfy

$$\Delta_Y \otimes \Delta_Y |\textsc{aux}\rangle \approx \Lambda_F \otimes \Lambda_F |\textsc{aux}\rangle \approx |\textsc{aux}\rangle$$

it follows that the (subnormalized) densities τ_λ have (approximately) orthogonal support. In particular the provers' strategy in part (b) of the test is well-approximated by a mixture of four strategies, labeled by $(\lambda_Y, \lambda_F) \in \{\pm 1\}^2$, such that the strategy with label (λ_Y, λ_F) uses the observables

$$(X, Z, Y, F, G) = \Big(\sigma_X,\ \sigma_Z,\ \lambda_Y \sigma_Y,\ \frac{1}{\sqrt{2}} \lambda_F\big(-\sigma_X + \lambda_Y \sigma_Y\big),\ \frac{1}{\sqrt{2}} \lambda_F\big(\sigma_X + \lambda_Y \sigma_Y\big)\Big).$$

Among these four strategies, the two with $\lambda_F = -1$ fail part (b) of the test with probability exponentially close to 1. Success in both parts of the test with probability at least $1 - 2\varepsilon$ each thus implies

$$\mathrm{Tr}\big(\tau_{+-}\big) + \mathrm{Tr}\big(\tau_{--}\big) = \mathrm{poly}(\varepsilon). \tag{3.21}$$

For $W \in \Sigma^m$ and $c \in \{0, 1\}^m$ the observable $W(c) = \otimes_i W_i^{c_i}$ can be expanded in terms of a 2^m-outcome projective measurement $\{W^u\}$ as

$$W(c) = \sum_{u \in \{0,1\}^m} (-1)^{u \cdot c}\, W^u.$$

Similarly, by definition the projective measurement associated with the commuting Pauli observables $\tau_W(c) = \otimes_i \tau_{W_i}^{c_i}$, $c \in \{0, 1\}^m$, is

$$\tau_W^u = \bigotimes_i \Big(\mathop{\mathrm{E}}_{c \in \{0,1\}^m} (-1)^{u \cdot c} \tau_W(c)\Big).$$

Thus,

$$\begin{aligned}
&\mathop{\mathrm{E}}_{c\in\{0,1\}^m}\left\|\mathrm{Id}_A\otimes\big(W(c)-V_B^\dagger\tau_W(c)V_B\big)|\psi\rangle_{\mathsf{AB}}\right\|^2\\
&\quad=\mathop{\mathrm{E}}_{c\in\{0,1\}^m}\left\|\sum_u(-1)^{u\cdot c}\,\mathrm{Id}_A\otimes\big(W^u-V_B^\dagger\tau_W^uV_B\big)|\psi\rangle_{\mathsf{AB}}\right\|^2\\
&\quad=\sum_{u\in\{0,1\}^m}\left\|\mathrm{Id}_A\otimes\big(W^u-V_B^\dagger\tau_W^uV_B\big)|\psi\rangle_{\mathsf{AB}}\right\|^2,
\end{aligned}\tag{3.22}$$

where the third line is obtained by expanding the square and using $\mathrm{E}_{c\in\{0,1\}^m}(-1)^{v\cdot c}=1$ if $v=0^m$, and 0 otherwise. Using (3.19), the expression in (3.22), when averaged over all $W\in\Sigma^m$, is bounded by $O(\mathrm{poly}(\varepsilon))$. Using the Fuchs-van de Graaf inequality and the fact that trace distance cannot increase under tracing out, we get that the following is $O(\mathrm{poly}(\varepsilon))$:

$$\mathop{\mathrm{E}}_{W\in\Sigma^m}\sum_u\left\|V_A\mathrm{Tr}_{\mathsf{B}}\big((\mathrm{Id}_{\mathsf{A}}\otimes W^u)|\psi\rangle\langle\psi|(\mathrm{Id}_{\mathsf{A}}\otimes W^u)^\dagger\big)V_A^\dagger-\mathrm{Tr}_{\mathsf{B}}\big((\mathrm{Id}_{\mathsf{A}}\otimes\tau_W^u)|\psi\rangle\langle\psi|(\mathrm{Id}_{\mathsf{A}}\otimes\tau_W^u)^\dagger\big)\right\|_1.\tag{3.23}$$

Using that $\tau_X=\sigma_X$, $\tau_Z=\sigma_Z$, and $\tau_Y=\sigma_Y\Delta_Y$, we deduce the post-measurement states for $u\in\{\pm1\}$

$$\tau_X^u=\sigma_X^u,\qquad\tau_Z^u=\sigma_Z^u,\qquad\tau_Y^u=\sigma_Y^u\otimes(\tau_{++}+\tau_{+-})+\sigma_Y^{-u}\otimes(\tau_{-+}+\tau_{--}).$$

Similarly, from $\tau_F=(-\tau_X+\tau_Y)\Lambda_F$ and $\tau_G=(\tau_X+\tau_Y)\Lambda_F$ we get, e. g., that the +1 eigenspace of τ_F is the combination of:

- The simultaneous +1 eigenspace of $\sigma_F=(-\sigma_X+\sigma_Y)/\sqrt{2}$, +1 eigenspace of Δ_Y, and +1 eigenspace of Λ_F;
- The simultaneous −1 eigenspace of σ_F, +1 eigenspace of Δ_Y, and −1 eigenspace of Λ_F;
- The simultaneous −1 eigenspace of $\sigma_G=-(-\sigma_X-\sigma_Y)/\sqrt{2}$, −1 eigenspace of Δ_Y, and +1 eigenspace of Λ_F;
- The simultaneous +1 eigenspace of σ_G, −1 eigenspace of Δ_Y, and −1 eigenspace of Λ_F.

Proceeding similarly with τ_G, we obtain

$$\begin{aligned}
\tau_F^u&=\sigma_F^u\otimes\tau_{++}+\sigma_F^{-u}\otimes\tau_{+-}+\sigma_G^{-u}\otimes\tau_{-+}+\sigma_G^u\otimes\tau_{--},\\
\tau_G^u&=\sigma_G^u\otimes\tau_{++}+\sigma_G^{-u}\otimes\tau_{+-}+\sigma_F^{-u}\otimes\tau_{-+}+\sigma_F^u\otimes\tau_{--}.
\end{aligned}$$

Starting from (3.23) and using (3.18) we obtain

$$\begin{aligned}
&\mathop{\mathrm{E}}_{W\in\Sigma^m}\sum_u\Big\|V_A\mathrm{Tr}_{\mathsf{B}}\big((\mathrm{Id}_{\mathsf{A}}\otimes W^u)|\psi\rangle\langle\psi|(\mathrm{Id}_{\mathsf{A}}\otimes W^u)^\dagger\big)V_A^\dagger\\
&\qquad-\mathrm{Tr}_{\mathsf{B}}\big((\mathrm{Id}_{\mathsf{A}}\otimes\tau_W^u)|\mathrm{EPR}\rangle\langle\mathrm{EPR}|^{\otimes m}\otimes|\textsc{aux}\rangle\langle\textsc{aux}|_{\hat{\mathsf{A}}\hat{\mathsf{B}}}(\mathrm{Id}_{\mathsf{A}}\otimes\tau_W^u)^\dagger\big)\Big\|_1=O(\mathrm{poly}(\varepsilon)).
\end{aligned}$$

Since $\mathrm{Tr}_{\mathsf{B}}(\mathrm{Id}\otimes B|\mathrm{EPR}\rangle\langle\mathrm{EPR}|_{\mathsf{AB}}\,\mathrm{Id}\otimes B^\dagger)=(B^\dagger B)^T/2$ for any single-qubit operator B, to conclude the bound claimed in the theorem it only remains to apply the calculations above and use (3.21) to eliminate the contribution of τ_{+-} and τ_{--}; the factor $\frac{1}{2}$ comes from the reduced density matrix of an EPR pair. □

3.6 Tomography

Theorem 3.8 and Theorem 3.1 show that success in test RIGID(Σ, m) gives us control over the players' observables and post-measurement states in the test. This allows us to use one of the players to perform some kind of limited tomography (limited to post-measurement states obtained from measurements in Σ), that will be useful for our analysis of the Dog-Walker Protocol from Section 5.[12]

Let $1 \le m' \le m$ and consider the test TOM(Σ, m', m) described in Figure 8. In this test, one player is sent a question $W \in \Sigma^m$ chosen uniformly at random. Assuming the players are also successful in the test RIGID(Σ, m) (which can be checked independently, with some probability), using that the input distribution μ in RIGID(Σ, m) assigns weight at least $|\Sigma|^{-m}/2$ to any $W' \in \Sigma^m$, from Theorem 3.1 it follows that the second player's post-measurement state is close to a state consistent with the first player's reported outcomes. Now suppose the second player is sent a random subset $S \subseteq [m]$ of size $|S| = m'$, and is allowed to report an arbitrary string $W' \in \Sigma^{m'}$, together with outcomes u. Suppose also that for each $i \in S$, we require that $u_i = a_i$ whenever $W'_i = W_i$. Since the latter condition is satisfied by a constant fraction of $i \in \{1, \dots, m'\}$, irrespective of W', with very high probability, it follows that the only possibility for the second player to satisfy the condition is to actually measure his qubits precisely in the basis that he indicates. This allows us to check that a player performs a measurement of its choice correctly (i. e., the player is forced to report the correct measurement made).

Tomography Test TOM(Σ, m', m):

- Input: Integer $1 \le m' \le m$ and a subset $\Sigma = \{X, Y, Z, F, G\}$ of the single-qubit Clifford group.
- Test: Let $S \subseteq [m]$ be chosen uniformly at random among all sets of size $|S| = m'$. Select $W \in \Sigma^m$ uniformly at random. Send W to the first player, and the set S to the second. Receive a from the first player, and $W' \in \Sigma^{m'}$ and u from the second. Accept only if $a_i = u_i$ whenever $i \in S$ and $W_i = W'_i$.

Figure 8: The m-qubit tomography test TOM(Σ, m', m).

Corollary 3.9. *Let $\varepsilon > 0$ and $1 \le m' \le m$ integer. Suppose a strategy for the players succeeds with probability $1 - \varepsilon$ in both tests* RIGID(Σ, m) *(Figure 7) and* TOM(Σ, m', m) *(Figure 8). Let V_A, V_B be the isometries specified in Theorem 3.1. Let $\{Q^{W',u}\}$ be the projective measurement applied by the second*

[12] The tomography test described in this section is different from subtest (b) in RIGID(Σ, m) (Figure 7). The tomography test described here is more general and designed to verify that a player prepares post-measurement states of its choice.

player in TOM(Σ, m', m). *Then there exists a distribution q on $\Sigma^{m'} \times \{\pm\}$ such that*

$$\sum_{W' \in \Sigma^{m'}} \sum_{u \in \{\pm 1\}^{m'}} \Big\| \mathrm{Tr}_{A\hat{B}}\big((\mathrm{Id}_A \otimes V_B Q^{W',u})|\psi\rangle\langle\psi|_{AB}(\mathrm{Id}_A \otimes V_B Q^{W',u})^\dagger\big) - \sum_{\lambda \in \{\pm\}} q(W', \lambda)\Big(\bigotimes_{i=1}^{m'} \frac{1}{2}\sigma^{u_i}_{W'_i,\lambda}\Big)\Big\|_1 = O(\mathrm{poly}(\varepsilon)),$$

where the notation is the same as in Theorem 3.1.

Moreover, players employing the honest strategy succeed with probability 1 *in the* TOM(Σ, m', m).

Proof. Success in RIGID(Σ, m) allows us to apply Theorem 3.1. For any (W', u) let $\rho^{W',u}_{\mathsf{A}',\lambda}$ be the post-measurement state on the first player's space, conditioned on the second player's answer in test TOM(Σ, m', m) being (W', u), after application of the isometry V_A, and conditioned on $\mathcal{H}_{\hat{\mathsf{A}}}$ being in a state that lies in the support of τ_λ (note this makes sense since τ_+, τ_- have orthogonal support). Using that for any $i \in S$, $W_i = W'_i$ with constant probability $|\Sigma|^{-1}$, it follows from (3.1) and (3.2) in Theorem 3.1 that success in TOM(Σ, m) implies the condition

$$\mathop{\mathrm{E}}_{\substack{S \subseteq \{1,\dots,m\} \\ |S| = m'}} \sum_{W', \lambda, u} \mathrm{Tr}(\tau_\lambda)\,\mathrm{Tr}\Big(\Big(\frac{|\Sigma| - 1}{|\Sigma|}\,\mathrm{Id} + \frac{1}{|\Sigma|} \otimes_{i \in S} \sigma^{u_i}_{W'_i,\lambda}\Big)\rho^{W',u}_{\mathsf{A}',\lambda}\Big) = 1 - O(\mathrm{poly}(\varepsilon)). \tag{3.24}$$

Eq (3.24) concludes the proof, for some distribution $q(W', \lambda) \approx \sum_u \mathrm{Tr}(\rho^{W',u}_{\mathsf{A}',\lambda})\mathrm{Tr}(\tau_\lambda)$ (the approximation is due to the fact that the latter expression only specifies a distribution up to error $O(\mathrm{poly}(\varepsilon))$. □

4 The Verifier-on-a-Leash protocol

4.1 Protocol and statement of results

The Verifier-on-a-Leash Protocol (or "Leash Protocol" for short) involves a classical verifier and two quantum provers. The idea behind the Leash Protocol is to have a first prover, nicknamed PV for Prover V, carry out the quantum part of V_{EPR} from Broadbent's EPR Protocol by implementing the procedure V^r_{EPR}.[13] A second prover, nicknamed PP for Prover P, will play the part of the prover P_{EPR}. Unlike in the EPR Protocol, the interaction with PV (i. e., running V^r_{EPR}) will take place first, and PV will be asked to perform random measurements from the set $\Sigma = \{X, Y, Z, F, G\}$. The values $\vec{z}$, rather than being chosen at random, will be chosen based on the corresponding choice of observable. We let n be the number of input bits and t be the number of T gates in Q.

The protocol is divided into two subgames; which game is played is chosen by the verifier by flipping a biased coin with probability $(p_r, p_d = 1 - p_r)$.

[13] Throughout this section we assume that the circuit Q provided as input is compiled in the format described in Section 2.4, which also provides a summary of the protocol and a description of V_{EPR}.

- The first game is a sequential version of the rigidity game $\textsc{rigid}(\Sigma, m)$ described in Figure 11. This aims to enforce that PV performs precisely the right measurements;
- The second game is the delegation game, described in Figures 12, 13, and 14, and whose structure is summarized in Figure 9. Here the verifier guides PP through the computation in a similar way as in the EPR Protocol.

We call the resulting protocol the Leash Protocol with parameters (p_r, p_d). In both subgames the parameter $m = \Theta(n+t)$ is chosen large enough so that with probability close to 1 each symbol in Σ appears in a random $W \in \Sigma^m$ at least $n+t$ times. It is important that PV is not able to tell which kind of game is being played. Notice also that in order to ensure blindness, we will require that the interaction with PV in the delegation game is sequential (more details on this are found in Section 4.4). In order for the two subgames to be indistinguishable, we also require that the rigidity game $\textsc{rigid}(\Sigma, m)$ be played sequentially (i. e., certain subsets of questions and answers are exchanged sequentially, but the acceptance condition in the test is the same). Note, importantly, that the rigidity guarantees of $\textsc{rigid}(\Sigma, m)$ hold verbatim when the game is played sequentially, since this only reduces the number of ways that the provers can cheat. The following theorem states the guarantees of the Leash Protocol.

Theorem 4.1. *There are constants $p_r, p_d = 1 - p_r$, and $\Delta > 0$ such that the following hold of the Verifier-on-a-Leash Protocol with parameters (p_r, p_d), when executed on an input $(Q, |\vec{x}\rangle)$.*

- (Completeness:) *Suppose that $\|\Pi_0 Q|\vec{x}\rangle\|^2 \geq 2/3$. Then there is a strategy for PV and PP that is accepted with probability at least $p_{\text{compl}} = p_r(1 - \mathrm{e}^{-\Omega(n+t)}) + 8p_d/9$.*
- (Soundness:) *Suppose that $\|\Pi_0 Q|\vec{x}\rangle\|^2 \leq 1/3$. Then any strategy for PV and PP is accepted with probability at most $p_{\text{sound}} = p_{\text{compl}} - \Delta$.*

Further, for any strategy of PV and PP, the reduced state of PV and PP, resp., at the end of the leash protocol is independent of the input $\vec{x}$, aside from its length.

The proof of the completeness property is given in Lemma 4.2. The soundness property is shown in Lemma 4.5. Blindness is established in Section 4.4. We first give a detailed description of the protocol. We start by describing the delegation game, specified in Figures 12, 13 and 14, which describe the protocol from the verifier's view, an honest PV's view, and an honest PP's view, respectively. This will motivate the need for a sequential version of the game $\textsc{rigid}(\Sigma, m)$, described in Figure 11. As we will show, the rigidity game forces PV to behave honestly. Thus, for the purpose of exposition, we assume for now that PV behaves honestly, which results in the joint behavior of PV and V being similar to that of the verifier V_{EPR} in the EPR Protocol.

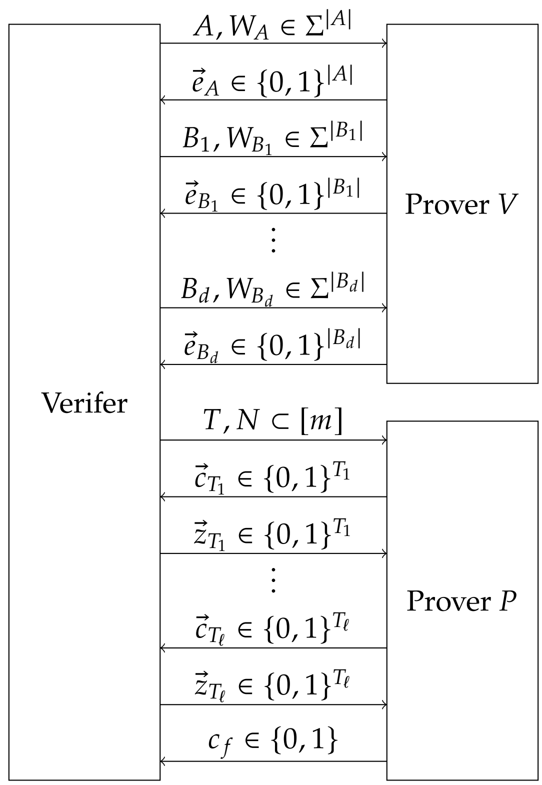


Figure 9: Structure of the delegation game.

From the rigidity game we may also assume that PV and PP share m EPR pairs, labeled $\{1,\ldots,m\}$, for $m = \Theta(n+t)$. We will assume that the circuit Q is broken into d layers, $Q = Q_1 \ldots Q_d$, such that in every Q_ℓ, each wire has at most one T gate applied to it, after which no other gates are applied to that wire. We will refer to d as the T-depth of the circuit. We will suppose the T gates are indexed from 1 to t, in order of layer.

The protocol begins with an interaction between the verifier and PV. The verifier selects a uniformly random partition $A, B_1, \ldots, B_d$ of $\{1,\ldots,m\}$, with $|A| = \Theta(n)$, and for every $\ell \in \{1,\ldots,d\}$, $|B_\ell| = \Theta(t_\ell)$, where t_ℓ is the number of T gates in Q_ℓ. The verifier also selects a uniformly random $W \in \Sigma^m$, and partitions it into substrings W_A and $W_{B_1},\ldots,W_{B_d}$, meant to contain observables to initialize the computation qubits and auxiliary qubits, respectively, for each layer of T gates. The verifier instructs PV to measure his halves of the EPR pairs using the observables W_A first, and then $W_{B_1},\ldots,W_{B_d}$, sequentially. Upon being instructed to measure a set of observables, PV measures the corresponding half-EPR pairs and returns the results $\vec{e}$ to the verifier. Breaking this interaction into multiple rounds is meant to enforce that, for example, the results output by PV upon receiving W_{B_ℓ}, which we call $\vec{e}_{B_\ell}$, cannot depend on the choice of observables $W_{B_{\ell+1}}$. This is required for blindness.

Once the interaction with PV has been completed, as in the EPR Protocol, V selects one of three run types: computation ($r = 0$), X-test ($r = 1$), and Z-test ($r = 2$). The verifier selects a subset $N \subset A$ of size n of qubits to play the role of inputs to the computation. These are chosen from the subset of A corresponding to wires that PV has measured in the appropriate observable for the run type (see Table 4). For example, in an X-test run, PV's EPR halves corresponding to input wires should be measured in the Z basis so that PP is left with a one-time pad of the state $|0\rangle^{\otimes n}$, so in an X-test run, the computation wires are chosen from the set $\{i \in A : W_i = Z\}$. The input wires N are labeled by $\mathcal{X}_1, \ldots, \mathcal{X}_n$.

The verifier also chooses subsets $T_\ell = T_\ell^0 \cup T_\ell^1 \subset B_\ell$ where T_ℓ^0 and T_ℓ^1 have sizes $t_{\ell,0}$ and $t_{\ell,1} = t_\ell - t_{\ell,0}$, respectively, where $t_{\ell,0}$ is the number of odd T gates in the ℓ-th layer of Q (recall the definition of even and odd T gates from Section 2.4). The wires T_ℓ^0 and T_ℓ^1 will play the role of auxiliary states used to perform T gates from the ℓ-th layer. They are chosen from those wires from B_ℓ whose corresponding EPR halves have been measured in a correct basis, depending on the run type. For example, in an X-test run, the auxiliaries corresponding to odd T gates should be prepared by measuring the corresponding EPR half in either the X or Y basis (see Table 3), so in an X-test run, T_ℓ^1 is chosen from $\{i \in B_\ell : W_i \in \{X, Y\}\}$ (see Table 4). We will let $\mathcal{T}_1, \ldots, \mathcal{T}_t$ label those EPR pairs that will be used as auxiliary states. In particular, the system $\mathcal{T}_i$ will be used for the i-th T gate in the circuit, so if the i-th T gate is even, $\mathcal{T}_i$ should be chosen from $T^0 = \cup_\ell T_\ell^0$, and otherwise it should be chosen from $T_1 = \cup_\ell T_\ell^1$. The verifier sends labels $\mathcal{T}_1, \ldots, \mathcal{T}_t$ and $\mathcal{X}_1, \ldots, \mathcal{X}_n$ to PP, who will act as P_{EPR} on the $n + t$ qubits specified by these labels.

Just as in the EPR Protocol, the input on PP's system specified by $\mathcal{X}_1, \ldots, \mathcal{X}_n$ is a quantum one-time pad of either $|\vec{x}\rangle$, $|0\rangle^{\otimes n}$, or $|+\rangle^{\otimes n}$, depending on the run type, with V holding the keys (determined by $\vec{e}$). Throughout the interaction, PP always maintains a one-time pad of the current state of the computation, with the verifier in possession of the one-time-pad keys. The verifier updates her keys as the computation is carried out, using the rules in Table 2.

