Towards a universal gateset for QMA_1

Dorian Rudolph[*]

October 5, 2024

Abstract

QMA_1 is QMA with perfect completeness, i.e., the prover must accept with a probability of *exactly* 1 in the YES-case. Whether QMA_1 and QMA are equal is still a major open problem (classically, we have $\mathsf{MA}_1 = \mathsf{MA}$), and only a quantum oracle separation due to Aaronson (QIC 2009) is known. Furthermore, QMA_1 does not actually have a single agreed-upon definition, since it depends on the choice of gateset, and the Solovay-Kitaev theorem only approximately synthesizes arbitrary gates from a universal gateset, not necessarily preserving perfect completeness. For a gateset $\mathcal{G}$, we define $\mathsf{QMA}_1^{\mathcal{G}}$ as QMA_1 restricted to verifiers only using gates of $\mathcal{G}$. Generally, it is not clear at all what the relationship of $\mathsf{QMA}_1^{\mathcal{G}}$ and $\mathsf{QMA}_1^{\mathcal{G}'}$, even for two universal gatesets $\mathcal{G}$ and $\mathcal{G}'$. Therefore, the $\mathsf{QMA}_1^{\mathcal{G}}$ classes form a potentially infinite hierarchy!

In this paper, we bring some structure to this chaos by proving that for each $k \in \mathbb{N}$, there exists a universal gateset $\mathcal{G}_{2^k}$ (defined by Amy et al., Reversible Computation, 2024), so that $\mathsf{QMA}_1^{\mathcal{G}} \subseteq \mathsf{QMA}_1^{\mathcal{G}_{2^k}}$ for all gatesets $\mathcal{G}$ consisting of unitaries in the cyclotomic field $\mathbb{Q}(\zeta_{2^k})$, where $\zeta_{2^k} = e^{2\pi \mathrm{i}/2^k}$ is a primitive 2^k-th root of unity. For BQP_1, we can even show that $\mathcal{G}_2$ suffices for all 2^k-th cyclotomic fields, i.e., $\mathsf{BQP}_1^{\mathcal{G}} \subseteq \mathsf{BQP}_1^{\mathcal{G}_2}$ for all $\mathcal{G}$ in $\mathbb{Q}(\zeta_{2^k})$. We exhibit complete problems for all $\mathsf{QMA}_1^{\mathcal{G}_{2^k}}$: Quantum l-SAT in $\mathbb{Q}(\zeta_{2^k})$ is complete for $\mathsf{QMA}_1^{\mathcal{G}_{2^k}}$ for all $l \geq 4$, and $l = 3$ if $k \geq 3$, where quantum l-SAT is the problem of deciding whether a set of l-local Hamiltonians has a common ground state.

Our techniques rely on representing operators as linear combinations of unitaries, which was pioneered by Childs and Wiebe (QIC 2012), and allows us to exactly apply even non-unitary operators to a quantum state, using postselection. We show the first QMA_1-complete 2-local Hamiltonian problem: It is $\mathsf{QMA}_1^{\mathcal{G}_{2^k}}$-complete (for $k \geq 3$) to decide whether a given 2-local Hamiltonian H in $\mathbb{Q}(\zeta_{2^k})$ has a nonempty nullspace (i.e. $\sigma_1(H)$) or $\sigma_1(H) \geq 1/\mathrm{poly}$, where σ_1 denotes the smallest singular value. Our techniques also extend to sparse Hamiltonians, and so we can prove the first $\mathsf{QMA}_1(2)$-complete (i.e. QMA_1 with two unentangled Merlins) Hamiltonian problem, which is a variant of the separable sparse Hamiltonian problem (Chailloux and Sattath, CCC 2012). Finally, we prove that the Gapped Clique Homology problem defined by King and Kohler (FOCS 2024) is $\mathsf{QMA}_1^{\mathcal{G}_2}$-complete, and the Clique Homology problem without promise gap is PSPACE-complete.

1 Introduction

The complexity class QMA_1 was introduced by Bravyi in 2006 [Bra06] as QMA with one-sided error (or *perfect completeness*), i.e., in the YES-case there exists a proof that the verifier accepts with a probability of *exactly* 1. Bravyi shows that the Quantum k-SAT problem (k-QSAT) is QMA_1-complete for $k \geq 4$ and in P for $k = 2$, where k-QSAT is the problem of deciding whether a given collection of k-local Hamiltonians has a common ground state. k-QSAT can be seen as a quantum analogue of the classical k-SAT problem, which is NP-complete for $k \geq 3$ [Coo71; Lev73; Kar72], and in P for $k = 2$ [Qui59; DP60; Kro67; EIS76; APT79; Pap91]. Later works even show that 2-QSAT is solvable in linear time [ASSZ16; BG16], and 3-QSAT is QMA_1-complete [GN13]. Quantum 2-SAT on qu$d$its is QMA_1-complete [ER08; Nag08; RGN24], with the most recent result being the QMA_1-completeness of $(3,4)$-QSAT and $(2,5)$-QSAT [RGN24], where in (k,l)-QSAT each local term acts on one qu-k-it and one qu-l-it. k-QSAT is a special case of the more well-known k-local Hamiltonian problem (k-LH),

[*] Department of Computer Science and Institute for Photonic Quantum Systems (PhoQS), Paderborn University, Germany. Email: dorian.rudolph@upb.de

where the goal is to approximate $\lambda_{\min}(H)$ for a k-local Hamiltonian H. k-LH can be seen as a quantum analogue of the classical MAX-k-SAT problem (i.e. what is the maximum number of simultaneously satisfiable constraints in a 2-CNF formula?). The 2-local Hamiltonian problem is QMA-complete [KSV02; KKR05; CM16], just as $\mathsf{MAX\text{-}2\text{-}SAT}$ is NP-complete [GJS76].

An interesting question to ask is now whether quantum k-SAT is also QMA-complete, or in other words, is $\mathsf{QMA} = \mathsf{QMA}_1$? Classically, we have $\mathsf{MA} = \mathsf{MA}_1$ [ZF87; GZ11]. Quantum interactive proof systems (QIP) also have perfect completeness [KW00; KLN15]. QMA even has a two-message quantum interactive proof system with perfect completeness, i.e., $\mathsf{QMA} \in \mathsf{QIP}_1(2)$ [KLN15]. Jordan et al. [JKNN12] have shown that QCMA (i.e., QMA with classical proofs) has perfect completeness, i.e., $\mathsf{QCMA} \subseteq \mathsf{QMA}_1$. Despite these positive results, the question whether $\mathsf{QMA} = \mathsf{QMA}_1$ remains open to this day. Aaronson [Aar09] gives some negative evidence in the form of a *quantum* oracle separation between QMA and QMA_1. The idea is to give the verifier access to an oracle performing a rotation by some angle θ, and the problem is to distinguish the cases $\theta \in [1, 2]$ (YES-case) or $\theta = 0$ (NO-case). Aaronson uses techniques from real analysis to prove that if the verifier accepts with probability 1 for all θ in an open set, then it must accept for all θ.

So far we have not touched upon the "gateset issue". That is, the definition of QMA_1 depends on which gateset the verifier uses. We write $\mathsf{QMA}_1^{\mathcal{G}}$ to denote QMA_1 with gateset $\mathcal{G}$, where $\mathcal{G}$ is a set of unitaries. Notably, we cannot use the Solovay-Kitaev algorithm [Kit97; DN05; BG21] to synthesize gates because that only approximates gates, not necessarily preserving perfect completeness. Therefore, we do not in general know whether $\mathsf{QMA}_1^{\mathcal{G}} = \mathsf{QMA}_1^{\mathcal{G}'}$ for two different universal gatesets $\mathcal{G}$ and $\mathcal{G}'$. Thus, the $\mathsf{QMA}_1^{\mathcal{G}}$ complexity classes form a potentially infinite hierarchy!

Bravyi [Bra06] defines QMA_1 as $\mathsf{QMA}_1^{\mathcal{G}}$, where $\mathcal{G}$ is the set of all 3-qubit unitaries in some subfield $\mathbb{F} \subseteq \mathbb{C}$ with exact representation. The corresponding complete 4-QSAT problem also allows all projectors with elements in $\mathbb{F}$. Thus, k-$\mathsf{QSAT} \in \mathsf{QMA}_1$ requires the verifier to be constructed specifically for the instance.[1] We cannot just give a classical description of the Hamiltonian to the quantum verifier.

Gosset and Nagaj [GN13] instead only consider the gateset $\{\mathsf{H}, \mathsf{CX}, \mathsf{T}\}$ (Hadamard, CNOT, T-gate), and show completeness for k-QSAT, where each local projector Π is in $\mathbb{Z}[\frac{1}{\sqrt{2}}, \mathrm{i}]$ [2], or there exists a unitary with only these elements, such that $U\Pi U^\dagger = (\sqrt{1/3}|000\rangle - \sqrt{2/3}|001\rangle)(\sqrt{1/3}\langle 000| - \sqrt{2/3}\langle 001|)$. That definition of k-QSAT unfortunately appears somewhat "unnatural". In this work we will "bridge the gap" between the definitions of [Bra06] and [GN13] in that we show completeness for k-QSAT in a *field* for $\mathsf{QMA}_1^{\mathcal{G}}$ with a *finite* gateset $\mathcal{G}$.

The containment result for k-$\mathsf{QSAT} \in \mathsf{QMA}_1$ in [GN13] relies on Giles and Selinger's [GS13] algorithm for *exactly* synthesizing any n-qubit unitary with entries in the ring $\mathbb{Z}[1/\sqrt{2}, \mathrm{i}]$ with the "Clifford + T" gateset. Their work has been extended to further gatesets by Amy et al. [AGR20]. Most recently Amy et al. [AGK+24] have shown that an n-qubit unitary matrix U can be exactly represented with the gateset $\mathcal{G}_{2^k}$ iff U's entries are in $\mathbb{Z}[1/2, \zeta_{2^k}]$ (see Theorem 3.1), where $\zeta_{2^k} = e^{2\pi\mathrm{i}/2^k}$ is a primitive 2^k-th root of unity, $\mathcal{G}_2 = \{\mathsf{X}, \mathsf{CX}, \mathsf{CCX}, \mathsf{H} \otimes \mathsf{H}\}$ (X, CNOT, Toffoli, Hadamard), $\mathcal{G}_4 = \{\mathsf{X}, \mathsf{CX}, \mathsf{CCX}, \mathsf{S}, \zeta_8\mathsf{H}\}$, and for $k \geq 3$, $\mathcal{G}_{2^k} = \{\mathsf{H}, \mathsf{CX}, \mathsf{T}_{2^k}\}$ with $\mathsf{T}_{2^k} = \left[\begin{smallmatrix} 1 & 0 \\ 0 & \zeta_{2^k} \end{smallmatrix}\right]$ ($\mathsf{T} \equiv \mathsf{T}_8$, $\mathsf{S} \equiv \mathsf{T}_4$).

Surprisingly, QMA_1 has recently appeared in computational topology: King and Kohler [KK23] have shown that the problem of determining wether the clique complex of a weighted graph has a hole, is QMA_1-hard and contained in QMA, given a suitable promise. The clique complex of a graph G is the simplicial complex obtained by declaring every $(k+1)$-clique in G to be a k-simplex. Their hardness result suggests that the quantum algorithm for topological data analysis [LGZ16] *cannot* be dequantized, which can compute the number of holes in persistent homology (see also the survey [Was18]). Prior work by Crichigno and Kohler [CK22] proved the QMA_1-hardness of the decision clique homology problem (i.e. without promise gap).

Results. Our first result is that for any finite gateset $\mathcal{G}$ consisting of unitaries with entries in the 2^k-th cyclotomic field, $\mathsf{QMA}_1^{\mathcal{G}}$ can be simulated using the finite gateset $\mathcal{G}_{2^k}$. We use the gatesets $\mathcal{G}_{2^k}$

[1] We remark that there is a slight issue with this procedure (see [Bra06, Lemma 5]), also mentioned by Gosset and Nagaj [GN13]. Decomposing general unitaries into 2-level unitaries (see [NC10]) does not necessary produce unitaries inside $\mathbb{F}$ (e.g. for $\mathbb{F} = \mathbb{Q}$).

[2] We use 'i' to denote the imaginary unit, disambiguating it from the index 'i'.

defined above from [AGK+24] (see Theorem 3.1). Additionally, we show that $\mathsf{QMA}_1^{\mathcal{G}_4} = \mathsf{QMA}_1^{\mathcal{G}_2}$, i.e., $\mathbb{Q}(\mathrm{i})$ gatesets can be simulated with just $\mathbb{Q}$ gates.

Theorem 1.1 (3.2, 6.4)**.** *For any finite gateset $\mathcal{G}$ in $\mathbb{Q}(\zeta_{2^k})$ with $k \in \mathbb{N}$, it holds that $\mathsf{QMA}_1^{\mathcal{G}} \subseteq \mathsf{QMA}_1^{\mathcal{G}_{2^k}}$. For any finite gateset $\mathcal{G}$ in $\mathbb{Q}(\mathrm{i})$, it holds that $\mathsf{QMA}_1^{\mathcal{G}} \subseteq \mathsf{QMA}_1^{\mathcal{G}_2}$.*

Note that $\mathsf{QMA}_1^{\mathcal{G}_2} = \mathsf{QMA}_1^{\mathcal{G}_4} \subseteq \mathsf{QMA}_1^{\mathcal{G}_8} \subseteq \mathsf{QMA}_1^{\mathcal{G}_{16}} \subseteq \cdots$. For BQP_1 we may almost claim universality since we can simulate all cyclotomic gatesets with $\mathcal{G}_2$.[3]

Theorem 1.2 (3.3)**.** *For any finite gateset $\mathcal{G}$ in $\mathbb{Q}(\zeta_{2^k})$ with $k \in \mathbb{N}$ it holds that $\mathsf{BQP}_1^{\mathcal{G}} \subseteq \mathsf{BQP}_1^{\mathcal{G}_2}$.*

We exhibit complete problems for the classes $\mathsf{QMA}_1^{\mathcal{G}_{2^k}}$. k-$\mathsf{QSAT}^{\mathbb{F}}$ denotes the quantum k-SAT problem with local Hamiltonians in $\mathbb{F}^{2^k \times 2^k}$. Notably, we also give the first 2-local QMA_1-complete Hamiltonian problem. We define the k-local Hamiltonian Singular Value problem (k-LHSV, see Problem 2.7) as the problem of deciding whether a k-local Hamiltonian on n qubits has a smallest singular value $\sigma_1(H) = 0$, or $\sigma_1(H) \geq 1/\mathrm{poly}(n)$. We have k-$\mathsf{QSAT} \subseteq k$-$\mathsf{LHSV} \subseteq 2k$-$\mathsf{LH}$. k-LHSV has a weaker promise than k-QSAT: In the YES-case only a nonempty nullspace is required, but H may still be frustrated (i.e. the local Hamiltonians do not have a common ground state). k-LHSV has a stronger promise than k-LH: In the YES-case not just low energy is required, but an eigenvalue of *exactly* 0.

Theorem 1.3 (4.2, 4.4, 5.1)**.** 4-$\mathsf{QSAT}^{\mathbb{Q}(\zeta_{2^k})}$ *is complete for* $\mathsf{QMA}_1^{\mathcal{G}_{2^k}}$ *for all* $k \in \mathbb{N}$.
3-$\mathsf{QSAT}^{\mathbb{Q}(\zeta_{2^k})}$ *is complete for* $\mathsf{QMA}_1^{\mathcal{G}_{2^k}}$ *for all* $k \geq 3$.
2-$\mathsf{LHSV}^{\mathbb{Q}(\zeta_{2^k})}$ *is* $\mathsf{QMA}_1^{\mathcal{G}_{2^k}}$*-complete for all* $k \geq 3$.

We can generalize Theorem 1.1 to $\mathsf{QMA}_1(2)$, and show the first complete Hamiltonian problem SSHSV (separable sparse Hamiltonian singular value problem, see Problem 2.11), which is the problem of deciding whether a sparse Hamiltonian H has a separable nullstate, or for all product states, we have $\|H|\psi_1\rangle|\psi_2\rangle\| \geq 1/\mathrm{poly}$. We also give the first complete problem for "high precision" $\mathsf{QMA}(2)$ (i.e. with a promise gap of less than 1/poly), which is an approximate version of SSHSV where in the YES-case the existence of a product state with negligible $\|H|\psi_1\rangle|\psi_2\rangle\|$ suffices. This solves an open problem of [GR23].

Theorem 1.4 (6.3, 6.4)**.** *For any finite gateset $\mathcal{G}$ in $\mathbb{Q}(\zeta_{2^k})$ with $k \in \mathbb{N}$, it holds that $\mathsf{QMA}_1^{\mathcal{G}}(2) \subseteq \mathsf{QMA}_1^{\mathcal{G}_{2^k}}(2)$. For any finite gateset $\mathcal{G}$ in $\mathbb{Q}(\mathrm{i})$, it holds that $\mathsf{QMA}_1^{\mathcal{G}}(2) \subseteq \mathsf{QMA}_1^{\mathcal{G}_2}(2)$.*

Theorem 1.5 (6.6, 6.7)**.** $\mathsf{SSHSV}^{\mathbb{Q}(\zeta_{2^k})}$ *is* $\mathsf{QMA}_1^{\mathcal{G}_{2^k}}(2)$*-complete for all* $k \in \mathbb{N}$.
$\mathsf{ASSHSV}_\varepsilon$ *is complete for* ε-$\mathsf{QMA}(2) \coloneqq \bigcup_{c \in 1-\varepsilon^{\omega(1)}, s \in 1-\varepsilon^{O(1)}} \mathsf{QMA}_{c,s}(2)$ *with* $\varepsilon \in n^{-O(1)}$.

Lastly, we give the first completeness results for the clique homology problem. CH is the problem of determining whether the clique complex of a given graph has a hole of a given dimension. GCH additionally promises that in the NO-case, the combinatorial Laplacian has a minimum eigenvalue of $1/\mathrm{poly}(n)$, where n is the number of vertices. The following result follows from the above theorem and plugging $\mathcal{G}_2$ into [KK23].

Theorem 1.6 (6.8, 6.9)**.** GCH *is* $\mathsf{QMA}_1^{\mathcal{G}_2}$*-complete.*
CH *is* PSPACE*-complete.*

Techniques. *Linear combinations of unitaries (LCU).* Our main technical contribution is as follows. Suppose we wish to apply some unitary U to our state, but we do not know how to do that with our gateset. Instead, we can write U as a linear combination of unitaries that we *can* efficiently implement. We follow the idea of Childs and Wiebe [CW12] in the context of Hamiltonian simulation, which allows us to apply U exactly after a successful measurement. Conveniently, the Pauli matrices $\{\mathsf{I}, \mathsf{X}, \mathsf{Y}, \mathsf{Z}\}$ form an orthonormal basis, and thus we can write any unitary as $U = \sum_x a_x P_x$, where the P_x are tensor products of Paulis. If we can prepare $|U\rangle = \sum_x a_x |x\rangle$, then we can conditionally apply P_x to

[3] This simulation even works for $k = O(\log n)$, which unfortunately does not suffice to simulate an n-qubit quantum Fourier transform.

an input state $|\psi\rangle$ to obtain $\sum_x a_x|x\rangle \otimes P_x|\psi\rangle$. Projecting the first register onto the all $|+\rangle$ state then gives $\sum_x a_x P_x|\psi\rangle = U|\psi\rangle$ in the second register. Although the success probability is only 2^{-2n} for an n-qubit operator, we can recover from the failure case, in which U conjugated with some Pauli is applied. Note that if U is in $\mathbb{Q}(\zeta_{2^k})$ ($k \geq 2$), then $|U\rangle$ is also in $\mathbb{Q}(\zeta_{2^k})$. We show how to efficiently prepare such states.

Simulating cyclotomic fields. In order to implement gates $\mathcal{G}_{2^k}$ with $\mathcal{G}_2$, we extend McKague's technique of simulating complex gates with real gates [McK10; McK13] to cyclotomic gates. We can write any $a \in \mathbb{Q}(\zeta_{2^k})$ as $a = \sum_{i=0}^{2^{k-1}-1} a_i \zeta_{2^k}^i$ with all $a_i \in \mathbb{Q}$. Then we represent a as a vector $|v(a)\rangle = \sum_i a_i|i\rangle$, and multiplication by b in $\mathbb{Q}(\zeta_{2^k})$ becomes matrix multiplication by some M_b in $\mathbb{Q}$ so that $M_b|v(a)\rangle = |v(ab)\rangle$. Formally, there exists a field isomorphism from $\mathbb{Q}(\zeta_{2^k})$ to a subfield of invertible $\mathbb{Q}^{2^{k-1}\times 2^{k-1}}$ matrices. Applying this field isomorphism elementwise to a unitary results in an orthogonal matrix. Formally, we have a group homomorphism $\Psi : \mathrm{U}(N, \mathbb{Q}(\zeta_{2^k})) \to \mathrm{O}(2^{k-1}N, \mathbb{Q})$.[4]

Nullspace testing. We observe that the LCU technique also applies to non-unitary matrices. We can directly apply the Hamiltonian to a quantum state (i.e., not $e^{\mathrm{i}H}$ as in Hamiltonian simulation). However, the success probability is proportional to $\|H|\psi\rangle\|$. Thus, if $|\psi\rangle \in \mathcal{N}(H)$, then multiplying $|\psi\rangle$ with H fails with probability 1. Hence, we can check in QMA_1 whether a frustrated Hamiltonian has a nonempty nullspace. We further extend this technique to sparse Hamiltonians by applying tools from Hamiltonian simulation [BCC+14; KL21] (modified for cyclotomic fields), to write a sparse Hamiltonian as a linear combination of 1-sparse unitaries.

