Lecture 6

Verifying a single qubit-Hamiltonian

In the previous lecture we introduced the circuit-to-Hamiltonian constructions, that given a quantum circuit $\mathcal{C}$ and an input x to it returns a Hamiltonian $H_{\mathcal{C}}$ of the form (5.3) such that the completeness and soundness properties stated in Theorem 5.7 hold. This construction allowed us to reduce the problem of delegating a quantum computation to the problem of deciding if a certain publicly known, explicitly specified exponential-size Hermitian matrix $H_{\mathcal{C}}$ has an eigenvalue below a certain threshold a, or all its eigenvalues are above $b+\delta$ for a δ that is at least inverse polynomial in the number of qubits n on which $H_{\mathcal{C}}$ acts.[1] We then introduced the Fitzsimons-Morimae protocol (Figure 5.2) that is a protocol with one-way communication for verifying this fact.

Our goal in this lecture is to combine the Fitzsimons-Morimae protocol with the computational test for a qubit from lecture 4, Section 4.3 to obtain a classical protocol with similar guarantees to the Fitzsimons-Morimae protocol. For this we will develop a test that allows one to verify that a prover "has" a quantum state $|\psi\rangle$ with certain properties (e.g. it satisfies $\langle\psi|H|\psi\rangle \leq a+\delta/2$, i.e. certifies that the outcome of the computation is '1'. Note that even though in principle it is sufficient for the verifier to be convinced that such a $|\psi\rangle$ exists to make the right decision, we will see from the proofs that we can go a little further and give a precise meaning to the notion that the prover 'has' $|\psi\rangle$. This, however, will not be as strong as the claim that the prover 'has n qubits in state $|\psi\rangle$' in the sense that we gave to the phrase 'has n qubits', i.e. we will not quite exhibit $2n$ Pauli operators X_i, Z_i that satisfy all the required relations.

Remark 6.1. In passing to the Hamiltonian model of computation we relaxed our main goal, from obtaining a value $b \in \{0,1\}$ that is distributed as a measurement of the output qubit of the quantum circuit $\mathcal{C}$ in the standard basis to obtaining a value that is 1 whenever this measurement returns 1 with probability larger than $\frac{2}{3}$, and 0 whenever it is less than $\frac{1}{3}$. In particular, we make no requirement for circuits that are "undecided", e.g. return a random bit as output. This is typical to applications in complexity where it is assumed that circuits of interest make a clear-cut decision, 0 or 1; this is the setting discussed in Section 5.1. By tweaking the definition of $H_{\mathcal{C}}$ it is in fact possible to guarantee that any state $|\psi\rangle$ such that $\langle\psi|H_{\mathcal{C}}|\psi\rangle \leq a+\delta/2$ is such that a measurement of the first qubit of $|\psi\rangle$ in the standard basis yields an outcome whose distribution is within total variation distance, say, $\frac{1}{100}$ from a measurement of the output qubit of $\mathcal{C}$. Using this observation the protocol given at the end of this lecture can be adapted to return outcomes that are distributed close to the circuit output distribution, even in cases where the output is not assumed to be biased one way or the other. For simplicity we leave this extension as an exercise to the reader.

[1] In the previous lecture this number of qubits was called n', with n the number of qubits of the circuit $\mathcal{C}$. For the next two lectures, $\mathcal{C}$ disappears and so we re-use n to measure the size of $H_{\mathcal{C}}$.

6.1 A test for a specific single-qubit Hamiltonian

We start with an "easy" case: we show how the computational test for a qubit from lecture 4, protocol $\mathfrak{Q}$, can be cast as a verification protocol for the claim that the Hamiltonian $H = -\sigma_Z$ has a "low" eigenvalue, equal to -1. We go a little further by showing how such an eigenstate can be "extracted" from any successful prover in the protocol.

6.1.1 An explicit isometry

Our main result on the computational qubit test, Theorem 4.4, states that any successful prover in the protocol must "have a qubit". The proof achieves slightly more than that, as it explicitly states what the observables Z in (4.3) and X in (4.4) that define the qubit $(|\psi\rangle, Z, X)$ are. As we saw in Lemma 2.3 in lecture 2 the qubit implies the existence of an isometry $V : \mathcal{H} \to \mathbb{C}^2 \otimes \mathcal{H}'$ under which $Z \simeq \sigma_Z$, $X \simeq \sigma_Z$, and $|\psi\rangle \simeq |\psi'\rangle \in \mathbb{C}^2 \otimes \mathcal{H}'$, giving us an identification of the "abstract" qubit $(|\psi\rangle, Z, X)$ with a "concrete" qubit, i.e. the space $\mathbb{C}^2$ and its algebra of operators, of which σ_Z and σ_X form a linear basis.