From PP's perspective, the protocol works just as the EPR Protocol, except that he does not receive the bit z_i needed to implement the T gadget until *during* the T gadget, after he has sent V his measurement result c_i (see Figure 10).

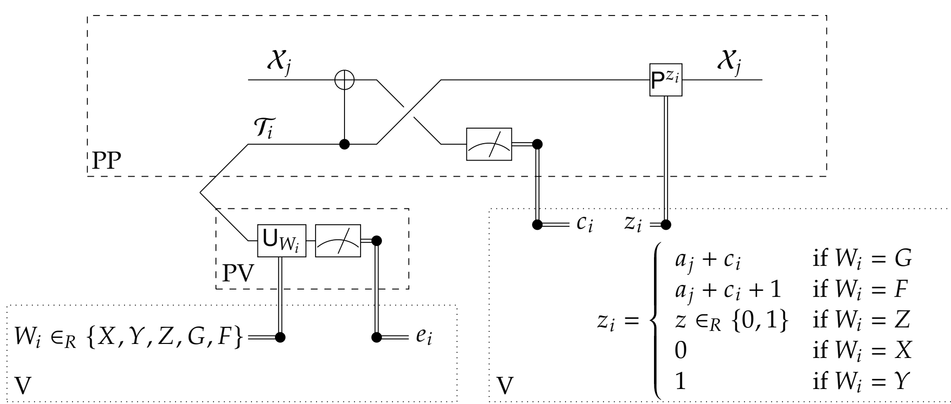


Figure 10: The gadget for implementing the i-th T gate, on the j-th wire.

To perform the i-th T gate on the j-th wire, PP performs the circuit shown in Figure 10. As Figure 10 shows, PV has already applied the observable specified by V to his half of the EPR pair. The T gadget requires interaction with the verifier, to compute the bit z_i, which depends on the measured c_i, the value W_i, and one-time-pad key a_j, however, this interaction can be done in parallel for T gates in the same layer.

It is simple to check that the T gadget in Figure 10 is the same as the T gadget for the EPR Protocol shown in Figure 1. Note that in the EPR Protocol, we let a'_i denote the one-time-pad key of the j-th wire just before application of the i-th T gate (to the j-th wire). Here we will assume a_j denotes the current updated one-time-pad key of the jth wire, so it is the same as a'_i in the EPR Protocol. In the case of the leash protocol, W is chosen at random, and then $\vec{z}$ is chosen accordingly, whereas in the case of the EPR Protocol, $\vec{z}$ is chosen at random and then W is chosen accordingly.

	Computation Run	X-test Run	Z-test Run
N	$\{i \in A : W_i = Z\}$	$\{i \in A : W_i = Z\}$	$\{i \in A : W_i = X\}$
T_ℓ^0	$\{i \in B_\ell : W_i \in \{G,F\}\}$	$\{i \in B_\ell : W_i = Z\}$	$\{i \in B_\ell : W_i \in \{X,Y\}\}$
T_ℓ^1	$\{i \in B_\ell : W_i \in \{G,F\}\}$	$\{i \in B_\ell : W_i \in \{X,Y\}\}$	$\{i \in B_\ell : W_i = Z\}$

Table 4: How the verifier chooses index sets $T = T^0 \cup T^1$ and N for each type of run. These sets determine which systems are labeled by $\{\mathcal{T}_i\}_{i=1}^t$ and $\{\mathcal{X}_j\}_{j=1}^n$, respectively.

Let m, n, and $t_1,\ldots,t_d$ be parameters provided as input, such that $m = \Theta(n + t_1 + \cdots + t_d)$.

1. The verifier selects questions W, W', for the first and second player, respectively, according to the distribution of questions in the game $\textsc{rigid}(\Sigma, m)$.

2. If $W \notin \Sigma^m$ or $W' \notin \Sigma^m$:

   (a) The verifier partitions $\{1,\ldots,m\}$ at random into subsets A and B_ℓ, for $\ell \in \{1,\ldots,d\}$, of size $|A| = \Theta(n)$ and $|B_\ell| = \Theta(t_\ell)$, exactly as in Step 1 of Figure 12.

   (b) The verifier sends $(A, W_A), (B_1, W_{B_1}), .., (B_d, W_{B_d})$ and $(A, W'_A), (B_1, W'_{B_1}), .., (B_d, W'_{B_d})$ in sequence to the first and second prover, respectively. They sequentially return $\vec{e}_A \in \{0,1\}^{|A|}$, $\vec{e}_{B_1} \in \{0,1\}^{|B_1|}, .., \vec{e}_{B_d} \in \{0,1\}^{|B_d|}$ and $\vec{e}'_A \in \{0,1\}^{|A|}$, $\vec{e}'_{B_1} \in \{0,1\}^{|B_1|}, .., \vec{e}'_{B_d} \in \{0,1\}^{|B_d|}$, respectively. Let $\vec{e}, \vec{e}'$ be the concatenation of $\vec{e}_{B_i}$ and $\vec{e}'_{B_i}$ in the correct order.

3. Otherwise: *(which happens when the verifier sends instructions for Bell measurements)*

   (a) The verifier sends W and W' to the first and second prover, respectively.

   (b) The first and second prover answer back with $\vec{e}$ and $\vec{e}'$, respectively.

4. The verifier accepts if and only if $\vec{e}, \vec{e}'$ and W, W' satisfy the winning condition of $\textsc{rigid}(\Sigma, m)$.

Figure 11: Sequential version of $\textsc{rigid}(\Sigma, m)$.

Let $(Q, \vec{x})$ be the input to the verifier, where Q is compiled in the form described in Section 2.4. Let n be the size of the input to Q. Let d be the T-depth, and for $\ell \in \{1, \ldots, d\}$ let t_ℓ be the number of T gates in the ℓ-th layer.

1. The verifier selects $W \in_R \Sigma^m$. She partitions $\{1, \ldots, m\}$ arbitrarily into non-overlapping subsets A and $B_1, \ldots, B_d$ such that W_A contains at least n copies of each symbol in Σ, and for each $\ell \in \{1, \ldots, d\}$, W_{B_ℓ} contains at least t_ℓ copies of each symbol in Σ.
2. The verifier sends A, W_A to PV, who returns $\vec{e}_A \in \{0,1\}^A$. The verifier sequentially sends $(B_1, W_{B_1}), \ldots, (B_d, W_{B_d})$ to PV, each time receiving $\vec{e}_{B_\ell} \in \{0,1\}^{B_\ell}$ as answer.
3. The verifier selects a run type uniformly at random. She selects sets $N \subseteq A$ and $T_\ell \subseteq B_\ell$, for $\ell \in \{1, \ldots, d\}$, of sizes $|N| = n$ and $|T_\ell| = t_\ell$, as follows:

   Computation Run: N is chosen at random from $\{i \in A : W_i = Z\}$. T_ℓ is chosen at random from $\{i \in B_\ell : W_i \in \{G, F\}\}$. She sets $\vec{a} = \vec{e}_N + \vec{x}$ and $\vec{b} = 0^n$.

   X**-test Run:** N is chosen at random from $\{i \in A : W_i = Z\}$. $T_\ell = T_\ell^0 \cup T_\ell^1$, where T_ℓ^0 is of size $t_{\ell,0}$ chosen at random from $\{i \in B_\ell : W_i = Z\}$ and T_ℓ^1 is of size $t_{\ell,1}$ chosen at random from $\{i \in B_\ell : W_i \in \{X, Y\}\}$. She sets $\vec{a} = \vec{e}_N$ and $\vec{b} = 0^n$.

   Z**-test Run:** N is chosen at random from $\{i \in A : W_i = X\}$. $T_\ell = T_\ell^0 \cup T_\ell^1$, where T_ℓ^0 is of size $t_{\ell,0}$ chosen at random from $\{i \in B_\ell : W_i \in \{X, Y\}\}$ and T_ℓ^1 is of size $t_{\ell,1}$ chosen at random from $\{i \in B_\ell : W_i = Z\}$. She sets $\vec{a} = 0^n$ and $\vec{b} = \vec{e}_N$.

   The verifier sends the sets N and T_ℓ^0, T_ℓ^1, for all $\ell \in \{1, \ldots, d\}$, to PP.
4. For $\ell = 1, \ldots, d$,
   (a) For each Clifford gate in the ℓ-th layer, perform the appropriate key update (Table 2).
   (b) The verifier receives $\vec{c} = \{c_i\}_{i \in T_\ell}$ from PP. If it is an X-test run and $i \in T_\ell^0$, or it is a Z-test run and $i \in T_\ell^1$, reject if $c_i \neq a_j + e_i$, where j is the wire to which the i-th T gate is applied.
   (c) For each $i \in T_\ell$, the verifier computes $\vec{z} = \{z_i\}_{i \in T_\ell}$ as follows:

   Computation Run $z_i = a_j + 1_{W_i = F} + c_i$;

   X**-test Run** if $i \in T_\ell^0$, $z_i \in_R \{0,1\}$; else if $i \in T_\ell^1$, $z_i = 1_{W_i = Y}$;

   Z**-test Run** if $i \in T_\ell^0$, $z_i = 1_{W_i = Y}$; else if $i \in T_\ell^1$, $z_i \in_R \{0,1\}$.

   (d) The verifier sends $\vec{z}$ to PP and updates keys for each T gate applied (Table 2).
5. The verifier receives a bit c_f from PP. She outputs reject if it is a computation or X-test run and $c_f + a_f \neq 0$, where a_f is the final X-key on the output wire; and accept otherwise.

Figure 12: The Delegation Game: Verifier's point of view. Note that the condition $c_i \neq a_j + e_i$ is the same as the condition $c_i \neq a'_i + e_i$ in the EPR Protocol — a_j here and a'_i in the EPR Protocol both represent the one-time-pad key just before application of the i-th T gate.

1. For $\ell = 0, 1, \ldots, d$,
   (a) PV receives a string $W_S \in \Sigma^S$, for some subset S of $\{1, \ldots, m\}$, from V.
   (b) For $i \in S$, PV measures his half of the i-th EPR pair using the observable indicated by W_i, obtaining an outcome $e_i \in \{0, 1\}$.
   (c) PV returns $\vec{e}_S$ to V.

Figure 13: Honest strategy for PV in the Delegation game

Before describing the Delegation game, we present now the sequential version of the game $\textsc{rigid}(\Sigma, m)$ (Figure 11). We notice that this sequential version is no different than $\textsc{rigid}(\Sigma, m)$, except for the fact that certain subsets of questions and answers are exchanged sequentially, but with the same acceptance condition. Running the game sequentially only reduces the provers' ability to cheat, hence the guarantees from $\textsc{rigid}(\Sigma, m)$ hold verbatim for the sequential version.

We now give the precise protocols for the delegation game V (Figure 12) and honest provers PV (Figure 13) and PP (Figure 14).

1. PP receives subsets N and T_ℓ^0, T_ℓ^1 of $\{1, \ldots, m\}$, for $\ell \in \{1, \ldots, d\}$, from the verifier.
2. For $\ell = 1, \ldots, d$,
   (a) PP does the Clifford computations in the ℓ-th layer.
   (b) For each $i \in T_\ell = T_\ell^0 \cup T_\ell^1$, PP applies a CNOT from $\mathcal{T}_i$ into the input register corresponding to the wire on which this T gate should be performed, $\mathcal{X}_j$, and measures this wire to get a value c_i. The register $\mathcal{T}_i$ is relabeled $\mathcal{X}_j$. He sends $\vec{c}_{T_\ell} = \{c_i\}_{i \in T_\ell}$ to V.
   (c) PP receives $\vec{z}_{T_\ell} = \{z_i\}_{i \in T_\ell}$ from V. For each $i \in T_\ell$, he applies P^{z_i} to the corresponding $\mathcal{X}_j$.
3. PP performs the final computations that occur after the d-th layer of T gates, measures the output qubit, $\mathcal{X}_1$, and sends the resulting bit, c_f, to V.

Figure 14: Honest strategy for PP in the Delegation game

With all of these subprotocols in hand, we can now present the Leash protocol (Figure 15). Figure 16 illustrates the tree-like structure of all the different subgames and tests used within the protocol.

1. With probability p_r, the players run the sequential version of RIGID(Σ, m) as described in Figure 11.

2. With probability p_d, the players run the delegation game, described in Figures 12, 13, and 14.

Figure 15: Leash protocol with parameters p_r and p_d.

4.2 Leash completeness

The honest provers in the Leash Protocol are essentially executing the EPR Protocol, with the only difference being that in the case of the leash protocol, W is chosen at random and then $\vec{z}$ is chosen accordingly, whereas in the case of the EPR Protocol, $\vec{z}$ is chosen at random and then W is chosen accordingly. The resulting distribution on $\vec{z}$ and W is the same, and so completeness follows from that of the EPR Protocol.

Lemma 4.2. *Suppose the verifier executes the rigidity game with probability p_r and the delegation game with probability $p_d = 1 - p_r$, on an input $(Q, |\vec{x}\rangle)$ such that $\|\Pi_0 Q|\vec{x}\rangle\|^2 \geq 2/3$. Then there is a strategy for the provers which is accepted with probability at least $p_{\mathrm{compl}} = p_r(1 - \mathrm{e}^{-\Omega(n+t)}) + \frac{8}{9}p_d$.*

Proof. The provers PV and PP play the rigidity game in accordance with the honest strategy, and the delegation game as described in Figures 13 and 14, respectively. Their success probability in the delegation game is the same as the honest strategy in the EPR Protocol, which is at least $\frac{2}{3} + \frac{2}{3}\frac{1}{3} = \frac{8}{9}$, by Theorem 2.2 and since the verifier chooses each of the three types of runs uniformly. ◻

4.3 Leash soundness

We divide the soundness analysis into three parts. First we analyze the case of an honest PV, and a cheating PP (Lemma 4.3). Then we show that if PV and PP pass the rigidity game with almost optimal probability, then one can construct new provers PV′ and PP′, with PV′ honest, such that the probability that they are accepted in the delegation game is not changed by much (Lemma 4.4). In Lemma 4.5, we combine the previous to derive the desired constant soundness-completeness gap, where we exclude that the acceptance probability of the provers in the rigidity game is too low by picking a p_r large enough.

Lemma 4.3 (Soundness against PP). *Suppose the verifier executes the delegation game on input $(Q, |\vec{x}\rangle)$ such that $\|\Pi_0 Q|\vec{x}\rangle\|^2 \leq 1/3$ with provers (PV, PP^*) such that PV plays the honest strategy. Then the verifier accepts with probability at most $7/9$.*

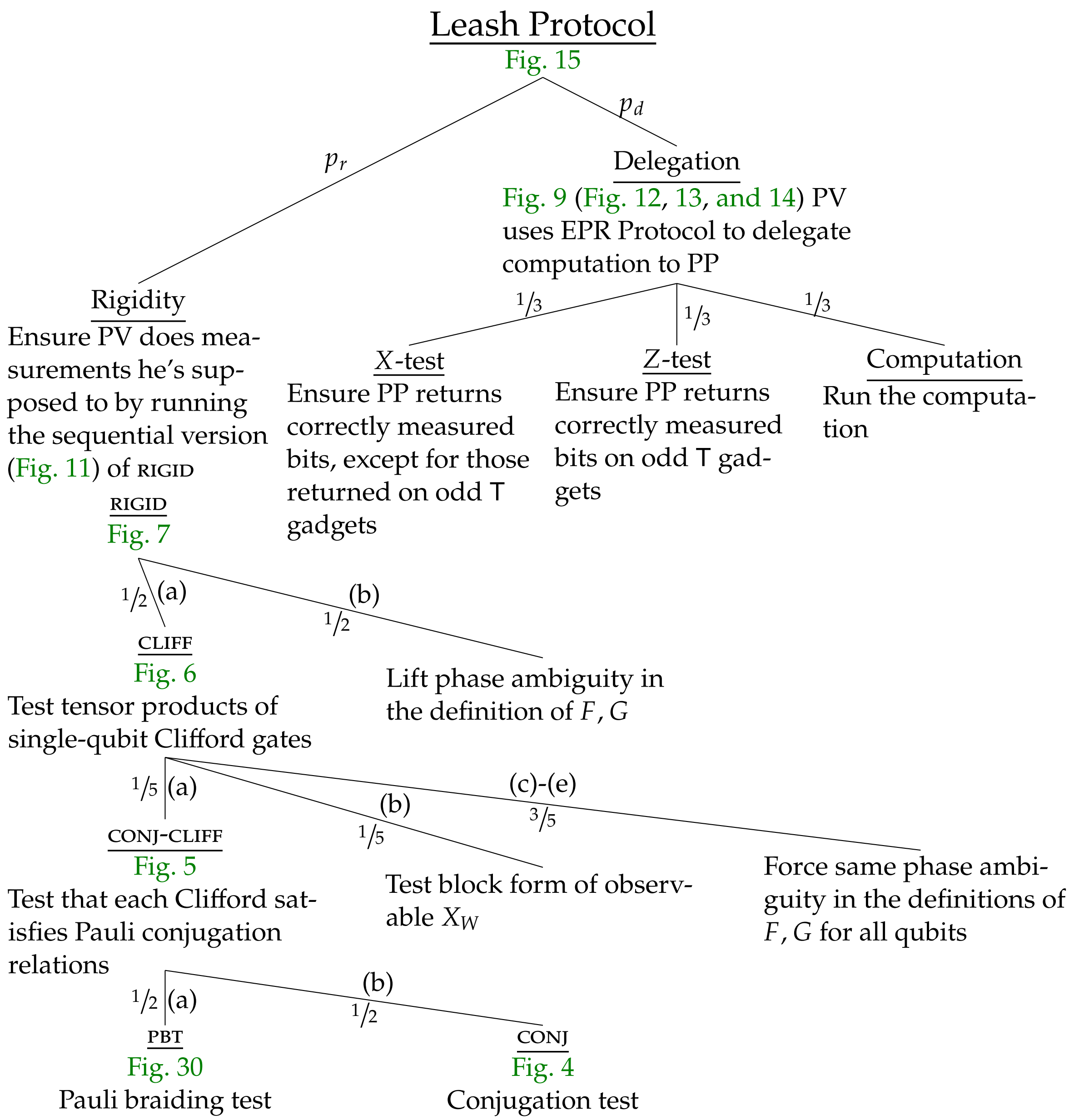


Figure 16: Structure of the Leash Protocol. The Verifier plays the rigidity game with probability p_r, and the delegation game with probability $p_d = 1 - p_r$. In either case, a subgame is chosen, some of which involve their own subgames. We illustrate this structure here, letting probabilities label branches in the tree. Note that not all random choices are shown. For example, when CONJ is played, it is with a random choice of inputs, but this figure illustrates the high-level structure of the protocol, and connection to different tests.

Proof. Let PP* be any prover. Assume that PV behaves honestly and applies the measurements specified by his query W on halves of EPR pairs shared with PP*. As a result the corresponding half-EPR pair at PP* is projected onto the post-measurement state associated with the outcome reported by PV to V.

From PP*, we define another prover, P^*, such that if P^* interacts with V_{EPR}, the honest verifer for the EPR Protocol (Figure 3a), then V_{EPR} rejects with the same probability that V would reject on interaction with PP*. The main idea of the proof can be seen by looking at Figure 10, and noticing that: (1) the combined action of V and PV is unchanged if instead of choosing the W_i-values at random and then choosing z_i as a function of these, the z_i are chosen uniformly at random, and then the W_i are chosen as a function of these; and (2) with this transformation, the combined action of V and PV is now the same as the action of V_{EPR} in the EPR Protocol.

We now define P^*. P^* acts on a system that includes $n+t$ qubits that, in an honest run of the EPR Protocol, are halves of EPR pairs shared with V_{EPR}. P^* receives $\{z_i\}_{i=1}^t$ from V_{EPR}. P^* creates $m-(n+t)$ half EPR pairs (i. e., single-qubit maximally mixed states) and randomly permutes these with his $n+t$ unmeasured qubits, n of which correspond to computation qubits on systems $\mathcal{X}_1,\dots,\mathcal{X}_n$ — he sets N to be the indices of these qubits — and t of which correspond to T-auxiliary states — he sets T^0 and T^1 to be the indices of these qubits. P^* simulates PP* on these m qubits in the following way. First, P^* gives PP* the index sets N, T^0, and T^1. In the ℓ-th iteration of the loop (Step 2. in Figure 14), PP* returns some bits $\{c_i\}_{i\in T_\ell}$, and then expects inputs $\{z_i\}_{i\in T_\ell}$, which P^* provides, using the bits he received from V_{EPR}. Finally, at the end of the computation, PP* returns a bit c_f, and P^* outputs $\{c_i\}_{i\in T}$ and c_f.

This completes the description of P^*. To show the lemma we argue that for any input $(Q,|\vec{x}\rangle)$ the probability that V outputs accept on interaction with PV and PP* is the same as the probability that V_{EPR} outputs accept on interaction with P^*, which is at most $\frac{2}{3}q_t+\frac{1}{3}q_c$ whenever $\|\Pi_0 Q|\vec{x}\rangle\|^2\le 1/3$, by Theorem 2.3. Using $\delta=\frac{1}{3}$, Theorem 2.3 gives $q_c\le\frac{5}{3}-\frac{4}{3}q_t$, which yields

$$\frac{2}{3}q_t+\frac{1}{3}q_c\le\frac{5}{9}+\frac{2}{9}q_t\le\frac{7}{9}.$$

There are two reasons that V_{EPR} might reject: (1) in a computation or X-test run, the output qubit decodes to 1; or (2) in an evaluation of the gadget in Figure 10 (either an X-test run for an even T gate, or a Z-test run for an odd T gate) the condition $c_i=a_j\oplus e_i$ fails. Note that in the description of the EPR Protocol, the one-time-pad key just before application of the i-th T gate is denoted a'_i, which we denote here by a_j.

We first consider case (1). This occurs exactly when $c_f\oplus a_f=1$, where a_f is the final X key of the output wire, held by V_{EPR}. We note that a_f is exactly the final X key that V would hold in the Verifier-on-a-Leash Protocol, which follows from the fact that the update rules in both the EPR Protocol and the leash protocol are the same. Thus, the probability that V_{EPR} finds $v_f\oplus a_f=1$ on interaction with P^* is exactly the probability that V finds $c_f\oplus a_f=1$ in Step 5 of Figure 12.

Next, consider case (2). The condition $c_i\ne a_j\oplus e_i$ is exactly the condition in which a verifier interacting with P^* as in Figure 12 would reject (see Step 4.(b)).