Hamiltonians. We construct our Hamiltonians via the Nullspace Connection Lemma of [RGN24], which effectively gives a blueprint for circuit-to-Hamiltonian constructions and only requires us to prove properties of local gadgets. We do this computationally [Rud24]. Nevertheless, our 2-local QMA_1-complete Hamiltonian requires some new tricks, since the 2-local QMA-complete circuit-to-Hamiltonian construction of [KKR05] does not have the history state as eigenstate. We follow the idea of splitting the computation path inside the history state, conditioned on a computational register [ER08; GN13; RGN24]. The new idea is to split the computation path conditioned on the eigenstates of a single-qubit gate (not just on $|0\rangle, |1\rangle$). Then we can apply a single-qubit gate as a "zero-qubit" gate (i.e. a global phase), which we can implement with a 2-local transition by using a "one-hot encoding" for the clock register.

Open questions. Despite having made significant progress, the big question whether QMA_1 equals QMA remains wide open. Does there exist a classical oracle separation? We also have "smaller" open questions. Can Theorem 1.2 be extended to QMA, i.e., does a single gateset suffice to simulate all 2^k-th cyclotomic gatesets for QMA? The issue here is that our encoding allows a malicious prover to send an effective "zero-state", as for $k > 2$ the powers of ζ_{2^k} are not linearly independent in the complex plane. More generally, can we extend these results to other roots of unity, i.e., not just powers of two?

Lastly, a few Hamiltonian completeness results are still open for $k < 3$ (3-QSAT, 2-LHSV), where our constructions need the eighths root of unity to implement to implement CNOT and Hadamard gates, respectively.

2 Preliminaries

In this section, we introduce notation and give formal definitions of the complexity classes and problems used in this paper.

2.1 BQP and QMA with perfect completeness

For a quantum verifier circuit Q with n_1 ancilla qubits and n_2 proof qubits, we define the acceptance probability on input $|\psi\rangle \in \mathbb{C}^{2^{n_2}}$ as

$$p_{\mathrm{acc}}(Q, \psi) = \mathrm{Tr}\left((|1\rangle\langle 1|_1 \otimes I_{2,\ldots,n_1+n_2})\, Q\, (|0\rangle\langle 0|^{\otimes n_1} \otimes |\psi\rangle\langle\psi|) \right). \tag{1}$$

[4] This only works for the 2^k-th roots of unity, since they have the unique property $M_b^T = M_{\bar{b}}$, which preserves orthogonality when applied to a unitary.

For a BQP circuit, we just write $p_{\text{acc}}(Q)$ for the acceptance probability. We denote the ancilla register by $\mathcal{A}$ and the proof register by $\mathcal{B}$.

Definition 2.1 (QMA_1)**.** A promise problem $A = (A_{\text{yes}}, A_{\text{no}})$ is in $\mathsf{QMA}_1^{\mathcal{G}}$ if there exists a poly-time uniform family of quantum circuits $\{Q_x\}$[5] and polynomials n_1, n_2, where each Q_x only uses gates from the gateset $\mathcal{G}$ and acts on $n_1(|x|)$ ancilla qubits and $n_2(|x|)$ proof qubits, such that:

- (Completeness) If $x \in A_{\text{yes}}$, then there exists a proof $|\psi\rangle \in \mathbb{C}^{2^{n_2}}$ with $p_{\text{acc}}(Q_x, \psi) = 1$.
- (Soundness) If $x \in A_{\text{no}}$, then for all proofs $|\psi\rangle \in \mathbb{C}^{2^{n_2}}$, $p_{\text{acc}}(Q_x, \psi) \leq 1 - 1/\text{poly}(|x|)$.

We additionally define $\mathsf{QMA}_1^{\mathcal{G}}(2)$ in the same way, but the proof is a product state $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ with $|\psi_1\rangle, |\psi_2\rangle \in \mathbb{C}^{2^{n_2}}$. We also write $\mathsf{QMA}_{1,c}$ for soundness c, i.e., the verifier accepts with probability $\leq c$ in the NO-case.

Definition 2.2 (BQP_1)**.** A promise problem $A = (A_{\text{yes}}, A_{\text{no}})$ is in $\mathsf{BQP}_1^{\mathcal{G}}$ if there exists a poly-time uniform family of quantum circuits $\{Q_x\}$ and polynomial n_1, where each Q_x only uses gates from the gateset $\mathcal{G}$ and acts on $n_1(|x|)$ ancilla qubits, such that:

- (Completeness) If $x \in A_{\text{yes}}$, then $p_{\text{acc}}(Q_x) = 1$.
- (Soundness) If $x \in A_{\text{no}}$, then $p_{\text{acc}}(Q_x) \leq 1 - 1/\text{poly}(|x|)$.

Standard error reduction results also hold as long as we have at least the gates

$$\mathcal{G}_2 \coloneqq \{\mathsf{X}, \mathsf{CX}, \mathsf{CCX}, \mathsf{H} \otimes \mathsf{H}\} \qquad \text{(Pauli } X\text{, CNOT, Toffoli, Hadamard)}, \tag{2}$$

since they allow us to implement any qubit unitary with entries in $\mathbb{Z}[1/2]$ [AGR20; AGK+24]. This also extends to $\mathsf{QMA}_1(2)$ since the product test has perfect completeness [HM13].

Lemma 2.3. *Let $\mathcal{G} \supseteq \mathcal{G}_2$. Then $\mathsf{BQP}_1^{\mathcal{G}}, \mathsf{QMA}_1^{\mathcal{G}}, \mathsf{QMA}_1^{\mathcal{G}}(2)$ have soundness $1/\exp(n)$. Also, $\mathsf{QMA}_1^{\mathcal{G}}(2) = \mathsf{QMA}_1^{\mathcal{G}}(\text{poly})$.*

2.2 Hamiltonian problems

The k-local Hamiltonian problem defined below is considered the canonical QMA-complete problem.

Problem 2.4 (k-local Hamiltonian problem (k-LH_ε))**.** Given a classical description of a k-local Hamiltonian $H = \sum_{S \subseteq [n]}^m H_S \otimes I_{[n] \setminus S}$ on n qubits with $\|H_S\| \leq 1$, and α, β with $\beta - \alpha \geq \varepsilon(n)$, decide:

- (YES) $\lambda_{\min}(H) \leq \alpha$.
- (NO) $\lambda_{\min}(H) \geq \beta$.

Definition 2.5. Let HP_ε one of the Hamiltonian problems defined in this section. We omit ε if $\varepsilon \in n^{-O(1)}$, i.e., $\mathsf{HP} \coloneqq \bigcup_{\varepsilon \in n^{-O(1)}} \mathsf{HP}_\varepsilon$.

The quantum k-SAT problem is considered the canonical QMA_1-complete problem. It differs from the local Hamiltonian problem in that the local terms are required to be projectors and in the YES-case they must have a common (zero energy) ground state (i.e. H is frustration-free). The QMA_1-completeness of k-QSAT is quite subtle, however, due to the requirement of perfect completeness. Bravyi [Bra06] defined k-QSAT in the same way as below, i.e., the Hamiltonian is restricted to a subfield $\mathbb{F} \subseteq \mathbb{C}$ with exact representation, and shows completeness for $\mathsf{QMA}_1^{\mathcal{G}}$, where $\mathcal{G}$ contains all three-qubit gates with entries in $\mathbb{F}$. Gosset and Nagaj [GN13] instead consider the gateset $\{\mathsf{H}, \mathsf{CX}, \mathsf{T}\}$, and show completeness for k-QSAT, where each local projector Π is in $\mathbb{Z}[\frac{1}{\sqrt{2}}, \mathrm{i}]$, or there exists a unitary with only these elements, such that $U\Pi U^\dagger = (\sqrt{1/3}|000\rangle - \sqrt{2/3}|001\rangle)(\sqrt{1/3}\langle 000| - \sqrt{2/3}\langle 001|)$.

Problem 2.6 (Quantum k-SAT (k-$\mathsf{QSAT}_\varepsilon^{\mathbb{F}}$))**.** Let $\mathbb{F} \subseteq \mathbb{C}$ be a field. Given a classical description of a k-local Hamiltonian $H = \sum_{S \subseteq [n]}^m H_S \otimes I_{[n] \setminus S}$ on n qubits with $H_S \succeq 0$ and $\|H_S\| \leq 1$ [6], decide:

[5] Here, we allow the "circuit constructor" access to the instance x, as in [Bra06]. Sometimes QMA is also defined with a universal family of circuits $\{Q_n\}$, i.e., the "circuit constructor" only has access to the size of the instance. These definitions are equivalent for the gatesets we consider, i.e., $\mathcal{G}_{2^k}$ of [AGK+24].

[6] Commonly the H_S are assumed to be projectors, but here we only require H_S to be positive semidefinite so that, e.g., projectors onto $|+\rangle$ can be represented in $\mathbb{Q}$. We will see in Theorem 4.2, that this does not add power for $k \geq 4$. For the $k = 3$ case (see Theorem 4.4), we leave this issue open for future work.

- (YES) $\lambda_{\min}(H) = 0$.
- (NO) $\lambda_{\min}(H) \geq \varepsilon(n)$.

In this work, we "bridge the gap" between the definitions of [Bra06] and [GN13] in that we show completeness for k-QSAT in a *field* for $\mathsf{QMA}_1^{\mathcal{G}}$ with a *finite* gateset $\mathcal{G}$. Our definition of k-QSAT is more general than that of [GN13] and we have 3-$\mathsf{QSAT}^{[\mathrm{GN13}]} \subseteq$ 3-$\mathsf{QSAT}^{\mathbb{Q}(\zeta_8)}$ (see Theorem 4.4). Specifically, we give a gateset for every 2^k-th cyclotomic field $\mathbb{Q}(\zeta_{2^k})$, where $\zeta_{2^k} = e^{2\pi \mathrm{i}/2^k}$, i.e., the field extension of $\mathbb{Q}$ generated by a primitive 2^k-th root of unity. Note that the T-gate is in $\mathbb{Q}(\zeta_8)$.

We also define a new variant of the local Hamiltonian problem with a stronger promise in the YES-case, where we only have to distinguish between the cases $\sigma_1(H) = 0$ and $\sigma_1(H) \geq 1/\mathrm{poly}(n)$, for σ_1 the smallest singular value.

Problem 2.7 (k-local Hamiltonian Singular Value problem (k-$\mathsf{LHSV}_\varepsilon^{\mathbb{F}}$))**.** Given a classical description of a k-local Hamiltonian $H = \sum_{S\subseteq[n]}^m H_S \otimes I_{[n]\setminus S}$ on n qubits such that all entries of the H_S are in $\mathbb{F}$, decide:

- (YES) $\sigma_1(H) = 0$.
- (NO) $\sigma_1(H) \geq \varepsilon(n)$.

Note that k-LHSV as defined above is equivalent to the problem of deciding whether H has some given eigenvalue $\alpha \in \mathbb{F}$, or if for all eigenvalues λ of H, $|\alpha - \lambda| \geq \varepsilon(n)$. The reduction is trivial by transforming H into $H' = H - \alpha I$. In that sense, we can view k-LHSV as an "exact" variant of the local Hamiltonian problem.

Next, we also define sparse variants of the above problems. We say an operator A on n qubits is *sparse* if there exists a poly(n)-size circuit that given a row/column of A, computes the indices and values of all non-zero entries of that row/column.

Problem 2.8 (Sparse Hamiltonian problem (SH_ε))**.** Given a classical description of a sparse Hamiltonian H on n qubits and α, β with $\beta - \alpha \geq \varepsilon(n)$, decide:

- (YES) $\lambda_{\min}(H) \leq \alpha$.
- (NO) $\lambda_{\min}(H) \geq \beta$.

Problem 2.9 (Sparse Hamiltonian Singular Value problem ($\mathsf{SHSV}_\varepsilon^{\mathbb{F}}$))**.** Given a classical description of a sparse Hamiltonian H on n qubits with all entries in $\mathbb{F}$ and $\|H\| \leq 1$, decide:

- (YES) $\sigma_1(H) = 0$.
- (NO) $\sigma_1(H) \geq \varepsilon(n)$.

Problem 2.10 (Separable sparse Hamiltonian problem (SSH_ε) [CS12])**.** Given a classical description of a sparse Hamiltonian H on $2n$ qubits with $\|H\| \leq 1$ and α, β with $\beta - \alpha \geq \varepsilon(n)$, decide:

- (YES) There exists $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ with $|\psi_1\rangle, |\psi_2\rangle \in \mathbb{C}^{2^n}$ such that $\langle\psi|H|\psi\rangle \leq \alpha$.
- (NO) For all such $|\psi\rangle$, $\langle\psi|H|\psi\rangle \geq \beta$.

Note that $\mathsf{SH} \in \mathsf{QMA}$ [CS12] (hardness is trivial) via phase estimation [NC10] and simulatability of sparse Hamiltonians [AT03]. The following separable sparse Hamiltonian problem is the first non-trivial $\mathsf{QMA}_1(2)$-complete problem.

Problem 2.11 (Separable sparse Hamiltonian singular value problem ($\mathsf{SSHSV}_\varepsilon^{\mathbb{F}}$))**.** Given a classical description of a sparse Hamiltonian H on n qubits with all entries in $\mathbb{F}$ and $\|H\| \leq 1$, decide:

- (YES) There exists $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ with $|\psi_1\rangle, |\psi_2\rangle \in \mathbb{C}^{2^n}$ such that $H|\psi\rangle = 0$.
- (NO) For all such $|\psi\rangle$, $\|H|\psi\rangle\| \geq \varepsilon(n)$.

We also define an approximate version of this problem, $\mathsf{ASSHSV}_\varepsilon^{\mathbb{F}}$, where the YES-case only requires $\|H|\psi\rangle\| \leq \varepsilon^{\omega(1)}$.

Definition 2.12 ($\mathbb{F} = \mathbb{Q}(\zeta_{2^k})$)**.** For the above problems with $\mathbb{F} = \mathbb{Q}(\zeta_{2^k})$ with $k \in \mathbb{N}$, we require the numerators and denominators of rational coefficients of the Hamiltonian entries to be bounded by poly(ε^{-1}, n) in absolute value.[7] For the sparse problems, we also require that the common denominator is bounded by poly(ε^{-1}, n), i.e., $H = H'/h$ with $H' \in \mathbb{Z}[\zeta_{2^k}]$ and $h \in \mathbb{N}, h \leq \mathrm{poly}(n)$.

[7] For $k \in \{1, 2\}$ we still get containment if we allow poly(n) bit complexity of entries. But for $k \geq 3$, we are limited by our integer state preparation routine in Lemma 3.9. We allow entries to grow proportionally with ε^{-1}, since for $\varepsilon \in n^{-\omega(n)}$, state preparation is no longer the bottleneck.

2.3 Clique homology

We give a brief summary of the clique homology problem to the extent that we require for this paper. We refer the reader to [KK23] for a more complete treatment.

Definition 2.13 (Clique complex [KK23])**.**
- A *simplicial complex* $\mathcal{K}$ is a collection of subsets $\mathcal{K} = \mathcal{K}^0 \cup \mathcal{K}^1 \cup \cdots$, such that $\forall \sigma \in \mathcal{K}^k \colon |\sigma| = k+1$ and $\forall \sigma \in \mathcal{K}\ \forall \tau \subset \sigma \colon \tau \in \mathcal{K}$.
- Let $\mathcal{C}^k(\mathcal{K})$ be the complex vector space formally spanned by $\mathcal{K}^k$, picking a conventional ordering for each simplex $\sigma = [v_0, \ldots, v_k]$ and identifying $|[\pi(v_0), \ldots, \pi(v_k)]\rangle = (-1)^{\mathrm{sgn}(\pi)}|\sigma\rangle$ for all permutations $\pi \in S_{k+1}$. $\mathrm{sgn}(\pi)$ denotes the sign of the permutation and is also known as the *orientation* of the simplex.
- For a k-simplex $\sigma \in \mathcal{K}^k$, let $\mathrm{up}(\sigma) \subseteq \mathcal{K}^0$ be the set of vertices v, such that $\sigma \cup \{v\} \in \mathcal{K}^{k+1}$.
- The *coboundary map* is given by $d^k : \mathcal{C}^k(\mathcal{K}) \to \mathcal{C}^{k+1}(\mathcal{K})$, $d^k|\sigma\rangle := \sum_{v \in \mathrm{up}(\sigma)} |[v] + \sigma\rangle$, where $[v] + \sigma \equiv [v, v_0, \ldots, v_k]$ for $\sigma = [v_0, \ldots, v_k]$.[8]
- A *chain complex* is a chain of complex vector spaces $\mathcal{C}^k$ with linear maps $d^k : \mathcal{C}^k \to \mathcal{C}^{k+1}$ satisfying $d^k \circ d^{k-1} = 0$ for all k.

$$\begin{tikzcd} \mathcal{C}^{-1} \arrow[r, "d^{-1}"] & \mathcal{C}^0 \arrow[r, "d^0"] & \mathcal{C}^1 \arrow[r, "d^1"] & \mathcal{C}^2 \arrow[r, "d^2"] & \cdots \end{tikzcd}$$

- The *cohomology groups* are defined as $H^k = \dfrac{\mathrm{Ker}\, d^k}{\mathrm{Im}\, d^{k-1}}$, noting $\mathrm{Im}\, d^{k-1} \subseteq \mathrm{Ker}\, d^k$.
- Defining an inner product on $\mathcal{C}^k$ yields a Hilbert space, and we define the *boundary map* as $\partial^k = (d^{k-1})^\dagger$ and the *Laplacian* as $\Delta^k = d^{k-1}\partial^k + \partial^{k+1}d^k$. For now we just declare the simplices to be an orthonormal basis, so that $\langle\sigma|\tau\rangle = \begin{cases} 1, & \text{if } \sigma = \tau \\ 0 & \text{otherwise} \end{cases}$.
- To derive a chain complex from a simplicial complex, set $\mathcal{C}^{-1}(\mathcal{K}) = \mathrm{Span}\{|\emptyset\rangle\} \cong \mathbb{C}$ and define $d^{-1}|\emptyset\rangle = \sum_{v \in \mathcal{K}^k} |v\rangle$.
- The *clique complex* of a graph G, denoted $\mathrm{Cl}(G)$ is the simplicial complex consisting of the cliques of G.

Proposition 2.14 ([KK23])**.** *It holds that* $\langle\psi|\Delta^k|\psi\rangle = \|\partial^k|\psi\rangle\|^2 + \|d^k|\psi\rangle\|$. $\mathrm{Ker}\,\Delta^k$ *is canonically isomorphic to* H^k*, which means that every homology class has a unique* harmonic *representative, i.e., in the kernel of the Laplacian.*

Problem 2.15 (Clique homology problem (CH) [KK23])**.** Given a graph G and integer k, decide whether the k-th homology group of $\mathrm{Cl}(G)$ is non-empty:
- (YES) The k-th homology group of $\mathrm{Cl}(G)$ is non-trivial: $H^k(G) \neq 0$ (i.e. $\lambda_{\min}(\Delta^k) = 0$).
- (NO) The k-th homology group of $\mathrm{Cl}(G)$ is trivial: $H^k(G) = 0$ (i.e. $\lambda_{\min}(\Delta^k) \neq 0$).

Definition 2.16 (Weighted chain complex [KK23])**.** A *weighted simplicial complex* is defined by a simplicial complex $\mathcal{K}$ and a weighting function $w : \mathcal{K} \to \mathbb{R}_{\geq 0}$, such that $w(\sigma) = \prod_{v \in \sigma} w(v)$ for all $\sigma \in \mathcal{K}$. The inner product on the weighted complex is given by

$$\langle\sigma|\tau\rangle = \begin{cases} w(\sigma)^2, & \text{if } \sigma = \tau \\ 0 & \text{otherwise} \end{cases}. \tag{3}$$

Then an orthonormal basis for $\mathcal{C}^k(\mathcal{K})$ is $\{|\sigma'\rangle \mid \sigma \in \mathcal{K}^k\}$ with $|\sigma'\rangle = \frac{1}{w(\sigma)}|\sigma\rangle$ the unit vector of $|\sigma\rangle$.