With our present goal of "extracting" a specific quantum state (a low-energy eigenstate for the Hamiltonian H_C) it is worthwhile making V a little more explicit. Indeed, an important point that we did not emphasize so far is that this identification is not "canonical". If you remember the proof of Lemma 2.3, it involves an application of Jordan's lemma to identify a block structure such that in each block, Z and X act like σ_Z and σ_X respectively. These blocks were obtained by diagonalizing the operator $(X + Z)$. In the case where X and Z anti-commute this operator has only two eigenvalues, $\pm\sqrt{2}$, and the associated eigenspaces are highly degenerate. Any choice of a basis for one of the eigenspaces can be used to specify an isometry V (a basis for the other eigenspace is determined by the first). (That there would be such a degeneracy is easily seen by observing that composing V by any unitary on $\mathcal{H}'$ still gives a valid isometry with the same properties.)

It is, in fact, possible to define a canonical choice for the isometry. This choice has the advantage that it is explicit and from a computational viewpoint leads to a circuit for V that can be constructed from circuits for X and Z. The idea behind the definition is to use the operators X and Z to "teleport" the abstract qubit $(|\psi\rangle, Z, X)$ into a "concrete" qubit $(|\varphi\rangle, \sigma_Z, \sigma_X)$ by means of an EPR pair. This is done in the following proposition.

Proposition 6.2. *Let $(|\psi\rangle, Z, X)$ be a qubit on $\mathcal{H}$. Let $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle) \in \mathbb{C}^2 \otimes \mathbb{C}^2$ be the state of an EPR pair. Let $\mathcal{H}' = \mathbb{C}^2_A \otimes \mathcal{H}$ and $V : \mathcal{H} \to \mathbb{C}^2_Q \otimes \mathcal{H}'$ defined by*

$$\forall |\varphi\rangle \in \mathcal{H}\ , \quad V|\varphi\rangle = \frac{1}{2}\big(\mathrm{Id} \otimes \mathrm{Id}_A \otimes \mathrm{Id}_Q + X \otimes \sigma_X \otimes \mathrm{Id}_Q + Z \otimes \sigma_Z \otimes \mathrm{Id}_Q + XZ \otimes \sigma_X\sigma_Z \otimes \mathrm{Id}_Q\big)|\varphi\rangle|\phi^+\rangle_{AQ}\ , \tag{6.1}$$

where the systems in the range of V are re-ordered so that the first factor $\mathbb{C}^2$ is associated with the second qubit of $|\phi^+\rangle_{AQ}$ in (6.1)*, and $\mathcal{H}'$ consists of the state of the first qubit of $|\phi^+\rangle$, i.e. register A, as well as the part of the state in $\mathcal{H}$. Then V is an isometry and for all $W \in \{X, Z\}$,*

$$VW|\psi\rangle = (\sigma_W \otimes \mathrm{Id})V|\psi\rangle\ . \tag{6.2}$$

Proof. The proof is by direct calculation. First we verify that V is indeed an isometry. This is simply because the four states $\{(\sigma_X(a)\sigma_Z(b) \otimes \mathrm{Id})|\phi^+\rangle,\ a, b \in \{0,1\}\}$ are orthonormal[2] and X and Z are observables, so

[2]For $a, b \in \{0,1\}$ we use the notation $\sigma_X(a)$ for σ_X^a and similarly $\sigma_Z(b)$ for σ_Z^b. The motivation for this notation will be seen later when we consider n-qubit Pauli operators.

that for normalized $|\varphi\rangle$ each of the four terms on the right-hand side of (6.1) has norm exactly 1. Note that this does not require any other condition on X, Z than that they are observables (in fact, unitarity suffices). In particular, they do not need to anti-commute. Next we verify (6.2). Take $W = X$. Then

$$\begin{aligned} VX|\psi\rangle &= \frac{1}{2}\big(X\otimes \mathrm{Id}\otimes \mathrm{Id} + \mathrm{Id}\otimes\sigma_X\otimes \mathrm{Id} - XZ\otimes\sigma_Z\otimes \mathrm{Id} - Z\otimes\sigma_X\sigma_Z\otimes \mathrm{Id}\big)|\psi\rangle|\phi^+\rangle \\ &= \frac{1}{2}\big(X\otimes \mathrm{Id}\otimes \mathrm{Id} + \mathrm{Id}\otimes\sigma_X\otimes \mathrm{Id} - XZ\otimes\sigma_Z\otimes \mathrm{Id} - Z\otimes\sigma_X\sigma_Z\otimes \mathrm{Id}\big)|\psi\rangle(\sigma_X\otimes\sigma_X)|\phi^+\rangle \\ &= \frac{1}{2}\big(X\otimes\sigma_X\otimes\sigma_X + \mathrm{Id}\otimes \mathrm{Id}\otimes\sigma_X + XZ\otimes\sigma_X\sigma_Z\otimes\sigma_X + Z\otimes\sigma_Z\otimes\sigma_X\big)|\psi\rangle|\phi^+\rangle \\ &= (\sigma_X\otimes \mathrm{Id})V|\psi\rangle\ , \end{aligned}$$

where for the first line we used that X and Z anti-commute on $|\psi\rangle$, for the second that $\sigma_X\otimes\sigma_X|\phi^+\rangle = |\phi^+\rangle$, for the third that σ_X and σ_Z anti-commute, and for the last we re-ordered terms. □