Thus, the probability that V_{EPR} outputs reject upon interaction with P^* is exactly the probability that V outputs reject on interaction with PP*, which, as discussed above, is at most 7/9. □

The following lemma shows soundness against cheating PV*.

Lemma 4.4. *Suppose the verifier executes the leash protocol on input $(Q, |\vec{x}\rangle)$ such that $\|\Pi_0 Q|\vec{x}\rangle\|^2 \leq 1/3$ with provers (PV^*, PP^*), such that the provers are accepted with probability $1-\varepsilon$, for some $\varepsilon > 0$, in the rigidity game, and with probability at least q in the delegation game. Then there exist provers PP' and PV' such that PV' applies the honest strategy and PP' and PV' are accepted with probability at least $q - \mathrm{poly}(\varepsilon)$ in the delegation game.*

Proof. By assumption, PP* and PV* are accepted in the rigidity game with probability at least $1-\varepsilon$. Let V_A, V_B be the local isometries guaranteed to exist by Theorem 3.1, and $\{\tau_\lambda\}$ the subnormalized densities associated with PP*'s Hilbert space (recall that playing the rigidity game sequentially leaves the guarantees from Theorem 3.1 unchanged, since it only reduces the provers' ability to cheat).

First define provers PV″ and PP″ as follows. PP″ and PV″ initially share the state

$$|\psi'\rangle_{\mathsf{AB}} = \otimes_{i=1}^m |\mathrm{EPR}\rangle\langle\mathrm{EPR}|_{\mathsf{AB}} \otimes \sum_{\lambda\in\{\pm\}} |\lambda\rangle\langle\lambda|_{\mathsf{A}'} \otimes |\lambda\rangle\langle\lambda|_{\mathsf{B}'} \otimes (\tau_\lambda)_{\mathsf{A}''} \ ,$$

with registers $\mathsf{AA}'\mathsf{A}''$ in the possession of PP″ and BB' in the possession of PV″. Upon receiving a query $W \in \Sigma^m$, PV″ measures B' to obtain a $\lambda \in \{\pm\}$. If $\lambda = +$, he proceeds honestly, measuring his half-EPR pairs exactly as instructed. If $\lambda = -$, he proceeds honestly except that for every honest single-qubit observable specified by W, he instead measures the complex conjugate observable. Note that this strategy can be implemented irrespective of whether W is given at once, as in the game RIGID, or sequentially, as in the Delegation Game. PP″ simply acts like PP*, just with the isometry V_A applied.

First note that by Theorem 3.1, the distribution of answers of PV″ to the verifier, as well as the subsequent interaction between the verifier and PP, generate (classical) transcripts that are within statistical distance $\mathrm{poly}(\varepsilon)$ from those generated by PV* and PP* with the same verifier.

Next we observe that taking the complex conjugate of both provers' actions does not change their acceptance probability in the delegation game, since the interaction with the verifier is completely classical. Define PP′ as follows: PP′ measures A' to obtain the same λ as PV″, and then executes PP″ or its complex conjugate depending on the value of λ. Define PV′ to execute the honest behavior (he measures to obtain λ, but then discards it and does not take any complex conjugates).

Then PV′ applies the honest strategy, and (PV′, PP′) applies either the same strategy as (PV″, PP″) (if $\lambda = +$) or its complex conjugate (if $\lambda = -$). Therefore they are accepted in the delegation game with exactly the same probability. □

Combining Lemma 4.3 and Lemma 4.4 gives us the final soundness guarantee.

Lemma 4.5. *(Constant soundness-completeness gap) There exist constants $p_r, p_d = 1 - p_r$ and $\Delta > 0$ such that if the verifier executes the leash protocol with parameters (p_r, p_d) on input $(Q, |\vec{x}\rangle)$ such that $\|\Pi_0 Q|\vec{x}\rangle\|^2 \leq 1/3$, any provers (PV^*, PP^*) are accepted with probability at most $p_{\mathrm{sound}} = p_{\mathrm{compl}} - \Delta$.*

Proof. Suppose provers PP^* and PV^* succeed in the delegation game with probability $\frac{7}{9} + w$ for some $w > 0$, and the testing game with probability $1 - \varepsilon_*(w)$, where $\varepsilon_*(w)$ will be specified below. By Lemma 4.4, this implies that there exist provers PP′ and PV′ such that PV′ is honest and the provers succeed in the delegation game with probability at least $\frac{7}{9} + w - g(\varepsilon_*(w))$, where $g(\varepsilon) = \mathrm{poly}(\varepsilon)$ is the function from the guarantee of Lemma 4.4. Let $\varepsilon_*(w)$ be such that $g(\varepsilon_*(w)) \le \frac{w}{2}$. In particular, $\frac{7}{9} + w - g(\varepsilon_*(w)) \ge \frac{7}{9} + \frac{w}{2} > \frac{7}{9}$. This contradicts Lemma 4.3.

Thus if provers PP and PV succeed in the delegation game with probability $\frac{7}{9} + w$ they must succeed in the rigidity game with probability less than $1 - \varepsilon_*(w)$. This implies that for any strategy of the provers, on any *no* instance, the probability that they are accepted is at most

$$\max\left\{p_r + (1-p_r)\left(\frac{7}{9} + \frac{1}{18}\right),\ p_r\left(1 - \varepsilon_*\left(\frac{1}{18}\right)\right) + (1-p_r)\cdot 1\right\}. \tag{4.1}$$

Since $\varepsilon_*(\frac{1}{18})$ is a positive constant, it is clear that one can pick p_r large enough so that

$$p_r\left(1 - \varepsilon_*\left(\frac{1}{18}\right)\right) + (1-p_r)\cdot 1 < p_r + (1-p_r)\left(\frac{7}{9} + \frac{1}{18}\right). \tag{4.2}$$

Select the smallest such p_r. Then the probability that the two provers are accepted is at most

$$p_{\mathrm{sound}} := p_r + (1-p_r)\left(\frac{7}{9} + \frac{1}{18}\right) < p_r\left(1 - \mathrm{e}^{-\Omega(n+t)}\right) + (1-p_r)\frac{8}{9} = p_{\mathrm{compl}}\,,$$

which gives the desired constant completeness-soundness gap Δ. □

4.4 Blindness

We now establish blindness of the Leash Protocol. In Lemma 4.6, we will prove that the protocol has the property that neither prover can learn anything about the input to the circuit, $\vec{x}$, aside from its length. Thus, the protocol can be turned into a blind protocol, where Q is also hidden, by modifying any input $(Q, \vec{x})$ where Q has g gates and acts on n qubits, to an input $(U_{g,n}, (Q, \vec{x}))$, where $U_{g,n}$ is a universal circuit that takes as input a description of a g-gate circuit Q on n qubits, and a string $\vec{x}$, and outputs $Q|\vec{x}\rangle$. The universal circuit $U_{g,n}$ can be implemented in $O(g \log n)$ gates. By Lemma 4.6, running the Leash Protocol on $(U_{g,n}, (Q, \vec{x}))$ reveals nothing about Q or $\vec{x}$ aside from g and n.

In the form presented in Figure 12, the verifier V interacts first with PV, sending him random questions that are independent from the input $\vec{x}$, aside from the input length n. It is thus clear that the protocol is blind with respect to PV.

In contrast, the questions to PP depend on PV's answers and on the input, so it may a priori seem like the questions can leak information to PP. To show that the protocol is also blind with respect to PP, we show that there is an alternative formulation, in which the verifier first interacts with PP, sending him random messages, and then only with PV, with whom the interaction is now adaptive. We argue that, for an arbitrary strategy of the provers, the reduced state of all registers available to either prover, PP or PV, is exactly the same in both formulations of the protocol — the *original* and the *alternative* one. This establishes blindness for both provers. This technique for proving blindness is already used in [37] to establish blindness of a two-prover protocol based on computation by teleportation.

Lemma 4.6 (Blindness of the Leash Protocol)**.** *For any strategy of PV* and PP*, the reduced state of PV* and PP*, resp., at the end of the leash protocol is independent of the input $\vec{x}$, aside from its length.*

Proof. Let PV* and PP* denote two arbitrary strategies for the provers in the leash protocol. Each of these strategies can be modeled as a super-operator

$$\mathcal{T}_{\mathrm{PV}} : \mathrm{L}(\mathcal{H}_{T_{\mathrm{PV}}} \otimes \mathcal{H}_{\mathrm{PV}}) \to \mathrm{L}(\mathcal{H}_{T'_{\mathrm{PV}}} \otimes \mathcal{H}_{\mathrm{PV}}),$$

$$\mathcal{T}_{\mathrm{PP},ad} : \mathrm{L}(\mathcal{H}_{T_{\mathrm{PP}}} \otimes \mathcal{H}_{\mathrm{PP}}) \to \mathrm{L}(\mathcal{H}_{T'_{\mathrm{PP}}} \otimes \mathcal{H}_{\mathrm{PP}}).$$

Here $\mathcal{H}_{T_{\mathrm{PV}}}$ and $\mathcal{H}_{T'_{\mathrm{PV}}}$ ($\mathcal{H}_{T_{\mathrm{PP}}}$ and $\mathcal{H}_{T'_{\mathrm{PP}}}$) are classical registers containing the inputs and outputs to and from PV* (PP*, resp.) and $\mathcal{H}_{\mathrm{PV}}$ ($\mathcal{H}_{\mathrm{PP}}$) is the private space of PV* (PP*, resp.). Note that the interaction of each prover with the verifier is sequential, and we use $\mathcal{T}_{\mathrm{PV}}$ and $\mathcal{T}_{\mathrm{PP},ad}$ to denote the combined action of the verifier and the prover, resp., across all rounds of interaction (formally these are sequences of superoperators).

Consider an alternative protocol, which proceeds as follows. The verifier first interacts with PP. From Figure 14 we see that the inputs required for PP are subsets N and $T_1, \ldots, T_d$, and values $\{z_i\}_{i \in T_\ell}$ for each $\ell \in \{1, \ldots, d\}$. To select the former, the verifier proceeds as in the first step of the Delegation Game. She selects the latter uniformly at random. The verifier collects values $\{c_i\}_{i \in T_\ell}$ from PP exactly as in the original Delegation Game.

Once the interaction with PP has been completed, the verifier interacts with PV. First, she selects a random string $W_N \in \Sigma^N$, conditioned on the event that W_N contains at least n copies of each symbol in Σ, and sends it to PV, collecting answers $\vec{e}_N$. The verifier then follows the same update rules as in the delegation game. We describe this explicitly for computation runs. First, the verifier sets $\vec{a} = \vec{e}_N$. Depending on the values $\{c_i\}_{i \in T_1}$ and $\{z_i\}_{i \in T_1}$ obtained in the interaction with PP, using the equation $z_i = a_j + 1_{W_i = F} + c_i$ she deduces a value for $1_{W_i = F}$ for each $i \in T_1 \subseteq B_1$. She then selects a uniformly random $W_{B_1} \in \Sigma^{B_1}$, conditioned on the event that W_{B_1} contains at least t_1 copies of each symbol from Σ, and for $i \in T_1$ it holds that $W_i = F$ if and only if $z_i = a_j + 1 + c_i$. The important observation is that, if T_1 is a uniformly random, unknown subset, the marginal distribution on W_{B_1} induced by the distribution described above is independent of whether $z_i = a_j + 1 + c_i$ or $z_i = a_j + 0 + c_i$: precisely, it is uniform conditioned on the event that W_{B_1} contains at least t_1 copies of each symbol from Σ. The verifier receives outcomes $\vec{e}_{B_1} \in \{0,1\}^{B_1}$ from PV, and using these outcomes performs the appropriate key update rules; she then proceeds to the second layer of the circuit, until the end of the computation. Finally, the verifier accepts using the same rule as in the last step of the original delegation game.

We claim that both the original and alternative protocols generate the same joint final state:

$$\mathcal{T}_{\mathrm{PP},ad} \circ \mathcal{T}_{\mathrm{PV}}(\rho_{orig}) = \mathcal{T}_{\mathrm{PV},ad} \circ \mathcal{T}_{\mathrm{PP}}(\rho_{alt}) \in \mathcal{H}_{\mathrm{PP}} \otimes \mathcal{H}_{T'_{\mathrm{PP}}} \otimes \mathcal{H}_{\mathrm{V}} \otimes \mathcal{H}_{T'_{\mathrm{PV}}} \otimes \mathcal{H}_{\mathrm{PV}}, \tag{4.3}$$

where we use ρ_{orig} and ρ_{alt} to denote the joint initial state of the provers, as well as the verifier's initialization of her workspace, in the original and alternative protocols, respectively, and $\mathcal{T}_{\mathrm{PV},ad}$ and $\mathcal{T}_{\mathrm{PP}}$ are the equivalent of $\mathcal{T}_{\mathrm{PV}}$ and $\mathcal{T}_{\mathrm{PP},ad}$ for the reversed protocol (in particular they correspond to the same strategies PV* and PP* used to define $\mathcal{T}_{\mathrm{PV}}$ and $\mathcal{T}_{\mathrm{PP},ad}$). Notice that $\mathcal{T}_{\mathrm{PV},ad}$ and $\mathcal{T}_{\mathrm{PP}}$ are well-defined since neither prover can distinguish an execution of the original from the alternative protocol.[14] To see that equality holds in (4.3), it is possible to re-write the final state of the protocol as the result of the following sequence of operations. First, the verifier initializes the message registers with PP* and PV* using half-EPR pairs, keeping the other halves in her private workspace. This simulates the generation of uniform random messages to both provers. Then, the superoperator $\mathcal{T}_{\mathrm{PV}} \otimes \mathcal{T}_{\mathrm{PP}}$ is executed. Finally, the verifier post-selects by applying a projection operator on $\mathcal{H}_{T_{\mathrm{PV}}} \otimes \mathcal{H}_{T'_{\mathrm{PV}}} \otimes \mathcal{H}_{T_{\mathrm{PP}}} \otimes \mathcal{H}_{T'_{\mathrm{PP}}}$ that projects onto valid transcripts for the original protocol (i. e., transcripts in which the adaptive questions are chosen correctly). This projection can be implemented in two equivalent ways: either the verifier first measures $\mathcal{H}_{T_{\mathrm{PV}}} \otimes \mathcal{H}_{T'_{\mathrm{PV}}}$, and then $\mathcal{H}_{T_{\mathrm{PP}}} \otimes \mathcal{H}_{T'_{\mathrm{PP}}}$; based on the outcomes she accepts a valid transcript for the original protocol or she rejects. Or, she first measures $\mathcal{H}_{T_{\mathrm{PP}}} \otimes \mathcal{H}_{T'_{\mathrm{PP}}}$, and then $\mathcal{H}_{T_{\mathrm{PV}}} \otimes \mathcal{H}_{T'_{\mathrm{PV}}}$; based on the outcomes she accepts a valid transcript for the alternative protocol or she rejects. Using the commutation of the provers' actions, conditioned on the transcript being accepted, the first gives rise to the first final state in (4.3), and the second to the second final state. The two are equivalent because the acceptance condition for a valid transcript is identical in the two versions of the protocol.

Since in the first case the reduced state on $\mathcal{H}_{T'_{\mathrm{PV}}} \otimes \mathcal{H}_{\mathrm{PV}}$ is independent of the input to the computation, $\vec{x}$, and in the second the reduced state on $\mathcal{H}_{\mathrm{PP}} \otimes \mathcal{H}_{T'_{\mathrm{PP}}}$ is independent of $\vec{x}$, we deduce that the protocol hides the input from each of PV* and PP*. □

5 Dog-Walker protocol

The Dog-Walker Protocol again involves a classical verifier V and two provers PV and PP. As in the leash protocol presented in Section 4, PP and PV take the roles of P_{EPR} and V_{EPR} from [7], respectively. The main difference is that the Dog-Walker Protocol gives up blindness in order to reduce the number of rounds to two (one round of interaction with each prover, played sequentially). After one round of communication with PP, who returns a sequence of measurement outcomes, V communicates all of PP's outcomes, except for the one corresponding to the output bit of the computation, as well as the input $\vec{x}$, to PV. With these, PV can perform the required adaptive measurements without the need to interact with V. It may seem risky to communicate bits sent by PP directly to PV — this seems to allow for communication between the two provers! Indeed, blindness is lost. However, if PP is honest, his outcomes $\{c_i\}_i$ in the computation run are the result of measurements he performs on half-EPR pairs, and are uniform random bits. If he is dishonest, and does not return the outcomes obtained by performing the right measurements, he will be caught in the test runs. It is only in computation runs that V sends the measurement results $\{c_i\}_i$ to PV.

We note that PV has a much more important role in this protocol: he decides himself the measurements to perform according to previous measurements' outcomes as well as the input x. For this reason, we must use the Tomography test discussed in Section 3.6, in order to test if PV remains honest with respect to these new tasks. With the tomography test, we can achieve

[14]One must ensure that a prover does not realize if the alternative protocol is executed instead of the original; this is easily enforced by only interacting with any of the provers at specific, publicly decided times.

a rigidity theorem that will allow us to prove the soundness of the Dog-walker protocol (see Figure 21 for a glimpse of the proof structure).

Finally, the Dog-Walker Protocol can be easily extended to a classical-verifier two-prover protocol for all languages in QMA. Along the same lines of the proof that QMIP = MIP* from [37], one of the provers plays the role of PP, running the QMA verification circuit, while the second prover creates and teleports the corresponding QMA witness. In our case, it is not hard to see that the second prover can be re-used as PV in the Dog-Walker Protocol, creating the necessary gadgets for the computation and allowing the Verifier to check the operations performed by the first prover. We describe the protocol in Section 5.4.

5.1 Protocol and statement of results

Throughout this section we let $\Sigma = \{X, Y, Z, F, G\}$, and let $m = \Theta(n + t)$ be chosen large enough so that each symbol in Σ appears at least $n + t$ times in a uniform random $W \in \Sigma^m$, with probability close to 1. Let $\mu(W)$ denote the probability that a player receives input W while playing $\textsc{rigid}(\Sigma, m)$ (recall that both players have the same marginals in $\textsc{rigid}$). Let $\mu(W'|W)$ denote the probability that one player receives W' given that the other player receives W.

The full protocols are presented in Figure 18 (verifier's point of view), Figure 19 (PV's point of view) and Figure 20 (PP's point of view). The protocol has two types of runs: EPR and Rigidity. Within an EPR run are three types of subruns: Computation subrun, X-test subrun, and Z-test subrun. We will generally think of X- and Z-test subruns as one subrun type (Test subrun). Within a Rigidity run are two types of subruns: Tomography subrun, which should be thought of as the Rigidity version of the EPR-Computation run; and Clifford subrun, which should be thought of as the Rigidity version of the EPR-Test run. With some probability p_1, V runs a Rigidity run, Clifford subrun; with some probability p_2, V runs an EPR run, Test subrun; with some probability p_3, V runs an EPR run, Computation subrun; and with probability $p_4 = 1 - p_1 - p_2 - p_3$, V runs a Rigidity run, Tomography subrun. This structure is illustrated in Figure 17. We call this the Dog-Walker Protocol with parameters (p_1, p_2, p_3, p_4).

The following theorem states the guarantees of the Dog-Walker Protocol.

Theorem 5.1. *There exist constants p_1, p_2, p_3, $p_4 = 1 - p_1 - p_2 - p_3$, and $\Delta > 0$ such that the following hold of the Dog-Walker Protocol with parameters (p_1, p_2, p_3, p_4), when executed on input $(Q, |\vec{x}\rangle)$.*

- *(Completeness:) Suppose that $\left\|\Pi_0 Q|\vec{x}\rangle\right\|^2 \geq 2/3$. Then there is a strategy for PV and PP that is accepted with probability at least $p_{\text{compl}} = p_1(1 - e^{-\Omega(n+t)}) + p_2 + \frac{2}{3}p_3 + p_4$.*
- *(Soundness:) Suppose that $\left\|\Pi_0 Q|\vec{x}\rangle\right\|^2 \leq 1/3$. Then any strategy for PV and PP is accepted with probability at most $p_{\text{sound}} = p_{\text{compl}} - \Delta$.*

The proof of completeness is given in Lemma 5.2, and proof of soundness is given in Lemma 5.7.

5.2 Dog-Walker completeness

Lemma 5.2. *Suppose V executes the Dog-Walker Protocol with parameters (p_1, p_2, p_3, p_4). There is a strategy for the provers such that, on any input $(Q, |\vec{x}\rangle)$ such that $\left\|\Pi_0 Q|\vec{x}\rangle\right\|^2 \geq \frac{2}{3}$, V accepts with*

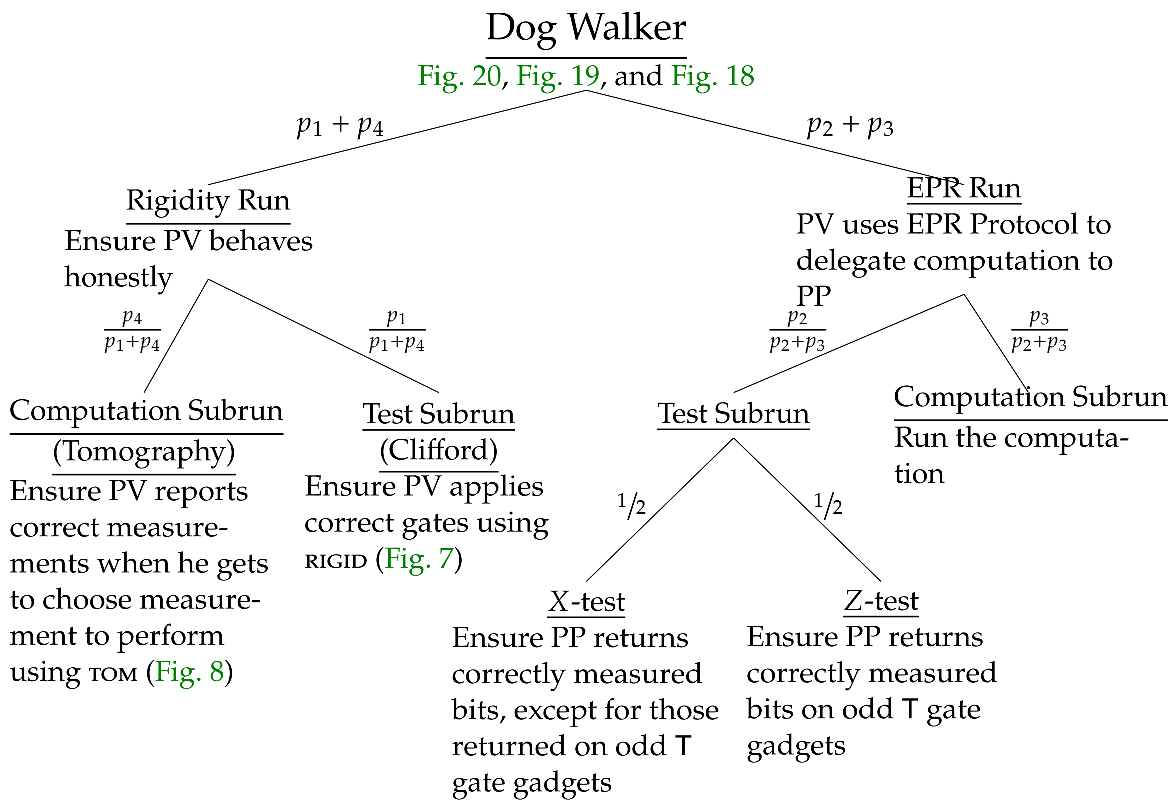


Figure 17: The structure of the Dog-Walker Protocol. We illustrate the structure of different runs, subruns, and games/tests, letting probabilities label branches.

probability at least $p_{\text{compl}} = p_1(1-\delta_c) + p_2 + \frac{2}{3}p_3 + p_4$, *for some* $\delta_c = \mathrm{e}^{-\Omega(n+t)}$.