The coboundary and boundary operators act as follows on our new orthonormal basis:

[8] Our notation in the definition of d^k differs from [KK23], which uses "set notation" $|\sigma \cup [v]\rangle$. When the orientation of simplices is important, we use a "list notation", i.e., $[v] + \sigma$ to denote prepending v to σ. This way $d^k \circ d^{k-1} = 0$ is easy to see.

Lemma 2.17 (Proof in Appendix A)**.** *Let $\sigma = [v_0, \ldots, v_k] \in \mathcal{K}$ in a weighted simplicial complex. Then*

$$d^k|\sigma'\rangle = \sum_{v \in \mathrm{up}(\sigma)} w(v)|([v] + \sigma)'\rangle, \tag{4a}$$

$$\partial^k|\sigma'\rangle = \sum_{j=0}^{k} (-1)^j \cdot w(v_j)|\sigma'_{-j}\rangle, \tag{4b}$$

where $\sigma_{-j} = [v_0, \ldots, v_{j-1}, v_{j+1}, \ldots, v_k]$.

Next, we describe the action of the Laplacian Δ^k on the $|\sigma'\rangle$.

Lemma 2.18 ([KK23, Fact 7.12], [Gol02, Theorem 3.3.4]; proof in Appendix A[9])**.** *Let $\sigma, \tau \in \mathcal{K}^k$. We say σ and τ have a* similar/dissimilar common lower simplex *if there exist $v_\sigma \in \sigma, v_\tau \in \tau$, such that removing v_σ from σ and v_τ from τ gives the same $(k-1)$-simplex η, and $|\eta\rangle$ has the same/different sign in $\partial^k|\sigma\rangle$ and $\partial^k|\tau\rangle$. We say σ and τ are* upper adjacent *if their union forms a $(k+1)$-simplex, i.e., they are both faces of the same $(k+1)$-simplex.*

$$\langle\sigma'|\Delta^k|\tau'\rangle = \begin{cases} \sum_{u \in \mathrm{up}(\sigma)} w(u)^2 + \sum_{v \in \sigma} w(v)^2, & \text{if } \sigma = \tau. \\ w(v_\sigma)w(v_\tau), & \text{if } \sigma \text{ and } \tau \text{ have a similar common lower simplex and are not upper adjacent} \\ -w(v_\sigma)w(v_\tau), & \text{if } \sigma \text{ and } \tau \text{ have a dissimilar common lower simplex and are not upper adjacent} \\ 0, & \text{otherwise} \end{cases}$$

It is easy to see that the Laplacian is sparse and positive semidefinite.

Problem 2.19 (Gapped clique homology (GCH_ε) [KK23])**.** Given a vertex-weighted graph G on n vertices and integer k, decide whether the k-th homology group of $\mathrm{Cl}(G)$ is non-empty with the additional promise that in the NO-case $\lambda_{\min}(\Delta^k) \geq \varepsilon(n)$ for Δ^k the Laplacian of $\mathrm{Cl}(G)$:

- (YES) The k-th homology group of $\mathrm{Cl}(G)$ is non-trivial: $H^k(G) \neq 0$.
- (NO) The k-th homology group of $\mathrm{Cl}(G)$ is trivial: $H^k(G) = 0$.

Define GCH as in Definition 2.5.

3 (Towards) universal gatesets

Amy et al. [AGK+24] prove that the gatesets $\mathcal{G}_{2^k}$ can exactly synthesize all unitaries with entries in $\mathbb{Z}[1/2, \zeta_{2^k}]$.

$$\mathcal{G}_2 = \{\mathsf{X}, \mathsf{CX}, \mathsf{CCX}, \mathsf{H} \otimes \mathsf{H}\}, \tag{5}$$

$$\mathcal{G}_4 = \{\mathsf{X}, \mathsf{CX}, \mathsf{CCX}, \zeta_8\mathsf{H}\}, \tag{6}$$

$$\mathcal{G}_{2^k} = \{\mathsf{H}, \mathsf{CX}, \mathsf{T}_{2^k}\}, \quad \mathsf{T}_{2^k} = \begin{pmatrix} 1 & 0 \\ 0 & \zeta_{2^k} \end{pmatrix}, \tag{7}$$

Theorem 3.1 ([AGK+24])**.** *Let $k, m \in \mathbb{N}$. A $2^m \times 2^m$ unitary U can be exactly represented by an m-qubit circuit over $\mathcal{G}_{2^k}$ if and only if $U \in \mathrm{U}(2^m, \mathbb{D}[\zeta_{2^k}])$, where $\mathbb{D}[\zeta_{2^k}] \equiv \mathbb{Z}[1/2, \zeta_{2^k}]$ and $\mathrm{U}(N, R)$ denotes the set of unitary $N \times N$ matrices in R. For $k \leq 2$ a single ancilla suffices and $k-2$ ancillas for $k > 2$.*

We prove the following results in this section.

Theorem 3.2. *For any finite gateset $\mathcal{G}$ in $\mathbb{Q}(\mathrm{i})$, it holds that $\mathsf{QMA}_1^{\mathcal{G}} \subseteq \mathsf{QMA}_1^{\mathcal{G}_2}$.*

For BQP_1 we may almost claim universality since we can simulate all cyclotomic gatesets with $\mathcal{G}_2$.

Theorem 3.3. *For any finite gateset $\mathcal{G}$ in $\mathbb{Q}(\zeta_{2^k})$ with $k \in \mathbb{N}$, it holds that $\mathsf{BQP}_1^{\mathcal{G}} \subseteq \mathsf{BQP}_1^{\mathcal{G}_2}$.*

[9] We give a proof in the appendix since [KK23, Fact 7.12] is given without proof and has a very minor bug in that there is a superfluous "+1" in the first case.

3.1 Integer state preparation

Proposition 3.4 (Proof in Appendix A)**.** *Let $\mathcal{G}$ be a finite gateset in $\mathbb{Q}(\zeta_n)$. It is impossible to synthesize all rational single-qubit unitaries with $\mathcal{G}$, even with $|0\rangle$-initialized ancillas.*

However, we can use postselection to circumvent this issue. The first technical tool we need is preparing integer states, i.e., states that are proportional to (unnormalized) states with only integer amplitudes.

Lemma 3.5. *Let $|\psi\rangle \propto \sum_{i=0}^{d-1} a_i|i\rangle$ with $a_i \in \mathbb{Z}$. We can prepare $|\psi\rangle$ with probability $\geq 1/4d$ with gateset $\mathcal{G}_2$ in time $\mathrm{poly}(d, \log A)$ and space $O(\log d + \log A)$, where $A := \sum_i |a_i|$.*

Proof. For simplicity, it suffices to consider states with all $a_i > 0$, as it is trivial to transform such a state into the target state via CZ gates and permutations. Let $e_i := \lceil \log a_i \rceil$, and $n := \lceil \log A \rceil$. Prepare $|\psi_0\rangle = H^{\otimes n}|0\rangle \propto \sum_{j=0}^{2^n-1}|j\rangle_{\mathcal{A}}$. Perform measurement $M = \sum_{j=0}^{A-1}|j\rangle\langle j|$, which accepts with probability $\geq 1/2$. The post-measurement state is $|\psi_1\rangle \propto \sum_{j=0}^{A-1}|j\rangle_{\mathcal{A}}$. Let $k_i = \sum_{j=0}^{i-1} a_j$. Using a simple classical circuit, we tag $|j\rangle$ with i if $j \in [k_i, k_{i+1})$, obtaining $|\psi_2\rangle \propto \sum_{i=0}^{d-1}|i\rangle_{\mathcal{A}} \sum_{j=0}^{a_i-1}|j + k_i\rangle_{\mathcal{B}}$, which is further transformed to $|\psi_3\rangle \propto \sum_{i=0}^{d-1}|i\rangle_{\mathcal{A}} \sum_{j=0}^{a_i-1}|j\rangle_{\mathcal{B}}$ using a classical circuit ($|i\rangle_{\mathcal{A}}|j\rangle_{\mathcal{B}} \mapsto |i\rangle_{\mathcal{A}}|j - k_i\rangle_{\mathcal{B}}$). Let $a^* := \max_i a_i$ and $m = \lceil \log a^* \rceil$, and measure $\mathcal{B}$ in the Hadamard basis, where $M = |+\rangle\langle+|_{\mathcal{B}}^{\otimes m}$ is the accepting projector. For $|\phi\rangle := \frac{1}{\sqrt{a^*}} \sum_{i=0}^{a^*-1}|i\rangle$, we have

$$\langle+|^{\otimes m}|\phi\rangle = \frac{1}{\sqrt{2^m \cdot a^*}} \left(\sum_{i=0}^{2^m-1}\langle i|\right)\left(\sum_{i=0}^{a^*-1}|i\rangle\right) = \frac{a^*}{\sqrt{2^m \cdot a^*}} = \sqrt{\frac{a^*}{2^m}} > \sqrt{\frac{1}{2}}. \tag{8}$$

Hence, the measurement accepts with probability at least $1/2d$. The post-measurement state is $|\psi_4\rangle \propto M_{\mathcal{B}}|\psi_3\rangle \propto \sum_{i=0}^{d-1} a_i|i\rangle_{\mathcal{A}}|+\rangle_{\mathcal{B}}^{\otimes m} \propto |\psi\rangle$.

Note, this algorithm only requires classical circuits on $O(n + \log d)$ qubits as well as (controlled) Hadamard gates, which can be implemented with Toffoli, Hadamard, CNOT, X gates using standard techniques [NC10]. We also need to take care to always use two Hadamard gates at the same time, since $\mathcal{G}_2$ only contains $\mathsf{H} \otimes \mathsf{H}$. So if n is odd, we can apply an additional H to a later unused ancilla during the preparation of $|\psi_0\rangle$. If m is odd, we can prepare $|+\rangle|+\rangle$ by applying $\mathsf{H} \otimes \mathsf{H}$ to two fresh ancillas before the measurement M, and then also include one of these ancillas in the measurement. □

Remark 3.6. By repeating the algorithm described in Lemma 3.5 $\mathrm{poly}(d)$ times, we can boost the success probability to $1 - 1/\exp(d)$.

Lemma 3.7. *Let $|\psi\rangle \propto \sum_{i=0}^{d-1}(a_i + b_i\mathrm{i})|i\rangle$ with $a_i, b_i \in \mathbb{Z}$ such that $a_i + b_i\mathrm{i} \neq 0$ for all i. We can prepare $|\psi\rangle$ with probability $\geq 1/16d$ using gateset $\mathcal{G}_4$ in time $\mathrm{poly}(d, \log A)$ and space $O(\log d + \log A)$, where $A := \sum_i |a_i| + |b_i|$.*

Proof. First, prepare state $|\psi_0\rangle \propto \sum_{i=0}^{d-1}(a_i|i\rangle + b_i|i + d\rangle)$ using Lemma 3.5, which succeeds with probability $\geq 1/8d$. Use a classical circuit to transform to $|\psi_1\rangle \propto \sum_{i=0}^{d-1}(a_i|i\rangle_{\mathcal{A}}|0\rangle_{\mathcal{B}} + b_i\mathrm{i}|i\rangle_{\mathcal{A}}|1\rangle_{\mathcal{B}})$. Then, measure $\mathcal{B}$ in Hadamard basis and accept on outcome $|+\rangle$. The post-measurement state is then given by $|\psi_2\rangle \propto \sum_{i=0}^{d-1}(a_i + b_i\mathrm{i})|i\rangle_{\mathcal{A}} \otimes |+\rangle_{\mathcal{B}} \propto |\psi\rangle$. The measurement succeeds with probability $1/2$ since on outcome $|-\rangle$, we just get the complex complement of $|\psi\rangle$. □

Lemma 3.7 also trivially extends to the other cyclotomic fields of degree 2, which are $\mathbb{Q}(\zeta_3)$ and $\mathbb{Q}(\zeta_6)$ (see [Rom06] for the necessary background on field extensions and cyclotomic fields). However, cyclotomic fields of higher degree are more difficult since there it is possible to add integer multiples of powers ζ_n to get arbitrarily close to 0. We can still lower bound the success probability by a polynomial in the sum of absolute values of the integer coefficients:

Lemma 3.8 ([Mye86])**.** *Fix a constant $n \in \mathbb{N}$. Let $a_0, \ldots, a_{n-1} \in \mathbb{Z}$, such that there exists an i with $a_i \neq 0$. Then*

$$\left|\sum_{i=0}^{n-1} a_i \zeta_n^i\right| \geq \left(\sum_{i=0}^{n-1}|a_i|\right)^{-n}. \tag{9}$$

Lemma 3.9. *Let $n = 2^k$ and $|\psi\rangle \propto \sum_{i=0}^{n/2-1} a_i|i\rangle$ with $a_i \in \mathbb{Z}[\zeta_n^k]$ with $a_i = \sum_{j=0}^{n/2-1} b_{ij}\zeta_n^j \neq 0$ [10] for all i. We can prepare $|\psi\rangle$ with probability $\geq 1/(d \cdot \mathrm{poly}(A))$ using gateset $\mathcal{G}_{2^k}$ in time $\mathrm{poly}(d, \log A)$ and space $O(\log d + \log A)$, where $A \coloneqq \sum_{i=0}^{d-1} \sum_{j=0}^{n/2-1} |b_{ij}|$.*

Proof. The procedure is analogous to Lemma 3.7, but we can only lower bound the success probability of the final measurement by $1/\mathrm{poly}(A)$ via Lemma 3.8. □

3.2 Implementing integer gates

Childs and Wiebe [CW12] show how to implement any non-unitary operation via decomposition into a linear combination of unitaries. We say a unitary U is integer if there exists an $s^2 \in \mathbb{Z}$ such that $sU \in \mathbb{Z}[\mathrm{i}]^{2^n \times 2^n}$. Here, we use a similar approach to implement any integer unitary with a finite gateset. It is somewhat similar to the magic state construction by Bravyi and Kitaev [BK05] to implement Z-rotations exactly.

Lemma 3.10. *Let U be an n-qubit unitary with $sU \in \mathbb{Z}[\mathrm{i}]$ for $s^2 \in \mathbb{N}$. U can be implemented with success probability $2^{-2n} - 2^{-2^{\mathrm{poly}(n)}}$ in time and space $\mathrm{poly}(2^n, \log s)$ using the gateset $\mathcal{G}_4$.*

Proof. Applying U probabilistically. We begin by describing a procedure to apply U with a success probability of 2^{-2n}, provided that prior integer state preparation by Lemma 3.7 succeeds. Decompose $U = \sum_{x\in\{0,1\}^{2n}} a_x P_x$ in the Pauli basis with $P_x = \bigotimes_{j=1}^{n} \sigma_{x_{2j-1}x_{2j}}$, where $\sigma_{00} = \mathsf{I}, \sigma_{01} = \mathsf{X}, \sigma_{10} = \mathsf{Y}, \sigma_{11} = \mathsf{Z}$. We have $\sum_{x\in\{0,1\}^{2n}} |a_x|^2 = 1$, as

$$2^n = \|U\|_{\mathrm{F}}^2 = \operatorname{Tr} UU^\dagger = \sum_{x,y} a_x a_y^\dagger \operatorname{Tr} P_x P_y = 2^n \sum_x |a_x|^2. \tag{10}$$

Since sU has a unique representation in the Pauli basis as a vector in $\mathbb{Q}(\mathrm{i})^{2^{2n}}$, we have for all x, $sa_x \in \mathbb{Q}(\mathrm{i})$.

To implement U, first prepare $|U\rangle_{\mathcal{A}} = \sum_{x\in\{0,1\}^{2n}} a_x|x\rangle$ using Lemma 3.7. Then, conditioned on $|x\rangle_{\mathcal{A}}$, apply $(P_x)_{\mathcal{B}}$, and measure $\mathcal{A}$ in the Hadamard basis. On input $|\phi\rangle_{\mathcal{B}}$, we thus get

$$|U\rangle_{\mathcal{A}}|\phi\rangle_{\mathcal{B}} = \sum_{x\in\{0,1\}^{2n}} a_x|x\rangle_{\mathcal{A}}|\phi\rangle_{\mathcal{B}} \mapsto \sum_{x\in\{0,1\}^{2n}} a_x|x\rangle_{\mathcal{A}} \otimes P_x|\phi\rangle_{\mathcal{B}} \eqqcolon |\psi'\rangle. \tag{11}$$

If we get outcome $y \in \{0,1\}^{2n}$ for the Hadamard measurement, we project register $\mathcal{A}$ onto

$$|y_H\rangle \coloneqq H^{\otimes 2n}|y\rangle = 2^{-n} \sum_{x\in\{0,1\}^{2n}} (-1)^{x\cdot y}|x\rangle, \tag{12}$$

where $x \cdot y$ denotes the inner product between x and y as vectors. Hence, the post-measurement state is given by

$$(|y_H\rangle\langle y_H|_{\mathcal{A}} \otimes I_{\mathcal{B}})|\psi'\rangle \propto |y_H\rangle_{\mathcal{A}} \otimes \sum_{x\in\{0,1\}^{2n}} (-1)^{x\cdot y} a_x P_x|\phi\rangle_{\mathcal{B}}. \tag{13}$$

Note, if $y = 0^{2n}$, then $(-1)^{x\cdot y} = 1$ for all x, and thus we get $U|\phi\rangle_{\mathcal{B}}$. Otherwise, the following operator is applied:

$$U_y = \sum_{x\in\{0,1\}^{2n}} (-1)^{x\cdot y} a_x P_x = \sum_{x\in\{0,1\}^{2n}} a_x \bigotimes_{i=1}^{n} (-1)^{x_{2i-1}y_{2i-1}+x_{2i}y_{2i}} \sigma_{x_{2i-i}x_{2i}} \tag{14}$$

We argue that it is of the form $P_z U P_z$ for some $z \in \{0,1\}^{2n}$. For a fixed $y \in \{0,1\}^2$, the individual terms in the tensor product are of the form $\tilde{\sigma}_x = (-1)^{x\cdot y}\sigma_x$ for all $x \in \{0,1\}^2$.

(a) If $y = 00$, we have $\tilde{\sigma}_x = \sigma_x$.

(b) If $y = 01$, the phase -1 is injected for $x \in \{01, 11\}$ (i.e. $\sigma_x \in \{\mathsf{X}, \mathsf{Z}\}$) and so $\tilde{\sigma}_x = \mathsf{Y}\sigma_x\mathsf{Y}$ as $\mathsf{YIY} = \mathsf{I}, \mathsf{YXY} = -\mathsf{X}, \mathsf{YYY} = \mathsf{Y}, \mathsf{YZY} = -\mathsf{Z}$.

[10] It suffices to only use powers of ζ_n up to the degree of ζ_n, which 2^{k-1} in this case.

(c) If $y = 10$, the phase -1 is injected for $x \in \{10, 11\}$ (i.e. $\sigma_x \in \{\mathsf{Y}, \mathsf{Z}\}$) and so $\tilde{\sigma}_x = \mathsf{X}\sigma_x\mathsf{X}$ as $\mathsf{XIX} = \mathsf{I}, \mathsf{XXX} = \mathsf{X}, \mathsf{XYX} = -\mathsf{Y}, \mathsf{XZX} = -\mathsf{Z}$.

(d) If $y = 11$, the phase -1 is injected for $x \in \{01, 10\}$ (i.e. $\sigma_x \in \{\mathsf{X}, \mathsf{Y}\}$) and so $\tilde{\sigma}_x = \mathsf{Z}\sigma_x\mathsf{Z}$ as $\mathsf{ZIZ} = \mathsf{I}, \mathsf{ZXZ} = -\mathsf{X}, \mathsf{ZYZ} = -\mathsf{Y}, \mathsf{ZZZ} = \mathsf{Z}$.

Hence, $\tilde{\sigma}_x = \sigma_{\tilde{y}}\sigma_x\sigma_{\tilde{y}}$, where $\tilde{y} = y_2y_1$ (swap the bits of y). Since the correction terms do not depend on x, they can be factored out and we have $U_y = P_{\tilde{y}}UP_{\tilde{y}}$, where now $\tilde{y} = y_2y_1y_4y_3\cdots y_{2n}y_{2n-1}$.

The probability of measuring y is given by

$$\begin{aligned} \|(|y_H\rangle\langle y_H|_{\mathcal{A}} \otimes I_{\mathcal{B}})|\psi'\rangle\|^2 &= \left\| |y_H\rangle_{\mathcal{A}} \otimes 2^{-n} \sum_{x\in\{0,1\}^{2n}} (-1)^{x\cdot y} a_x P_x |\phi\rangle_{\mathcal{B}} \right\|^2 \\ &= \left\| 2^{-n} U_y |\phi\rangle_{\mathcal{B}} \right\|^2 = 2^{-2n}, \end{aligned} \tag{15}$$

as U_y is unitary if U is unitary.