6.1.2 Extraction of prover's qubit

In the proof of Theorem 4.4 we defined a specific X and Z from the prover's actions and showed that they anti-commute. Moreover, we showed that for a prover that always succeeds in the equation test (case $c = 1$) it must be the case that the state $|\psi\rangle$ of the prover is a $+1$ eigenstate of X, $X|\psi\rangle = |\psi\rangle$. For the definition of $|\psi\rangle \in \mathcal{H}_{\mathsf{X}}\otimes\mathcal{H}_{\mathsf{P}}$, recall that we had assumed that the prover directly measures the qubits in register X on challenge $c = 0$, and applies an arbitrary unitary U before measuring in the Hadamard basis on challenge $c = 1$. This means that after the isometry V, the prover's state $|\psi\rangle$ is mapped to a $+1$ eigenstate of σ_X, i.e. the state $|+\rangle$. The following corollary summarizes this discussion.

Corollary 6.3. *Suppose that a prover succeeds with probability* 1 *in the protocol. Then the isometry V defined from the observables Z in* (4.3) *and X in* (4.4) *sends $|\psi\rangle$ to $|+\rangle_{\mathsf{Q}}|aux\rangle$, for some state $|aux\rangle$ on $\mathcal{H}'$.*

In the context of this lecture we interpret Corollary 6.3 as our first test for a quantum computation in the Hamiltonian-based model: in this test, the verifier is effectively checking that the prover has prepared a $+1$ eigenstate of the Hamiltonian σ_X, or in other words a ground state of $H = -\sigma_X$. While we know that this eigenstate always exists, the analysis of the protocol shows that in some sense the prover has prepared the state. This additional observation allows us to make stronger conclusions from the protocol. For example, just as a measurement of $|+\rangle$ in the computational basis yields an unbiased random bit, we are able to deduce that the value of $b(x)$ with x the prover's answer on challenge $c = 0$ is an unbiased random bit. This ties in to the discussion in Section 3.4.1, where we observed that high success probability in the magic square game could be used to certify the generation of a random bit, and makes the protocol potentially useful for cryptographic applications where the generation of certified unbiased randomness serves as a resource.

In the development of our test we were greatly aided by the fact that we *know* what is the ground state of $H = -\sigma_X$, and in particular we know that a Hadamard basis measurement of it yields the outcome 0 (for '+') with probability 1. This "knowledge" was indirectly encapsulated in the test performed for the case $c = 1$, the analysis of which led us to conclude that $X|\psi\rangle = +|\psi\rangle$. But what if we didn't? What if H is a general Hamiltonian of the form (5.3), for which we can't a priori predict measurement outcomes?

6.2 Extracting a qubit: general case

In Section 6.1.1 we made the important observation that the map V in (6.1) is a well-defined isometry for any choice of the two observables X and Z. In particular, this map allows us to make a meaningful definition

of a *space* for a qubit, and a *state* for that qubit, associated with *any* prover in protocol $\mathfrak{Q}$, the computational test for a qubit described in Figure 4.1. This definition does not guarantee that the prover "has a qubit," because it does not say anything about how the prover's observables operate on it. However, it still allows us to define a *candidate* for a single-qubit state on which σ_X and σ_Z measurements can *in principle* be made. The next claim evaluates how outcomes of these measurements when performed on the extracted qubit are a distributed as a function of the observables X and Z on the prover's state $|\psi\rangle$.

Claim 6.4. *Let $|\psi\rangle \in \mathcal{H}$ and X, Z observables on $\mathcal{H}$ be arbitrary. Let V be defined as in* (6.1)*. Then the following hold:*

$$\langle\psi|V^\dagger\big(\sigma_Z \otimes \mathrm{Id}\,\big)V|\psi\rangle = \langle\psi|Z|\psi\rangle\ , \tag{6.3}$$

$$\langle\psi|V^\dagger\big(\sigma_X \otimes \mathrm{Id}\,\big)V|\psi\rangle = \frac{1}{2}\big(\langle\psi|X|\psi\rangle - \langle\psi|ZXZ|\psi\rangle\big)\ , \tag{6.4}$$

where the σ_Z and σ_X operators act on the first tensor factor $\mathbb{C}^2$ in the range of V and the identities act on $\mathcal{H}'$.