Proof. The provers PV and PP play the strategy described in Figures 19 and 20, respectively. In the Rigidity-Tomography run, the verification performed by V amounts to playing $\text{TOM}(\Sigma, n+t, m)$ with the provers (with an extra constraint on the output W of PV that is always satisfied by the honest strategy). This game has perfect completeness, which makes the V accept with probability 1 in the Rigidity-Tomography run. In the Rigidity-Clifford run, V plays $\text{RIGID}(\Sigma, m)$ with the provers. The game has completeness at least $1-\delta_c$ for some $\delta_c = \mathrm{e}^{-\Omega(n+t)}$, since $m = \Omega(n+t)$, therefore their success probability in this run is at least $1-\delta_c$.

In the EPR run, the provers are exactly carrying out the EPR Protocol, with V using PV to run V^r_{EPR}, and PP playing the role of P_{EPR}. Thus, test runs result in acceptance with probability 1, and the computation run results in acceptance with probability $\left\|\Pi_0 Q|\vec{x}\rangle\right\|^2$, by Theorem 2.2. □

---

1. Select a run type **EPR** or **Rigidity**, and disjoint sets $N, T^0, T^1 \subset \{1, \ldots, m\}$ of sizes n, t_0 and $t - t_0$.

EPR Choose $\vec{z}$ uniformly at random from $\{0,1\}^t$ and send it, along with N, T^0 and T^1, to PP. Receive measurement outcomes $\vec{c} \in \{0,1\}^t$ and $c_f \in \{0,1\}$ from PP.

Rigidity Choose W' according to $\mu(\cdot)$ and send it to PP. Receive $\vec{e}' \in \{0,1\}^m$ from PP.

2. Select a subrun type at random from **Computation**, X**-test** or Z**-test**.

Computation Based on whether it is an EPR or a Rigidity Run:

EPR (i) Send $\vec{x}$, $\vec{z}$, $\vec{c}$ and sets N, T^0 and T^1 to PV, and receive measurement outcomes $\vec{a}, \vec{b} \in \{0,1\}^n$ and $\vec{e} \in \{0,1\}^t$.

(ii) Apply the update rules from Table 2 gate-by-gate to obtain the final X key for the output wire a'_f. If $c_f + a'_f \neq 0$, reject.

Rigidity (Tomography) (i) Choose uniform random strings $\vec{c}, \vec{z} \in \{0,1\}^t$, $\vec{x} \in \{0,1\}^n$ to send to PV, along with N and T, and receive measurement outcomes $\vec{d} \in \{0,1\}^n$ and $\vec{e} \in \{0,1\}^t$.

(ii) From $\vec{x}$, $\vec{c}$, $\vec{z}$, $\vec{d}$, and $\vec{e}$, determine the adaptive measurements $W \in \Sigma^{n+t}$ that V^0_{EPR} would have performed (based on Figure 3b), and reject if the input-output pairs $(W', \vec{e}')$ and $(N \cup T, (W, \vec{e}))$ do not satisfy the winning criterion for $\textsc{tom}(\Sigma, n+t, m)$.

X**-test** Based on whether it is an EPR or a Rigidity Run:

EPR (i) Choose $W \in \Sigma^m$ uniformly at random among all strings satisfying: $W_i = Z$ for all $i \in N$; $W_i = Z$ for all $i \in T^0$; and $W_i \in \{X, Y\}$ for all $i \in T^1$. Send W to PV and receive measurement results $\vec{e} \in \{0,1\}^m$. Let $(\vec{a}, \vec{b}) = (\vec{e}_N, 0^n)$.

(ii) Apply update rules from Table 2 gate-by-gate to obtain $\forall i \in [t]$ the X key before the i-th T gate is applied, a'_i, and the final X key for the output wire, a'_f. If $\exists i$ s.t. the i-th T gate is even and $c_i \neq a'_i + e_i$, reject. If $c_f + a'_f \neq 0$, reject.

Rigidity (Clifford) Choose W according to the marginal conditioned on W', $\mu(\cdot|W')$. Send W to PV and receive $\vec{e} \in \{0,1\}^m$. Reject if $(W', \vec{e}', W, \vec{e})$ does not win $\textsc{rigid}(\Sigma, m)$.

Z**-test** Based on whether it is an EPR or a Rigidity Run:

EPR (i) Choose $W \in \Sigma^m$ uniformly at random among all strings satisfying: $W_i = X$ for all $i \in N$; $W_i \in \{X, Y\}$ for all $i \in T^0$; and $W_i = Z$ for all $i \in T^1$. Send W to PV and receive measurement results $\vec{e} \in \{0,1\}^m$. Let $(\vec{a}, \vec{b}) = (0^n, \vec{e}_N)$.

(ii) Apply update rules from Table 2 gate-by-gate to obtain $\forall i \in [t]$, the X key before the i-th T gate is applied, a'_i. If $\exists i$ s.t. the i-th T gate is odd and $c_i \neq a'_i + e_i$, reject.

Rigidity (Clifford) Identical to X-test case.

Figure 18: The Dog-Walker Protocol: Verifier's point of view.

---

1. If PV receives a question W from V (he is playing RIGID or an X- or Z-test Run):

    Measure the m qubits in the observable indicated by W — for example, if $W \in \Sigma^m$, for $i \in \{1, \ldots, m\}$, measure the i-th qubit in the basis indicated by W_i — and report the outcomes $\vec{e}$ to V.

2. If PV receives $\vec{x}$, $\vec{z}$, $\vec{c}$ and sets N, T^0 and T^1 from V (he is playing TOM or a Computation Run):

    Run the procedure V^0_{EPR} from Figure 3b on input $\vec{x}$, $\vec{c}$, $\vec{z}$, the n qubits in N, and the t qubits in $T^0 \cup T^1$. Report the outputs $\vec{d}$ and $\vec{e}$ of V^0_{EPR} to V.

Figure 19: The Dog-Walker Protocol: Honest strategy for PV.

---

1. If PP receives a question W' from V (he is playing TOM or RIGID):

    Measure the m qubits in the observable indicated by W' — for example, if $W' \in \Sigma^m$, for $i \in \{1, \ldots, m\}$, measure the i-th qubit in the basis indicated by W'_i — and report the outcomes $\vec{e}'$ to V.

2. If PP receives $\vec{z}$, and sets N, T^0 and T^1 from V (he is playing the role of P_{EPR} from the EPR Protocol):

    Run the prover P_{EPR} from Figure 3c on input $\vec{z}$, the n qubits in N, and the t qubits in $T^0 \cup T^1$. Report the outputs $\vec{c} \in \{0, 1\}^t$ and $c_f \in \{0, 1\}$ of P_{EPR} to V.

Figure 20: The Dog-Walker Protocol: Honest strategy for PP.

5.3 Dog-Walker soundness

Figure 21 summarizes the high-level structure of the soundness analysis. Intuitively, our ultimate goal is to argue that both provers either apply the correct operations in EPR-Computation runs, or are rejected with constant probability. This will be achieved by employing a form of "hybrid argument" whereby it is argued that the provers, if they are not caught, must be using the honest strategies described in Figure 20 and Figure 19 in the different types of runs considered in the protocol. Towards this, we divide the run types into the following four scenarios:

1. Rigidity-Clifford: The run type is **Rigidity** and the subrun type is either X**-test** or Z**-test**. (When the provers are honest) PV behaves as in Item 1 of Figure 19, and PP behaves as in Item 1 of Figure 20.

2. EPR-Test: The run type is **EPR** and the subrun type is either X**-test** or Z**-test**. PV behaves as in Item 1 of Figure 19, and PP behaves as in Item 2 of Figure 20.

3. EPR-Computation: The run type is **EPR** and the subrun type is **Computation**. PV behaves as in Item 2 of Figure 19, and PP behaves as in Item 2 of Figure 20.

4. Rigidity-Tomography: The run type is **Rigidity** and the subrun type is **Computation**. PV behaves as in Item 2 of Figure 19, and PP behaves as in Item 1 of Figure 20.

Examining Figure 18, we can see the following. In the Rigidity-Clifford scenario, the verifier is precisely playing the game RIGID with the provers, as the provers receive questions W' and W distributed according to $\mu(\cdot,\cdot)$, the distribution of questions for RIGID(Σ, m); their answers are tested against the winning conditions of RIGID(Σ, m). In the Rigidity-Tomography scenario, the verifier plays a variant of the game TOM with the provers, in which PV's choice of observable W is uniquely determined by his inputs $\vec{x}$, $\vec{c}$ and $\vec{z}$: it should match the observable implemented by V^0_{EPR} on these inputs. In EPR runs, PV plays the part of V^r_{EPR} from the EPR Protocol, and PP plays the part of P_{EPR}. The EPR-Test scenario corresponds to X- and Z-tests from the EPR Protocol, whereas the EPR-Computation scenario corresponds to computation runs from the EPR Protocol.

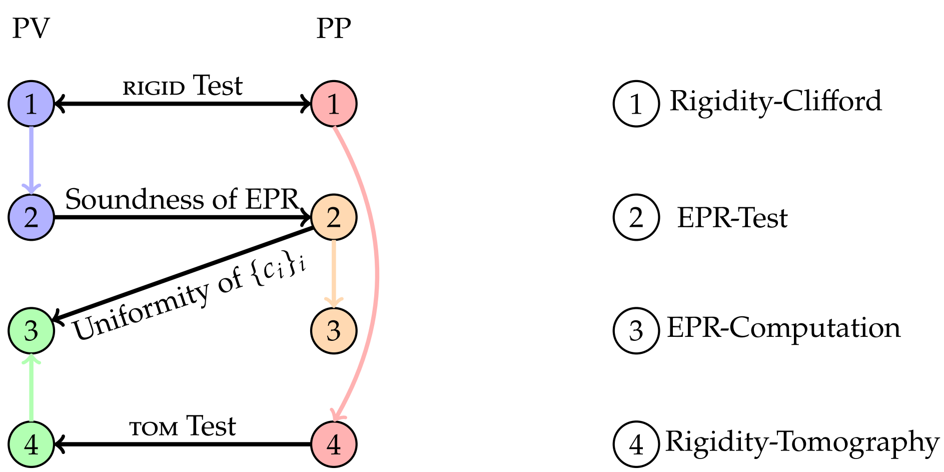


Figure 21: Overview of the soundness of the Dog-Walker Protocol

The structure of the proof is as follows (see also Figure 21):

(i) By the game RIGID, in the Rigidity-Clifford runs, both PP and PV must be honest, or they would lose the game.

(ii) Since PV cannot distinguish between Rigidity-Clifford and EPR-Test (both are Figure 19 Item 1 from his perspective, and the input distributions, while not identical, have total variation distance $1-\eta$, for some constant $\eta > 0$), PV must be honest in the EPR-Test runs, by (i).

(iii) Since PP cannot distinguish between Rigidity-Clifford and Rigidity-Tomography (both are Figure 20 Item 1 from his perspective), PP must be honest in the Rigidity-Tomography runs, by (i).

(iv) Since PV is honest in EPR-Test runs by (ii), PP must be honest in EPR-Test runs or he will get caught, but in particular, he must output values $\{c_i\}_{i\in[t]}$ that are uniform random and independent of $\vec{z}$. Since PP cannot distinguish between EPR-Test and EPR-Computation runs, this is also true in EPR-Computation runs, when the verifier sends the values $\{c_i\}_i$ to PV.

(v) PV must be honest in Rigidity-Tomography runs, or the provers would lose the game TOM.

(vi) Since PV cannot distinguish between Rigidity-Tomography runs and EPR-Computation runs (both are Figure 19 Item 2 from his perspective), PV must be honest in EPR-Computation runs, by (v), and his input distribution to both runs has total variation distance $1 - \eta'$, for some constant $\eta' > 0$, by (iv).

(vii) Since PV is honest in EPR-Test runs by (ii), and EPR-Computation runs by (vi), the combined behavior of V and PV in the EPR runs is that of V_{EPR} in the EPR Protocol, so by the soundness of the EPR Protocol, PP must be honest in EPR-Computation runs, or get caught in the EPR-Test runs with high probability.

The following lemma establishes (i), (ii) and (iii).

Lemma 5.3. *Suppose the verifier executes the Dog-Walker Protocol with provers (PV^*, PP^*) such that the provers are accepted with probability $q_1 \geq 1 - \varepsilon$ in the Rigidity-Clifford Run, q_2 in the EPR-Test Run, q_3 in the EPR-Computation Run, and q_4 in the Rigidity-Tomography Run. Then there exist provers (PV', PP') such that:*

- *PV' and PP' both apply the honest strategy in the Rigidity-Clifford runs, PV' applies the honest strategy in the EPR-Test runs, and PP' applies the honest strategy in the Rigidity-Tomography runs; in particular, the state shared by the provers at the beginning of the protocol is a tensor product of the honest state consisting of m shared EPR pairs and an arbitrary shared ancilla;*
- *The provers are accepted with probability $q_2' = q_2 - O(\mathrm{poly}(\varepsilon))$ in the EPR-Test Run, $q_3' = q_3$ in the EPR-Computation Run, and $q_4' = q_4 - O(\mathrm{poly}(\varepsilon))$ in the Rigidity-Tomography Run.*

Proof. Using a similar argument as in Lemma 4.4, the strategy of PV* in Rigidity-Clifford runs, which is also his strategy in EPR-Test runs (Figure 19 Item 1); and the strategy of PP* in Rigidity-Clifford runs, which is also his strategy in Rigidity-Tomography runs (Figure 20 Item 1); can both be replaced with the honest strategies. Since the distribution of inputs to PP* in the Rigidity-Tomography runs and Rigidity-Clifford runs is the same, the success probability in the Rigidity-Tomography runs is changed by at most $O(\mathrm{poly}(\varepsilon))$ by using the honest strategy. On the other hand, PV*'s input distribution in EPR-Test runs is uniform on Σ^m, whereas his distribution in Rigidity-Clifford runs is given by μ. However, from the description of the test RIGID it is clear that for all $W \in \Sigma^m$, $\mu(W) \geq \frac{1}{c|\Sigma|^m}$ for some constant $c > 1$, thus the total variation distance between the two distributions is at most $1 - \frac{1}{c}$. Thus, replacing PV* with the honest strategy in the EPR-Test runs will change the success probability by at most $O(\mathrm{poly}(\varepsilon))$.

Finally, since the provers' strategy in the EPR-Computation run has not changed, the acceptance probability in it remains unchanged. □

Next, we will show that whenever PV* is honest in the EPR-Test runs this forces PP* to output (close to) uniformly random $\{c_i\}_{i\in[t]}$ that are independent of the run type, even given $\vec{z}$. This will allow us to verify that PP* is unable to signal to PV* whether the run is an EPR Run in the EPR-Computation run, when PV* is sent $\vec{z}$ and $\vec{c}$. This establishes (iv).

Lemma 5.4. *Suppose the verifier executes the Dog-Walker Protocol with provers (PV*, PP*) such that the initial shared state of the provers consists of m shared EPR pairs, together with an arbitrary shared auxiliary state; PV* plays the honest strategy in the EPR-Test runs; the provers are accepted with probability q_1 in the Rigidity-Clifford Run, $q_2 = 1-\varepsilon'$ in the EPR-Test Run, q_3 in the EPR-Computation Run, and q_4 in the Rigidity-Tomography Run. Then the input $(\vec{c},\vec{z})$ given by the verifier to PV* in the EPR-Computation runs has a distribution that is within $O(\varepsilon')$ total variation distance of uniform on $\{0,1\}^t \times \{0,1\}^t$.*

Proof. Let a_i' denote the X key of the wire to which the i-th T gate is applied, just before the i-th T gate is applied, and let D_i be a random variable defined as follows. If the i-th T gate is even, let $D_i = e_i + a_i'$, where we interpret e_i and a_i' as the random variables representing the measurement result and key V would get if she chooses to execute an X-test run. If the i-th T gate is odd, let $D_i = e_i + a_i'$, where we interpret e_i and a_i' as the measurement result and key V would get if she chooses to execute an Z-test run. Since PV* is assumed to play honestly in EPR-Test runs, $\vec{D}$ is uniformly distributed in $\{0,1\}^t$. In particular, we have, for any $\vec{d},\vec{z} \in \{0,1\}^t$,

$$\Pr[\vec{D} = \vec{d}, \vec{Z} = \vec{z}] = \frac{1}{4^t}. \tag{5.1}$$

Let C_i be the random variable that corresponds to the measurement output of the i-th T gadget by PP* in X-test run if the i-th T gate is even, or the measurement output of the i-th T gadget by PP* in Z-test run if the i-th T gate is odd.

Let $T^0 \subset [t]$ be the set of even T gates and $T^1 \subset [t]$ the set of odd T gates. In an X-test Run, the provers are rejected whenever $i \in T^0$ and $c_i \neq d_i$, and in a Z-test Run, they are rejected whenever $i \in T^1$ and $c_i \neq d_i$. An EPR-Test Run consists of running one of these two runs with equal probability, so:

$$\Pr[\vec{C} \neq \vec{D}] \leq 2\varepsilon'. \tag{5.2}$$

We can express (5.2) as

$$\Pr[(\vec{C},\vec{Z}) \neq (\vec{D},\vec{Z})] \leq 2\varepsilon'.$$

We conclude by using the easily verifiable fact that for any random variables X and Y such that $\Pr[X = Y] \geq 1 - 2\varepsilon'$, the total variation distance between the marginal distributions on X and Y is at most $2\varepsilon'$. □

Next, we can use the tomography test TOM to establish (v), and then the fact that by Lemma 5.4 the input to PV is not very different in EPR-Computation and Rigidity-Tomography runs to establish (vi):

Lemma 5.5. *Suppose the verifier executes the Dog-Walker Protocol with provers (PV^*, PP^*) such that: PV^* applies the honest strategy in EPR-Test runs; PP^* applies the honest strategy in the Rigidity-Tomography runs; and the provers are accepted with probability q_1 in the Rigidity-Clifford Run, $q_2 = 1 - \varepsilon'$ in the EPR-Test Run, q_3 in the EPR-Computation Run, and $q_4 = 1 - \varepsilon$ in the Rigidity-Tomography Run. Then there exist provers (PV', PP') such that PV' applies the honest strategy in the Rigidity-Tomography runs and EPR-Computation runs, PP' applies the honest strategy in Rigidity-Tomography runs, and the provers are accepted with probability q_1 in the Rigidity-Clifford Run, $q_2 = 1 - \varepsilon'$ in the EPR-Test Run and $q_3 - \mathrm{poly}(\varepsilon) - O(\varepsilon')$ in the EPR-Computation run.*

Proof. The Rigidity-Tomography runs can be seen as V playing the Tomography Game with the provers, except that whereas PV* gets no non-trivial input in the Tomography Game, in the Rigidity-Tomography run, he gets random values $\vec{c}$ and $\vec{z}$ on which his strategy can depend. Fix $\vec{x}$, and let $\{Q^u_{\vec{c},\vec{z}}\}_u$ be the projective measurement that PV* applies upon receiving $\vec{c}, \vec{z}, \vec{x}$, where $u = (\vec{d}, \vec{e})$ is the string of outcomes obtained by PV on the $n + t$ single-qubit measurements he is to perform according to Step 2 in Figure 19.

By Corollary 3.9, since the provers win the Rigidity-Tomography run with probability $1 - \varepsilon$, for every $\vec{c}, \vec{z} \in \{0,1\}^t$, there exist distributions $q_{\vec{c},\vec{z}}$ on $\Sigma^m \times \{\pm\}$ such that the following is $O(\mathrm{poly}(\varepsilon))$:

$$\mathop{\mathrm{E}}_{\vec{c},\vec{z}} \sum_{u\in\{0,1\}^m} \Big\|\mathrm{Tr}_{\mathsf{A},\hat{\mathsf{B}}}\Big((\mathrm{Id}_{\mathsf{A}} \otimes V_{\mathsf{B}} Q^u_{\vec{c},\vec{z}})|\psi\rangle\langle\psi|_{\mathsf{AB}}(\mathrm{Id}_{\mathsf{A}} \otimes V_{\mathsf{B}} Q^u_{\vec{c},\vec{z}})^\dagger\Big) - \sum_{\lambda\in\{\pm\}} q_{\vec{c},\vec{z}}(W',\lambda)\left(\bigotimes_{i=1}^m \frac{\sigma^{u_i}_{W'_i,\lambda}}{2}\right)\Big\|_1. \tag{5.3}$$

Here we use the notation from Theorem 3.1 and 3.9. The string $W' = W(\vec{c}, \vec{z}, \vec{u}) \in \Sigma^m$ is uniquely determined by $\vec{c}, \vec{z}$, and the outcomes u reported by PV*; indeed it is using this string that PV*'s answers are checked against the measurement outcomes obtained by PP*, who by assumption applies the honest strategy. For any fixed (W', λ) the distribution on outcomes u obtained in the "honest" strategy represented by the right-hand side in (5.3) is uniform. Thus the outcomes u reported by PV* are within $\mathrm{poly}(\varepsilon)$ of uniform. From this it follows that the joint distribution on transcripts $(\vec{c}, \vec{z}, u, W' = W(\vec{c}, \vec{z}, u))$ that results from an interaction with PV* is within statistical distance $\mathrm{poly}(\varepsilon)$ of the distribution generated by an interaction with the honest PV; furthermore, by (5.3) the resulting post-measurement states on PP* are also $\mathrm{poly}(\varepsilon)$ close to the honest ones, on average over this distribution.