Complexity analysis. We can compute the Pauli coefficients efficiently with the Hilbert-Schmidt product $a_x = 2^{-n}\operatorname{Tr}(P_xU)$. By Lemma 3.7, we can prepare $|U\rangle$ in time $\operatorname{poly}(2^n, \log s)$ with success probability $p \geq 2^{-2n-4}$. If we run the state preparation r/p times, then the probability that all fail is at most $(1-p)^{r/p} \leq e^{-r}$. □

Lemma 3.11. *Let $\mathcal{G}$ be a fixed finite gateset in $\mathbb{Q}(\mathrm{i})$. We can simulate each gate of $\mathcal{G}$ using $\mathcal{G}_4$ with success probability $1 - 1/\mathrm{poly}(m)$ in time $\mathrm{poly}(m)$.*

Proof. The idea is to apply the n-qubit gate $U \in \mathcal{G}$ using Lemma 3.10. As noted in the proof, even if the final Hadamard measurement fails by giving $y \neq 0^{2n}$, we still know that some unitary U_y was applied.[11] So we can repeat the procedure with $U' = UU_y^\dagger$, which again succeeds with probability 2^{-2n}. Unfortunately, the bit complexity of U' grows exponentially in the worst case, and therefore we only have a logarithmic number of attempts before the correction terms grow too big. Still, if we treat n as a constant, then the success probability is also a constant and $O(\log(m))$ attempts suffice for a success probability of $1 - 1/\mathrm{poly}(m)$. Otherwise, the runtime would be doubly exponential in n. □

Lemma 3.10 also extends to cyclotomic integer unitaries, but with the caveat that the success probability now depends on the unitary as in Lemma 3.9.

Lemma 3.12. *Let $k > 2$ and U be an n-qubit unitary with $sU \in \mathbb{Z}[\zeta_{2^k}]$ for $s^2 \in \mathbb{N}$. U can be implemented with success probability $1/\mathrm{poly}(2^{2n}, s)$ in time and space $\mathrm{poly}(2^n, \log s)$ using the gateset $\mathcal{G}_{2^k}$.*

Remark 3.13. Lemma 3.10 only requires U to be unitary to have success probability 2^{-2n} for all outcomes y in Eq. (15) independent of the input state. If U is not unitary, then the success probability on input is given by

$$\frac{1}{\|U\|_{\mathrm{F}}^2} \cdot \left\| U_y|\phi\rangle \right\|^2, \tag{16}$$

where $|\phi\rangle$ is the input. Notably, the success probability is 0 if $U|\phi\rangle = 0$.

3.3 Simulating cyclotomic gates with integer gates

In this section, we show how to use above constructions to simulate gatesets with entries from a cyclotomic field $\mathbb{K} = \mathbb{Q}(\zeta_n)$ with $n = 2^k$. The case $k = 2$ was already proven by McKague [McK10, Section 2.4], and used prove that $\mathsf{QMA}(k), \mathsf{QIP}(k), \mathsf{MIP}, \mathsf{QSZK}$ over $\mathbb{R}$ are equivalent to their original definitions over $\mathbb{C}$ [McK13].

Let $d = 2^{k-1}$ be the degree of ζ_n. We encode $a = \sum_{i=0}^{d-1} a_i\zeta_n^i \in \mathbb{K}$ as $|v(a)\rangle = \sum_{i=0}^{d-1} a_i|i\rangle$ with all $a_i \in \mathbb{Q}$, and a vector $|\psi\rangle \in \mathbb{K}^N$ as

$$|\psi\rangle = \sum_{i=0}^{N-2} a_i|i\rangle \qquad \mapsto \qquad |v(\psi)\rangle \propto \sum_{i=0}^{d-1} |i\rangle_\alpha |v(a_i)\rangle. \tag{17}$$

[11] If U is Clifford, then a Pauli correction suffices and we can succeed with probability 1 (ignoring state preparation).

Note that this encoding is unique.

Lemma 3.14. *There exists a group homomorphism $\Psi : \mathrm{U}(N, \mathbb{K}) \to \mathrm{O}(dN, \mathbb{Q})$ such that $\Psi(U)$ implements U inside the encoding, i.e., $\Psi(U)|v(\psi)\rangle = |v(U|\psi\rangle)\rangle$ for all $|\psi\rangle \in \mathbb{K}^N$.*

Proof. $\mathbb{K}$ is isomorphic to $\mathbb{Q}[x]/\Phi_n(x)$, where $\Phi_n(x)$ is the n-th cyclotomic polynomial, which has degree $d = \varphi(n)$, where φ is Euler's totient function. An integral basis of $\mathbb{K}$ is given by $\{1, \zeta_n, \dots, \zeta_n^{d-1}\}$. Thus, we can treat $\mathbb{K}$ as a d-dimensional vector space over $\mathbb{Q}$. Any $a \in \mathbb{K}$ has therefore a unique decomposition $a = \sum_{i=0}^{n-1} a_i \zeta_n^i$ with $a_i \in \mathbb{Q}$. Denote by v_a the vector with coefficients $a_0, \dots, a_{d-1}$. The product of $a, b \in \mathbb{K}$ is then $ab = \sum_{i,j=0}^{d-1} a_i b_j \zeta_n^{i+j}$. If we fix a, this expression is linear in v_b.

Thus, there exists a unique matrix M_a such that $M_a v_b = v_{ab}$ for all a, b. In fact, the map $\Psi : a \mapsto M_a$ preserves multiplication and addition, and therefore Ψ is a field isomorphism between $\mathbb{K}$ and a subfield of $\mathbb{Q}^{d\times d}$.[12] Note that $n = 2^k$, $d = 2^{k-1}$ and $\zeta_n^d = -1$. Therefore, we get $M_a^T = M_{\overline{a}}$, because $\overline{\zeta_n} = \zeta_n^{-1} = \zeta_n^{n-1} = -\zeta_n^{d-1}$ with

$$M_{\zeta_n} = \begin{pmatrix} 0 & & & -1 \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ & & 1 & 0 \end{pmatrix}, \qquad M_{-\zeta_n^{d-1}} = -M_{\zeta_n^{d-1}} = -M_{\zeta_n}^{d-1} = \begin{pmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ -1 & & & 0 \end{pmatrix}. \tag{18}$$

Since Ψ is an isomorphism,

$$(M_{\zeta_n^j})^T = (M_{\zeta_n}^j)^T = (M_{\zeta_n}^T)^j = M_{\overline{\zeta_n}}^j = M_{\overline{\zeta_n^j}}. \tag{19}$$

By linearity, we have

$$M_a^T = \sum_{i=0}^{d-1} a_i M_{\zeta_n^i}^T = \sum_{i=0}^{d-1} a_i M_{\overline{\zeta_n^i}} = M_{\sum_{i=0}^{d-1} a_i \overline{\zeta_n^i}} = M_{\overline{a}}. \tag{20}$$

Thus, applying Ψ to the entries of a unitary gives an orthogonal matrix, i.e., $\Psi\colon \mathrm{U}(N, \mathbb{K}) \to \mathrm{O}(dN, \mathbb{Q})$ is a group homomorphism: For $U \in \mathrm{U}(N, \mathbb{K})$, $\Psi(U)$ is a $N \times N$ block matrix with blocks $\Psi(u_{ij})$ of size $d \times d$. Let $A = \Psi(U)^T \Psi(U)$ with blocks

$$A_{ij} = \sum_{k=1}^{N} \Psi(U)_{ik}^T \Psi(U)_{kj} = \sum_{k=1}^{N} \Psi(u_{ki})^T \Psi(u_{kj}) = \Psi\left(\sum_{k=1}^{N} \overline{u_{ki}} u_{kj}\right) = \Psi(\delta_{ij}) = \delta_{ij} I, \tag{21}$$

where δ_{ij} is the Kronecker delta. Thus, $A = I$ and $\Psi(U)$ is orthogonal.

Writing $U = \sum_{i,j} u_{ij} |i\rangle\langle j|$, we get $\Psi(U) = \sum_{i,j} |i\rangle\langle j|_\alpha \otimes \Psi(u_{ij})_\zeta$, where the ζ register contains the corresponding powers of ζ_n, and the α register the actual qubits. Using the encoding of Eq. (17), a quantum state $|\psi\rangle = \sum_{i=0}^{N-1} a_i |i\rangle$ with $a_i = \sum_{j=0}^{d-1} a_{ij} \zeta_n^j$ is written as

$$|v(\psi)\rangle = \sum_{i=0}^{N-1} |i\rangle_\alpha |v(a_i)\rangle_\zeta = \sum_{i=0}^{N-1} \sum_{j=0}^{d-1} a_{ij} |i\rangle_\alpha |j\rangle_\zeta. \tag{22}$$

Thus,

$$\begin{aligned} \Psi(U)|v(\psi)\rangle &= \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} |i\rangle_\alpha \otimes \Psi(u_{ij}) |v(a_j)\rangle_\zeta = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} |i\rangle_\alpha \otimes |v(u_{ij} a_j)\rangle_\zeta \\ &= \sum_{i=0}^{N-1} |i\rangle_\alpha \otimes \left| v\left(\textstyle\sum_{j=0}^{N-1} u_{ij} a_j\right)\right\rangle_\zeta = \big|v\big(U|\psi\rangle\big)\big\rangle. \end{aligned} \tag{23}$$

□

[12] M_a is also known as the regular representation (see e.g. [Die09]). We took the idea of treating the regular representation as a field isomorphism from [Vau05].

See Appendix B for an example of applying Ψ to $\sqrt{\mathsf{H}}$ and F_8 in $\mathbb{Q}(\zeta_8)$.

Proof of Theorem 3.3. First, we transform the gates of $\mathcal{G}$ to $\mathcal{G}'$ in $\mathbb{Q}$ with Lemma 3.14. Then we simulate these with $\mathcal{G}_4$ using Lemma 3.11. Finally, we apply Lemma 3.14 again to $\mathcal{G}_4$ to obtain a gateset $\mathcal{G}_4'$ in $\mathbb{Z}[1/2]$, which we can implement exactly with $\mathcal{G}_2$ by Theorem 3.1.

It remains to argue that applying Lemma 3.14 to a BQP_1 verifier yields a valid BQP_1 verifier. To avoid clutter, write $\widehat{|\psi\rangle} := |v(\psi)\rangle, \widehat{U} := \Psi(U)$. Let $V = U_T \cdots U_1$ be a BQP_1 verifier with soundness ε. We will show that $\widehat{V} = \widehat{U}_T \cdots \widehat{U}_1$ is also a valid BQP_1 verifier for the same problem. First, consider the initial state for V: $|\psi_{\text{init}}\rangle = |0\rangle_\alpha |x\rangle_\beta$. Since $|\psi_{\text{init}}\rangle$ is rational, we have $|\widehat{\psi_{\text{init}}}\rangle = |\psi_{\text{init}}\rangle_{\alpha\beta}|0\rangle_\zeta$.

In the YES-case, $V|\psi_{\text{init}}\rangle = |1\rangle_{\alpha_1}|\phi_1\rangle_{\overline{\alpha_1}} = |\phi\rangle$. Therefore, $\widehat{V}|\widehat{\psi_{\text{init}}}\rangle = |1\rangle_{\alpha_1}|\widehat{\phi_1}\rangle_{\overline{\alpha_1}} = |\widehat{\phi}\rangle$. Thus, perfect completeness is preserved.

In the NO-case, let $|\phi\rangle = V|\psi_{\text{init}}\rangle = |0\rangle|\phi_0\rangle + |1\rangle|\phi_1\rangle$, where $\widehat{|\phi_0\rangle, |\phi_1\rangle}$ are not normalized and $\||\phi_0\rangle\|^2 \geq 1 - \varepsilon$ is the rejectance probability of V. Now consider $|\widehat{\phi}\rangle = \widehat{V}|\widehat{\psi_{i,\text{init}}}\rangle = |0\rangle|\widehat{\phi_0}\rangle + |1\rangle|\widehat{\phi_1}\rangle$, where $p = \langle\widehat{\phi_0}|\widehat{\phi_0}\rangle$ is the rejectance probability of $\widehat{V}$. Let $\Lambda = \sum_{i=0}^{d-1} I \otimes \zeta_n^i \langle i|_\zeta$ be the operator that maps $|\widehat{\psi}\rangle$ to $|\psi\rangle$. Then $\Lambda|\widehat{\phi}\rangle = |\phi\rangle$ and thus $\Lambda|\widehat{\phi_0}\rangle = |\phi_0\rangle$. Thus, $\|\Lambda|\widehat{\phi_0}\rangle\|^2 = \||\phi_0\rangle\|^2 \geq 1 - \varepsilon$. Hence, $\||\widehat{\phi_0}\rangle\|^2 \geq (1-\varepsilon)\|\Lambda\|^{-2} \geq 1/2n^2$ for small ε.

Thus, the soundness of the BQP_1 verifier $\widehat{V}$ is inverse polynomial in n. □

For the special case $k = 2$, the above idea also works for QMA_1 as shown in [McK10; McK13], but for $k > 2$ there does not seem be a way to prevent the prover from sending a state $|\psi\rangle$ with $\Lambda|\psi\rangle = 0$.

Proof of Theorem 3.2. Note that applying Lemma 3.14 to a QMA_1-verifier V creates a verifier V' that "expects" a proof with real amplitudes. With standard error reduction techniques, we can transform V' to V'' with soundness ε (on proofs with real amplitudes). Then V'' still has soundness 4ε against proofs with complex amplitudes. Hence, we can simulate $\mathcal{G}$ in the same way as in Theorem 3.3, but with additional error reduction steps. □

4 Quantum SAT

The first key idea is that we can verify the k-local Hamiltonian singular value problem in QMA_1 using the insight of Remark 3.13.

Lemma 4.1. *l-$\mathsf{LHSV}^{\mathbb{Q}(\mathrm{i})} \in \mathsf{QMA}_1^{\mathcal{G}_2}$ and l-$\mathsf{LHSV}_\varepsilon^{\mathbb{Q}(\zeta_{2k})} \in \mathsf{QMA}_{1,1-\varepsilon'}^{\mathcal{G}_{2k}}$ with $l \in O(\log n)$,*[13] *$\varepsilon \leq n^{-O(1)}$ and $\varepsilon' \in \varepsilon^{O(1)}$, where n is the number of qubits of the instance.*

Proof. The first case l-$\mathsf{LHSV}^{\mathbb{Q}(\mathrm{i})} \in \mathsf{QMA}_1^{\mathcal{G}_2}$ follows from l-$\mathsf{LHSV}^{\mathbb{Q}(\mathrm{i})} \in \mathsf{QMA}_1^{\mathcal{G}_4}$ and Theorem 3.2. Note that this requires a gap of at least $1/\text{poly}(n)$, since Theorem 3.2 makes use of error reduction.

We next describe the QMA_1-verifier. Let $H = \sum_{S \in \binom{[n]}{l}} H_S$ be the input Hamiltonian with all $\|H_S\| \leq 1$. We need to distinguish between $\sigma_1(H) = 0$ and $\sigma_1(H) \geq \varepsilon$. The QMA_1-verifier classically computes the Pauli decomposition of the local H_S terms $H_S = \sum_{x \in \{0,1\}^{2l}} a_{S,x} P_x$, where $a_{S,x} \in \mathbb{Q}(\zeta_{2^k})$. Let $2^s \leq n^{O(1)}$ be an upper bound on the number of nonzero A_S and identify each such set $S = S_z$ for $z \in \{0,1\}^s$. Then it prepares the state

$$|H\rangle_{\mathcal{A}} = \sum_{z \in \{0,1\}^s} \sum_{x \in \{0,1\}^{2l}} a_{zx} |z\rangle_{\mathcal{A}_1} |x\rangle_{\mathcal{A}_2}, \tag{24}$$

using Lemma 3.9, which succeeds with probability $p_{\text{prep}} \geq \varepsilon^{O(1)}$ since entries are polynomially bounded (see Definition 2.12), and accepts if the preparation fails. As $|H\rangle$ is not necessarily normalized, we in fact prepare $\eta|H\rangle$, for some $\eta \geq (\sum_z \|H_{S_z}\|_{\text{F}})^{-2} \geq n^{-O(1)}$.

Let U be the unitary that applies $(P_x)_{S_z}$ (on register $\mathcal{B}$) conditioned on $|z\rangle_{\mathcal{A}_1}|x\rangle_{\mathcal{A}_2}$. U can be efficiently implemented with a polynomial number of $\mathcal{G}_4$ gates. Apply U to $|H\rangle$ and the proof $|\psi\rangle$:

$$|\phi\rangle := U\eta|H\rangle_{\mathcal{A}}|\psi\rangle_{\mathcal{B}} := \sum_{z \in \{0,1\}^s} \sum_{x \in \{0,1\}^{2l}} \eta a_{zx} |z\rangle_{\mathcal{A}_1} |x\rangle_{\mathcal{A}_2} \otimes ((P_x)_{S_z} \otimes I_{[n]\setminus S_z})|\psi\rangle_{\mathcal{B}} \tag{25}$$

[13] For $l \in \omega(1)$, we assume that there are only $\text{poly}(n)$ nonzero H_S terms in $H = \sum_S H_S$.

Then measure the $\mathcal{A}$ register in the Hadamard basis and reject on outcome $|0_H\rangle := (H|0\rangle)^{\otimes(s+2l)} = 2^{-s/2-l}\sum_{z\in\{0,1\}^s}\sum_{z\in\{0,1\}^{2l}}|z\rangle_{\mathcal{A}_1}|x\rangle_{\mathcal{A}_2}$. That means, we *reject if we succeed* to apply the non-unitary operator H to the proof, which can only happen if the proof is not in the nullspace of H.

The rejecting projector is then $\Pi_{\mathrm{rej}} = |0_H\rangle\langle 0_H|_{\mathcal{A}} \otimes I_{\mathcal{B}}$ and the rejectance probability is $\|\Pi_{\mathrm{rej}}|\phi\rangle\|^2$ with

$$\Pi_{\mathrm{rej}}|\phi\rangle = |0_H\rangle_{\mathcal{A}} \otimes 2^{-s/2-l}\sum_{z\in\{0,1\}^s}\sum_{x\in\{0,1\}^{2l}} \eta a_{zx}((P_x)_{S_z}\otimes I_{[n]\setminus S_z})|\psi\rangle_{\mathcal{B}} \tag{26a}$$

$$= |0_H\rangle_{\mathcal{A}} \otimes 2^{-s/2-l}\sum_{z\in\{0,1\}^s} \eta(H_{S_z}\otimes I_{[n]\setminus S_z})|\psi\rangle_{\mathcal{B}} \tag{26b}$$

$$= |0_H\rangle_{\mathcal{A}} \otimes 2^{-s/2-l}\eta H|\psi\rangle_{\mathcal{B}}. \tag{26c}$$

Thus, the rejectance probability is given by $p_{\mathrm{rej}} = 2^{-s-2l}\eta\|H|\psi\rangle\|^2$. Hence, we get perfect completeness in the YES-case as an honest prover can send a state in the kernel of H. In the NO-case, we have $\|H|\psi\rangle\| \geq \sigma_1(H) \geq \varepsilon$, and thus $p_{\mathrm{rej}} \geq 2^{-s-2l}\eta\varepsilon^2 \geq \varepsilon^{O(1)}$. With state preparation, the verifier rejects with probability $p_{\mathrm{prep}}\cdot p_{\mathrm{rej}} \geq \varepsilon^{O(1)}$. □

Theorem 4.2. $4\text{-}\mathsf{QSAT}^{\mathbb{Q}(\zeta_{2^k})}$ *is complete for* $\mathsf{QMA}_1^{\mathcal{G}_{2^k}}$ *for all* $k \in \mathbb{N}$.

Proof. Hardness for $k \geq 2$ follows directly by applying Bravyi's 4-QSAT construction [Bra06]. For $\mathcal{G}_4$ we need to replace the Toffoli gate with a controlled-S gate so that all gates are 2-local (see Appendix C). For $k = 1$, we need to slightly alter Bravyi's construction to implement the Toffoli gate 4-locally. The basic idea is to implement logical qu-5-its on 4 physical qubits, and then use the "triangle Hamiltonian" gadget of [ER08] to conditionally split the computation paths. See Appendix C for more details. Containment follows from Lemma 4.1. □

We can now also generalize Theorem 3.2 to cyclotomic gatesets, since the Hamiltonian problem allows us to circumvent the success probability issue of integer state preparation (see Lemma 3.9).

Theorem 4.3. *For any finite gateset* $\mathcal{G}$ *in* $\mathbb{Q}(\zeta_{2^k})$ *with* $k \in \mathbb{N}$, *it holds that* $\mathsf{QMA}_1^{\mathcal{G}} \subseteq \mathsf{QMA}_1^{\mathcal{G}_{2^k}}$.