Proof. Let $W \in \{X, Z\}$. Expanding from the definition of V,

$$\begin{aligned}\langle\psi|V^\dagger\big(\sigma_W \otimes \mathrm{Id}\,\big)V|\psi\rangle &= \frac{1}{4}\sum_{P,Q\in\{I,X,Z,XZ\}} \langle\psi|P^\dagger Q|\psi\rangle \cdot \langle\phi^+|\sigma_P^\dagger\sigma_Q \otimes \sigma_W|\psi\rangle \\ &= \frac{1}{4}\sum_{P,Q:\,\sigma_P^\dagger\sigma_Q=\sigma_W} \langle\psi|P^\dagger Q|\psi\rangle\ ,\end{aligned}$$

where for the second line we used that $\langle\phi^+|\sigma_W \otimes \sigma_{W'}|\phi^+\rangle = \delta_{W,W'}$ with δ the Kronecker symbol. In case $W = Z$ the pairs P, Q that appear in the last summation above are $(X, I), (I, X), (XZ, X)$ and (X, XZ). Using $X^2 = \mathrm{Id}$ we obtain (6.3). In case $W = X$ then the summation is over $(Z, I), (I, Z), (XZ, Z)$ and (Z, XZ) and has a minus sign for the last two terms due to $\sigma_X\sigma_Z = -\sigma_Z\sigma_X$. Thus we get (6.4) as well. □

Observe that if X and Z anti-commute then Claim 6.4 gives us the result that we expect: in this case $(|\psi\rangle, Z, X)$ is a qubit so Proposition 6.2 applies and the isometry "intertwines" measurements X and Z on $|\psi\rangle$ with σ_X and σ_Z respectively on the first factor of $V|\psi\rangle$. At the other extreme, if X and Z commute then (6.4) indicates that a measurement in the Hadamard basis of the extracted qubit returns an unbiased random bit. This is expected of a "classical" state, which always leads to uniformly random results in the Hadamard basis. The lemma in some sense interpolates between these results. Importantly, it allows us to associate a qubit with the state of an arbitrary prover in the protocol, that is such that the distribution of measurements on the extracted qubit can be related to quantities that involve the prover's state and observables in the protocol. For convenience we make this into a definition.

Definition 6.5 (Extracted qubit)**.** Let P be a prover in protocol $\mathfrak{Q}$. Let $|\psi\rangle$ be the state of P after having sent y in the first round of interaction. Let V be defined as in (6.1). Then we call the reduced density of $V|\psi\rangle$ on the first factor $\mathbb{C}^2$, associated with register Q, the *extracted qubit* and denote it by ρ_{Q}.

Lemma 6.6. *Let P be a prover that succeeds with probability 1 in the pre-image test of protocol $\mathfrak{Q}$ and such that the string d returned in the equation test is $d = 0^m$ with probability that is negligibly small in λ. (No other assumption is made on the equation test.) Let ρ be the extracted qubit, as defined in Definition 6.5. Then the following hold:*

- *(Z-measurement:) The outcome of measuring ρ in the computational basis is identically distributed to the bit $(-1)^{b(x)}$ computed from the prover's answer x in case $c = 0$.*
- *(X-measurement:) Under assumption (**F.2**), the outcome of measuring ρ in the Hadamard basis is* computationally indistinguishable *from the bit $(-1)^{d\cdot(x_0+x_1)}$ where d is obtained from the prover in case $c = 1$.*

Remark 6.7 (Computational distinguishability). The statement of the lemma refers to two distributions being computationally indistinguishable. Informally, this means that no computationally efficient procedure can distinguish a sample taken from one distribution from a sample taken from the other. Formally, families of distributions $D = \{D_\lambda\}$ and $D' = \{D'_\lambda\}$ on universes $\{\mathcal{X}_\lambda\}$ are said to be computationally indistinguishable if for any PPT (or QPT for computational indistinguishability against quantum adversaries) procedure $\mathcal{A}$ there is a negligible function μ such that for every λ,

$$\Big| \Pr_{x\leftarrow D_\lambda}\big(\mathcal{A}(1^\lambda, x) = 1\big) - \Pr_{x'\leftarrow D'_\lambda}\big(\mathcal{A}(1^\lambda, x') = 1\big)\Big| \leq \mu(\lambda)\,.$$

Here, when we refer to computational indistinguishability we will always mean against QPT adversaries. Note that for distributions on a family of universes $\{\mathcal{X}_\lambda\}$ such that $|\mathcal{X}_\lambda|$ grows at most polynomially with λ the notion of computational indistinguishability is equivalent to statistical indistinguishability, i.e. the total variation distance between D_λ and D'_λ goes to 0 as fast as some negligible function. (Showing this formally is a good exercise to practice with the definitions.)

Proof. The first item follows immediately from (6.3) in Claim 6.4 and the definition of Z in (4.3), which guarantees that the bit $(-1)^{b(x)}$ obtained from the prover in case $c = 0$ has expectation precisely $\langle\psi|Z|\psi\rangle$.