We can now consider two provers PV′ and PP′ who, in Rigidity-Tomography runs, first apply the isometries V_A, V_B from Corollary 3.9, then measure their auxiliary systems $\hat{\mathsf{A}}$ and $\hat{\mathsf{B}}$ using Δ_Y, obtaining a shared outcome $\lambda \in \{\pm\}$, and finally apply the honest strategy shown in Item 2 of Figure 19 ($\lambda = +$) or its conjugate ($\lambda = -$). Furthermore, conjugating the honest strategy produces exactly the same statistics as the honest strategy itself, so we may in fact assume that PV′ and PP′ both apply the honest strategy in Rigidity-Tomography runs.

A consequence of PV′ applying the honest strategy in Figure 19 Item 2 is that PV′ also plays the honest strategy in EPR-Computation runs. Since PV′ is still honest in the EPR-Test run and $q_2 = 1 - \varepsilon'$, Lemma 5.4 implies that the distribution of the input to PV′ in EPR-Computation runs is within $\mathrm{poly}(\varepsilon) + O(\varepsilon')$ total variation distance of his input in Rigidity-Tomography runs, therefore the provers' success probability in EPR-Computation runs changes at most by $\mathrm{poly}(\varepsilon) + O(\varepsilon')$. □

Finally, we show that if PV is honest, PP must be honest in EPR computation runs, or the acceptance probability would be low, establishing (vii):

Lemma 5.6. *Suppose V executes the Dog-Walker Protocol on an input $(Q, |\vec{x}\rangle)$ such that $\left\|\Pi_0 Q|\vec{x}\rangle\right\|^2 \leq 1/3$, with provers (PV, PP) such that PV plays the honest strategy. Let q_2 be the provers' acceptance probability in EPR-Test runs. Then the verifier accepts with probability at most $p_1(1-\delta_c) + p_2 q_2 + p_3(5/3 - 4q_2/3) + p_4$.*

Proof. With probability $p_2 + p_3$, V executes an EPR run, in which case, she executes EPR-Computation with probability $\frac{p_3}{p_2+p_3}$ and EPR-Test with probability $\frac{p_2}{p_2+p_3}$. In the former case, since PV is honest, he is executing V^0_{EPR}. In fact, the behavior of an honest PV in the EPR-Test runs is also that of V^r_{EPR}. Thus, the combined behavior of V and PV is that of V_{EPR}. Then the result follows from Theorem 2.3. □

We can now combine Lemmas 5.3, 5.5, and 5.6 to get the main result of this section, the "soundness" part of Theorem 5.1.

Lemma 5.7 (Constant soundness-completeness gap)**.** *There exist constants p_1, p_2, p_3, $p_4 = 1 - p_1 - p_2 - p_3$ and $\Delta > 0$ such that if the verifier executes the Dog-Walker Protocol with parameters (p_1, p_2, p_3, p_4) on input $(Q, |\vec{x}\rangle)$ such that $\left\|\Pi_0 Q|\vec{x}\rangle\right\|^2 \leq 1/3$, then any provers (PV^*, PP^*) are accepted with probability at most $p_{\text{sound}} = p_{\text{compl}} - \Delta$.*

Proof. Suppose the provers PV* and PP* are such that the lowest acceptance probability in either the Rigidity-Clifford run or the Rigidity-Tomography run is $1-\varepsilon$, and they are accepted with probability $1-\varepsilon'$ in the EPR-Test run, and with probability $1/3 + w$ in the Computation Run. Applying Lemma 5.3 and Lemma 5.5 in sequence, we deduce the existence of provers (PV′, PP′) for which

$$
\begin{aligned}
q_1' &= 1 - O(\delta_c),\\
q_2' &= 1 - \varepsilon' - \mathrm{poly}(\varepsilon),\\
q_3' &= \frac{1}{3} + w - \mathrm{poly}(\varepsilon) - O(\varepsilon'),\\
q_4' &= 1,
\end{aligned}
$$

where q_1', q_2', q_3' and q_4' are their success probabilities in the four types of runs, and $1-\delta_c$ is the completeness of the RIGID test; from Theorem 3.1 we have $\delta_c = 2^{-\Omega(n+t)}$. Moreover PV′ applies the honest strategy in all runs, while PP′ applies the honest strategy in the Rigidity-Clifford and Rigidity-Tomography runs. Applying Lemma 5.6, it follows that

$$
w \leq O(\varepsilon') + \mathrm{poly}(\varepsilon) + p_1 \cdot O(\delta_c).
$$

Therefore the prover's overall success probability is at most

$$\begin{aligned}&\min(p_1, p_4)(1-\varepsilon) + \max(p_1, p_4) + p_2(1-\varepsilon') + p_3\left(\frac{1}{3} + w\right)\\ \leq & p_{\text{compl}} - \left(\frac{p_3}{3} + \varepsilon' p_2 + \varepsilon \min(p_1, p_4)\right) + p_3\left(O(\varepsilon') + \text{poly}(\varepsilon)\right) + (p_1 + p_3 p_1)\cdot O(\delta_c),\end{aligned}$$

where recall from Lemma 5.2 that $p_{\text{compl}} = p_1(1-\delta_c) + p_2 + p_4 + \frac{2}{3}p_3$. Fixing p_2 to be a large enough multiple of p_1 and of p_3 we can ensure that the net contribution of the terms involving ε' and δ_c on the right-hand side is always non-positive. Choosing $p_1 = p_4$ and p_3 so that the ratio p_3/p_1 is small enough we can ensure that the right-hand side is less than $p_{\text{compl}} - \Delta$, for some universal constant $\Delta > 0$ and all $\varepsilon, \varepsilon' \geq 0$. □

5.4 Two-prover game for QMA

In this section we propose a new two-prover game for QMA, which is based on the Dog-Walker protocol. Such type of games are important in the context of the Quantum PCP conjecture [1], more specifically to its game version that was recently proved [36].

A promise problem L is in QMA if there is a uniform family of quantum circuits $\{V_x\}_{x\in L}$ such that if x is a yes-instance, then there exists a quantum state $|\psi\rangle \in \left(\mathbb{C}^2\right)^{\otimes n_w}$, such that V_x accepts on input $|\psi\rangle|0\rangle^{\otimes n_a}$ with probability at least $\frac{2}{3}$, while for a no-instance x and all states $|\psi\rangle \in \left(\mathbb{C}^2\right)^{\otimes n_w}$, V_x rejects on input $|\psi\rangle|0\rangle^{\otimes n_a}$ with probability at least $\frac{2}{3}$. The run-time of the circuit V_x and the values n_w and n_a are polynomially bounded in $|x|$.

In a multi-prover game for a promise problem L, an instance $x \in L$ is reduced to a game G_x such that if x is a yes-instance, then the maximum acceptance probability in the game is at least c, whereas if x is a no-instance, then the maximum acceptance probability in the game is at most s, for $c > s$.

Here, we are interested in multi-prover games where the verifier is classical, the honest provers run a polynomially bounded quantum computation on copies of an accepting witness and the completeness-soundness gap $c - s$ is constant. Using the Dog-Walker protocol, we are able to construct, to the best of our knowledge, the first two-prover game for QMA with these parameters. In our protocol the Verifier and provers exchange messages of polynomial size in two rounds of communication, one with each prover.

Our protocol consists in the Verifier running the Dog-Walker protocol, with the following changes:

- On X-test runs and Z-test runs, the Verifier randomly selects positions where PV has measured in the Z basis and X basis, respectively, and sends them to PP. PP uses the EPR pair halves in these positions as the witness register when he executes the circuit V_x.
- On Rigidity-Computation runs, the Verifier informs PV of the halves of EPR pairs that should be used to teleport the witness state to PP, and PV reports the outcomes of the teleportation measurements along with the answers for the original Dog-Walker protocol.

The Verifier ignores the measurements corresponding to the teleportation and uses the remaining bits to perform the same checks as in the original Dog-Walker protocol.

- On EPR-Computation runs, the Verifier informs PP of the EPR pair halves that should be used as the witness when he performs the circuit V_x. The Verifier also informs PV of these positions, who should use them to teleport the witness state to PP. The outcomes of the teleportation measurements are reported to the Verifier along with the answers for the original Dog-Walker protocol, in order that the Verifier can decrypt the output of the computation.

The full description of the protocol is presented in Figures 22, 23 and 25, where the differences to the original Dog-Walker protocol are underlined. We state our result in Lemma 5.8 and provide a proof sketch for it.

Let x be an instance of a language $L \in$ QMA and V_x the associated verification circuit. V_x takes as input an n_w-qubit witness register and an n_a-qubit ancilla register. It has t T gates, t_0 of which are even and $t - t_0$ are odd (see Section 2.4 for the definition of even and odd T gates).

1. Select a run type **EPR** or **Rigidity**, and disjoint sets $N^w, N^a, T^0, T^1 \subset \{1, \ldots, m\}$ of sizes n_w, n_a, t_0 and $t - t_0$, respectively.

EPR Choose $\vec{z}$ uniformly at random from $\{0,1\}^t$ and send it, along with $\vec{x}$, N^w, N^a, T^0 and T^1, to PP. Receive measurement outcomes $\vec{c} \in \{0,1\}^t$ and $c_f \in \{0,1\}$ from PP.

Rigidity Choose W' according to $\mu(\cdot)$ and send it to PP. Receive $\vec{e}' \in \{0,1\}^m$ from PP.

2. Select a subrun type at random from **Computation**, **X-test** or **Z-test**. Based on this choice, as well as the run type (**EPR** or Rigidity), proceed as in Figure 24.

Figure 22: QMA Protocol: Verifier's point of view.

---

1. If PP receives a question W' from V (he is playing TOM or RIGID):

   Measure the m qubits in the observable indicated by W' — for example, if $W' \in \Sigma^m$, for $i \in \{1, \ldots, m\}$, measure the i-th qubit in the basis indicated by W'_i — and report the outcomes $\vec{e}'$ to V.

2. If PP receives $\vec{x}, \vec{z}$, and sets N^w,N^a, T^0 and T^1 from V (he is playing the role of P_{EPR} from the EPR Protocol):

   Run prover P_{EPR} from Figure 3c with the V_x as the circuit Q, on input $\vec{z}$, <u>the n_w qubits in N^w as the witness</u>, the n_a qubits in N^a as the ancilla, and the t qubits in $T^0 \cup T^1$ for T gadgets. Report the outputs $\vec{c} \in \{0,1\}^t$ and $c_f \in \{0,1\}$ of P_{EPR} to V.

Figure 23: QMA Protocol: Honest strategy for PP.

Computation Based on whether it is an EPR or a Rigidity Run:

EPR (i) Send $\vec{x}$, $\vec{z}$, $\vec{c}$ and sets $\underline{N^w}$, N^a, T^0 and T^1 to PV, and receive measurement outcomes $\underline{\vec{a}, \vec{b} \in \{0,1\}^{n_w+n_a}}$ and $\vec{e} \in \{0,1\}^t$.

(ii) Apply the update rules from Table 2 gate-by-gate to obtain the final X key for the output wire a'_f. If $c_f + a'_f \neq 0$, reject.

Rigidity (Tomography) (i) Choose uniform random strings $\vec{c}, \vec{z} \in \{0,1\}^t$, $\vec{x} \in \{0,1\}^n$ to send to PV, along with $\underline{N^w}$, N^a and T, and receive measurement outcomes $\underline{\vec{a}, \vec{b} \in \{0,1\}^{n_w+n_a}}$ and $\vec{e} \in \{0,1\}^t$.

(ii) From $\vec{x}$, $\vec{c}$, $\vec{z}$, $\vec{a}$, $\vec{b}$ and $\vec{e}$, determine the adaptive measurements $W \in \Sigma^{n+t}$ that V^0_{EPR} would have performed (based on Figure 3b), and reject if the input-output pairs $(W', \vec{e}')$ and $(N \cup T, (W, \vec{e}))$ do not satisfy the winning criterion for $\textsc{tom}(\Sigma, n+t, m)$.

X**-test** Based on whether it is an EPR or a Rigidity Run:

EPR (i) Choose $W \in \Sigma^m$ uniformly at random among all strings satisfying: $W_i = Z$ for all $i \in \underline{N^w} \cup N^a$; $W_i = Z$ for all $i \in T^0$; and $W_i \in \{X, Y\}$ for all $i \in T^1$. Send W to PV and receive measurement results $\vec{e} \in \{0,1\}^m$. Let $(\vec{a}, \vec{b}) = (\vec{e}_N, 0^n)$.

(ii) Apply update rules from Table 2 gate-by-gate to obtain $\forall i \in [t]$ the X key before the i-th T gate is applied, a'_i, and the final X key for the output wire, a'_f. If $\exists i$ s.t. the i-th T gate is even and $c_i \neq a'_i + e_i$, reject. If $c_f + a'_f \neq 0$, reject.

Rigidity (Clifford) Choose W according to the marginal conditioned on W', $\mu(\cdot|W')$. Send W to PV and receive $\vec{e} \in \{0,1\}^m$. Reject if $(W', \vec{e}', W, \vec{e})$ does not win $\textsc{rigid}(\Sigma, m)$.

Z**-test** Based on whether it is an EPR or a Rigidity Run:

EPR (i) Choose $W \in \Sigma^m$ uniformly at random among all strings satisfying: $W_i = X$ for all $i \in \underline{N^w} \cup N^a$; $W_i \in \{X, Y\}$ for all $i \in T^0$; and $W_i = Z$ for all $i \in T^1$. Send W to PV and receive measurement results $\vec{e} \in \{0,1\}^m$. Let $(\vec{a}, \vec{b}) = (0^n, \vec{e}_N)$.

(ii) Apply update rules from Table 2 gate-by-gate to obtain $\forall i \in [t]$, the X key before the i-th T gate is applied, a'_i. If $\exists i$ s.t. the i-th T gate is odd and $c_i \neq a'_i + e_i$, reject.

Rigidity (Clifford) Identical to X-test case.

Figure 24: QMA Protocol: Step 2 of Verifier's point of view. Verifier's behavior in Step 2 is determined by the subrun type (**Computation**, **X-test** or **Z-test**) as well as the run type (**EPR** or **Rigidity**).

1. If PV receives a question W from V (he is playing RIGID or an X- or Z-test Run):

   Measure the m qubits in the observable indicated by W — for example, if $W \in \Sigma^m$, for $i \in \{1, \ldots, m\}$, measure the i-th qubit in the basis indicated by W_i — and report the outcomes $\vec{e}$ to V.

2. If PV receives $\vec{x}, \vec{z}, \vec{c}$ and sets N^w, N^a, T^0 and T^1 from V (he is playing TOM or a Computation Run):

   Using the EPR pairs in N^w, teleports the witness state $|\psi\rangle$ that makes V_x accept with high probability. Let $(\vec{a}_{N^w}, \vec{b}_{N^w})$ be the corresponding outcomes of the teleportation measurements.

   Measure each qubit in N^a in the Z basis with outcomes $\vec{d}$ and let $(\vec{a}_{N^a}, \vec{b}_{N^a}) = (\vec{d}, \vec{0})$

   Run the second step of procedure V^0_{EPR} from Figure 3b with V_x as the circuit Q, and the values $\vec{c}, \vec{z}$, the n_w qubits in N^w as the witness, the n_a qubits in N^a as the ancilla, and the t qubits in $T^0 \cup T^1$ for T gadgets. Report the outputs $\vec{a}, \vec{b}$ and $\vec{e}$ of V^0_{EPR} to V.

Figure 25: QMA Protocol: Honest strategy for PV.

Lemma 5.8. *There exist universal constants $0 \leq p_{\text{compl}} \leq 1$ and $\Delta > 0$ such that the following holds. Let L be a language in QMA and x an instance of L such that $n = |x|$. Let V_x be the verification circuit for this instance and g the number of gates in V_x (in the compiled form as described in Section 2). Then there exists a two-round interactive protocol between a classical verifier and two entangled provers where the Verifier sends $O(n+g)$-bit questions to the provers, the provers answer with $O(n+g)$ bits and the protocol satisfies the following properties.*

Completeness: *If x is a yes-instance, then there is a strategy for the provers such that the Verifier accepts with probability at least p_{compl}.*

Soundness: *If x is a no-instance, then for all strategies of the provers, the Verifier accepts with probability at most $p_{\text{sound}} = p_{\text{compl}} - \Delta$.*

Proof sketch. The Verifier performs the operations described in Figure 22.

The completeness of the protocol is straightforward: if PP and PV use the strategy in Figures 23 and 25, respectively, then the Verifier accepts with high probability.

The soundness of the protocol follows from the combination of the soundness of the Dog-Walker protocol and the soundness of the QMA verification circuit. Along the same lines as Lemmas 5.3, 5.4 and 5.5, we can show that if the acceptance probability in Rigidity-Test, Rigidity-Computation and EPR-Test runs is sufficiently high, then there is a strategy where the provers follow the honest strategy and the acceptance probability in EPR-Computation run is only slightly changed. In the case where the provers are honest in the Rigidity-Test, Rigidity-Computation and EPR-Test runs, no matter which state is held by PP as witness state,

V_x rejects with high probability in the EPR-Computation run, by the soundness of the QMA verification circuit. The proof of soundness can be completed by repeating the arguments in Lemma 5.7. □

6 Running our protocols in sequence

In order to make a fair comparison between previous delegated computation protocols and ours (see Figure 1) the resource requirements are computed under the condition that they produce the correct outcome of the computation with 99% probability. For most protocols, this is achieved by sequentially repeating the original version, in order to amplify the completeness-soundness gap.

In this section, we describe a sequential procedure that, starting from our protocols in Sections 4 and 5, ensures that either the verifier aborts, or she obtains the correct outcome of the computation with probability 99%. Moreover, for honest provers, the probability that the procedure aborts is exponentially small in the number of sequential repetitions. Our sequential procedure has a number of rounds which depends on the desired soundness. As long as one only requires amplification of an arbitrarily small, but constant, soundness, to a fixed constant, the number of sequential repetitions remains constant.

To emphasize the importance of having such a sequential procedure, we note that, firstly, the current completeness-soundness gap between acceptance probability on *yes* and *no* instances, for both the leash and the Dog-Walker protocol, is a very small constant. Secondly, if a classical client wishes to employ our protocols to delegate a computation, we need to specify what the client interprets, at the end of the protocol, as the outcome of the delegated computation. The natural approach is to have the verifier interpret accept as a *yes* outcome and reject as a *no* outcome. However, this is not enough, as our security model based on the constant gap between acceptance probability for *yes* and *no* instances means that, while the provers have a low probability of making the verifier accept a *no* instance as a *yes*, they can always make the verifier accept a *yes* instance as a *no*, simply by behaving so that they are rejected.

The first point is addressed by running copies of the original protocol in sequence to amplify the completeness-soundness gap. The second point is addressed by having the verifier run the protocol twice: once for the circuit Q, and once for the circuit Q' defined by appending an X gate to the output wire of Q. If $f : X \to \{0,1\}$ for some $X \subseteq \{0,1\}^n$ is defined by $f(x) = 1$ if $\|\Pi_0 Q|x\rangle\|^2 \geq 2/3$, and $f(x) = 0$ if $\|\Pi_0 Q|x\rangle\|^2 \leq 1/3$, i. e., Q decides f with bounded error $1/3$, then it is easy to see that Q' decides $1 - f$ with bounded error $1/3$. Thus, the verifier will accept x as a *yes* instance of f if the protocol outputs accept when running Q on x and outputs reject when running Q' on x. The verifier accepts x as a *no* instance of f if the protocol outputs reject when running Q on x and outputs accept when running Q' on x. The verifier aborts if she sees accept-accept or reject-reject.

6.1 Sequential version of our protocols

Let P denote either the Verifier-on-a-Leash or the Dog-Walker protocol from Sections 4 and 5, respectively, and let c and Δ denote the completeness and the completeness-soundness gap, resp. Let κ be a security parameter.

Protocol Seq(P, c, Δ, κ): Let (Q, x) be the verifier's input.

1. The verifier runs κ copies of protocol P in sequence on input (Q, x) with PP and PV. Then she runs κ copies in sequence on input (Q', x).

2. Let $\vec{o}, \vec{\tilde{o}} \in \{0,1\}^\kappa$ be such that $o_i = 1$ iff the i-th copy on input (Q, x) accepts, and $\tilde{o}_i = 1$ iff the i-th copy on input (Q', x) accepts. Let $wt(\vec{o})$ and $wt(\vec{\tilde{o}})$ be their Hamming weights. Then, the verifier accepts 1 as the outcome of the delegated computation if $wt(\vec{o}) \geq (c - \frac{\Delta}{2}) \cdot \kappa$ and $wt(\vec{\tilde{o}}) < (c - \frac{\Delta}{2}) \cdot \kappa$, and she accepts 0 as the outcome of the computation if $wt(\vec{o}) < (c - \frac{\Delta}{2}) \cdot \kappa$ and $wt(\vec{\tilde{o}}) \geq (c - \frac{\Delta}{2}) \cdot \kappa$. Otherwise the verifier aborts.

Figure 26: Sequential version of our protocols

We state and prove completeness and soundness for the sequential protocol.

Theorem 6.1. *Let c and Δ be respectively the completeness and completeness-soundness gap of protocol P. On input (Q, x):*

- *If the provers are honest,*

$$\Pr\left(\textit{Seq}(P, c, \Delta, \kappa) \textit{ outputs } f(x)\right) \geq 1 - 2\exp\left(-\frac{\Delta^2 \kappa}{2}\right).$$

- *For any cheating provers,*

$$\Pr\left(\textit{Seq}(P, c, \Delta, \kappa) \textit{ outputs } 1 - f(x)\right) \leq \exp\left(-\frac{\Delta^2 \kappa}{8}\right).$$

Proof. We first show completeness. Let $s = c - \Delta$ be the soundness of protocol P. Suppose $f(x) = 1$ (the case $f(x) = 0$ is analogous). If the provers are honest, then the probability that the verifier outputs 1 is:

$$\begin{aligned}\Pr(\text{Verifier outputs } 1) &= \Pr\left(wt(\vec{o}) \geq \left(c - \frac{\Delta}{2}\right)\cdot\kappa \ \wedge \ wt(\vec{\tilde{o}}) < \left(c - \frac{\Delta}{2}\right)\cdot\kappa\right) \\ &\geq 1 - \Pr\left(wt(\vec{o}) < \left(c - \frac{\Delta}{2}\right)\cdot\kappa\right) - \Pr\left(wt(\vec{\tilde{o}}) \geq \left(c - \frac{\Delta}{2}\right)\cdot\kappa\right) \\ &\geq 1 - 2\exp\left(-\frac{\Delta^2\kappa}{2}\right)\end{aligned}$$

by the Azuma–Hoeffding inequality (Theorem 2.1).