Proof. By the same argument as Theorem 4.2, $k\text{-}\mathsf{QSAT}^{\mathbb{Q}(\zeta_{2^k})}$ is $\mathsf{QMA}_1^{\mathcal{G}}$-hard. By Lemma 4.1, we also have $k\text{-}\mathsf{QSAT}^{\mathbb{Q}(\zeta_{2^k})} \in \mathsf{QMA}_1^{\mathcal{G}_{2^k}}$. □

Theorem 4.4. $3\text{-}\mathsf{QSAT}^{\mathbb{Q}(\zeta_{2^k})}$ *is complete for* $\mathsf{QMA}_1^{\mathcal{G}_{2^k}}$ *for all* $k \geq 3$.

Proof. The 3-QSAT construction of [GN13] is in $\mathbb{Q}(\zeta_8)$ and uses the gateset $\mathcal{G}_8$. Note that one of their projectors is of the form $\Pi = \frac{1}{\sqrt{3}}H$ with H in $\mathbb{Q}(\zeta_8)$, so we take $H = \sqrt{3}\Pi$, which is allowed in our definition of QSAT (see Problem 2.6). Their construction easily generalizes when replacing $\mathsf{T} \equiv \mathsf{T}_8$ with T_{2^k}. □

5 A 2-local QMA$_1$-complete Hamiltonian problem

Here we prove the first 2-local QMA_1-complete Hamiltonian problem.

Theorem 5.1. $2\text{-}\mathsf{LHSV}^{\mathbb{Q}(\zeta_{2^k})}$ *is* $\mathsf{QMA}_1^{\mathcal{G}_{2^k}}$*-complete for all* $k \geq 3$.

Bravyi proved that quantum 2-SAT is in P. In fact, a frustration-free Hamiltonian always has a ground state that is the tensor product of one- and two qubit states [CCD+11; JWZ11]. Therefore, we will need to use a frustrated Hamiltonian. Unfortunately, we cannot just use the 2-local Hamiltonian of [KKR05] since the accepting history state is not an eigenvector. We need a new 2-local Hamiltonian construction with the added feature that the history state is also an eigenstate.

Let $V = U_T \cdots U_1$ be the QMA_1-verifier circuit to embed. Suppose V acts on a register $\mathcal{A}$ of n_1 qubits for the ancillas, and n_2 qubits for the proof ($n := n_1 + n_2 \leq T$). We embed V into a Hamiltonian H on computational register $\mathcal{A}$ and clock register $\mathcal{C}$ of $T+1$ qubits. H has a similar structure to Kitaev's circuit-to-Hamiltonian construction [KSV02]: H_{clock} enforces a logical clock state, H_{prop} enforces application of the gates between clock states, H_{in} enforces correct initialization of the ancillas, and H_{out} enforces acceptance.

$$H = H_{\text{prop}} + H_{\text{in}} + H_{\text{out}} + J_{\text{clock}} H_{\text{clock}} \tag{27}$$

The factor J_{clock} will be chosen sufficiently large to apply the Projection Lemma [KKR05] (see Lemma 5.3). H_{prop}, H_{in}, H_{out} will be defined later.

5.1 Clock Hamiltonian

We begin by defining H_{clock}:

$$H_{\text{clock}} = 4T \sum_{1\le i<j\le T+1} |11\rangle\langle 11|_{\mathcal{C}_i,\mathcal{C}_j} + \sum_{t=1}^{T+1} \Big(|0\rangle\langle 0| - T|1\rangle\langle 1|\Big)_{\mathcal{C}_t} \tag{28}$$

Claim 5.2. *It holds that $H_{\text{clock}} \succeq 0$,*

$$\mathcal{N}(H_{\text{clock}}) = \mathscr{C} \coloneqq \operatorname{Span}\big\{|\widehat{t}\rangle \mid t \in \{0,\dots,T\}\big\}, \qquad |\widehat{t}\rangle \coloneqq \big|0^t\,1\,0^{T-t}\big\rangle, \tag{29}$$

and $\gamma(H_{\text{clock}}) \ge T$, where $\gamma(\cdot)$ denotes the smallest non-zero eigenvalue.

Proof. Since H_{clock} is diagonal, its eigenbasis is the computational basis. Clearly, $H_{\text{clock}}|\widehat{t}\rangle = 0$ for all $t \in \{0,\dots,T+1\}$. Further, $H_{\text{clock}}|0^{T+1}\rangle = (T+1)|0^{T+1}\rangle$, and for $x \in \{0,1\}^{T+1}$ with Hamming weight $h \ge 2$, we have $\langle x|H_{\text{clock}}|x\rangle = (2(h-1)h - h)T \ge hT$. □

We use a "one-hot encoding" for the clock, whereas more commonly a unary clock is used (e.g., [KSV02; KKR05]; see also [CLN18] for an overview of different clock constructions). Note that a one-hot clock is not possible with quantum SAT, as, if $\mathscr{C}$ is in the kernel of a k-local QSAT instance with $k \le T$, then the all-zero state $|0^{T+1}\rangle$ will also be in the kernel. Next, we leverage the Projection Lemma, reproduced below for convenience, to argue that it suffices to consider H inside the clock space $\mathscr{C}$.

Lemma 5.3 (Projection Lemma [KKR05])**.** *Let $H = H_1 + H_2$ be the sum of two Hamiltonians on Hilbert space $\mathcal{H} = \mathcal{S} + \mathcal{S}^\perp$, such that $\mathcal{S}$ is a zero eigenspace of H_2 and the eigenvectors in $\mathcal{S}^\perp$ have eigenvalue $J > 2\|H_2\|$. Then*

$$\lambda_{\min}(H_1|_{\mathcal{S}}) - \frac{\|H_1\|^2}{J - 2\|H_1\|} \le \lambda_{\min}(H) \le \lambda_{\min}(H_1|_{\mathcal{S}}), \tag{30}$$

where $H|_{\mathcal{S}} = \Pi_{\mathcal{S}} H \Pi_{\mathcal{S}}$ and $\Pi_{\mathcal{S}}$ denotes the projector onto $\mathcal{S}$.

Claim 5.4. *$\lambda_{\min}(H) \ge \lambda_{\min}(H|_{\mathscr{C}}) - \varepsilon$ for sufficiently large $J_{\text{clock}} \in (n\varepsilon)^{-O(1)}$.*

Proof. Let $H = H_1 + H_2$ with $H_1 = H_{\text{prop}} + H_{\text{in}} + H_{\text{out}}$ and $H_2 = J_{\text{clock}} H_{\text{clock}}$. The statement then follows from Lemma 5.3, Claim 5.2, and $\|H_{\text{prop}} + H_{\text{in}} + H_{\text{out}}\| \in n^{O(1)}$, which we will see later. □

5.2 Gate gadgets

Next, we define H_{prop}, i.e., the terms of the Hamiltonian that enforce application of the gates between timesteps, so that

$$\mathcal{N}(H_{\text{prop}} + H_{\text{clock}}) = \operatorname{Span}\big\{|\psi_{\text{hist}}(x)\rangle \mid x \in \{0,1\}^n\big\} \tag{31}$$

$$|\psi_{\text{hist}}(x)\rangle \coloneqq \frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} U_t \cdots U_1 |x\rangle_{\mathcal{AB}} |\widehat{t}\rangle_{\mathcal{C}} \tag{32}$$

To prove Eq. (31), we will use the "Nullspace Connection Lemma" of [RGN24], which allows us to analyze the "gate gadgets" individually, which we restate below for convenience.

Lemma 5.5 (Nullspace Connection Lemma [RGN24]). *Let*

(1) $K_1, \dots, K_m$ be a disjoint partition of the clock states with $u_i, v_i \in K_i, u_i \neq v_i$ for all $i \in [m]$.

(2) $H_1 = \sum_{i=1}^m H_{1,i}$ be a Hamiltonian such that for all $i \in [m]$:

- *(a) $\mathcal{N}(H_{1,i}|_{\mathcal{K}_i}) = \mathrm{Span}\{|\psi_i(\alpha_j)\rangle \mid j \in [d]\}$, where $\mathcal{K}_i = \mathbb{C}^d_{\mathcal{A}} \otimes \mathrm{Span}\{|v\rangle_{\mathcal{C}} \mid v \in K_i\}$, and $|\alpha_1\rangle, \dots, |\alpha_d\rangle$ is an orthonormal basis of the ancilla space,*
- *(b) $\exists$ linear map L_i with $L_i|\alpha\rangle = |\psi_i(\alpha)\rangle$ and $L_i^\dagger L_i = \lambda_i I$ for some constant λ_i,*
- *(c) H_i has support only on clock states K_i,*
- *(d) $\||\psi_i(\alpha)\rangle\|^2 =: \delta_i \in [1, \Delta]$,*
- *(e) $(I_{\mathcal{A}} \otimes \langle u_i|_{\mathcal{C}})|\psi_i(\alpha)\rangle = |\alpha\rangle_{\mathcal{A}}$,*
- *(f) $(I_{\mathcal{A}} \otimes \langle v_i|_{\mathcal{C}})|\psi_i(\alpha)\rangle = U_i|\alpha\rangle_{\mathcal{A}}$ for some unitary U_i.*

(3) $H_2 = \sum_{i=1}^{m-1} h_{v_i,u_{i+1}}(V_i)$ with $h_{v_i,u_{i+1}}(V_i) = I \otimes |v_i\rangle\langle v_i| + I \otimes |u_{i+1}\rangle\langle u_{i+1}| - V_i^\dagger \otimes |v_i\rangle\langle u_{i+1}| - V_i \otimes |u_{i+1}\rangle\langle v_i|$ for unitaries V_i.

(4) $|\alpha_{ij}\rangle = V_{i-1}U_{i-1} \cdots V_1 U_1 |\alpha_j\rangle$.

Then for $H = H_1 + H_2$, $\mathcal{N}(H) = \mathrm{Span}\{\sum_{i=1}^m |\psi_i(\alpha_{ij})\rangle \mid j \in [d]\}$ and $\gamma(H) = \Omega(\gamma(H_1)/(m^2\Delta))$.

The idea is to apply Lemma 5.5 to $H_{\mathrm{prop}}|_{\mathscr{C}}$ and split $H_{\mathrm{prop}} = H_1 + H_2$ with $H_1 = \sum_{t=1}^T H_{1,t}$ implementing the individual gates, and H_2 implementing identity transitions between these gadgets. H_2 is straightforward to implement 2-locally with $V_i = \mathsf{I}$ as

$$h_{i,j} = (|10\rangle - |01\rangle)(\langle 10| - \langle 01|)_{\mathcal{C}_i\mathcal{C}_j} = |10\rangle\langle 10| + |01\rangle\langle 01| - |10\rangle\langle 01| - |01\rangle\langle 10| \tag{33}$$

with $h_{i,j}|_{\mathscr{C}} = (|\widehat{i}\rangle - |\widehat{j}\rangle)(\langle\widehat{i}| - \langle\widehat{j}|)$.

5.3 Split gadget

At the heart of the gate gadgets is the "split gadget". It effectively splits the computation path to implement controlled unitaries. This idea first appeared in QMA_1-completeness proof of (3, 5)-QSAT [ER08], dubbed the "triangle Hamiltonian construction", and similar ideas were also used in [GN13; RGN24]. Let $|\psi_0\rangle, |\psi_1\rangle \in \mathbb{C}^2$ be orthonormal. The split gadget H_{split} acts on a computational register $\mathcal{A}$ of one qubit and a clock register $\mathcal{C}$ of 3 qubits $(\mathcal{C}_0, \mathcal{C}_1, \mathcal{C}_2)$.

$$\begin{aligned} H_{\mathrm{split}} = |\psi_1\rangle\langle\psi_1|_{\mathcal{A}} \otimes |1\rangle\langle 1|_{\mathcal{C}_1} + |\psi_0\rangle\langle\psi_0|_{\mathcal{A}} \otimes |1\rangle\langle 1|_{\mathcal{C}_2} +& \\ |1\rangle\langle 1|_{\mathcal{C}_0} - |10\rangle\langle 01|_{\mathcal{C}_0\mathcal{C}_1} - |10\rangle\langle 01|_{\mathcal{C}_0\mathcal{C}_2} +& \\ |1\rangle\langle 1|_{\mathcal{C}_1} - |10\rangle\langle 01|_{\mathcal{C}_1\mathcal{C}_0} + |10\rangle\langle 01|_{\mathcal{C}_1\mathcal{C}_2} +& \\ |1\rangle\langle 1|_{\mathcal{C}_2} - |10\rangle\langle 01|_{\mathcal{C}_2\mathcal{C}_0} + |10\rangle\langle 01|_{\mathcal{C}_2\mathcal{C}_1}& \end{aligned} \tag{34}$$

Claim 5.6. *H_{split} is Hermitian with $H_{\mathrm{split}}|_{\mathscr{C}} \succeq 0$, $\mathcal{N}(H_{\mathrm{split}}|_{\mathscr{C}}) = \{|\phi_0\rangle, |\phi_1\rangle\}$, where*

$$\begin{aligned} |\phi_0\rangle &= \frac{1}{\sqrt{2}}|\psi_0\rangle(|100\rangle + |010\rangle), \\ |\phi_1\rangle &= \frac{1}{\sqrt{2}}|\psi_1\rangle(|100\rangle + |001\rangle), \end{aligned} \tag{35}$$

and $H_{\mathrm{split}}|\phi_0\rangle = H_{\mathrm{split}}|\phi_1\rangle = 0$.

Proof. Observe that $\Pi_{\mathscr{C}} H_{\mathrm{split}} \Pi_{\mathscr{C}} = H_{\mathrm{split}} \Pi_{\mathscr{C}}$ since H_{split} maps logical clock states to logical states, where here $\Pi_{\mathscr{C}}$ acts as identity on $\mathcal{A}$ and projects $\mathcal{C}$ onto the clock space $\mathscr{C}$. Therefore, it suffices to compute the nullspace of $H_{\mathrm{clock}}|_{\mathscr{C}}$. After a change of basis, we have $|\psi_0\rangle = |0\rangle, |\psi_1\rangle = |1\rangle$ and

$$\begin{aligned} H_{\mathrm{split}}|_{\mathscr{C}} = |1\rangle\langle 1|_{\mathcal{A}} \otimes |\widehat{1}\rangle\langle\widehat{1}|_{\mathcal{C}} + |0\rangle\langle 0|_{\mathcal{A}} \otimes |\widehat{2}\rangle\langle\widehat{2}|_{\mathcal{C}} +& \\ |\widehat{0}\rangle\langle\widehat{0}|_{\mathcal{C}} - |\widehat{0}\rangle\langle\widehat{1}|_{\mathcal{C}} - |\widehat{0}\rangle\langle\widehat{2}|_{\mathcal{C}} +& \\ |\widehat{1}\rangle\langle\widehat{1}|_{\mathcal{C}} - |\widehat{1}\rangle\langle\widehat{0}|_{\mathcal{C}} + |\widehat{1}\rangle\langle\widehat{2}|_{\mathcal{C}} +& \\ |\widehat{2}\rangle\langle\widehat{2}|_{\mathcal{C}} - |\widehat{2}\rangle\langle\widehat{0}|_{\mathcal{C}} + |\widehat{2}\rangle\langle\widehat{1}|_{\mathcal{C}}.& \end{aligned} \tag{36}$$

We compute $\mathrm{corank}(H_{\mathrm{split}}|_{\mathscr{C}}) = 2$ using SageMath [The24] in the supplementary material [Rud24]. □

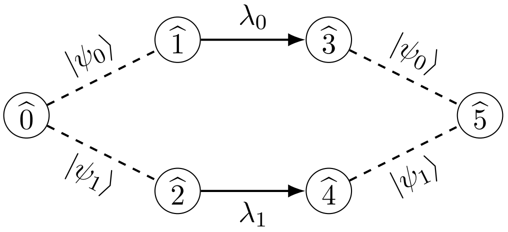


Figure 1: Graphical representation of the gadget H_U defined in Eq. (37). Dashed edges indicate "conditional transitions", and the arrows indicate "unitary transitions" (which are of the form λI here), following the conventions of [RGN24].

5.4 Single-qubit gate gadget

Combining two split gadgets, we can implement a single-qubit unitary $U = \lambda_0|\psi_0\rangle\langle\psi_0| + \lambda_1|\psi_1\rangle\langle\psi_1|$ (see also Fig. 1):

$$\begin{aligned} H_U &= (H_{\text{split}})_{\mathcal{C}_0\mathcal{C}_1\mathcal{C}_2} + (H_{\text{split}})_{\mathcal{C}_5\mathcal{C}_3\mathcal{C}_4} + h_{1,3}(\lambda_0) + h_{2,4}(\lambda_1), \\ h_{i,j}(\lambda) &= (|10\rangle\langle 10| + |01\rangle\langle 01| - \lambda^*|10\rangle\langle 01| - \lambda|01\rangle\langle 10|)_{\mathcal{C}_i\mathcal{C}_j} \end{aligned} \tag{37}$$

where $(H_{\text{split}})_{\mathcal{C}_5\mathcal{C}_3\mathcal{C}_4}$ means that we replace the register $\mathcal{C}_0, \mathcal{C}_1, \mathcal{C}_2$ in H_{split} with $\mathcal{C}_5, \mathcal{C}_3, \mathcal{C}_4$.

Claim 5.7. *H_U is Hermitian with $H_U|_{\mathscr{C}} \succeq 0$, $\mathcal{N}(H_U|_{\mathscr{C}}) = \{|\phi_0\rangle, |\phi_1\rangle\}$, where*

$$\begin{aligned} |\phi_0\rangle &= \frac{1}{2}|\psi_0\rangle_{\mathcal{A}}(|\widehat{0}\rangle + |\widehat{1}\rangle + \lambda_0|\widehat{3}\rangle + \lambda_0|\widehat{5}\rangle)_{\mathcal{C}}, \\ |\phi_1\rangle &= \frac{1}{2}|\psi_1\rangle_{\mathcal{A}}(|\widehat{0}\rangle + |\widehat{2}\rangle + \lambda_1|\widehat{4}\rangle + \lambda_1|\widehat{5}\rangle)_{\mathcal{C}}, \end{aligned} \tag{38}$$

and $H_U|\phi_0\rangle = H_U|\phi_1\rangle = 0$. H_U satisfies the conditions (2) of Lemma 5.5.

Proof. As in Claim 5.6, observe that $\Pi_{\mathscr{C}} H_U \Pi_{\mathscr{C}} = H_U \Pi_{\mathscr{C}}$. The analysis of the nullspace is similar to [RGN24, Lemma 3.2]. Let $\Pi_i = |\psi_i\rangle\langle\psi_i|_{\mathcal{A}} \otimes I_{\mathcal{C}}$ for $i \in \{0, 1\}$. Then we have $H_U = \Pi_0 H_U \Pi_0 + \Pi_1 H_U \Pi_1$ with

$$\begin{aligned} \Pi_0 H_U \Pi_0|_{\mathscr{C}} = |\psi_0\rangle\langle\psi_0|_{\mathcal{A}} \otimes \big(&|\widehat{2}\rangle\langle\widehat{2}| + |\widehat{4}\rangle\langle\widehat{4}| + \\ &|\widehat{0}\rangle\langle\widehat{0}| + |\widehat{1}\rangle\langle\widehat{1}| - |\widehat{0}\rangle\langle\widehat{1}| - |\widehat{1}\rangle\langle\widehat{0}| + \\ &|\widehat{1}\rangle\langle\widehat{1}| + |\widehat{3}\rangle\langle\widehat{3}| - \lambda_0^*|\widehat{1}\rangle\langle\widehat{3}| - \lambda_0|\widehat{3}\rangle\langle\widehat{1}| + \\ &|\widehat{3}\rangle\langle\widehat{3}| + |\widehat{5}\rangle\langle\widehat{5}| - |\widehat{3}\rangle\langle\widehat{5}| - |\widehat{5}\rangle\langle\widehat{3}|\big)_{\mathcal{C}}. \end{aligned} \tag{39}$$

Equation (39) now resembles the Kitaev's circuit Hamiltonian [KSV02] with four timesteps and three gates $I, \lambda_0 I, I$. Therefore $\mathcal{N}(\Pi_i H_U \Pi_i|_{\mathcal{C}}) = \text{Span}\{|\phi_i\rangle\}$ for $i \in \{0, 1\}$ ($i = 1$ is analogous).