To show the second item we assume for contradiction that the two distributions are computationally distinguishable. Since the distributions are over a single bit, as recalled in Remark 6.7 this is equivalent to statistical distinguishability: there must exist a polynomial $q(\lambda)$ such that for infinitely many values of λ,

$$\big|\langle\psi|X|\psi\rangle + \langle\psi|ZXZ|\psi\rangle\big| > \frac{1}{q(\lambda)}\,, \tag{6.5}$$

where recall that the expression on the left should be understood on average over the generation of pk by the verifier and the message y sent by the prover in the first round of interaction. We derive a contradiction with (**F.2**) by constructing an adversary in (4.2). Given λ and pk as input, $\mathcal{A}$ prepares the state $|\psi\rangle$. $\mathcal{A}$ then measures register X in the standard basis to obtain an outcome x. Using the assumption that the prover succeeds with probability 1 in the pre-image test, $f_{pk}(x) = y$ and the (unnormalized) post-measurement state is exactly $Z_{b(x)}|\psi\rangle$, where as usual $Z_b = (\mathrm{Id} + (-1)^b Z)/2$. Finally, the adversary applies the prover's unitary U and measures in the Hadamard basis to obtain a string d. It returns the pair (x, d). The expected value of $(-1)^{d\cdot(x_0+x_1)}$ under this procedure is

$$\langle\psi|Z_0XZ_0|\psi\rangle + \langle\psi|Z_1XZ_1|\psi\rangle = \frac{1}{2}\big(\langle\psi|X|\psi\rangle + \langle\psi|ZXZ|\psi\rangle\big)\,,$$

which can be seen by expanding $Z_b = (\mathrm{Id} + (-1)^b Z)/2$ for $b \in \{0,1\}$ and canceling cross-terms. Using (6.5) and the fact that, $\mathcal{A}$ violates (4.2).[3] □

[3] The end of the proof glosses over a detail: one needs to guarantee that the equation d returned by $\mathcal{A}$ is not 0. While the lemma assumes that this is the case when the equation is measured directly on $|\psi\rangle$, here $\mathcal{A}$ measures after $|\psi\rangle$ has already been measured using the observable Z. To show that the assumption that $d \neq 0^m$ with probability negligibly close to 1 still holds one needs to use the "collapsing" property of f_pk, that we will introduce in the next lecture. For the time being we set aside this detail.

6.3 A single-qubit verification protocol

In the previous section we showed how to identify a "qubit" such that for any prover in the protocol, as long as the prover succeeds in the preimage test then it is possible for the verifier to infer from the prover's answers a bit whose distribution is statistically indistinguishable from outcomes of σ_Z or σ_X measurements on a well-defined quantum state. In order to turn this into a verification protocol for a single-qubit Hamiltonian, we are missing the completeness statement: while in Section 4.3 we saw how a prover could behave in such a way that the extracted qubit is a $|+\rangle$ state, we do not yet know if it is possible to use the protocol for the verification of other single-qubit states. In order for this to work out, we make the following assumption that replaces assumption (**F.4**):

(**F.4'**) For any pk and any y in the range of f_{pk} the two preimages of y take the form (b, x_b) where $b \in \{0,1\}$ and $x_b \in \{0,1\}^{m(\lambda)-1}$. In particular, the function $b : \{0,1\}^m \to \{0,1\}$ returns the first bit of its input.

This assumption is mainly for convenience and holds for most constructions of claw-free functions, including the one that we sketch in the next lecture. Given a 2-to-1 function family that satisfies (**F.4'**) the following lemma shows how a prover can behave in the protocol so that the extracted qubit defined in the previous section is a state $|\psi\rangle$ of its choice.

Lemma 6.8. *Let $|\varphi\rangle \in \mathbb{C}^2$ be any state. Then there is a way for the prover to behave in protocol $\mathfrak{Q}$ such that the prover is accepted with probability 1 in the preimage test and moreover the extracted qubit satisfies $\rho_{\mathsf{Q}} = |\varphi\rangle\langle\varphi|$.*

Proof. Let $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$ for $\alpha, \beta \in \mathbb{C}$ such that $|\alpha|^2 + |\beta|^2 = 1$. The prover performs the following steps:

1. Prepare the initial state

$$|\psi^{(0)}\rangle_{\mathsf{BXY}} \;=\; |\varphi\rangle_{\mathsf{B}} \otimes \Big(\frac{1}{2^{m-1}} \sum_{x\in\{0,1\}^{m-1}} |x\rangle_{\mathsf{X}}\Big)|0\rangle_{\mathsf{Y}} \;,$$

   where B is a one-qubit register, X an $(m-1)$ and Y an m-qubit register, for $m = m(\lambda)$.