Next we show soundness. Again suppose $f(x) = 1$ (the case $f(x) = 0$ is analogous). Let W_j be an indicator random variable for the event $\tilde{o}_j = 1$, and let $F_j = W_j - s$. One might be tempted to immediately assert that $\mathrm{E}(F_j|F_{j-1},..,F_1) \leq 0$. However, because of the sequentiality of the runs of protocol P, this is not in general true, and an analysis that treats protocol P as a black-box does not suffice when P is the verifier-on-a-leash protocol (because such a protocol is blind). We argue more precisely that $\mathrm{E}(F_j|F_{j-1},..,F_1) \leq 0$:

- When P is the Dog-Walker protocol from Section 5 (which is not blind): suppose for a contradiction that there were provers PV and PP, and a j such that $\mathrm{E}(F_j|F_{j-1},..,F_1) \leq 0$. Then one can construct provers PV′ and PP′ which break the soundness of protocol P. Namely PV′ and PP′ simulate $j-1$ runs of protocol P. They then respectively invoke PV and PP and forward to them the transcripts previously generated. PV′ and PP′ then participate in the challenge protocol P by forwarding all of the incoming messages to the invocations of PV and PP, respectively. By the initial hypothesis, such PV′ and PP′ would break the soundness of P.

- When P is the Verifier-on-a-leash protocol from Section 4: the key observation is that protocol P remains sound even when x is revealed to the provers. Then, notice that if it is possible for provers to force $\mathrm{E}(F_j|F_{j-1},..,F_1) \leq 0$ when x is not revealed, it is clearly also possible to do so when x is revealed. However, the latter is not possible, by an analogous reduction to the one for the dog-walker protocol.

Define $X_0 = 0$ and $X_\ell = \sum_{j=1}^{\ell} F_j$, for $\ell = 1,..,\kappa$. The the sequence $\{X_\ell\}$ constitutes a supermartingale with $|X_\ell - X_{\ell-1}| = |F_\ell| \leq 1 \ \forall \ell$. Hence,by the Azuma–Hoeffding inequality (Theorem 2.1), for any $\kappa \geq 1$ and $t \geq 0$, $\Pr(X_\kappa \geq t) \leq \exp(-\frac{t^2}{2\kappa})$. This implies that

$$\Pr\left(\sum_{j=1}^{\kappa} W_j - \kappa\cdot s \geq t\right) = \Pr\left(\sum_{j=1}^{\kappa} F_j \geq t\right) = \Pr\left(X_\kappa \geq t\right) \leq \exp\left(-\frac{t^2}{2\kappa}\right).$$

Then, for any provers PP and PV,

$$\begin{aligned}\Pr(\text{Verifier outputs } 0) &\leq \Pr\left(wt(\vec{o}) \geq (c - \frac{\Delta}{2}) \cdot \kappa\right) \\ &= \Pr\left(\sum_{j=1}^{\kappa} W_j \geq (c - \frac{\Delta}{2}) \cdot \kappa\right) \\ &= \Pr\left(\sum_{j=1}^{\kappa} W_j - \kappa \cdot s \geq \kappa \cdot \frac{\Delta}{2}\right) \\ &\leq \exp\left(-\frac{\Delta^2 \kappa}{8}\right). \end{aligned}$$

□

Finally, one can check that when P is the verifier-on-a-leash protocol, then $\mathrm{Seq}(P, c, \Delta, \kappa)$ remains blind. This follows from a similar argument as in the proof of Lemma 4.6.

A Some simple tests

In this appendix we collect simple tests that will be used as building blocks. In Section A.1 and Section A.2 we review elementary tests whose analysis is either immediate or can be found in the literature. In Section A.3 we formulate a simple test for measurements in the Bell basis and the associated two-qubit SWAP observable. Finally, in Section A.4, we show how to extend the results from [35] to derive a robust self-test for the m-qubit Pauli group.

A.1 The Magic Square game

We use the Magic Square game [29] as a building block, noting that it provides a robust self-test for the two-qubit Weyl–Heisenberg group (see Section 2.1 for the definition). A question in this game is specified, either by a label corresponding to an entry from the square pictured in Figure 27 (9 questions, labeled IZ, etc.), or by a triple of labels corresponding to the same row or column (6 questions, labeled (IZ, XI, XZ), etc.); there are 15 questions in total. An answer is composed of three values in $\{\pm 1\}$, one for each of the labels making up the question. Answers from the prover should be entrywise consistent, and such that the product of the answers associated to any row or column except the last should be $+1$; for the last column it should be -1. The labels indicate the "honest" strategy for the game, which consists of each prover measuring two half-EPR pairs using the commuting Pauli observables indicated by the labels of his question.

IZ	ZI	ZZ
XI	IX	XX
XZ	ZX	YY

Figure 27: Questions, and a strategy, for the Magic Square game

The following lemma states some properties of the Magic Square game, interpreted as a self-test (see, e. g., [40]).

Lemma A.1. *Suppose a strategy for the provers, using state $|\psi\rangle$ and observables W, succeeds with probability at least $1-\varepsilon$ in the Magic Square game. Then there exist isometries $V_D : \mathcal{H}_D \to (\mathbb{C}^2 \otimes \mathbb{C}^2)_{D'} \otimes \mathcal{H}_{\hat{D}}$, for $D \in \{A, B\}$ and a state $|\textsc{aux}\rangle_{\hat{A}\hat{B}} \in \mathcal{H}_{\hat{A}} \otimes \mathcal{H}_{\hat{B}}$ such that*

$$\left\|(V_A \otimes V_B)|\psi\rangle_{AB} - |\mathrm{EPR}\rangle_{A'B'}^{\otimes 2}|\textsc{aux}\rangle_{\hat{A}\hat{B}}\right\|^2 = O(\sqrt{\varepsilon}),$$

and for $W \in \{I, X, Z\}^2 \cup \{YY\}$,

$$\left\|\left(W - V_A^\dagger \sigma_W V_A\right) \otimes \mathrm{Id}_B\, |\psi\rangle\right\|^2 = O(\sqrt{\varepsilon}).$$

A.2 Elementary tests

Figure 28 summarizes some elementary tests. For each test, “Inputs” refers to a subset of designated questions in the test; “Relation” indicates a relation that the test aims to certify (in the sense of Section 3.1); “Test” describes the certification protocol. (Recall that all our protocols implicitly include a “consistency” test in which a question is chosen uniformly at random from the marginal distribution and sent to both provers, whose answers are accepted if and only if they are equal.)

Test $\textsc{id}(A, B)$:

- Inputs: A, B two observables on the same space $\mathcal{H}$.
- Relation: $A = B$.
- Test: Send $W \in \{A, B\}$ and $W' \in \{A, B\}$, chosen uniformly at random, to the first and second prover, respectively. Receive an answer in $\{\pm 1\}$ from each prover. Accept if and only if the answers are equal whenever the questions are identical.

Test $\textsc{ac}(X, Z)$:

- Inputs: X, Z two observables on the same space $\mathcal{H}$.
- Relation: $XZ = -ZX$.
- Test: Execute the Magic Square game, using the label "X" for the "XI" query and "Z" for the "ZI" query. All other queries, such as IZ, or (IZ, ZI, ZZ), are sent together with the pair (X, Z). (So, for example, the query "ZI" in the Magic Square becomes "Z" here, whereas the query "IZ" becomes "$IZ, (X, Z)$", where the first IZ are simply letters, whereas in (X, Z) the X and Z should be replaced by the inputs to this test.)

Test $\textsc{com}(A, B)$:

- Inputs: A, B two observables on the same space $\mathcal{H}$.
- Relation: $AB = BA$.
- Test: Send $W \in \{A, B\}$ chosen uniformly at random to the first prover. Send (A, B) to the second prover. Receive a bit $c \in \{\pm 1\}$ from the first prover, and two bits $(a', b') \in \{\pm 1\}^2$ from the second. Accept if and only if $c = a'$ if $W = A$, and $c = b'$ if $W = B$.

Test $\textsc{prod}(A, B, C)$:

- Inputs: A, B and C three observables on the same space $\mathcal{H}$.
- Relations: $AB = BA = C$.
- Test: Similar to the commutation game, but use C to label the question (A, B).

Figure 28: Some elementary tests.

Lemma A.2. *Each of the tests described in Figure 28 is a robust $(1, \delta)$ self-test for the indicated relation(s), for some $\delta = O(\varepsilon^{1/2})$.*

Proof. The proof for each test is similar. As an example we give it for the commutation test $\textsc{com}(A, B)$.

First we verify completeness. Let A, B be two commuting observables on $\mathcal{H}_\mathsf{A} = \mathcal{H}_\mathsf{B} = \mathcal{H}$, and $|\mathrm{EPR}\rangle_{\mathsf{AB}}$ the maximally entangled state in $\mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B}$. Upon receiving question A or B, the prover measures the corresponding observable. If the question is (A, B), he jointly measures A and B. This strategy succeeds with probability 1 in the test.

Next we establish soundness. Let $|\psi\rangle \in \mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B}$ be a state shared by the provers, A, B their observables on questions A, B, and $\{C^{a,b}\}$ the four-outcome PVM applied on question (A, B). Assume the strategy succeeds with probability at least $1-\varepsilon$. Recall that this includes both the test described in Figure 28, and the automatic consistency test. Let $C_A = \sum_{a,b}(-1)^a C^{a,b}$ and $C_B = \sum_{a,b}(-1)^b C^{a,b}$. Then C_A and C_B commute. Thus

$$\begin{aligned}
A_\mathsf{A} B_\mathsf{A} \otimes \mathrm{Id}_\mathsf{B} &\approx_{\sqrt{\varepsilon}} A_\mathsf{A} \otimes (C_B)_\mathsf{B} \\
&\approx_{\sqrt{\varepsilon}} \mathrm{Id}_\mathsf{A} \otimes (C_B)_\mathsf{B} (C_A)_\mathsf{B} \\
&= \mathrm{Id}_\mathsf{A} \otimes (C_A)_\mathsf{B} (C_B)_\mathsf{B} \\
&\approx_{\sqrt{\varepsilon}} B_\mathsf{A} \otimes (C_A)_\mathsf{B} \\
&\approx_{\sqrt{\varepsilon}} B_\mathsf{A} A_\mathsf{A} \otimes \mathrm{Id}_\mathsf{B}\,.
\end{aligned}$$

Here each approximation uses the consistency condition provided by the test, as explained in (3.3). Thus $[A, B] = (AB - BA) \approx_{\sqrt{\varepsilon}} 0$, as desired. □

We will often make use of the following simple lemma, which expresses an application of the above tests. Recall the notations $[A, B]$ for $AB - BA$ and $\{A, B\}$ for $AB + BA$.

Lemma A.3. *Let $|\psi\rangle \in \mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B}$ and A, X observables on $\mathcal{H}_\mathsf{A}$ such that there exists an isometry $\mathcal{H}_\mathsf{A} \simeq \mathbb{C}^2 \otimes \mathcal{H}_{\hat{\mathsf{A}}}$ under which the following conditions hold, for some $\delta_1, \delta_2, \delta_3$:*[15]

(i) There exists an observable A' on $\mathcal{H}_\mathsf{B}$ such that $A \otimes \mathrm{Id} \approx_{\delta_1} \mathrm{Id} \otimes A'$;

(ii) $|\psi\rangle \simeq_{\delta_1} |\mathrm{EPR}\rangle|\textsc{aux}\rangle$ and $X \simeq_{\delta_1} \sigma_X \otimes \mathrm{Id}$;

(iii) $[A, X] \approx_{\delta_2} 0$;

(iv) $\{A, X\} \approx_{\delta_3} 0$.

Then there exist Hermitian A_I, A_X, A_Y, A_Z on $\mathcal{H}_{\hat{\mathsf{A}}}$ such that $A \simeq_{\delta_1+\delta_2} \mathrm{Id} \otimes A_I + \sigma_X \otimes A_X$ and $A \simeq_{\delta_1+\delta_3} \sigma_Y \otimes A_Y + \sigma_Z \otimes A_Z$. (A similar claim holds with X replaced by Z.)

Proof. After application of the isometry, an arbitrary observable $\tilde{A}$ on $\mathbb{C}^2 \otimes \mathcal{H}_{\hat{\mathsf{A}}}$ has a decomposition $\tilde{A} = \sum_{P \in \{I,X,Y,Z\}} \sigma_P \otimes A_P$, for Hermitian operators A_P on $\mathcal{H}_{\hat{\mathsf{A}}}$. We can compute

$$[\tilde{A}, \sigma_X \otimes \mathrm{Id}] = -2i\, \sigma_Z \otimes A_Y + 2i\, \sigma_Y \otimes A_Z, \tag{A.1}$$

$$\{\tilde{A}, \sigma_X \otimes \mathrm{Id}\} = 2\, \sigma_X \otimes A_I + 2\, \sigma_I \otimes A_X. \tag{A.2}$$

Assumptions (i) and (ii) imply $[A, X] \simeq_{\delta_1} [\tilde{A}, \sigma_X \otimes \mathrm{Id}]$, so by (iii) and (A.1) we get $\|A_Y|\textsc{aux}\rangle\|^2 + \|A_Z|\textsc{aux}\rangle\|^2 = O(\delta_1+\delta_2)$. Similarly, (iv) and (A.2) give $\|A_I|\textsc{aux}\rangle\|^2 + \|A_X|\textsc{aux}\rangle\|^2 = O(\delta_1+\delta_3)$. □

[15]Note that we allow either δ_i to equal 1. The lemma is interesting when δ_1 and *either* δ_2 *or* δ_3 is small (but it is correct for all triples of values in $[0, 1]$)

A.3 The Bell basis

Given two commuting pairs of anti-commuting observables $\{X_1, Z_1\}$ and $\{X_2, Z_2\}$ we provide a test for a four-outcome projective measurement in the Bell basis specified by these observables, i. e., the joint eigenbasis of X_1X_2 and Z_1Z_2. The same test can be extended to test the "SW" observable,

$$\mathrm{SW} = \frac{1}{2}\big(\mathrm{Id} + X_1X_2 + Z_1Z_2 - (X_1Z_1)(X_2Z_2)\big), \tag{A.3}$$

which exchanges the qubits specified by each pair of observables. The Bell measurement test described in Figure 29 tests for both.

Test $\textsc{Bell}(X_1, X_2, Z_1, Z_2)$:

- Inputs: For $i \in \{1,2\}$, $\{X_i, Z_i\}$ observables, $\{\Phi^{ab}\}_{a,b\in\{0,1\}}$ a four-outcome projective measurement, and SW an observable, all acting on the same space $\mathcal{H}$.
- Relations: for all $a, b \in \{0,1\}$, $\Phi^{ab} = \frac{1}{4}\big(\mathrm{Id} + (-1)^a Z_1Z_2\big)\big(\mathrm{Id} + (-1)^b X_1X_2\big)$, and $\mathrm{SW} = \Phi^{00} + \Phi^{01} + \Phi^{10} - \Phi^{11}$.
- Test: execute each of the following with equal probability:
  (a) Execute the Magic Square game, labeling each entry of the square from Figure 27 (except entry $(3,3)$, labeled as Y_1Y_2) using the observables X_1, Z_1 and X_2, Z_2.
  (b) Send Φ to one prover and the labels (X_1X_2, Z_1Z_2, Y_1Y_2) associated with the third column of the Magic Square to the other. The first prover replies with $a, b \in \{0,1\}$, and the second with $c, d, e \in \{\pm 1\}$. The referee checks the provers' answers for the obvious consistency conditions. For example, if the first prover reports the outcome $(0,0)$, then the referee rejects if $(c, d) \neq (+1, +1)$.
  (c) Send Φ to one prover and SW to the other. The first prover replies with $a, b \in \{0,1\}$, and the second with $c \in \{\pm 1\}$. Accept if and only $c = (-1)^{ab}$.

Figure 29: The Bell measurement test.

Lemma A.4. *The test* $\textsc{Bell}(X_1, X_2, Z_1, Z_2)$ *is a robust* $(1, \delta)$ *self-test for the Hermitian operators* X_1, X_2, Z_1, Z_2, $\{\Phi^{ab}\}_{a,b\in\{0,1\}}$ *and SW and the relations*

$$\begin{aligned}\mathcal{R} = \Big\{\big\{\Phi^{ab}\big\}_{a,b\in\{0,1\}} \in \mathrm{Proj},\ SW \in \mathrm{Obs}\Big\} \\ \cup \Big\{\Phi^{ab} = \frac{1}{4}\big(1 + (-1)^a Z_1Z_2\big)\big(1 + (-1)^b X_1X_2\big)\Big\} \\ \cup \big\{SW = \Phi^{00} + \Phi^{01} + \Phi^{10} - \Phi^{11}\big\},\end{aligned}$$

for some $\delta(\varepsilon) = O(\sqrt{\varepsilon})$.

Proof. Completeness is clear: the provers can play the honest strategy for the Magic Square game, use a measurement in the Bell basis on their two qubits for Φ, and measure the observable in (A.3) for SW.

For soundness, let $|\psi\rangle \in \mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}}$, $\{W_1 W_2' : W, W' \in \{I, X, Z\}\}$, $\{\Phi^{ab}\}$ and SW denote a state and operators for a strategy that succeeds with probability at least $1-\varepsilon$ in the test. From the analysis of the Magic Square game (Lemma A.1) it follows that the provers' observables X_1X_2 and Z_1Z_2 associated to questions with those labels approximately commute, and are each the product of two commuting observables X_1I, IX_2 and Z_1I, IZ_2, respectively, such that X_1I and Z_1I, and IX_2 and IZ_2, anti-commute; all approximate identities hold up to error $O(\sqrt{\varepsilon})$.

Since X_1X_2 and Z_1Z_2 appear together in the same question (the last column of the Magic Square, Figure 27), each prover has a four-outcome projective measurement $\{W^{c,d}\}_{c,d\in\{0,1\}}$ such that $\sum_d (-1)^c W^{c,d} = X_1X_2$ and $\sum_c (-1)^d W^{c,d} = Z_1Z_2$, from which it follows that $W^{c,d} = (1/4)(1+(-1)^c Z_1Z_2)(1+(-1)^d X_1X_2)$.

The prover's success probability in part (b) of the test is then

$$\sum_{a,b} \langle\psi|\Phi^{ab} \otimes W^{a,b}|\psi\rangle = \sum_{a,b} \langle\psi|\Phi^{ab} \otimes \frac{1}{4}\big(1+(-1)^a Z_1Z_2\big)\big(1+(-1)^b X_1X_2\big)|\psi\rangle.$$

Using that, by assumption, $\{\Phi^{ab}\}$ is a projective measurement, the condition that this expression be at least $1-O(\varepsilon)$ implies

$$\Phi^{ab} \otimes \mathrm{Id} \approx_{\sqrt{\varepsilon}} \mathrm{Id} \otimes \frac{1}{4}\big(1+(-1)^a Z_1Z_2\big)\big(1+(-1)^b X_1X_2\big).$$

Combining this with the implicit consistency test yields the first relation. The last is guaranteed by part (c) of the test, which checks for the correct relationship between SW and Φ; the analysis is similar. ◻

A.4 Multi-qubit tests

In this section we formulate a robust self-test for the m-qubit Pauli group. The result is an extension of the results from [35] to allow testing of σ_Y observables.

A.4.1 The m-qubit Weyl–Heisenberg group

We start by giving a self-test for tensor products of σ_X and σ_Z observables acting on m qubits, i. e., the m-qubit Weyl–Heisenberg group $\mathcal{H}^{(m)}$ (see Section 2.1). Let $\mathcal{P}^{(m)}$ denote the relations

$$\begin{aligned}\mathcal{P}^{(m)}\{X,Z\} = &\Big\{W(a) \in \mathrm{Obs} \,:\, W \in \prod_{i=1}^m \{X_i, Z_i\},\, a \in \{0,1\}^m\Big\}\\ &\cup \Big\{W(a)W'(a') = (-1)^{|\{i:\, W_i \neq W_i' \wedge a_i a_i' = 1\}|} W'(a')W(a) \,:\, W, W' \in \prod_{i=1}^m \{X_i, Z_i\},\, a, a' \in \{0,1\}^m\Big\}\\ &\cup \Big\{W(a)W(a') = W(a+a') \,:\, W \in \prod_{i=1}^m \{X_i, Z_i\},\, a, a' \in \{0,1\}^m\Big\}.\end{aligned}$$

Recall the notation $W(a)$ for the string that is W_i when $a_i = 1$ and I otherwise. The set of relations on the second line expresses the canonical anti-commutation relations. The last set of relations expresses the obvious relations $\sigma_W \,\mathrm{Id} = \mathrm{Id}\, \sigma_W$ and $\sigma_W^2 = \mathrm{Id}$, for $W \in \{X, Z\}$, coordinate-wise. It is easy to verify that $\mathcal{P}^{(m)}$ forms a defining set of relations for $\mathcal{H}^{(m)}$. Our choice of relations is suggested by the Pauli Braiding Test introduced in [35], which shows that the relations are testable with a robustness parameter $\delta(\varepsilon)$ that is independent of m. The test is denoted $\textsc{pbt}(X, Z)$. For convenience here we use a slight variant of the test which includes more questions and more answers; the test is summarized in Figure 30.

Test $\textsc{pbt}(X, Z)$:

- Inputs: (W, a), for $W \in \prod_{i=1}^{m}\{X_i, Z_i\}$ and $a \in \{0, 1\}^m$.
- Relations: $\mathcal{P}^{(m)}\{X, Z\}$.
- Test: Perform the following with probability 1/3 each. In each test, the question to a prover takes the form W or (W, a) for W, a as above. The answer from the prover is an m-bit string $c \in \{0, 1\}^m$ or a single bit $d \in \{0, 1\}$, respectively.
  (a) Select $W, W' \in \prod_i\{X_i, Z_i\}$, and $a, a' \in \{0, 1\}^m$, uniformly at random. If $\{i : W_i \neq W'_i \wedge a_i = a'_i = 1\}$ has even cardinality then execute test $\textsc{com}((W, a),(W', a'))$. Otherwise, execute test $\textsc{ac}((W, a),(W', a'))$.
  (b) Select $(a, a') \in \{0, 1\}^m$ and $W \in \prod_{i=1}^{m}\{X_i, Z_i\}$ uniformly at random. Execute test $\textsc{prod}((W, a),(W, a'),(W, a + a'))$.
  (c) Select $W \in \prod_{i=1}^{m}\{X_i, Z_i\}$ and $a \in \{0, 1\}^m$ uniformly at random. Send W to one prover, receiving a string c as answer, and (W, a) to the other, receiving a bit d. Accept if and only if $d = c \cdot a$, the inner product modulo 2.

Figure 30: The Pauli braiding test, $\textsc{pbt}(X, Z)$.