It remains to verify the conditions of Lemma 5.5. (a) follows from the nullspace. For (b), define $L = 2|\phi_0\rangle\langle\psi_0| + 2|\phi_1\rangle\langle\psi_1|$. (c) and (d) are obvious. For (e) and (f), let $|\alpha\rangle = \alpha_0|\psi_0\rangle + \alpha_1|\psi_1\rangle$. We get $\langle\widehat{0}|_{\mathcal{C}} L|\alpha\rangle = |\alpha\rangle$ and $\langle\widehat{5}|_{\mathcal{C}} L|\alpha\rangle = \alpha_0\lambda_0|\psi_0\rangle + \alpha_1\lambda_1|\psi_1\rangle = U|\alpha\rangle$. □

For $U = \mathsf{T}_{2^k}$, the gadget H_U is clearly in $\mathbb{Q}(\zeta_{2^k})$. For $U = \mathsf{H}$, this is less obvious. H has eigenvalues ±1 with eigenvectors

$$|\mathsf{H}_+\rangle = \begin{pmatrix} a \\ b \end{pmatrix}, \quad |\mathsf{H}_-\rangle = \begin{pmatrix} -b \\ a \end{pmatrix}, \qquad a = \frac{\sqrt{2+\sqrt{2}}}{2} = \cos\frac{\pi}{8}, \quad b = \frac{\sqrt{2-\sqrt{2}}}{2} = \sin\frac{\pi}{8}, \tag{40}$$

with $|\mathsf{H}_+\rangle\langle\mathsf{H}_+|, |\mathsf{H}_-\rangle\langle\mathsf{H}_-|$ in $\mathbb{Q}(\zeta_8)$, as

$$a^2 = \frac{2+\sqrt{2}}{4}, \quad b^2 = \frac{2-\sqrt{2}}{4}, \quad ab = \frac{2}{4}. \tag{41}$$

Hence, H_{H} in $\mathbb{Q}(\zeta_8)$.

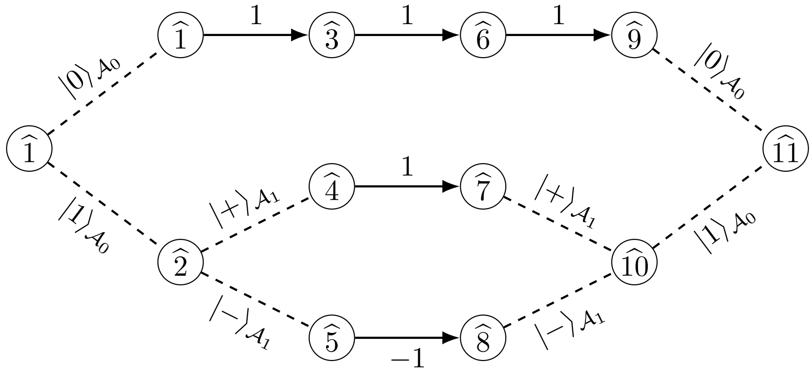

$\hat{1}$
$\hat{1}$
$\hat{3}$
$\hat{6}$
$\hat{9}$
1
1
1
$|0\rangle_{\mathcal{A}_0}$
$|1\rangle_{\mathcal{A}_0}$
$\hat{2}$
$|+\rangle_{\mathcal{A}_1}$
$|-\rangle_{\mathcal{A}_1}$
$\hat{4}$
1
$\hat{7}$
$\hat{5}$
-1
$\hat{8}$
$|+\rangle_{\mathcal{A}_1}$
$|-\rangle_{\mathcal{A}_1}$
$\hat{10}$
$|0\rangle_{\mathcal{A}_0}$
$|1\rangle_{\mathcal{A}_0}$
$\hat{11}$

Figure 2: Graphical representation of the gadget H_{CX} defined in Eq. (42).

5.5 Two-qubit gate gadget

The last gadget we need is the CNOT gadget H_{CX} (depicted in Fig. 2), which acts on a logical register $\mathcal{A}$ of two qubits $\mathcal{A}_0, \mathcal{A}_1$ and a clock register $\mathcal{C}$ of 12 qubits $\mathcal{C}_0, \dots, \mathcal{C}_{11}$. H_{CX} is constructed by effectively nesting two instances of the single-qubit gadget. Let $H_{\text{split}}(|\eta_0\rangle, |\eta_1\rangle)_{\mathcal{A}_i\mathcal{C}_u\mathcal{C}_v\mathcal{C}_t}$ denote an instance of H_{split} obtained by substituting $|\eta_0\rangle, |\eta_1\rangle$ for $|\psi_0\rangle, |\psi_1\rangle$, $\mathcal{A}_i$ for $\mathcal{A}$, and $\mathcal{C}_u, \mathcal{C}_v, \mathcal{C}_t$ for $\mathcal{C}_0, \mathcal{C}_1, \mathcal{C}_2$ in Eq. (37).

$$\begin{aligned}H_{\mathsf{CX}} = {} & H_{\text{split}}(|0\rangle, |1\rangle)_{\mathcal{A}_0\mathcal{C}_0\mathcal{C}_1\mathcal{C}_2} + H_{\text{split}}(|+\rangle, |-\rangle)_{\mathcal{A}_1\mathcal{C}_2\mathcal{C}_4\mathcal{C}_5} + \\ & H_{\text{split}}(|+\rangle, |-\rangle)_{\mathcal{A}_1\mathcal{C}_{10}\mathcal{C}_7\mathcal{C}_8} + H_{\text{split}}(|0\rangle, |1\rangle)_{\mathcal{A}_0\mathcal{C}_{11}\mathcal{C}_9\mathcal{C}_{10}} + \\ & h_{1,3}(1) + h_{3,6}(1) + h_{6,9}(1) + h_{4,7}(1) + h_{5,8}(-1) + \\ & |11\rangle\langle 11|_{\mathcal{A}_0\mathcal{C}_3} + |11\rangle\langle 11|_{\mathcal{A}_0\mathcal{C}_6}\end{aligned} \tag{42}$$

Claim 5.8. *H_{CX} is Hermitian with $\mathcal{H}_{\mathsf{CX}}|_{\mathscr{C}} \succeq 0$, $\mathcal{N}(H_{\mathsf{CX}}|_{\mathscr{C}}) = \{|\phi_{00}\rangle, |\phi_{01}\rangle, |\phi_{10}\rangle, |\phi_{11}\rangle\}$, where*

$$\begin{aligned}|\phi_{00}\rangle &= \frac{1}{\sqrt{6}}|0\rangle_{\mathcal{A}_0}|+\rangle_{\mathcal{A}_1}(|\hat{0}\rangle + |\hat{1}\rangle + |\hat{3}\rangle + |\hat{6}\rangle + |\hat{9}\rangle + |\widehat{11}\rangle)_{\mathcal{C}}, \\ |\phi_{01}\rangle &= \frac{1}{\sqrt{6}}|0\rangle_{\mathcal{A}_0}|-\rangle_{\mathcal{A}_1}(|\hat{0}\rangle + |\hat{1}\rangle + |\hat{3}\rangle + |\hat{6}\rangle + |\hat{9}\rangle + |\widehat{11}\rangle)_{\mathcal{C}}, \\ |\phi_{10}\rangle &= \frac{1}{\sqrt{6}}|1\rangle_{\mathcal{A}_0}|+\rangle_{\mathcal{A}_1}(|\hat{0}\rangle + |\hat{2}\rangle + |\hat{4}\rangle + |\hat{7}\rangle + |\widehat{10}\rangle + |\widehat{11}\rangle)_{\mathcal{C}}, \\ |\phi_{11}\rangle &= \frac{1}{\sqrt{6}}|1\rangle_{\mathcal{A}_0}|-\rangle_{\mathcal{A}_1}(|\hat{0}\rangle + |\hat{2}\rangle + |\hat{5}\rangle - |\hat{8}\rangle - |\widehat{10}\rangle - |\widehat{11}\rangle)_{\mathcal{C}},\end{aligned} \tag{43}$$

and $H_{\mathsf{CX}}|\phi_{00}\rangle = H_{\mathsf{CX}}|\phi_{01}\rangle = H_{\mathsf{CX}}|\phi_{10}\rangle = H_{\mathsf{CX}}|\phi_{11}\rangle = 0$. H_{CX} satisfies the conditions (2) of Lemma 5.5.

Proof. Analogous to Claim 5.7. □

We verify the positivity and nullspaces of $H_{\mathsf{H}}, H_{\mathsf{T}}, H_{\mathsf{CX}}$ with SageMath in [Rud24].

5.6 Assembling the Hamiltonian

Proof of Theorem 5.1. Define H_{prop} as in the Nullspace Connection Lemma, with H_1 made up of the gate gadgets defined in Eqs. (37) and (42), and connected with H_2 defined in Eq. (33). By Claim 5.4, we can just apply Lemma 5.5 to $H_{\text{prop}}|_{\mathscr{C}}$, since the lemma's requirements have been proven in Claims 5.7 and 5.8. Thus, we know that $H_{\text{prop}}|_{\mathscr{C}} \succeq 0$, $\gamma(H_{\text{prop}}|_{\mathscr{C}}) \geq 1/\text{poly}(n)$, and its nullspace is spanned by history states. Finally, we enforce correct ancilla initialization and an accepting computation with the projectors

$$H_{\text{in}} = \sum_{i=1}^{n_1} |11\rangle\langle 11|_{\mathcal{A}_i\mathcal{C}_0}, \tag{44}$$

$$H_{\text{out}} = |01\rangle\langle 01|_{\mathcal{A}_1\mathcal{C}_T}. \tag{45}$$

We can complete the proof analogously to [RGN24, Theorem 3.1]. □

6 Sparse Hamiltonian problems

In this section, we show completeness results for sparse Hamiltonian problems. We begin by extending Lemma 4.1 to sparse Hamiltonians.

Lemma 6.1. *$\mathsf{SHSV}^{\mathbb{Q}(\mathrm{i})} \in \mathsf{QMA}_1^{\mathcal{G}_2}$ and $\mathsf{SHSV}_\varepsilon^{\mathbb{Q}(\zeta_{2^k})} \in \mathsf{QMA}_{1,1-\varepsilon'}^{\mathcal{G}_{2^k}}$ with $\varepsilon \leq n^{-O(1)}$ and $\varepsilon' \in \varepsilon^{O(1)}$ for all $k \in \mathbb{N}$, where n is the number of qubits of the instance.*

6.1 Sparse Hamiltonian as linear combination of unitaries

First, we need a technical lemma that extends [KL21, Lemma 1] to cyclotomic fields.

Lemma 6.2. *Let $H \in \mathbb{Z}[\zeta_{2^k}]^{2^n \times 2^n}$ be an n-qubit 1-sparse Hamiltonian with coefficients of at most L bits. We can write $H = \sum_{l=0}^{L-1} \sum_{i=1}^{2^{k+1}} 2^{l-1} U^{l,i}$ with 1-sparse unitaries $U_{l,i}$, which can be efficiently implemented with the gateset $\mathcal{G}_{2^k}$ for all $k \in \mathbb{N}$.*

Proof. This proof is based on the proof of [KL21, Lemma 1] and [BCC+14, Lemma 4.3]. Let $d = 2^{k-1}$. H has a unique decomposition

$$H = \sum_{l=0}^{L-1} 2^l \sum_{m=0}^{d-1} (C^{m,l} + D^{m,l}), \tag{46}$$

such that each $C^{m,l}$ is 1-sparse, Hermitian, only has entries $\pm\zeta_{2^k}^m$ above the diagonal, and $\pm\zeta_{2^k}^{-m}$ below the diagonal, and only zeros on the diagonal. Each $D^{m,l}$ is diagonal with entries $\pm\zeta_{2^k}^m$. Example in $\mathbb{Z}[\zeta_8]$:

$$\begin{aligned}
\begin{pmatrix} 1 & \cdot & \cdot & \cdot \\ \cdot & \sqrt{2} & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1+\mathrm{i} \\ \cdot & \cdot & 1-\mathrm{i} & \cdot \end{pmatrix} &= \begin{pmatrix} 1 & \cdot & \cdot & \cdot \\ \cdot & \zeta_8 - \zeta_8^3 & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1+\zeta_8^2 \\ \cdot & \cdot & 1-\zeta_8^2 & \cdot \end{pmatrix} \qquad (47) \\
&= \begin{pmatrix} 1 & \cdot & \cdot & \cdot \\ \cdot & 0 & \cdot & \cdot \\ \cdot & \cdot & 0 & \cdot \\ \cdot & \cdot & \cdot & 0 \end{pmatrix} + \begin{pmatrix} 0 & \cdot & \cdot & \cdot \\ \cdot & \zeta_8 & \cdot & \cdot \\ \cdot & \cdot & 0 & \cdot \\ \cdot & \cdot & \cdot & 0 \end{pmatrix} + \begin{pmatrix} 0 & \cdot & \cdot & \cdot \\ \cdot & -\zeta_8^3 & \cdot & \cdot \\ \cdot & \cdot & \cdot & 0 \\ \cdot & \cdot & 0 & \cdot \end{pmatrix} + \begin{pmatrix} 0 & \cdot & \cdot & \cdot \\ \cdot & 0 & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & 1 & \cdot \end{pmatrix} + \begin{pmatrix} 0 & \cdot & \cdot & \cdot \\ \cdot & 0 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \zeta_8^2 \\ \cdot & \cdot & \zeta_8^{-2} & \cdot \end{pmatrix}
\end{aligned}$$

Note that $C^{m,l}$ and $D^{m,l}$ are not yet unitary. Therefore, we decompose the $C^{m,l} = \frac{1}{2}(C^{m,l,+} + C^{m,l,-})$ and $D^{m,l} = \frac{1}{2}(D^{m,l,+} + D^{m,l,-})$ into unitaries by replacing the 0's in the example above with $+1$ and -1. Since H is 1-sparse, we can define for each row i, the index j_i for the non-zero entry in row i. If row i has no non-zero entry, we set $j_i = i$. The unitaries are defined as follows:

$$C_{ij_i}^{m,l,\pm} = \begin{cases} C_{ij_i}^{m,l} & \text{if } C_{ij_i}^{m,l} \neq 0 \\ \pm 1 & \text{if } C_{ij_i}^{m,l} = 0 \end{cases}, \qquad D_{ii}^{m,l,\pm} = \begin{cases} D_{ii}^{m,l} & \text{if } D_{ii}^{m,l} \neq 0 \\ \pm 1 & \text{if } D_{ii}^{m,l} = 0 \end{cases} \tag{48}$$

The $D^{m,l,\pm}$ are unitary since they are diagonal with only powers of ζ_{2^k} on the diagonal. We can write

$$C^{m,l,\pm} = \sum_{i:i=j_i} C_{ii}^{m,l,\pm} |i\rangle\langle i| + \sum_{i:i\neq j_i} \left(C_{ij_i}^{m,l,\pm} |i\rangle\langle j_i| + (C_{ij_i}^{m,l,\pm})^* |j_i\rangle\langle i| \right), \tag{49}$$

where $C_{ii}^{m,l,\pm} \in \{1,-1\}$ for $i = j_i$ (which implies $H_{ij_i} = C_{ij_i}^{m,l} = 0$) and $\left| C_{ij_i}^{m,l,\pm} \right| = 1$ for all i. Thus, the $C^{m,l,\pm}$ are also unitary. The efficient implementation of these unitaries is analogous to [KL21]. □

Proof of Lemma 6.1. Let H be a d-sparse Hamiltonian on n qubits ($d = \mathrm{poly}(n)$) in $\mathbb{Z}[\zeta_{2^k}]$ with coefficients of at most L bits, i.e., H has at most d non-zero entries in each row and column. By [BCC+14, Lemma 4.4], we can write $H = \sum_{j=1}^{d^2} H_j$, where each H_j is 1-sparse and a query to any H_j can be simulated with $O(1)$ queries to H. This decomposition assumes that the graph of H is bipartite, which holds without loss of generality because $\mathsf{X} \otimes H$ has the same singular values as H.

The idea is to construct a d^2-coloring of the edges of the graph of G, and letting each H_j consist of the edges of color j. Hence, each H_j is also in $\mathbb{Z}[\zeta_{2^k}]$ with coefficients of at most L bits.

Next, we prepare the QMA_1-verifier. By Lemma 6.2, we can write

$$H = \sum_{j=1}^{d^2} \sum_{l=0}^{L-1} \sum_{i=1}^{2^{k+1}} 2^{l-1} U_j^{l,i} \tag{50}$$

As in Lemma 4.1, we prepare

$$|H\rangle_{\mathcal{A}} \propto \sum_{l=0}^{L-1} \sum_{j=1}^{d^2} \sum_{i=1}^{2^{k+1}} 2^{l-1} |i,j,l\rangle, \tag{51}$$

and then apply the unitary $U_{\mathcal{AB}} = \sum_{ijl} |i,j,l\rangle\langle i,j,l|_{\mathcal{A}} \otimes (U_j^{l,i})_{\mathcal{B}}$ with the proof in register $\mathcal{B}$. Soundness follows analogously to Lemma 4.1, noting $L = O(\log(n))$ (see Definition 2.12) and that flipping signs increases the norm by at most $\mathrm{poly}(n)$ due to sparsity. □

6.2 QMA(2)

It is straightforward to generalize Theorems 3.2 and 4.3 to $\mathsf{QMA}(2)$. Simulating complex gates with real gates in the $\mathsf{QMA}(2)$ setting requires special consideration, for which we refer to [McK13].

Theorem 6.3. *For any finite gateset $\mathcal{G}$ in $\mathbb{Q}(\mathrm{i})$, it holds that $\mathsf{QMA}_1^{\mathcal{G}}(2) \subseteq \mathsf{QMA}_1^{\mathcal{G}_2}(2)$.*

Theorem 6.4. *For any finite gateset $\mathcal{G}$ in $\mathbb{Q}(\zeta_{2^k})$ with $k \in \mathbb{N}$, it holds that $\mathsf{QMA}_1^{\mathcal{G}}(2) \subseteq \mathsf{QMA}_1^{\mathcal{G}_{2^k}}(2)$.*

Analogously to Lemma 6.1, we get for $\mathsf{QMA}_1(2)$:

Lemma 6.5. $\mathsf{SSHSV}^{\mathbb{Q}(\mathrm{i})} \in \mathsf{QMA}_1^{\mathcal{G}_2}(2)$ *and* $\mathsf{SSHSV}_\varepsilon^{\mathbb{Q}(\zeta_{2^k})} \in \mathsf{QMA}_{1,1-\varepsilon'}^{\mathcal{G}_{2^k}}(2)$ *with $\varepsilon \leq n^{-O(1)}$ and $\varepsilon' \in \varepsilon^{O(1)}$ for all $k \in \mathbb{N}$, where n is the number of qubits of the instance.*

Theorem 6.6. $\mathsf{SSHSV}^{\mathbb{Q}(\zeta_{2^k})}$ *is* $\mathsf{QMA}_1^{\mathcal{G}_{2^k}}(2)$*-complete for all $k \in \mathbb{N}$.*

Proof. Containment follows from Lemma 6.5, and hardness from [CS12]. □

We note that the key difference to the containment proof in [CS12], is that we directly (try to) apply the sparse Hamiltonian directly to the proof, whereas [CS12] uses Hamiltonian simulation (see [LC17] for an asymptotically optimal algorithm), combined with phase estimation (see [NC10]), which are both approximate techniques. Furthermore, to achieve L bits of precision using phase estimation, one needs to raise the unitary to the 2^L-th power, or, in this case, simulate the Hamiltonian for time 2^L, which generally takes exponential time [LC17].

Therefore, there was, to the best of our knowledge, no prior complete Hamiltonian problem for $\mathsf{QMA}(2)$ with a sub-polynomial promise gap (i.e. $n^{-\omega(1)}$). We can now show a complete problem for every "precision level" of $\mathsf{QMA}(2)$, with the caveat that the promise gap is always close to 1. The general case is left open for future work.

Theorem 6.7. $\mathsf{ASSHSV}_\varepsilon$ *is complete for* ε-$\mathsf{QMA}(2) := \bigcup_{c\in 1-\varepsilon^{\omega(1)}, s\in 1-\varepsilon^{O(1)}} \mathsf{QMA}_{c,s}(2)$ *with $\varepsilon \in n^{-O(1)}$.*

Proof. For containment, observe that applying H to the proof $|\psi\rangle$ in Lemma 6.1 succeeds with a probability of at least $\||H|\psi\rangle\|/\mathrm{poly}(n)$ and at most $\|H|\psi\rangle\| \cdot \mathrm{poly}(n)$. In the YES-case, the verifier therefore accepts with probability at least $1 - \varepsilon^{\omega(1)}$, and in the NO-case, it accepts with probability at most $1 - \varepsilon^{O(1)}$.

Hardness follows again from [CS12], noting that the Hamiltonian H constructed for an N-gate $\mathsf{QMA}_{c,s}(2)$-verifier is positive semidefinite, and a history state for a proof accepted with probability c, has energy $(1-c)/\mathrm{poly}(N) \leq \varepsilon^{\omega(1)}$. In the NO-case, we have $\langle\psi|H|\psi\rangle \geq (1-s)^{O(1)}/\mathrm{poly}(N) \geq \varepsilon^{O(1)}$ for all $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$. □

6.3 Clique homology

Theorem 6.8. GCH *is* $\mathsf{QMA}_1^{\mathcal{G}_2}$*-complete.*

Proof. Containment follows from Lemma 6.2 since the Laplacian is sparse by Lemma 2.18. Hardness follows from a slight modification of the hardness proof of King and Kohler [KK23].