2. Upon receipt of the function index pk, coherently evaluate f_{pk} on the input in registers BX, writing the output in register Y to obtain the state

$$|\psi^{(1)}\rangle_{\mathsf{BXY}} \;=\; \frac{\alpha}{2^{m-1}} \sum_{x\in\{0,1\}^{m-1}} |0\rangle_{\mathsf{B}}|x\rangle_{\mathsf{X}}|f(0x)\rangle_{\mathsf{Y}} + \frac{\beta}{2^{m-1}} \sum_{x\in\{0,1\}^{m-1}} |1\rangle_{\mathsf{B}}|x\rangle_{\mathsf{X}}|f(1x)\rangle_{\mathsf{Y}} \;.$$

3. Measure the last register to obtain a y. Let $(0, x_0)$ and $(1, x_1)$ be the two preimages of y under f_{pk}. Then the re-normalized post-measurement state is

$$|\psi^{(2)}\rangle_{\mathsf{BXY}} \;=\; \big(\alpha|0\rangle_{\mathsf{B}}|x_0\rangle_{\mathsf{X}} + \beta|1\rangle_{\mathsf{B}}|x_1\rangle_{\mathsf{X}}\big)|y\rangle_{\mathsf{Y}} \;.$$

4. Upon receipt of challenge c, perform as the honest prover in protocol $\mathfrak{Q}$: if $c = 0$ measure registers BX in the standard basis and return the outcome $x = (b, x_b)$; if $c = 1$ measure in the Hadamard basis and return the outcome d.

This prover always returns a valid preimage in the case of a challenge $c = 0$, so it is accepted with probability 1. Observe that the operator Z associated to this prover is equal to a σ_Z on register B. Regarding the operator X, a simple calculation reveals that the action of X restricted to the span of $|0, x_0\rangle_{\mathsf{BX}}$ and $|1, x_1\rangle_{\mathsf{BX}}$ consists in exchanging these two basis states. Using the explicit form of the isometry V given in (6.1) one can verify that

$$V|\psi^{(2)}\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle_{\mathsf{B}}|x_0\rangle_{\mathsf{X}}|0\rangle_{\mathsf{A}} + |1\rangle_{\mathsf{B}}|x_1\rangle_{\mathsf{X}}|1\rangle_{\mathsf{A}}\big) \otimes \big(\alpha|0\rangle_{\mathsf{Q}} + \beta|1\rangle_{\mathsf{Q}}\big) \otimes |y\rangle_{\mathsf{Y}} \,,$$

where AQ are the two registers introduced to hold the EPR pair $|\phi^+\rangle_{\mathsf{AQ}}$ used in the definition of V. Register Q contains the extracted qubit. □

Let $\mathcal{F}$ be a 2-to-1 trapdoor claw-free function family and $\lambda \in \mathbb{N}$ a security parameter. Let $\varepsilon, \delta > 0$ be accuracy parameters. Let $\gamma = 0$ and $N = \frac{C}{\delta^2}\ln(1/\varepsilon)$ for some large constant C. The verifier and prover repeat the following interaction N times.

1. The verifier generates $(pk, td) \leftarrow \textsc{Gen}(1^\lambda)$. It sends pk to the prover.
2. The prover returns $y \in \{0,1\}^m$, where $m = m(\lambda)$.
3. The verifier selects a uniformly random challenge $c \leftarrow_R \{0,1\}$ and sends c to the prover.
4. (a) *(Computational basis, $c = 0$:)* In case $c = 0$ the prover is expected to return an $x \in \{0,1\}^m$. If $f(x) \neq 0$ then the verifier immediately aborts. The verifier sets $a \leftarrow (-1)^{b(x)}$ and $\gamma \leftarrow \gamma - J_Z a$.
   (b) *(Hadamard basis, $c = 1$:)* In case $c = 1$ the prover is expected to return a $d \in \{0,1\}^m$. The verifier uses td to determine the two preimages (x_0, x_1) of y by f_{pk}. She sets $b \leftarrow (-1)^{d\cdot(x_0+x_1)}$ and $\gamma \leftarrow \gamma - J_X b$.

If the verifier has not aborted at any of the steps $c = 0$, she returns the real number $o = \frac{1}{N}\gamma$.

Figure 6.1: Verification protocol for a single-qubit Hamiltonian $H = -\frac{J_X}{2}\sigma_X - \frac{J_Z}{2}\sigma_Z$.

The following proposition summarizes what we have achieved so far, a verification protocol for single-qubit Hamiltonians and a completely classical verifier. (Of course a simpler protocol would be to have the verifier classically do the computation themselves! The point is that this protocol is not too hard to extend to n qubits, and we will see this later.) The protocol, which combines protocol $\mathfrak{Q}$ with the Fitzsimons-Morimae verification protocol, is summarized in Figure 6.1.