Lemma A.5 ([35])**.** *The test $\textsc{pbt}(X, Z)$ is a robust $(1, \delta)$ self-test for $\mathcal{P}^{(m)}\{X, Z\}$, for some $\delta(\varepsilon) = O(\varepsilon^{1/2})$. Moreover, suppose $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ and $W(a) \in \mathrm{Obs}(\mathcal{H}_A)$, for $W \in \{X, Z\}^m$ and $a \in \{0, 1\}^m$, and projective measurements $\{W_c\}_{c\in\{0,1\}^n}$ on $\mathcal{H}_A$, for each $W \in \{X, Z\}^m$, specify a strategy for the provers that has success probability at least $1 - \varepsilon$ in $\textsc{pbt}(X, Z)$. Then there exist isometries $V_D : \mathcal{H}_D \to ((\mathbb{C}^2)^{\otimes m})_{D'} \otimes \hat{\mathcal{H}}_{\hat{D}}$, for $D \in \{A, B\}$, such that*

$$\left\|(V_A \otimes V_B)|\psi\rangle_{AB} - |\mathrm{EPR}\rangle_{A'B'}^{\otimes n}|\textsc{aux}\rangle_{\hat{A}\hat{B}}\right\|^2 = O(\sqrt{\varepsilon}),$$

and on expectation over $W \in \{X, Z\}^m$,

$$\mathop{E}_{a\in\{0,1\}^m} \left\|\big(W(a) - V_A^\dagger(\sigma_W(a) \otimes \mathrm{Id})V_A\big) \otimes \mathrm{Id}_B\, |\psi\rangle\right\|^2 = O(\sqrt{\varepsilon}), \tag{A.4}$$

and

$$\sum_{c\in\{0,1\}^m} \left\| \left(W_c - V_A^\dagger(\sigma_W^c \otimes \mathrm{Id})V_A\right) \otimes \mathrm{Id}_B \,|\psi\rangle \right\|^2 = O(\sqrt{\varepsilon}) \,. \tag{A.5}$$

The fact that the test specified in Figure 30 self-tests the relations $\mathcal{P}^{(m)}\{X,Z\}$ follows immediately from the definition of $\mathcal{P}^{(m)}\{X,Z\}$ and the analysis of the tests COM, PROD and AC given in Section A.2. The remainder of the lemma follows directly from Theorem 13 and Theorem 14 in [35]. The only part not present in [35] is the last part, which considers the POVM obtained from requiring a prover to report the outcome for each of its m single-qubit measurement (as opposed to its inner product with the string a). Eq. (A.5) follows from part (c) of PBT(X,Z) and the preceding parts of the lemma.

The next lemma is an extension of Lemma A.3 to the case of multi-qubit Pauli observables; the lemma avoids any dependence of the error on the number of qubits, as would result from a sequential application of Lemma A.3.

Lemma A.6. *Let m be an integer and $c \in \{0,1\}^m$. Let $|\psi\rangle \in \mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}}$ be a state and A and $X(a)$, for $a \in \{0,1\}^m$, observables on $\mathcal{H}_{\mathsf{A}}$ such that there exists an isometry $\mathcal{H}_{\mathsf{A}} \simeq (\mathbb{C}^2)^{\otimes m} \otimes \mathcal{H}_{\hat{\mathsf{A}}}$ under which the following conditions hold, for some $\delta_1, \delta_2, \delta_3$:*

(i) There exists an observable A' on $\mathcal{H}_{\mathsf{B}}$ such that $A \otimes \mathrm{Id} \simeq_{\delta_1} \mathrm{Id} \otimes A'$;

(ii) $|\psi\rangle \simeq_{\delta_1} |\mathrm{EPR}\rangle^{\otimes m}|\textsc{aux}\rangle$, and $X(a) \simeq_{\delta_1} \sigma_X(a) \otimes \mathrm{Id}$;

(iii) $[A, X(a)] \simeq_{\delta_2} 0$;

(iv) Conditioned on $a \cdot c = 1$, $\{A, X(a)\} \simeq_{\delta_3} 0$;

where conditions (ii) and (iii) are meant on average over a uniformly random $a \in \{0,1\}^m$, and the last over a uniformly random a such that $a \cdot c = 1$. For any $P \in \{I,X,Y,Z\}^m$ let $x_P \in \{0,1\}^m$ be such that $(x_P)_i = 1$ if and only if $P_i \in \{Y,Z\}$. Then there exists Hermitian A_P, for $P \in \{I,X,Y,Z\}^m$, on $\mathcal{H}_{\hat{\mathsf{A}}}$ such that

$$A \simeq_{\delta_1+\delta_2} \sum_{P\in\{I,X\}^n} \sigma_P \otimes A_P, \qquad \text{and} \qquad A \simeq_{\delta_1+\delta_3} \sum_{\substack{P\in\{I,X,Y,Z\}^m:\\ c_i=1 \implies P_i\in\{Y,Z\}\\ c_i=0 \implies P_i\in\{I,X\}}} \sigma_P \otimes A_P. \tag{A.6}$$

(A similar claim holds with the roles of X and Z exchanged.)

Proof. After application of the isometry, an arbitrary observable $\tilde{A}$ on $(\mathbb{C}^2)^{\otimes m} \otimes \mathcal{H}_{\hat{\mathsf{A}}}$ has a decomposition $\tilde{A} = \sum_{P\in\{I,X,Y,Z\}^m} \sigma_P \otimes A_P$, for Hermitian operators A_P on $\mathcal{H}_{\hat{\mathsf{A}}}$. Then the analogue of (A.1) is

$$[\tilde{A}, \sigma_X(a) \otimes \mathrm{Id}] = 2 \sum_{P:\, a\cdot x_P = 1} \sigma_P \sigma_X(a) \otimes A_P \,.$$

Using that any string x_P which is not the 0^m string satisfies $a \cdot x_P = 1$ with probability almost $1/2$ for a uniform choice of a, orthogonality of the $\sigma_P \sigma_X(a)$ for distinct P lets us conclude the proof of the first relation as in Lemma A.3. Similarly, the analogue of (A.2) gives

$$\{\tilde{A}, \sigma_X(a) \otimes \mathrm{Id}\} = 2 \sum_{P:\, a \cdot x_P = 0} \sigma_P \sigma_X(a) \otimes A_P .$$

Using that any string x_P which is not c satisfies $a \cdot x_P = 0$ with probability almost $1/2$ for a uniform choice of a such that $a \cdot c = 1$, orthogonality of the $\sigma_P \sigma_X(a)$ for distinct P lets us conclude the proof of the second relation. □

A.4.2 The parallel Bell test

Before we move on to a test for the full Pauli group, including not only X, Z but also Y observables, we use the Pauli braiding test introduced in the previous section to develop a multi-qubit version of the Bell test from Section A.3.

Let $k \geq 1$ and $m = 2k$. Let τ be a bijection of $\{1, \ldots, m\}$, which we interpret as a pairing of the qubits: for $i \in \{1, \ldots, m\}$, qubit $\tau(2i-1)$ is paired with qubit $\tau(2i)$. The test ParBell(τ) described in Figure 31 certifies that an m-qubit measurement performed by a prover is consistent with a measurement of each pair of qubits (as specified by τ) in the Bell basis.

The test has three components. In part (a) we execute the test pbt(X, Z) in order to enforce an m-qubit structure and the existence of tensor product observables X and Z on them, from which the Bell basis is defined as in Section A.3. In part (b) we introduce questions W such that each pair of indices paired by τ contains the same label, XX or ZZ. Since such question labels have exponentially small probability under the uniform distribution, part (b) checks for consistency against a uniformly random question, for all those locations where the bases happen to match. In part (c) we ask one prover to measure in the Bell basis and check their results against those reported by the other prover when asked to perform a measurement of the same type as in part (b). Since the Bell basis is characterized as the joint eigenstates of XX and ZZ operators, checking consistency of these outcomes is enough the characterize the measurement.

Test PARBELL(τ). τ is a permutation on $\{1,\dots,m\}$ where $m = 2k$.
Execute each of the following with equal probability:

(a) Execute PBT(X,Z).

(b) Select $W \in \{X,Z\}^m$ uniformly at random conditioned on $W_{\tau(2i-1)} = W_{\tau(2i)}$ for each $i \in \{1,\dots,m\}$. Let $W' \in \{X,Z\}^m$ be such that $W'_{\tau(2i-1)} = W_{\tau(2i-1)}$ and $W'_{\tau(2i)}$ is uniformly random in $\{X,Z\}$ for each i. Similarly, let W'' be such that $W''_{\tau(2i)} = W_{\tau(2i)}$ and $W''_{\tau(2i-1)}$ is uniformly random. Send W to one prover and either W' or W'' (with probability half each) to the other. Receive $a \in \{0,1\}^m$ from the first prover and $b \in \{0,1\}^m$ from the second. Accept if and only if for each $i \in \{1,\dots,k\}$, $a_{\tau(2i-1)} = b_{\tau(2i-1)}$ in case W' was sent, and $a_{\tau(2i)} = b_{\tau(2i)}$ in case W'' was sent.

(c) Select $W \in \{X,Z\}^m$ uniformly at random conditioned on $W_{\tau(2i-1)} = W_{\tau(2i)}$ for each $i \in \{1,\dots,m\}$. Send W to a prover and (Φ,τ) to the other, where Φ is a label that means "measure in the Bell basis" with the qubits being paired according to τ. Receive $a \in \{0,1\}^m$ from the first prover and $b \in \{00,01,10,11\}^k$ from the second. Accept if and only if, whenever $W_{\tau(2i-1)}W_{\tau(2i)} = XX$ then $a_{\tau(2i-1)} \oplus a_{\tau(2i)} = b_{\tau(2i-1)}$ and whenever $W_{\tau(2i-1)}W_{\tau(2i)} = ZZ$ then $a_{\tau(2i-1)} \oplus a_{\tau(2i)} = b_{\tau(2i)}$.

Figure 31: The parallel bell test, PARBELL(τ).

Lemma A.7. *Let $k \geq 1$ and τ a permutation on $\{1,\dots,k\}$. Suppose given a strategy for the provers that succeeds with probability at least $1-\varepsilon$ in test PARBELL(τ). Let V_A and V_B be the isometries obtained from Lemma A.5. Then*

$$\sum_{b\in\{00,01,10,11\}^k} \Big\| \big(\Phi_b - V_A^\dagger(\otimes_i \sigma_{\Phi,i}^{b_i})V_A\big) \otimes \mathrm{Id}_B \,|\psi\rangle \Big\|^2 = O(\sqrt{\varepsilon}),$$

where $\{\Phi_b\}_b$ is the POVM applied by a prover upon question (Φ,τ) and $\sigma_{\Phi,i}^{b_i}$ denotes the projection on the joint eigenvector of $\sigma_{X,\tau(2i-1)}\sigma_{X,\tau(2i)}$ and $\sigma_{Z,\tau(2i-1)}\sigma_{Z,\tau(2i)}$ with associated eigenvalues b_i.

Proof sketch. For ease of notation we give the proof when τ is the identity, the general case being similar. Isometries V_A and V_B satisfying the conclusions of Lemma A.5 are obtained from part (a) of the test. Using the conclusion of Lemma A.5 it follows that on average over $W \in \{X,Z\}^m$,

$$\sum_{c\in\{0,1\}^m} \Big\| \big(W_c - V_A^\dagger(\sigma_W^c \otimes \mathrm{Id})V_A\big) \otimes \mathrm{Id}_B \,|\psi\rangle \Big\|^2 \;=\; O(\sqrt{\varepsilon})\;. \tag{A.7}$$

Part (b) of the test allows us to claim the same consequence, on average over $W \in \{XX,ZZ\}^k$. This can be seen as follows. For $W \in \{X,Z\}^m$ and $c \in \{0,1\}^k$ let $W_c^{(1)}$ be the sum of all $W_{c'}$ over $c' \in \{0,1\}^m$ such that $c'_{2i-1} = c_i$ for each $i \in \{1,\dots,k\}$, and define $W_c^{(2)}$ analogously, using the condition $c'_{2i} = c_i$. Using that both W' and W'' in part (b) are uniformly distributed, applying (A.7) and marginalizing over half the outcomes we get that on average over the choice of $W' \in \{X, Z\}^m$,

$$\sum_{c \in \{0,1\}^k} \left\| \left(W_c'^{(1)} - V_A^\dagger(\sigma_W^{(1),c} \otimes \mathrm{Id})V_A\right) \otimes \mathrm{Id}_B \left|\psi\right\rangle \right\|^2 = O(\sqrt{\varepsilon}) . \tag{A.8}$$

A similar relation holds for $W_c''^{(2)}$. Recall that measurement operators used by the provers are always assumed projective. Thus for W, W', W'' chosen as in part (b) it holds that $W_c = W_{c'}^{(1)} W_{c''}^{(2)}$ where c' and c'' are the odd and even substrings of c, respectively. Using this relation and (A.8) for both $W'^{(1)}$ and for $W''^{(2)}$ we deduce that success in part (b) implies that on average over $W \in \{XX, ZZ\}^k$,

$$\sum_{c \in \{0,1\}^m} \left\| \left(W_c - V_A^\dagger(\sigma_W^c \otimes \mathrm{Id})V_A\right) \otimes \mathrm{Id}_B \left|\psi\right\rangle \right\|^2 = O(\sqrt{\varepsilon}) . \tag{A.9}$$

To conclude the proof of the lemma we note that in the honest case

$$\sigma_\Phi^b = \bigotimes_{i=1}^k \Big(\sum_{c \oplus c' = b_{2i-1}} \sigma_{X,2i-1}^c \otimes \sigma_{X,2i}^{c'} \Big) \cdot \Big(\sum_{d \oplus d' = b_{2i}} \sigma_{Z,2i-1}^d \otimes \sigma_{Z,2i}^{d'} \Big) . \tag{A.10}$$

This is precisely the relation checked in part (c). Thus the conclusion of the lemma follows from (A.9), (A.10) and success in part (c). □

A.4.3 The m-qubit Pauli group

We will use an extended version of the Pauli braiding test introduced in Section A.4.1 which self-tests a third observable, Y_i, on each system. Ideally we would like to enforce the relation $Y_i = \sqrt{-1} X_i Z_i$. Unfortunately, the complex phase cannot be tested from classical correlations alone: complex conjugation leaves correlations invariant, but does not correspond to a unitary change of basis (see [38, Appendix A] for a discussion of this issue).

We represent the "choice" of complex phase, $\sqrt{-1}$ or its conjugate $-\sqrt{-1}$, by an observable Δ that the prover measures on a system that is in a tensor product with all other systems on which the prover acts. Informally, the outcome obtained when measuring Δ tells the prover to use $Y = iXZ$ or $Y = -iXZ$. While strategies determining the complex phase in such a way can certainly not be prevented, the goal of the test is to ensure that the provers have exactly that much freedom, and no more.

We first introduce Y and test that the triple $\{X, Y, Z\}$ pairwise anticommute in each coordinate. This corresponds to the following set of relations:

$$\begin{aligned} \mathcal{P}^{(m)}\{X, Y, Z\} = &\Big\{ W(a) \in \mathrm{Obs} \,:\, W \in \{I, X, Y, Z\}^m,\, a \in \{0,1\}^m \Big\} \\ &\cup \Big\{ W(a)W'(a') = (-1)^{|\{i:\, W_i \neq W_i' \wedge a_i a_i' = 1\}|} W'(a')W(a) \,:\, W, W' \in \{I, X, Y, Z\}^m,\, a, a' \in \{0,1\}^m \Big\} \\ &\cup \Big\{ W(a)W(a') = W(a + a') \,:\, W \in \{I, X, Y, Z\}^m,\, a, a' \in \{0,1\}^m \Big\} . \end{aligned}$$

Test PBT(X, Y, Z):

- Inputs: $W \in \prod_{i=1}^{m}\{I_i, X_i, Y_i, Z_i\}$
- Relations: $\mathcal{P}^{(m)}\{X, Y, Z\}$.
- Test: Perform the following with equal probability:
  - (a) Execute test PBT(X, Z).
  - (b) Let $W \in \{X, Z\}^m$ be chosen uniformly at random. Let $W' = Y^m$.
    - (i) Let $c, c' \in \{0,1\}^m$ be chosen uniformly at random. If $c \cdot c' = 0$ then execute COM$((W, c), (W', c'))$. If $c \cdot c' = 1$ then execute AC$((W, c), (W', c'))$.
    - (ii) Select $(a, a') \in \{0,1\}^m$. Execute test PROD$((W', a), (W', a'), (W', a + a'))$.
    - (iii) Select $W'' \in \{I, Y\}^m$ uniformly at random. Let c be the indicator of the positions in W'' such that $W''_i = 1$. Send one prover the string W'' and the other the pair (W', c). Let d be the string reported by the first prover and e the bit reported by the second. Accept if and only if $e = c \cdot d$.
  - (c) Select $W \in \{X, Z\}^m$ and $c \in \{0,1\}^m$ uniformly at random. Let $W' \in \{I, X, Y, Z\}$ be such that $W'_i = W_i$ whenever $c_i = 1$, and W'_i is uniform in $\{I, Y\}$ otherwise. Let W'' be equal to W' with the positions in which W' equals X or Z replaced by a uniformly random entry in $\{I, Y\}$. Send one of W, W', W'' at random to a prover, and another one to the other. Accept if and only if the prover's answers associated with identical coordinates are identical.
  - (d) Select a random permutation $\sigma \in \mathfrak{S}_{m/2}$, and $W \in \{I, Y\}^m$ uniformly at random. Write $W = W_1 W_2$, where $W_1, W_2 \in \{I, Y\}^{m/2}$. Let W_1^{σ} be the string W_1 with its entries permuted according to σ. Do the following with equal probability:
    - (i) Send one prover $W_1 W_1^{\sigma}$ and the other either $W_1 W_2$ or $W_2 W_1^{\sigma}$ (chosen with probability 1/2), and check consistency of the first or second half of the provers' answer bits, respectively.
    - (ii) Execute the test PARBELL(τ), where for $i \in \{1, \ldots, m/2\}$, $\tau(2i-1) = i$ and $\tau(2i) = \sigma(i)$.
    - (iii) Send one prover $W_1 W_1^{\sigma}$, and the other (Φ, τ). The first prover replies with $a \in \{0,1\}^m$ and the second with $b \in \{00, 01, 10, 11\}^{m/2}$. For each $i \in \{1, \ldots, m/2\}$ such that $b_i = 00$, check that $a_i = a_{m/2+\sigma(i)}$.
    - (iv) Let $W' \in \{X, Z\}^m$ be chosen uniformly at random. Send one prover W' and the other (Φ, τ). The first prover replies with $a \in \{0,1\}^m$ and the second with $b \in \{00, 01, 10, 11\}^{m/2}$. For each pair $(i, m/2 + \sigma(i))$ such that $W'_i = W'_{m/2+\sigma(i)}$ and $b_i = 00$ check that $a_i = a_{m/2+\sigma(i)}$.

Figure 32: The extended Pauli braiding test, PBT(X, Y, Z).

The test is described in Figure 32. It has four components. Part (a) of the test executes test $\textsc{pbt}(X, Z)$, which gives us multi-qubit Pauli X and Z observables. Part (b) of the test introduces $Y^m(c)$ observables, and uses commutation and anti-commutation relations with X and Z to force Y^m to respect the qubit structure obtained from part (a); the analysis of this part is based on Lemma A.6. Part (c) of the test, while not strictly necessary for our applications, justifies the test's name, by introducing an observable associated with any tensor product of Paulis and testing it for consistency against the observables tested in parts (a) and (b).

Part (d) of the test is meant to control the "phase" ambiguity in the definition of $Y(c)$ that remains after the analysis of part (b). Indeed, from that part it will follow that $Y(c) \simeq \sigma_Y(c) \otimes \Delta(c)$, where $\Delta(c)$ is an arbitrary observable acting on the ancilla system produced by the isometry obtained in part (a). We would like to impose $\Delta(c) \simeq \Delta_Y^{|c|}$ for a fixed observable Δ_Y which represents the irreducible phase degree of freedom in the definition of Y, as discussed above. To obtain this, part (c) of the test performs a form of SWAP test between different $Y(c)$ observables, enforcing, e. g., that $Y(1, 0, 1)$ is consistent with $Y(1, 0, 0)$ after an appropriate Bell measurement has "connected" registers 1 and 2. The Bell basis measurements are tested using $\textsc{ParBell}(\tau)$ from the previous section.

Claim A.8. *Let $A \in \mathrm{Obs}(\mathbb{C}^2_{A_1} \otimes \cdots \otimes \mathbb{C}^2_{A_k} \otimes \mathcal{H})$ and $B \in \mathrm{Obs}(\mathbb{C}^2_{B_1} \otimes \cdots \otimes \mathbb{C}^2_{B_k} \otimes \mathcal{H})$ be k-qubit observables acting on distinct registers A_j, B_j, as well as a common space $\mathcal{H}$, and $\Phi_{\mathsf{A'B'}} = \prod_{j=1}^k |\mathrm{EPR}\rangle\langle\mathrm{EPR}|_{\mathsf{A'}_j,\mathsf{B'}_j}$ the projector on k EPR pairs across registers $\mathsf{A'}_j$ and $\mathsf{B'}_j$. Then*

$$\Big(\bigotimes_j \langle\mathrm{EPR}|_{\mathsf{A}_j\mathsf{A'}_j}\langle\mathrm{EPR}|_{\mathsf{B}_j\mathsf{B'}_j} \otimes \mathrm{Id}_{\mathcal{H}}\Big)\Big(\big(A_{\mathsf{A}\mathcal{H}} \otimes \mathrm{Id}_{\mathsf{B}}\big)\big(\mathrm{Id}_{\mathsf{A}} \otimes B_{\mathsf{B}\mathcal{H}}\big) \otimes \Phi_{\mathsf{A'B'}}\Big) \cdot \Big(\bigotimes_j |\mathrm{EPR}\rangle_{\mathsf{A}_j\mathsf{A'}_j}|\mathrm{EPR}\rangle_{\mathsf{B}_j\mathsf{B'}_j} \otimes \mathrm{Id}_{\mathcal{H}}\Big) = \frac{1}{2^{2k}}\sum_i \mathrm{Tr}\big(A_iB_i\big)A'_iB'_i, \quad \text{(A.11)}$$

where we write $A = \sum_i A_i \otimes A'_i$ and $B = \sum_i B_i \otimes B'_i$, for A_i on $\mathcal{H}_{\mathsf{A}}$, B_i on $\mathcal{H}_{\mathsf{B}}$, and A'_i, B'_i on $\mathcal{H}$.