They show $\mathsf{GCH} \in \mathsf{QMA}$ and GCH is $\mathsf{QMA}_1^{\mathcal{G}_{\mathrm{Pyth}}}$-hard, where $\mathcal{G}_{\mathrm{Pyth}} = \{\mathsf{CX}, U_{\mathrm{Pyth}}\}$ with the Pythagorean gate $U_{\mathrm{Pyth}} = \frac{1}{5}\left(\begin{smallmatrix} 3 & 4 \\ -4 & 3 \end{smallmatrix}\right)$. By Theorem 3.2, $\mathsf{QMA}_1^{\mathcal{G}_{\mathrm{Pyth}}} \subseteq \mathsf{QMA}_1^{\mathcal{G}_2}$, but we are not aware of any lower bounds for $\mathsf{QMA}_1^{\mathcal{G}_{\mathrm{Pyth}}}$, since it is unclear how to even perform classical computation with perfect completeness using $\mathcal{G}_{\mathrm{Pyth}}$, although the gateset is certainly universal. It is straightforward to modify their construction to work with the gateset $\mathcal{G}_2$. A minor issue is that only the correctness for gadgets of the form $|\phi\rangle\langle\phi|$ is proven in [KK23] (although more general gadgets are defined), where $|\phi\rangle$ is a superposition of at most two 4-qubit standard basis states, or multiple 3-qubit standard basis states. Our 4-QSAT construction in Theorem 4.2 for $\mathcal{G}_2$ has this structure as can be seen in Appendix D. □

Theorem 6.9. CH *is* PSPACE*-complete.*

Proof. Containment follows from Lemma 6.1 and $\mathsf{PSPACE} = \mathsf{QMA}_{1,1-1/\exp(n)}$ [Li22]. Hardness follows from the fact that the $\mathsf{QMA}_{1,1-1/\exp(n)}$ protocol for PSPACE in [Li22, Algorithm 8] effectively just verifies the history state for a classical computation, and can therefore be implemented with $\mathcal{G}_2$. Then we can just embed the corresponding 4-QSAT instance into a clique homology as in Theorem 6.8. By [KK23, Theorem 10.7], we have for the Laplacian Δ^{2n-1}, $\lambda_{\min}(\Delta^{2n-1}) = 0$ iff $\lambda_{\min}(H) = 0$, where n is the number of qubits of the Hamiltonian H. □

Acknowledgements

I thank Tamara Kohler and Marcos Crichigno for helpful discussions, and especially Tamara Kohler for helping me understand Reference [KK23]. I also thank my supervisor Sevag Gharibian for his support and many discussions. DR was supported by the DFG under grant number 432788384.

References

[Aar09] S. Aaronson. "On perfect completeness for QMA." In: *Quantum Info. Comput.* 9.1 (Jan. 2009), pp. 81–89. ISSN: 1533-7146.

[AGK+24] M. Amy, A. N. Glaudell, S. Kelso, W. Maxwell, S. S. Mendelson, and N. J. Ross. "Exact Synthesis of Multiqubit Clifford-Cyclotomic Circuits." In: *Reversible Computation.* Ed. by T. Æ. Mogensen and Ł. Mikulski. Cham: Springer Nature Switzerland, 2024, pp. 238–245. ISBN: 978-3-031-62076-8.

[AGR20] M. Amy, A. N. Glaudell, and N. J. Ross. "Number-Theoretic Characterizations of Some Restricted Clifford+T Circuits." In: *Quantum* 4 (Apr. 2020), p. 252. ISSN: 2521-327X. DOI: 10.22331/q-2020-04-06-252.

[APT79] B. Aspvall, M. F. Plass, and R. E. Tarjan. "A Linear-Time Algorithm for Testing the Truth of Certain Quantified Boolean Formulas." In: *Information Processing Letters* 8.3 (1979), pp. 121–123.

[ASSZ16] I. Arad, M. Santha, A. Sundaram, and S. Zhang. "Linear Time Algorithm for Quantum 2SAT." In: *43rd International Colloquium on Automata, Languages, and Programming (ICALP 2016).* Vol. 55. Leibniz International Proceedings in Informatics (LIPIcs). 2016, 15:1–15:14.

[AT03] D. Aharonov and A. Ta-Shma. "Adiabatic quantum state generation and statistical zero knowledge." In: *Proceedings of the Thirty-Fifth Annual ACM Symposium on Theory of Computing.* STOC '03. San Diego, CA, USA: Association for Computing Machinery, 2003, pp. 20–29. ISBN: 1581136749. DOI: 10.1145/780542.780546.

[BCC+14] D. W. Berry, A. M. Childs, R. Cleve, R. Kothari, and R. D. Somma. "Exponential Improvement in Precision for Simulating Sparse Hamiltonians." In: *Proceedings of the Forty-Sixth Annual ACM Symposium on Theory of Computing.* STOC '14. New York, New York: Association for Computing Machinery, 2014, pp. 283–292. ISBN: 9781450327107. DOI: 10.1145/2591796.2591854.

[BG16] N. de Beaudrap and S. Gharibian. "A Linear Time Algorithm for Quantum 2-SAT." In: *31st Conference on Computational Complexity (CCC 2016).* Vol. 50. 2016, 27:1–27:21.

[BG21] A. Bouland and T. Giurgica-Tiron. *Efficient Universal Quantum Compilation: An Inverse-free Solovay-Kitaev Algorithm.* 2021. arXiv: 2112.02040 [quant-ph].

[BK05] S. Bravyi and A. Kitaev. "Universal quantum computation with ideal Clifford gates and noisy ancillas." In: *Phys. Rev. A* 71 (2 Feb. 2005), p. 022316. DOI: 10.1103/PhysRevA.71.022316.

[Bra06] S. Bravyi. *Efficient algorithm for a quantum analogue of 2-SAT.* 2006. arXiv: quant-ph/0602108 [quant-ph].

[CCD+11] J. Chen, X. Chen, R. Duan, Z. Ji, and B. Zeng. "No-go theorem for one-way quantum computing on naturally occurring two-level systems." In: *Phys. Rev. A* 83 (5 May 2011), p. 050301. DOI: 10.1103/PhysRevA.83.050301.

[CK22] M. Crichigno and T. Kohler. *Clique Homology is QMA1-hard.* 2022. arXiv: 2209.11793 [quant-ph].

[CLN18] L. Caha, Z. Landau, and D. Nagaj. "Clocks in Feynman's computer and Kitaev's local Hamiltonian: Bias, gaps, idling, and pulse tuning." In: *Phys. Rev. A* 97 (6 June 2018), p. 062306. DOI: 10.1103/PhysRevA.97.062306.

[CM16] T. Cubitt and A. Montanaro. "Complexity Classification of Local Hamiltonian Problems." In: *SIAM Journal on Computing* 45.2 (Jan. 2016), pp. 268–316. ISSN: 0097-5397. DOI: 10.1137/140998287.

[Coo71] S. A. Cook. "The Complexity of Theorem-Proving Procedures." In: *Proceedings of the Third Annual ACM Symposium on Theory of Computing.* STOC '71. New York, NY, USA: Association for Computing Machinery, May 1971, pp. 151–158. ISBN: 978-1-4503-7464-4. DOI: 10.1145/800157.805047.

[CS12] A. Chailloux and O. Sattath. "The Complexity of the Separable Hamiltonian Problem." In: *2012 IEEE 27th Conference on Computational Complexity.* IEEE, June 2012. DOI: 10.1109/ccc.2012.42.

[CW12] A. M. Childs and N. Wiebe. "Hamiltonian Simulation Using Linear Combinations of Unitary Operations." In: *Quantum Info. Comput.* 12.11–12 (Nov. 2012), pp. 901–924. ISSN: 1533-7146.

[Die09] T. tom Dieck. *Representation Theory.* 2009.

[DN05] C. M. Dawson and M. A. Nielsen. *The Solovay-Kitaev algorithm.* 2005. arXiv: quant-ph/0505030 [quant-ph].

[DP60] M. Davis and H. Putnam. "A Computing Procedure for Quantification Theory." In: *Journal of the ACM* 7.3 (1960), p. 201.

[EIS76] S. Even, A. Itai, and A. Shamir. "On the Complexity of the Time Table and Multi-Commodity Flow Problems." In: *SIAM Journal on Computing* 5.4 (1976), pp. 691–703.

[ER08] L. Eldar and O. Regev. "Quantum SAT for a Qutrit-Cinquit Pair Is QMA1-Complete." In: *Automata, Languages and Programming.* Ed. by L. Aceto, I. Damgård, L. A. Goldberg, M. M. Halldórsson, A. Ingólfsdóttir, and I. Walukiewicz. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 881–892. ISBN: 978-3-540-70575-8.

[GJS76] M. R. Garey, D. S. Johnson, and L. Stockmeyer. "Some Simplified NP-complete Graph Problems." In: *Theoretical Computer Science* 1.3 (Feb. 1976), pp. 237–267. ISSN: 0304-3975. DOI: 10.1016/0304-3975(76)90059-1.

[GN13] D. Gosset and D. Nagaj. “Quantum 3-SAT Is QMA1-Complete.” In: *2013 IEEE 54th Annual Symposium on Foundations of Computer Science*. IEEE, Oct. 2013. DOI: 10.1109/focs.2013.86.

[Gol02] T. E. Goldberg. “Combinatorial Laplacians of Simplicial Complexes.” Senior Thesis. Bard College, 2002. URL: https://www2.stat.duke.edu/~sayan/forkate/CombinatorialLaplacians.pdf.

[GR23] S. Gharibian and D. Rudolph. “Quantum Space, Ground Space Traversal, and How to Embed Multi-Prover Interactive Proofs into Unentanglement.” In: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2023. DOI: 10.4230/LIPICS.ITCS.2023.53.

[GS13] B. Giles and P. Selinger. “Exact synthesis of multiqubit Clifford+T circuits.” In: *Phys. Rev. A* 87 (3 Mar. 2013), p. 032332. DOI: 10.1103/PhysRevA.87.032332.

[GZ11] O. Goldreich and D. Zuckerman. “Another Proof That $\mathcal{BPP} \subseteq \mathcal{PH}$ (and More).” In: *Studies in Complexity and Cryptography. Miscellanea on the Interplay between Randomness and Computation: In Collaboration with Lidor Avigad, Mihir Bellare, Zvika Brakerski, Shafi Goldwasser, Shai Halevi, Tali Kaufman, Leonid Levin, Noam Nisan, Dana Ron, Madhu Sudan, Luca Trevisan, Salil Vadhan, Avi Wigderson, David Zuckerman*. Ed. by O. Goldreich. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 40–53. ISBN: 978-3-642-22670-0. DOI: 10.1007/978-3-642-22670-0_6.

[HM13] A. W. Harrow and A. Montanaro. “Testing Product States, Quantum Merlin-Arthur Games and Tensor Optimization.” In: *J. ACM* 60.1 (Feb. 2013). ISSN: 0004-5411. DOI: 10.1145/2432622.2432625.

[JKNN12] S. P. Jordan, H. Kobayashi, D. Nagaj, and H. Nishimura. “Achieving perfect completeness in classical-witness quantum merlin-arthur proof systems.” In: *Quantum Info. Comput.* 12.5–6 (May 2012), pp. 461–471. ISSN: 1533-7146.

[JWZ11] Z. Ji, Z. Wei, and B. Zeng. “Complete characterization of the ground-space structure of two-body frustration-free Hamiltonians for qubits.” In: *Phys. Rev. A* 84 (4 Oct. 2011), p. 042338. DOI: 10.1103/PhysRevA.84.042338.

[Kar72] R. M. Karp. “Reducibility among Combinatorial Problems.” In: *Complexity of Computer Computations: Proceedings of a Symposium on the Complexity of Computer Computations, Held March 20–22, 1972, at the IBM Thomas J. Watson Research Center, Yorktown Heights, New York, and Sponsored by the Office of Naval Research, Mathematics Program, IBM World Trade Corporation, and the IBM Research Mathematical Sciences Department*. Ed. by R. E. Miller, J. W. Thatcher, and J. D. Bohlinger. The IBM Research Symposia Series. Boston, MA: Springer US, 1972, pp. 85–103. ISBN: 978-1-4684-2001-2. DOI: 10.1007/978-1-4684-2001-2_9.

[Kit97] A. Y. Kitaev. “Quantum computations: algorithms and error correction.” In: *Russian Mathematical Surveys* 52.6 (Dec. 1997), p. 1191. DOI: 10.1070/RM1997v052n06ABEH002155.

[KK23] R. King and T. Kohler. *Promise Clique Homology on weighted graphs is QMA$_1$-hard and contained in QMA*. 2023. arXiv: 2311.17234 [quant-ph].

[KKR05] J. Kempe, A. Kitaev, and O. Regev. *The Complexity of the Local Hamiltonian Problem*. 2005. arXiv: quant-ph/0406180 [quant-ph].

[KL21] W. M. Kirby and P. J. Love. “Variational Quantum Eigensolvers for Sparse Hamiltonians.” In: *Physical Review Letters* 127.11 (Sept. 2021). DOI: 10.1103/physrevlett.127.110503.

[KLN15] H. Kobayashi, F. Le Gall, and H. Nishimura. “Stronger Methods of Making Quantum Interactive Proofs Perfectly Complete.” In: *SIAM Journal on Computing* 44.2 (2015), pp. 243–289. DOI: 10.1137/140971944.

[Kro67] M. R. Krom. “The Decision Problem for a Class of First-Order Formulas in Which All Disjunctions Are Binary.” In: *Zeitschrift für Mathematische Logik und Grundlagen der Mathematik* 13 (1967), pp. 15–20.

[KSV02] A. Y. Kitaev, A. H. Shen, and M. N. Vyalyi. *Classical and Quantum Computation.* USA: American Mathematical Society, 2002. ISBN: 0821832298.

[KW00] A. Kitaev and J. Watrous. “Parallelization, amplification, and exponential time simulation of quantum interactive proof systems.” In: *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing.* STOC ’00. Portland, Oregon, USA: Association for Computing Machinery, 2000, pp. 608–617. ISBN: 1581131844. DOI: 10.1145/335305.335387.

[LC17] G. H. Low and I. L. Chuang. “Optimal Hamiltonian Simulation by Quantum Signal Processing.” In: *Phys. Rev. Lett.* 118 (1 Jan. 2017), p. 010501. DOI: 10.1103/PhysRevLett.118.010501.

[Lev73] L. Levin. “Universal Search Problems.” In: *Problems of Information Transmission* 9.3 (1973), pp. 265–266.

[LGZ16] S. Lloyd, S. Garnerone, and P. Zanardi. “Quantum algorithms for topological and geometric analysis of data.” In: *Nature Communications* 7.1 (Jan. 2016), p. 10138. ISSN: 2041-1723. DOI: 10.1038/ncomms10138.

[Li22] Y. Li. *A Simple Proof of PreciseQMA = PSPACE.* 2022. arXiv: 2206.09230 [quant-ph].

[McK10] M. McKague. “Quantum Information Processing with Adversarial Devices.” PhD thesis. 2010. URL: http://hdl.handle.net/10012/5259.

[McK13] M. McKague. “On the power quantum computation over real hilbert spaces.” In: *International Journal of Quantum Information* 11.01 (2013). DOI: 10.1142/S0219749913500019.

[Mye86] G. Myerson. “How Small Can a Sum of Roots of Unity Be?” In: *The American Mathematical Monthly* 93.6 (1986), pp. 457–459. DOI: 10.1080/00029890.1986.11971853.

[Nag08] D. Nagaj. *Local Hamiltonians in Quantum Computation.* Aug. 2008. DOI: 10.48550/arXiv.0808.2117.

[NC10] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition.* Cambridge University Press, 2010. DOI: 10.1017/CBO9780511976667.

[Pap91] C. Papadimitriou. “On Selecting a Satisfying Truth Assignment.” In: *32nd Annual IEEE Symposium on Foundations of Computing (FOCS 1991).* 1991, pp. 163–169.

[Qui59] W. V. Quine. “On Cores and Prime Implicants of Truth Functions.” In: *The American Mathematical Monthly* 66.5 (1959), pp. 755–760.

[RGN24] D. Rudolph, S. Gharibian, and D. Nagaj. *Quantum 2-SAT on low dimensional systems is* QMA_1*-complete: Direct embeddings and black-box simulation.* 2024. arXiv: 2401.02368 [quant-ph].

[Rom06] S. Roman. *Field Theory.* 2nd ed. Graduate Texts in Mathematics. Springer, 2006.

[Rud24] D. Rudolph. *Supplementary material.* 2024. URL: https://github.com/DorianRudolph/QMA1-gateset-paper.

[The24] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 10.4).* https://www.sagemath.org. 2024.

[Vau05] V. Vaughn. *Extension fields isomorphic to fields of matrices.* 2005. URL: https://math.stackexchange.com/q/1180429.

[Was18] L. Wasserman. “Topological Data Analysis.” In: *Annual Review of Statistics and Its Application* 5.Volume 5, 2018 (2018), pp. 501–532. ISSN: 2326-831X. DOI: https://doi.org/10.1146/annurev-statistics-031017-100045.

[ZF87] S. Zachos and M. Furer. “Probabilistic quantifiers vs. distrustful adversaries.” In: *Proc. of the Seventh Conference on Foundations of Software Technology and Theoretical Computer Science*. Pune, India: Springer-Verlag, 1987, pp. 443–455. ISBN: 0387186255.

A Omitted proofs

Proof of Lemma 2.17. See [KK23, Eq. 5] for Eq. (4a). Note that $\partial^k|\sigma'\rangle$ only has support on those $|\tau\rangle$ with $\sigma \supset \tau \in \mathcal{K}^{k-1}$. Then

$$\partial^k|\sigma'\rangle = \sum_{j=0}^{k} |\sigma'_{-j}\rangle\langle\sigma'_{-j}|(d^{k-1})^\dagger|\sigma'\rangle = \sum_{j=0}^{k}(-1)^j \cdot w(v_j)|\sigma'_{-j}\rangle, \tag{52}$$

as $\langle\sigma'_{-j}|(d^{k-1})^\dagger|\sigma'\rangle = w(v_j)\Big\langle\sigma'_{-j}\Big|[v_j] + \sigma_{-j}\Big\rangle = (-1)^j \cdot w(v_j)$ because moving v_j in $[v_j] + \sigma_{-j}$ to the j-th position requires j swaps with 0 being the first position. □

Proof of Lemma 2.18. Recall $\Delta^k = d^{k-1}\partial^k + \partial^{k+1}d^k = (\partial^k)^\dagger\partial^k + (d^k)^\dagger d^k$. If $\sigma = \tau$, then we have by Eq. (4)

$$\langle\sigma'|\Delta^k|\sigma'\rangle = \|\partial^k|\sigma'\rangle\|^2 + \|d^k|\sigma'\rangle\|^2 = \sum_{v\in\sigma} w(v)^2 + \sum_{u\in\mathrm{up}(\sigma)} w(u)^2. \tag{53}$$

If σ and τ are not upper adjacent, then $d^k|\sigma'\rangle$ and $d^k|\tau'\rangle$ are orthogonal. Thus for the second and third case, we have

$$\langle\sigma'|\Delta^k|\tau'\rangle = \Big(\langle\sigma'|(\partial^k)^\dagger\Big)\,|\eta'\rangle\langle\eta'|\,\Big(\partial^k|\tau'\rangle\Big) = \pm w(v_\sigma)w(v_\tau), \tag{54}$$

since the common lower simplex η is always unique.

For the fourth case, consider the subcase that σ and τ are upper adjacent. Since then $|\sigma \cup \tau| = k + 2$, we have $|\sigma \cap \tau| = k$. Thus we can write (up to permutation) $\sigma = [v_\sigma, v_0, \ldots, v_{k-1}]$ and $\tau = [v_\tau, v_0, \ldots, v_{k-1}]$ (so that they have a similar lower complex). Thus,

$$\begin{aligned}\langle\sigma'|\Delta^k|\tau'\rangle &= \langle\sigma'|(\partial^k)^\dagger\partial^k|\tau'\rangle + \langle\sigma'|(d^k)^\dagger d^k|\tau'\rangle \\ &= w(v_\sigma)w(v_\tau) + w(v_\sigma)w(v_\tau)\big\langle[v_\tau, v_\sigma, v_0, \ldots, v_{k-1}]'\big|[v_\sigma, v_\tau, v_0, \ldots, v_{k-1}]'\big\rangle = 0.\end{aligned} \tag{55}$$

Finally, if σ and τ do not have a common lower complex and are not upper adjacent, then $d^k|\sigma\rangle, d^k|\tau\rangle$ are orthogonal as well as $\partial^k|\sigma\rangle, \partial^k|\tau\rangle$. □

Proof of Proposition 3.4. Let $\mathcal{G} = \{U_1, \ldots, U_k\}$ with $U_i \in \mathbb{Q}(\zeta_n)^{d\times d}$ for all $i = 1, \ldots, k$. We can write each U_i as

$$U_i = \sum_{j=0}^{n-1} \zeta_n^j \frac{A_{ij}}{a_{ij}} \tag{56}$$

with $A_{ij} \in \mathbb{Z}^{d\times d}$ and $a_{ij} \in \mathbb{N}$. Hence, we can also write any product of the U_i (possibly acting on different qubits) as $\frac{1}{b}\sum_{j=0}^{n-1}\zeta_n^j B_j$ with $B_j \in \mathbb{Z}^{d\times d}$ and b a product of the a_{ij}.