Proposition 6.9. *Let $H = -\frac{J_X}{2}\sigma_X - \frac{J_Z}{2}\sigma_Z$ be a single-qubit Hamiltonian and $\delta, \varepsilon > 0$ accuracy parameters. Then the verification protocol from Figure 6.1 has the following properties:*

1. *(Completeness:) For any single-qubit state $|\varphi\rangle$, there is a QPT prover that is accepted with probability 1 in the protocol and such that the value o returned by the verifier at the end of the protocol satisfies $\mathrm{E}[o] = \langle\varphi|H|\varphi\rangle$.*
2. *(Soundness:) For any QPT prover that is accepted with probability 1 in the protocol, there is a single-qubit state ρ such that the value o returned by the verifier at the end of the protocol satisfies $\mathrm{E}[o] = \mathrm{Tr}(H\rho)$.*

Moreover, with the value of N specified in the protocol in both cases it holds that $\Pr(|o - \mathrm{Tr}(H\rho)| > \delta) \leq \varepsilon$.

Remark 6.10. The assumption that the prover succeeds with probability negligibly close to 1 in the protocol can be relaxed to a constant sufficiently close to 1, where the distance to 1 will affect the distance $|\mathrm{E}[o] - \mathrm{Tr}(H\rho)|$. First we observe that a success probability negligibly close to 1 is sufficient; this can be verified by going through the argument again, and nothing needs to be changed. Second, it is possible to show that any prover with success probability $1 - \kappa$ for some $\kappa \geq 0$ can be transformed to a prover with success probability negligibly close to 1, affecting the distribution of o proportionately to κ. Intuitively, the new prover will test if the value y that the old prover would have returned will lead to success on challenge $c = 0$, in case that the test is actually executed by the verifier. This can be done efficiently by the prover by evaluating the pre-image condition on register X. If this test fails then the new prover simply re-executes the old prover from scratch, until it is certain to achieve success. With probability negligibly close to 1 this iterative procedure will stop in a polynomial number of steps, and using the "pretty-good lemma" it is possible to show that the prover's distribution of outcomes is affected by some $O(\sqrt{\kappa})$ in statistical distance. We omit the details.

Proof. The completeness statement follows from Lemma 6.8. For soundness we use Lemma 6.6. This shows that the expectation of the bit a in step 4.(a) satisfies $\mathrm{E}[a] = \mathrm{Tr}(\sigma_Z \rho)$ where ρ is the extracted qubit. Similarly, the bit b in step 4.(b) satisfies $\mathrm{E}[b] = \mathrm{Tr}(\sigma_Z \rho)$. Since by definition

$$\mathrm{E}[o] \;=\; -\frac{J_Z}{2}\,\mathrm{E}[a] - \frac{J_X}{2}\,\mathrm{E}[b]$$

the proposition follows. □

Bibliography

[Aar10] Scott Aaronson. Bqp and the polynomial hierarchy. In *Proceedings of the forty-second ACM symposium on Theory of computing*, pages 141–150. ACM, 2010.

[AB09] Sanjeev Arora and Boaz Barak. *Computational complexity: a modern approach*. Cambridge University Press, 2009.

[ACGK17] Scott Aaronson, Alexandru Cojocaru, Alexandru Gheorghiu, and Elham Kashefi. On the implausibility of classical client blind quantum computing. *arXiv preprint arXiv:1704.08482*, 2017.

[AG17] Dorit Aharonov and Ayal Green. A quantum inspired proof of $\mathrm{P}^{\setminus\#\mathrm{p}} \subseteq$ IP. *arXiv preprint arXiv:1710.09078*, 2017.

[AV12] Dorit Aharonov and Umesh Vazirani. Is quantum mechanics falsifiable? A computational perspective on the foundations of quantum mechanics. *arXiv preprint arXiv:1206.3686*, 2012.

[AV13] Dorit Aharonov and Umesh Vazirani. *Is quantum mechanics falsifiable? A computational perspective on the foundations of quantum mechanics*. Computability: Turing, Gödel, Church, and Beyond. MIT Press, 2013.

[BCM+18] Zvika Brakerski, Paul Christiano, Urmila Mahadev, Umesh Vazirani, and Thomas Vidick. A cryptographic test of quantumness and certifiable randomness from a single quantum device. In *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 320–331. IEEE, 2018.

[Bel64] John S Bell. On the einstein podolsky rosen paradox. *Physics Physique Fizika*, 1(3):195, 1964.

[Bre06] Frédéric Brechenmacher. *Histoire du théorème de Jordan de la décomposition matricielle (1870-1930). Formes de représentation et méthodes de décomposition.* PhD thesis, 2006.

[CCKW19] Alexandru Cojocaru, Léo Colisson, Elham Kashefi, and Petros Wallden. Qfactory: classically-instructed remote secret qubits preparation. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 615–645. Springer, 2019.

[CLS17] Richard Cleve, Li Liu, and William Slofstra. Perfect commuting-operator strategies for linear system games. *Journal of Mathematical Physics*, 58(1):012202, 2017.

[CM14] Richard Cleve and Rajat Mittal. Characterization of binary constraint system games. In *International Colloquium on Automata, Languages, and Programming*, pages 320–331. Springer, 2014.