Proof. We do the proof for $k = 1$, as the general case is similar. Using that for any operators X_{AB} and $Y_{\mathsf{A'B'}}$,

$$\langle\mathrm{EPR}|_{\mathsf{AA'}}\langle\mathrm{EPR}|_{\mathsf{BB'}}\big(X_{\mathsf{AB}} \otimes Y_{\mathsf{A'B'}}\big)|\mathrm{EPR}\rangle_{\mathsf{AA'}}|\mathrm{EPR}\rangle_{\mathsf{BB'}} = \frac{1}{4}\mathrm{Tr}(XY^T),$$

the left-hand side of (A.11) evaluates to

$$4^{-1}\mathrm{Tr}_{\mathsf{AB}}\Big(\big(A_{\mathsf{A}\mathcal{H}} \otimes \mathrm{Id}_{\mathsf{B}}\big)\big(\mathrm{Id}_{\mathsf{A}} \otimes B_{\mathsf{B}\mathcal{H}}\big)\big(\Phi^T_{\mathsf{A'B'}} \otimes \mathrm{Id}_{\mathcal{H}}\big)\Big),$$

which using the same identity again gives the right-hand side of (A.11). □

Lemma A.9. *Suppose $|\psi\rangle \in \mathcal{H}_{\mathsf{A}} \otimes \mathcal{H}_{\mathsf{B}}$ and $W(a) \in \mathrm{Obs}(\mathcal{H}_{\mathsf{A}})$, for $W \in \{I, X, Y, Z\}^m$ and $a \in \{0,1\}^m$, specify a strategy for the provers that has success probability at least $1 - \varepsilon$ in the extended Pauli braiding test $\textsc{pbt}(X, Y, Z)$ described in Figure 32. Then there exist isometries $V_D : \mathcal{H}_{\mathsf{D}} \to ((\mathbb{C}^2)^{\otimes m})_{\mathsf{D'}} \otimes \hat{\mathcal{H}}_{\hat{\mathsf{D}}}$, for $D \in \{A, B\}$, such that*

$$\Big\|(V_A \otimes V_B)|\psi\rangle_{\mathsf{AB}} - |\mathrm{EPR}\rangle^{\otimes m}_{\mathsf{A'B'}}|\textsc{aux}\rangle_{\hat{\mathsf{A}}\hat{\mathsf{B}}}\Big\|^2 = O(\sqrt{\varepsilon}),$$

and on expectation over $W \in \{I, X, Y, Z\}^m$*,*

$$\mathop{E}_{a\in\{0,1\}^m} \left\| \left(W(a) - V_A^\dagger(\sigma_W(a) \otimes \Delta_W(a))V_A\right) \otimes \mathrm{Id}_B \left|\psi\right\rangle \right\|^2 = O(\sqrt{\varepsilon}), \tag{A.12}$$

where $\Delta_W(a) = \prod_i \Delta_{W_i}^{a_i} \in \mathrm{Obs}(\mathcal{H}_{\hat{A}})$ *are observables with* $\Delta_X = \Delta_Z = \mathrm{Id}$ *and* Δ_Y *an arbitrary observable on* $\hat{\mathcal{H}}$ *such that*

$$\left\| \Delta_Y \otimes \Delta_Y |\textsc{aux}\rangle - |\textsc{aux}\rangle \right\|^2 = O(\sqrt{\varepsilon}).$$

Proof sketch. The existence of the isometries V_A and V_B follows Lemma A.5 and part (a) of $\textsc{pbt}(X, Y, Z)$. Under this isometry we have $W(a) \simeq_{\sqrt{\varepsilon}} \sigma_W(a)$, on average over uniformly random $W \in \{X, Z\}^m$ and $a \in \{0, 1\}^m$, and moreover $W_c \simeq \sigma_W^c$ on average over uniformly random $W \in \{X, Z\}^m$.

Applying Lemma A.6, the anti-commutation relations between $Y^m(c)$ and $W(c)$ verified in part (b)(i) of the test imply that under the same isometry,

$$Y(c) \simeq \sigma_Y(c) \otimes \Delta(c) \;, \tag{A.13}$$

for some observable $\Delta(c)$ on $\mathcal{H}_{\hat{A}}$. Here $Y(c)$ is shorthand for $Y^m(c)$. This is because, for any c, the test verifies that condition (iv) in Lemma A.6 is satisfied, where X in the lemma is replaced by any $W \in \{X, Z\}^n$ (more precisely, the condition holds on the average, for $W \in \{X, Z\}^m$ and $a \in \{0, 1\}^m$ both chosen uniformly at random). Thus the second centered equation in (A.6) holds, where by varying the choice of X in the lemma (corresponding to varying W here) we get that if $c_i = 1$ then $P_i \in \{Y, Z\} \cap \{Y, X\} = \{Y\}$ and if $c_i = 0$ then $P_i \in \{I, X\} \cap \{I, Z\} = \{I\}$. Thus the lemma implies the claimed form (A.13), where $\Delta(c)$ here is A_P in the lemma for $P = Y(c)$.

Using the linearity relations that are verified in part (b)(ii) we may in addition express $\Delta(c) = \prod_i \Delta_i^{c_i}$ for (perfectly) commuting observables Δ_i.

Using part (b)(iii) it follows that on average over uniformly random c, $Y(c) \simeq \sum_d (-1)^{d\cdot c} W_d^{(c)}$ where $W^{(c)} \in \{I, Y\}^m$ is the string that has a Y exactly at those positions i such that $c_i = 1$.

Using Claim A.8, success probability at least $1 - O(\varepsilon)$ in part (d) of the test implies that on average over a random permutation $\sigma \in \mathfrak{S}_{m/2}$,

$$\mathop{\mathrm{E}}_{\sigma} \mathop{\mathrm{E}}_{c\in\{0,1\}^{m/2}} 2^{-m} \mathrm{Tr}\big(\sigma_Y(c, c^\sigma)\big) \, \langle \textsc{aux} | \Big(\prod_{i=1}^{m/2} \big(\Delta_i \Delta_{m/2+\sigma(i)}\big)^{c_i} \Big) | \textsc{aux} \rangle = 1 - O(\sqrt{\varepsilon}), \tag{A.14}$$

where we wrote (c, c^σ) for the m-bit string $(c_1, \ldots, c_{m/2}, c_{\sigma(1)}, \ldots, c_{\sigma(m/2)})$. Defining

$$\Delta_Y \;=\; \mathop{\mathrm{E}}_{i\in\{\frac{m}{2}+1,\ldots,m\}} \frac{\Delta_i}{|\,\mathrm{E}_i \Delta_i|}, \tag{A.15}$$

We show that Eq. (A.14) implies that $\Delta(c) \approx_{\sqrt{\varepsilon}} \Delta_Y^{|c|}$. Towards this we first observe that

$$\mathop{\mathrm{E}}_{c\in\{0,1\}^{m/2}} \Big\| \Big(\prod_{i=1}^{m/2} \Delta_i^{c_i} - \big(\mathop{\mathrm{E}}_{i\in\{\frac{m}{2}+1,\dots,m\}} \Delta_i \big)^{|c|} \Big) |\textsc{aux}\rangle \Big\|^2 \tag{A.16}$$

$$\le \mathop{\mathrm{E}}_{c} \mathop{\mathrm{E}}_{g:\{1,\dots,\frac{m}{2}\}\to\{\frac{m}{2}+1,\dots,m\}} \Big\| \Big(\prod_{i=1}^{m/2} \Delta_i^{c_i} - \prod_i \Delta_{g(i)}^{c_i} \Big) |\textsc{aux}\rangle \Big\|^2. \tag{A.17}$$

where the first inequality is by convexity, with the expectation taken over a random function g. We would like to relate this last term to the expectation over a random permutation $\sigma \in \mathfrak{S}_{m/2}$. We do this by observing that with probability $1 - O(1/m)$ over the choice of a uniformly random g it is possible to write

$$\prod_i \Delta_{g(i)}^{c_i} = \Big(\prod_i \Delta_{m/2+\tau'(i)}^{c_i'} \Big) \Big(\prod_i \Delta_{m/2+\tau''(i)}^{c_i''} \Big),$$

where $c_i' + c_i'' = c_i$ for all i, τ', τ'' are permutations such that $m/2 + \tau'(i) = g(i)$ if $c_i' = c_i$, and $m/2 + \tau''(i) = g(i)$ if $c_i'' = c_i$; this is possible because g might have two-element collisions, but is unlikely to have any three-element collisions. Moreover, for uniformly random c and g we can ensure that the marginal distribution on (c', τ') and (c'', τ'') is uniform. Using this we can apply (A.14) twice to bound the right-hand side of (A.17) by $O(\sqrt{\varepsilon})$ (after having expanded the square). Thus the action of $\mathrm{E}_i \Delta_i$ on $|\textsc{aux}\rangle$ is close to the action of an observable. It is then relatively routine work to show that Δ_Y defined in (A.15) satisfies $\Delta(c) \approx_{\sqrt{\varepsilon}} \Delta_Y^{|c|}$, on average over a uniformly random c.

The last condition in the lemma follows from the consistency relations, which imply that $X(a) \otimes X(a)$, $Z(b) \otimes Z(b)$ and $Y(c) \otimes Y(c)$ all approximately stabilize $|\psi\rangle$; then $\Delta_Y^{|a|} \otimes \Delta_Y^{|a|} \approx X(a)Z(a)Y(a) \otimes X(a)Z(a)Y(a)$ also does. □

References

[1] DORIT AHARONOV, ITAI ARAD, AND THOMAS VIDICK: Guest column: The quantum PCP conjecture. *SIGACT News*, 44(2):47–79, 2013. [doi:10.1145/2491533.2491549, arXiv:1309.7495] 61

[2] DORIT AHARONOV, MICHAEL BEN-OR, AND ELAD EBAN: Interactive proofs for quantum computations. In *Proc. 1st Innovations in Comp. Sci. Conf. (ICS'10)*, pp. 453–469. Tsinghua U., 2010. Tsinghua. [arXiv:0810.5375] 4

[3] GORJAN ALAGIC, YFKE DULEK, CHRISTIAN SCHAFFNER, AND FLORIAN SPEELMAN: Quantum fully homomorphic encryption with verification. In *Proc. 23rd Internat. Conf. Theory Appl. of Cryptology and Inform. Security (ASIACRYPT'17)*, pp. 438–467. Springer, 2017. [doi:10.1007/978-3-319-70694-8_16, arXiv:1708.09156] 9

[4] JOHN S. BELL: On the Einstein-Podolsky-Rosen paradox. *Physics*, 1(3):195–200, 1964. [doi:10.1103/PhysicsPhysiqueFizika.1.195] 2

[5] DEBAJYOTI BERA, STEPHEN A. FENNER, FREDERIC GREEN, AND STEVEN HOMER: Efficient universal quantum circuits. *Quantum Inf. Comput.*, 10(1&2):16–27, 2010. Preliminary version in COCOON'09. [doi:10.26421/QIC10.1-2-2] 7

[6] JOSEPH BOWLES, IVAN ŠUPIĆ, DANIEL CAVALCANTI, AND ANTONIO ACÍN: Self-testing of Pauli observables for device-independent entanglement certification. *Phys. Rev. A*, 98(4/042336):1–24, 2018. [doi:10.1103/PhysRevA.98.042336, arXiv:1801.10446] 8

[7] ANNE BROADBENT: How to verify a quantum computation. *Theory of Computing*, 14(11):1–37, 2018. [doi:10.4086/toc.2018.v014a011, arXiv:1509.09180] 4, 5, 6, 12, 15, 16, 51

[8] DAVIDE CASTELVECCHI: IBM's quantum cloud computer goes commercial. *Nature News*, 543(7644), 9 March 2017. [doi:10.1038/nature.2017.21585] 3

[9] FAN CHUNG AND LINYUAN LU: Concentration inequalities and martingale inequalities: a survey. *Internet Mathematics*, 3(1):79–127, 2006. [doi:10.1080/15427951.2006.10129115] 11

[10] JOHN F. CLAUSER, MICHAEL A. HORNE, ABNER SHIMONY, AND RICHARD A. HOLT: Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23(15):880–884, 1969. [doi:10.1103/PhysRevLett.23.880] 2

[11] YFKE DULEK, CHRISTIAN SCHAFFNER, AND FLORIAN SPEELMAN: Quantum homomorphic encryption for polynomial-sized circuits. *Theory of Computing*, 14(7):1–45, 2018. Preliminary version in CRYPTO'16. [doi:10.4086/toc.2018.v014a007, arXiv:1603.09717] 9

[12] JOSEPH F. FITZSIMONS: Private quantum computation: An introduction to blind quantum computing and related protocols. *npj Quantum Information*, 3(23):1–11, 2017. [doi:10.1038/s41534-017-0025-3, arXiv:1611.10107] 4

[13] JOSEPH F. FITZSIMONS AND MICHAL HAJDUŠEK: Post hoc verification of quantum computation, 2015. [arXiv:1512.04375] 3, 5

[14] JOSEPH F. FITZSIMONS, MICHAL HAJDUŠEK, AND TOMOYUKI MORIMAE: *Post hoc* verification of quantum computation. *Phys. Rev. Lett.*, 120(4/040501):1–5, 2018. [doi:10.1103/PhysRevLett.120.040501, arXiv:1512.04375] 3, 4, 5

[15] JOSEPH F. FITZSIMONS AND ELHAM KASHEFI: Unconditionally verifiable blind quantum computation. *Phys. Rev. A*, 96(1/012303):1–27, 2017. [doi:10.1103/PhysRevA.96.012303, arXiv:1203.5217] 4, 8

[16] KEISUKE FUJII AND MASAHITO HAYASHI: Verifiable fault tolerance in measurement-based quantum computation. *Phys. Rev. A*, 96(3/030301(R)):1–6, 2017. [doi:10.1103/PhysRevA.96.030301, arXiv:1610.05216] 4

[17] ALEXANDRU GHEORGHIU, ELHAM KASHEFI, AND PETROS WALLDEN: Robustness and device independence of verifiable blind quantum computing. *New J. Physics*, 17(8/083040):1–22, 2015. [doi:10.1088/1367-2630/17/8/083040, arXiv:1610.05216] 3, 4

[18] ALEXANDRU GHEORGHIU AND THOMAS VIDICK: Computationally-secure and composable remote state preparation. In *Proc. 60th FOCS*, pp. 1024–1033. IEEE Comp. Soc., 2019. [doi:10.1109/FOCS.2019.00066, arXiv:1904.06320] 4

[19] ALEX B. GRILO: A simple protocol for verifiable delegation of quantum computation in one round. In *Proc. 46th Internat. Colloq. on Automata, Languages, and Programming (ICALP'19)*, pp. 28:1–13. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2019. [doi:10.4230/LIPIcs.ICALP.2019.28, arXiv:1711.09585] 8, 9

[20] MICHAL HAJDUŠEK, CARLOS A. PÉREZ-DELGADO, AND JOSEPH F. FITZSIMONS: Device-independent verifiable blind quantum computation, 2015. [arXiv:1502.02563] 3, 4

[21] MASAHITO HAYASHI AND MICHAL HAJDUŠEK: Self-guaranteed measurement-based quantum computation. *Phys. Rev. A*, 97(5/052308):1–16, 2018. [doi:10.1103/PhysRevA.97.052308, arXiv:1603.02195] 3, 4

[22] MASAHITO HAYASHI AND TOMOYUKI MORIMAE: Verifiable measurement-only blind quantum computing with stabilizer testing. *Phys. Rev. Lett.*, 115(22/220502):1–5, 2015. [doi:10.1103/PhysRevLett.115.220502, arXiv:1505.07535] 4

[23] HE-LIANG HUANG, QI ZHAO, XIONGFENG MA, CHANG LIU, ZU-EN SU, XI-LIN WANG, LI LI, NAI-LE LIU, BARRY C. SANDERS, CHAO-YANG LU, AND JIAN-WEI PAN: Experimental blind quantum computing for a classical client. *Phys. Rev. Lett.*, 119(5/050503):1–5, 2017. [doi:10.1103/PhysRevLett.119.050503, arXiv:1707.00400] 8

[24] ZHENGFENG JI: Classical verification of quantum proofs. *Theory of Computing*, 15(5):1–42, 2019. Preliminary version in STOC'16. [doi:10.4086/toc.2019.v015a005, arXiv:1505.07432] 3

[25] URMILA MAHADEV: Classical verification of quantum computations. *SIAM J. Comput.*, 51(4):1172–1229, 2022. Preliminary version in FOCS'18. [doi:10.1137/20M1371828, arXiv:1804.01082] 4, 9

[26] URMILA MAHADEV: Classical homomorphic encryption for quantum circuits. *SIAM J. Comput.*, 52(6):189–215, 2023. Preliminary version in FOCS'18. [doi:10.1137/18M1231055, arXiv:1708.02130] 9

[27] DOMINIC MAYERS AND ANDREW YAO: Self testing quantum apparatus. *Quantum Inf. Comput.*, 4(4):273–286, 2004. ACM DL. 2

[28] MATTHEW MCKAGUE: Interactive proofs for BQP via self-tested graph states. *Theory of Computing*, 12(3):1–42, 2016. [doi:10.4086/toc.2016.v012a003, arXiv:1309.5675] 3, 4

[29] N. DAVID MERMIN: Simple unified form for the major no-hidden-variables theorems. *Phys. Rev. Lett.*, 65(27):3373–3376, 1990. [doi:10.1103/PhysRevLett.65.3373] 68

[30] MICHAEL MITZENMACHER AND ELI UPFAL: *Probability and Computing: Randomized Algorithms and Probabilistic Analysis*. Cambridge Univ. Press, 2005. [doi:10.1017/CBO9780511813603] 11

[31] ASHELY MONTANARO: Quantum algorithms: an overview. *npj Quantum Information*, 2(15023), 2016. [doi:10.1038/npjqi.2015.23, arXiv:1511.04206] 2

[32] TOMOYUKI MORIMAE: Verification for measurement-only blind quantum computing. *Phys. Rev. A*, 89(6/060302(R)):1–4, 2014. [doi:10.1103/PhysRevA.89.060302] 4

[33] TOMOYUKI MORIMAE AND JOSEPH F. FITZSIMONS: Post hoc verification with a single prover, 2016. [arXiv:1603.06046] 4

[34] TOMOYUKI MORIMAE, YUKI TAKEUCHI, AND MASAHITO HAYASHI: Verification of hypergraph states. *Phys. Rev. A*, 96(062321), 2017. [doi:10.1103/PhysRevA.96.062321, arXiv:1701.05688] 4

[35] ANAND NATARAJAN AND THOMAS VIDICK: A quantum linearity test for robustly verifying entanglement. In *Proc. 49th STOC*, pp. 1003–1015. ACM Press, 2017. [doi:10.1145/3055399.3055468] 3, 5, 6, 20, 27, 68, 73, 74, 75

[36] ANAND NATARAJAN AND THOMAS VIDICK: Low-degree testing for quantum states, and a quantum entangled games PCP for QMA. In *Proc. 59th FOCS*, pp. 731–742. IEEE Comp. Soc., 2018. [doi:10.1109/FOCS.2018.00075] 61

[37] BEN W. REICHARDT, FALK UNGER, AND UMESH VAZIRANI: Classical command of quantum systems. *Nature*, 496:456–460, 2013. Full version arXiv:1209.0448. [doi:10.1038/nature12035] 3, 4, 5, 8, 49, 52

[38] BEN W. REICHARDT, FALK UNGER, AND UMESH VAZIRANI: A classical leash for a quantum system: Command of quantum systems via rigidity of CHSH games. In *Proc. 4th Innovations in Theoret. Comp. Sci. Conf. (ITCS'13)*. ACM Press, 2013. [doi:10.1145/2422436.2422473, arXiv:1209.0448] 18, 78

[39] WILLIAM SLOFSTRA: Tsirelson's problem and an embedding theorem for groups arising from non-local games. *J. AMS*, 33:1–56, 2020. [doi:10.1090/JAMS/929, arXiv:1606.03140] 6

[40] XINGYAO WU, JEAN-DANIEL BANCAL, MATTHEW MCKAGUE, AND VALERIO SCARANI: Device-independent parallel self-testing of two singlets. *Phys. Rev. A*, 93(6/062121), 2016. [doi:10.1103/PhysRevA.93.062121, arXiv:1512.02074] 69

AUTHORS

Andrea Coladangelo
Assistant Professor
Paul G. Allen School of Computer Science & Engineering
University of Washington
Seattle, Washington, USA
coladan@cs.washington.edu
https://andreacoladangelo.com

Alex Bredariol Grilo
CNRS Researcher
LIP6
Sorbonne Université and CNRS
Paris, France
Alex.Bredariol-Grilo@lip6.fr
http://abgrilo.org

Stacey Jeffery
Professor
QuSoft, CWI & University of Amsterdam
Amsterdam, the Netherlands
jeffery@cwi.nl
https://homepages.cwi.nl/~jeffery/

Thomas Vidick
Professor
Computer Science and Applied Mathematics
Weizmann Institute of Science
Rehovot, Israel
thomas.vidick@weizmann.ac.il
https://www.weizmann.ac.il/math/vidick/

ABOUT THE AUTHORS

ANDREA COLADANGELO graduated from Caltech in 2020, advised by Thomas Vidick. Andrea's thesis focused on the study of foundational properties of quantum correlations and entanglement, and their interplay with the certification of quantum devices. He was a postdoc at UC Berkeley and the Simons Institute for the Theory of Computing until the end of 2022. He is currently an Assistant Professor in the Paul G. Allen School of Computer Science & Engineering at the University of Washington.

ALEX BREDARIOL GRILO (he/him) graduated from Université Paris Diderot (currently Université de Paris) in 2018. During his Ph. D. studies he was affiliated with IRIF and his advisor was Iordanis Kerenidis. After that, he was a postdoc at CWI and QuSoft under the supervision of Stacey Jeffery, Ronald de Wolf and Christian Schaffner (informal supervisor). From January to May 2020, he was a Research Fellow at the Simons Institute for the Theory of Computing of UC Berkeley. Then, in 2020 he became a CNRS researcher LIP6 (CNRS/Sorbonne Université), where he focuses his research on quantum complexity theory and cryptography.

STACEY JEFFERY received her Ph. D. from the University of Waterloo in 2014, under the supervision of Michele Mosca, after retiring from a highly successful musical career, which culminated in singing the backup vocals for the soundtrack of the trailer for a documentary about the making of a commercial in Peru. After a postdoctoral fellowship at Caltech, she moved to CWI in Amsterdam, where she continues to research quantum algorithms and cryptographic protocols, as part of QuSoft, the research center for quantum software. Since 2023, she has also been a professor at the University of Amsterdam. In her spare time she sometimes reads Theory of Computing.

THOMAS VIDICK graduated from UC Berkeley in 2011; his advisor was Umesh Vazirani. His thesis focused on the study of quantum entanglement in multiprover interactive proof systems and in quantum cryptography. After a postdoctoral scholarship at MIT under the supervision of Scott Aaronson, he moved back to sunny California where he was a professor in Caltech's department of Computing and Mathematical Sciences and a member of the Institute of Quantum Information and Matter until 2024. In 2022 he crossed the Atlantic and moved to the Weizmann Institute of Science in Israel, where he currently resides and works.