Therefore, it is clearly not possible to implement exactly all Pythagorean unitaries (this term was introduced in [CK22]) of the form

$$\frac{1}{c}\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \tag{57}$$

with $a^2 + b^2 = c^2$ and prime c, as there exist an infinite number of Pythagorean primes c. □

B Examples for simulation of cyclotomic gates

Below we show how $\sqrt{H}$ is simulated in Lemma 3.14, writing all matrix elements in the integral basis $\{1, \zeta_8, \zeta_8^2, \zeta_8^3\}$:

$$\begin{pmatrix} -\frac{1}{2}\zeta_8^3 + \frac{1}{2}\zeta_8^2 + \frac{1}{2} & -\frac{1}{2}\zeta_8^3 \\ -\frac{1}{2}\zeta_8^3 & \frac{1}{2}\zeta_8^3 + \frac{1}{2}\zeta_8^2 + \frac{1}{2} \end{pmatrix} \xmapsto{\Psi} \left(\begin{array}{cccc|cccc} \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & 0 & 0 & \frac{1}{2} & 0 & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & 0 & 0 & \frac{1}{2} & 0 \\ \frac{1}{2} & 0 & \frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 & \frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} & 0 & \frac{1}{2} & -\frac{1}{2} & 0 & 0 & 0 \\ \hline 0 & \frac{1}{2} & 0 & 0 & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & 0 \\ 0 & 0 & \frac{1}{2} & 0 & 0 & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ 0 & 0 & 0 & \frac{1}{2} & \frac{1}{2} & 0 & \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & 0 & 0 & 0 & \frac{1}{2} & \frac{1}{2} & 0 & \frac{1}{2} \end{array}\right) \tag{58}$$

Also for the QFT F_8 on 3 qubits:

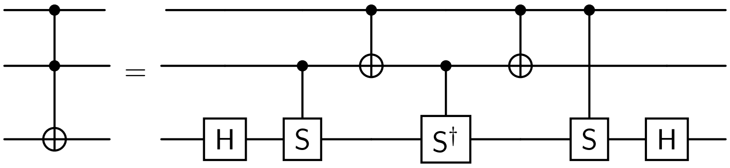
$$\begin{pmatrix}
-\frac{1}{4}\zeta_8^3+\frac{1}{4}\zeta_8 & -\frac{1}{4}\zeta_8^3+\frac{1}{4}\zeta_8 & -\frac{1}{4}\zeta_8^3+\frac{1}{4}\zeta_8 & -\frac{1}{4}\zeta_8^3+\frac{1}{4}\zeta_8 & -\frac{1}{4}\zeta_8^3+\frac{1}{4}\zeta_8 & -\frac{1}{4}\zeta_8^3+\frac{1}{4}\zeta_8 & -\frac{1}{4}\zeta_8^3+\frac{1}{4}\zeta_8 & -\frac{1}{4}\zeta_8^3+\frac{1}{4}\zeta_8 \\
-\frac{1}{4}\zeta_8^3+\frac{1}{4}\zeta_8 & \frac{1}{4}\zeta_8^2+\frac{1}{4} & \frac{1}{4}\zeta_8^3+\frac{1}{4}\zeta_8 & \frac{1}{4}\zeta_8^2-\frac{1}{4} & \frac{1}{4}\zeta_8^3-\frac{1}{4}\zeta_8 & -\frac{1}{4}\zeta_8^2-\frac{1}{4} & -\frac{1}{4}\zeta_8^3-\frac{1}{4}\zeta_8 & -\frac{1}{4}\zeta_8^2+\frac{1}{4} \\
-\frac{1}{4}\zeta_8^3+\frac{1}{4}\zeta_8 & \frac{1}{4}\zeta_8^3+\frac{1}{4}\zeta_8 & \frac{1}{4}\zeta_8^3-\frac{1}{4}\zeta_8 & -\frac{1}{4}\zeta_8^3-\frac{1}{4}\zeta_8 & -\frac{1}{4}\zeta_8^3+\frac{1}{4}\zeta_8 & \frac{1}{4}\zeta_8^3+\frac{1}{4}\zeta_8 & \frac{1}{4}\zeta_8^3-\frac{1}{4}\zeta_8 & -\frac{1}{4}\zeta_8^3-\frac{1}{4}\zeta_8 \\
-\frac{1}{4}\zeta_8^3+\frac{1}{4}\zeta_8 & \frac{1}{4}\zeta_8^2-\frac{1}{4} & -\frac{1}{4}\zeta_8^3-\frac{1}{4}\zeta_8 & \frac{1}{4}\zeta_8^2+\frac{1}{4} & \frac{1}{4}\zeta_8^3-\frac{1}{4}\zeta_8 & -\frac{1}{4}\zeta_8^2+\frac{1}{4} & \frac{1}{4}\zeta_8^3+\frac{1}{4}\zeta_8 & -\frac{1}{4}\zeta_8^2-\frac{1}{4} \\
-\frac{1}{4}\zeta_8^3+\frac{1}{4}\zeta_8 & \frac{1}{4}\zeta_8^3-\frac{1}{4}\zeta_8 & -\frac{1}{4}\zeta_8^3+\frac{1}{4}\zeta_8 & \frac{1}{4}\zeta_8^3-\frac{1}{4}\zeta_8 & -\frac{1}{4}\zeta_8^3+\frac{1}{4}\zeta_8 & \frac{1}{4}\zeta_8^3-\frac{1}{4}\zeta_8 & -\frac{1}{4}\zeta_8^3+\frac{1}{4}\zeta_8 & \frac{1}{4}\zeta_8^3-\frac{1}{4}\zeta_8 \\
-\frac{1}{4}\zeta_8^3+\frac{1}{4}\zeta_8 & -\frac{1}{4}\zeta_8^2-\frac{1}{4} & \frac{1}{4}\zeta_8^3+\frac{1}{4}\zeta_8 & -\frac{1}{4}\zeta_8^2+\frac{1}{4} & \frac{1}{4}\zeta_8^3-\frac{1}{4}\zeta_8 & \frac{1}{4}\zeta_8^2+\frac{1}{4} & -\frac{1}{4}\zeta_8^3-\frac{1}{4}\zeta_8 & \frac{1}{4}\zeta_8^2-\frac{1}{4} \\
-\frac{1}{4}\zeta_8^3+\frac{1}{4}\zeta_8 & -\frac{1}{4}\zeta_8^3-\frac{1}{4}\zeta_8 & \frac{1}{4}\zeta_8^3-\frac{1}{4}\zeta_8 & \frac{1}{4}\zeta_8^3+\frac{1}{4}\zeta_8 & -\frac{1}{4}\zeta_8^3+\frac{1}{4}\zeta_8 & -\frac{1}{4}\zeta_8^3-\frac{1}{4}\zeta_8 & \frac{1}{4}\zeta_8^3-\frac{1}{4}\zeta_8 & \frac{1}{4}\zeta_8^3+\frac{1}{4}\zeta_8 \\
-\frac{1}{4}\zeta_8^3+\frac{1}{4}\zeta_8 & -\frac{1}{4}\zeta_8^2+\frac{1}{4} & -\frac{1}{4}\zeta_8^3-\frac{1}{4}\zeta_8 & -\frac{1}{4}\zeta_8^2-\frac{1}{4} & \frac{1}{4}\zeta_8^3-\frac{1}{4}\zeta_8 & \frac{1}{4}\zeta_8^2-\frac{1}{4} & \frac{1}{4}\zeta_8^3+\frac{1}{4}\zeta_8 & \frac{1}{4}\zeta_8^2+\frac{1}{4}
\end{pmatrix}$$

$$\xmapsto{\Psi}$$

$$\left(\begin{array}{cccc|cccc|cccc|cccc|cccc|cccc|cccc|cccc}
0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} \\
\frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 \\
0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} \\
-\frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 \\
\hline
0 & \frac{1}{4} & 0 & -\frac{1}{4} & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & 0 & \frac{1}{4} & 0 & \frac{1}{4} & \frac{1}{4} & 0 & \frac{1}{4} & 0 \\
\frac{1}{4} & 0 & \frac{1}{4} & 0 & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & 0 & \frac{1}{4} & 0 & \frac{1}{4} \\
0 & \frac{1}{4} & 0 & \frac{1}{4} & \frac{1}{4} & 0 & \frac{1}{4} & 0 & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & -\frac{1}{4} & 0 & \frac{1}{4} & 0 \\
-\frac{1}{4} & 0 & \frac{1}{4} & 0 & 0 & \frac{1}{4} & 0 & \frac{1}{4} & \frac{1}{4} & 0 & \frac{1}{4} & 0 & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & 0 & -\frac{1}{4} & 0 & \frac{1}{4} \\
\hline
0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} \\
\frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 \\
0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} \\
-\frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 \\
\hline
0 & \frac{1}{4} & 0 & -\frac{1}{4} & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & 0 & \frac{1}{4} & 0 & \frac{1}{4} & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & \frac{1}{4} & 0 & \frac{1}{4} & 0 & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & -\frac{1}{4} & 0 & \frac{1}{4} & 0 \\
\frac{1}{4} & 0 & \frac{1}{4} & 0 & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & 0 & \frac{1}{4} & 0 & \frac{1}{4} & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & 0 & -\frac{1}{4} & 0 & \frac{1}{4} \\
0 & \frac{1}{4} & 0 & \frac{1}{4} & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & \frac{1}{4} & 0 & \frac{1}{4} & 0 & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 \\
-\frac{1}{4} & 0 & \frac{1}{4} & 0 & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & 0 & \frac{1}{4} & 0 & \frac{1}{4} & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & \frac{1}{4} & 0 & \frac{1}{4} & 0 & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} \\
\hline
0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} \\
\frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 \\
0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} \\
-\frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 \\
\hline
0 & \frac{1}{4} & 0 & -\frac{1}{4} & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & \frac{1}{4} & 0 & \frac{1}{4} & 0 & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & 0 & \frac{1}{4} & 0 & \frac{1}{4} & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 \\
\frac{1}{4} & 0 & \frac{1}{4} & 0 & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & 0 & \frac{1}{4} & 0 & \frac{1}{4} & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} \\
0 & \frac{1}{4} & 0 & \frac{1}{4} & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & \frac{1}{4} & 0 & \frac{1}{4} & 0 & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & \frac{1}{4} & 0 & -\frac{1}{4} & 0 \\
-\frac{1}{4} & 0 & \frac{1}{4} & 0 & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & \frac{1}{4} & 0 & \frac{1}{4} & 0 & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & 0 & \frac{1}{4} & 0 & \frac{1}{4} & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & 0 & \frac{1}{4} & 0 & -\frac{1}{4} \\
\hline
0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} \\
\frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 \\
0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} \\
-\frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & \frac{1}{4} & 0 \\
\hline
0 & \frac{1}{4} & 0 & -\frac{1}{4} & \frac{1}{4} & 0 & \frac{1}{4} & 0 & 0 & \frac{1}{4} & 0 & \frac{1}{4} & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & \frac{1}{4} & 0 & -\frac{1}{4} & 0 \\
\frac{1}{4} & 0 & \frac{1}{4} & 0 & 0 & \frac{1}{4} & 0 & \frac{1}{4} & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & 0 & \frac{1}{4} & 0 & -\frac{1}{4} \\
0 & \frac{1}{4} & 0 & \frac{1}{4} & -\frac{1}{4} & 0 & \frac{1}{4} & 0 & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & \frac{1}{4} & 0 & \frac{1}{4} & 0 \\
-\frac{1}{4} & 0 & \frac{1}{4} & 0 & 0 & -\frac{1}{4} & 0 & \frac{1}{4} & -\frac{1}{4} & 0 & -\frac{1}{4} & 0 & 0 & -\frac{1}{4} & 0 & -\frac{1}{4} & \frac{1}{4} & 0 & -\frac{1}{4} & 0 & 0 & \frac{1}{4} & 0 & -\frac{1}{4} & \frac{1}{4} & 0 & \frac{1}{4} & 0 & 0 & \frac{1}{4} & 0 & \frac{1}{4}
\end{array}\right)$$

C Toffoli from CS gate

Construction of Toffoli gate from $\{\omega\mathsf{H}, \mathsf{S}, \mathsf{CS}\}$ analogous to [NC10, Figure 4.8] using $\mathsf{CS}^2 = \mathsf{CZ}, \mathsf{CS}^3 = \mathsf{CS}^\dagger, \mathsf{CX} = (I \otimes \mathsf{H})\mathsf{CZ}(I \otimes \mathsf{H}), \mathsf{CCX} = (I \otimes I \otimes \mathsf{H})\mathsf{CCZ}(I \otimes I \otimes \mathsf{H})$:



D Quantum 4-SAT for $\mathcal{G}_2$

The correctness of this construction follows from the Nullspace Connection Lemma (see Lemma 5.5). We label the logical qu-5-its as $\mathbf{u}, \mathbf{a_1}, \mathbf{a_2}, \mathbf{a_3}, \mathbf{d}$ (unborn, alive 1–3, dead) and implement them using 4 physical qubits:

$$\begin{aligned} |\mathbf{u}\rangle &= |1000\rangle \\ |\mathbf{a_1}\rangle &= |0010\rangle \\ |\mathbf{a_2}\rangle &= |0011\rangle \\ |\mathbf{a_3}\rangle &= |0001\rangle \\ |\mathbf{d}\rangle &= |0100\rangle \end{aligned} \tag{59}$$

The remaining 4-qubit states are penalized with 4-local projectors. We can also easily enforce a clock space $|C_1\rangle, \ldots, |C_T\rangle$ of the form:

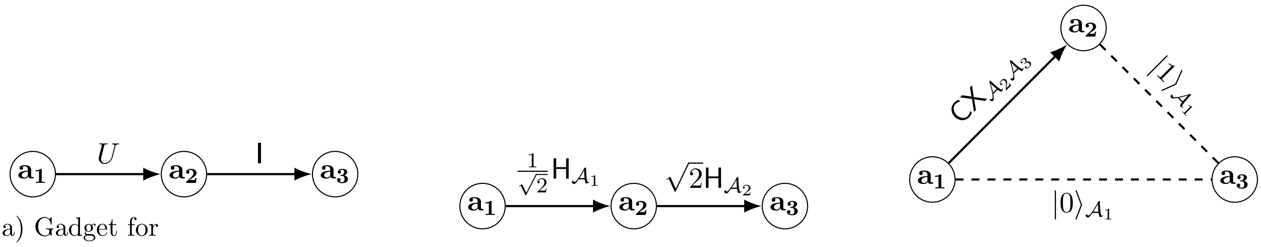
$$\begin{aligned}
|C_1\rangle &= |\ \mathbf{u} \quad \mathbf{u} \quad \mathbf{u} \quad \cdots \quad \mathbf{u}\ \rangle \\
|C_2\rangle &= |\ \mathbf{a_1} \quad \mathbf{u} \quad \mathbf{u} \quad \cdots \quad \mathbf{u}\ \rangle \\
|C_3\rangle &= |\ \mathbf{a_2} \quad \mathbf{u} \quad \mathbf{u} \quad \cdots \quad \mathbf{u}\ \rangle \\
|C_4\rangle &= |\ \mathbf{a_3} \quad \mathbf{u} \quad \mathbf{u} \quad \cdots \quad \mathbf{u}\ \rangle \\
|C_5\rangle &= |\ \mathbf{d} \quad \mathbf{u} \quad \mathbf{u} \quad \cdots \quad \mathbf{u}\ \rangle \\
|C_6\rangle &= |\ \mathbf{d} \quad \mathbf{a_1} \quad \mathbf{u} \quad \cdots \quad \mathbf{u}\ \rangle \\
|C_7\rangle &= |\ \mathbf{d} \quad \mathbf{a_2} \quad \mathbf{u} \quad \cdots \quad \mathbf{u}\ \rangle \\
|C_8\rangle &= |\ \mathbf{d} \quad \mathbf{a_3} \quad \mathbf{u} \quad \cdots \quad \mathbf{u}\ \rangle \\
|C_9\rangle &= |\ \mathbf{d} \quad \mathbf{d} \quad \mathbf{u} \quad \cdots \quad \mathbf{u}\ \rangle \\
|C_{10}\rangle &= |\ \mathbf{d} \quad \mathbf{d} \quad \mathbf{a_1} \quad \cdots \quad \mathbf{u}\ \rangle \\
&\vdots \\
|C_T\rangle &= |\ \mathbf{d} \quad \mathbf{d} \quad \mathbf{d} \quad \cdots \quad \mathbf{d}\ \rangle
\end{aligned}$$

Now we have 2-local transitions between, e.g., $|C_2\rangle, |C_3\rangle, |C_4\rangle$, and 4-local transitions between, e.g., $|C_4\rangle$ and $|C_5\rangle$. Indexing the physical qubits from 1 to 8, we can implement the transitions

$$|\mathbf{a_3u}\rangle \leftrightarrow |\mathbf{du}\rangle \quad \text{as} \quad (|0011\rangle - |1001\rangle)(\langle 0011| - \langle 1001|)_{2,3,4,5}, \tag{60}$$

$$|\mathbf{du}\rangle \leftrightarrow |\mathbf{da_1}\rangle \quad \text{as} \quad (|1100\rangle - |1010\rangle)(\langle 1100| - \langle 1010|)_{2,5,7,8}. \tag{61}$$

Thanks to Lemma 5.5, it now suffices to construct the gate gadgets on three timesteps $|\mathbf{a_1}\rangle, |\mathbf{a_2}\rangle, |\mathbf{a_3}\rangle$. See Section 5 for a more detailed description of how to apply the lemma. The gadgets are graphically



(a) Gadget for $U \in \{\mathsf{X}_{\mathcal{A}_1}, \mathsf{CX}_{\mathcal{A}_1\mathcal{A}_2}\}$.

(b) Gadget for $\mathsf{H} \otimes \mathsf{H}$.

(c) Gadget for CCX.

Figure 3: Gadgets to implement $\mathcal{G}_2$ with 4-QSAT. Arrows indicate unitary transitions, and dashed edges conditional transitions. The qubits of the computational register are denoted $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3$.

depicted in Fig. 3, and formally defined below.

$$H_{\mathsf{X}} = h_{12}(\mathsf{X}_{\mathcal{A}_1}) + h_{23}(\mathsf{I}) \tag{62}$$

$$H_{\mathsf{CX}} = h_{12}(\mathsf{CX}_{\mathcal{A}_1\mathcal{A}_2}) + h_{23}(\mathsf{I}) \tag{63}$$

$$H_{\mathsf{H}\otimes\mathsf{H}} = 2 \cdot h_{12}\left(\frac{1}{\sqrt{2}}\mathsf{H}_{\mathcal{A}_1}\right) + h_{23}\left(\sqrt{2}\mathsf{H}_{\mathcal{A}_2}\right) \tag{64}$$

$$H_{\mathsf{CCX}} = h_{12}(\mathsf{CX}_{\mathcal{A}_2\mathcal{A}_3}) + |0\rangle\langle 0|_{\mathcal{A}_1} \otimes h_{13}(\mathsf{I}) + |1\rangle\langle 1|_{\mathcal{A}_1} \otimes h_{23}(\mathsf{I}) \tag{65}$$

$$h_{ij}(U) = (I \otimes |\mathbf{a_i}\rangle\langle\mathbf{a_i}|_{\mathcal{C}} + I \otimes |\mathbf{a_j}\rangle\langle\mathbf{a_j}| - U^\dagger \otimes |\mathbf{a_i}\rangle\langle\mathbf{a_j}| - U \otimes |\mathbf{a_j}\rangle\langle\mathbf{a_i}|)_{\mathcal{A},\mathcal{C}} \tag{66}$$

The nullspaces of the gadgets are computed in the supplementary material [Rud24].

For Theorem 6.8, note that we can write all above gadgets $H_U = \sum_l |\phi_l\rangle\langle\phi_l|$, such that each $|\phi_l\rangle$ is an integer superposition of standard basis states on at most 4 qubits, and 4-qubit $|\phi_l\rangle$ are superpositions of only two standard basis states.