[CM16] Toby Cubitt and Ashley Montanaro. Complexity classification of local hamiltonian problems. *SIAM Journal on Computing*, 45(2):268–316, 2016.

[CR20] Rui Chao and Ben W Reichardt. Quantum dimension test using the uncertainty principle. *arXiv preprint arXiv:2002.12432*, 2020.

[CRSV17] Rui Chao, Ben W Reichardt, Chris Sutherland, and Thomas Vidick. Overlapping qubits. *arXiv preprint arXiv:1701.01062*, 2017.

[CRSV18] Rui Chao, Ben W Reichardt, Chris Sutherland, and Thomas Vidick. Test for a large amount of entanglement, using few measurements. *Quantum*, 2:92, 2018.

[CS17] Andrea Coladangelo and Jalex Stark. Robust self-testing for linear constraint system games. *arXiv preprint arXiv:1709.09267*, 2017.

[DFPR14] Vedran Dunjko, Joseph F Fitzsimons, Christopher Portmann, and Renato Renner. Composable security of delegated quantum computation. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 406–425. Springer, 2014.

[EPR35] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical review*, 47(10):777, 1935.

[Gen09] Craig Gentry. Fully homomorphic encryption using ideal lattices. In *STOC*, volume 9, pages 169–178, 2009.

[GKK19] Alexandru Gheorghiu, Theodoros Kapourniotis, and Elham Kashefi. Verification of quantum computation: An overview of existing approaches. *Theory of computing systems*, 63(4):715–808, 2019.

[GKR08] Shafi Goldwasser, Yael Tauman Kalai, and Guy N Rothblum. Delegating computation: interactive proofs for muggles. In *Proceedings of the fortieth annual ACM symposium on Theory of computing*, pages 113–122. ACM, 2008.

[GMR85] Shafi Goldwasser, Silvio Micali, and Ronald Rivest. A "paradoxical" solution to the signature problem. In *Advances in Cryptology*, pages 467–467. Springer, 1985.

[GVW01] Oded Goldreich, Salil Vadhan, and Avi Wigderson. On interactive proofs with a laconic prover. In *International Colloquium on Automata, Languages, and Programming*, pages 334–345. Springer, 2001.

[JNV+20] Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. MIP*= RE. *arXiv preprint arXiv:2001.04383*, 2020.

[KMW17] Elham Kashefi, Luka Music, and Petros Wallden. The quantum cut-and-choose technique and quantum two-party computation. *arXiv preprint arXiv:1703.03754*, 2017.

[KRR14] Yael Tauman Kalai, Ran Raz, and Ron D Rothblum. How to delegate computations: the power of no-signaling proofs. In *Proceedings of the forty-sixth annual ACM symposium on Theory of computing*, pages 485–494. ACM, 2014.

[Mah18] Urmila Mahadev. Classical verification of quantum computations. In *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 259–267. IEEE, 2018.

[Mer90] N David Mermin. Simple unified form for the major no-hidden-variables theorems. *Physical review letters*, 65(27):3373, 1990.

[Mer93] N David Mermin. Hidden variables and the two theorems of john bell. *Reviews of Modern Physics*, 65(3):803, 1993.

[MF16] Tomoyuki Morimae and Joseph F Fitzsimons. Post hoc verification with a single prover. *arXiv preprint arXiv:1603.06046*, 2016.

[MYS12] Matthew McKague, Tzyh Haur Yang, and Valerio Scarani. Robust self-testing of the singlet. *Journal of Physics A: Mathematical and Theoretical*, 45(45):455304, 2012.

[NC02] Michael A Nielsen and Isaac Chuang. Quantum computation and quantum information, 2002.

[RRR16] Omer Reingold, Guy N Rothblum, and Ron D Rothblum. Constant-round interactive proofs for delegating computation. In *Proceedings of the forty-eighth annual ACM symposium on Theory of Computing*, pages 49–62. ACM, 2016.

[RT19] Ran Raz and Avishay Tal. Oracle separation of bqp and ph. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, pages 13–23, 2019.

[RUV13] Ben W Reichardt, Falk Unger, and Umesh Vazirani. Classical command of quantum systems. *Nature*, 496(7446):456–460, 2013.

[SW87] Stephen J Summers and Reinhard Werner. Maximal violation of bell's inequalities is generic in quantum field theory. *Communications in Mathematical Physics*, 110(2):247–259, 1987.

[Vid20] Thomas Vidick. Verifying quantum computations at scale: A cryptographic leash on quantum devices. *Bulletin of the American Mathematical Society*, 57(1):39–76, 2020.

[VW16] Thomas Vidick and John Watrous. Quantum proofs. *Foundations and Trends® in Theoretical Computer Science*, 11(1-2):1–215, 2016.

[WBMS16] Xingyao Wu, Jean-Daniel Bancal, Matthew McKague, and Valerio Scarani. Device-independent parallel self-testing of two singlets. *Physical Review A*, 93(6):062121, 2016.