Low overhead universality and quantum supremacy using only Z-control

Brian Barch,1,2 Razieh Mohseninia,2 and Daniel Lidar1,2,3,4

1Department of Physics and Astronomy, University of Southern California, Los Angeles, California 90089, USA
2Center for Quantum Information Science & Technology, University of Southern California, Los Angeles, California 90089, USA
3Department of Electrical and Computer Engineering, University of Southern California, Los Angeles, California 90089, USA
4Department of Chemistry, University of Southern California, Los Angeles, California 90089, USA

We consider a model of quantum computation we call “Varying-Z” (VZ), defined by applying controllable Z-diagonal Hamiltonians in the presence of a uniform and constant external X-field, and prove that it is universal, even in 1D. Universality is demonstrated by construction of a universal gate set with $O(1)$ depth overhead. We then use this construction to describe a circuit whose output distribution cannot be classically simulated unless the polynomial hierarchy collapses, with the goal of providing a low-resource method of demonstrating quantum supremacy. The VZ model can achieve quantum supremacy in $O(n)$ depth, equivalent to the random circuit sampling models despite a higher degree of homogeneity: it requires no individually addressed X-control.

I. INTRODUCTION

In the current era of noisy intermediate scale quantum computers [1], quantum architectures are limited by connectivity, gate fidelity, and various other sources of errors that limit both circuit depth and width. In response, various models of quantum computation have been developed that are designed to be relatively easy to implement on existing hardware. The strength of these models is then confirmed by demonstrating their ability to achieve universality [2–6] or quantum supremacy [7–15]. Universality is a stronger attribute, as it implies the ability to reproduce the quantum supremacy results of other models.

In this spirit, here we propose a model of quantum computation that is computationally universal even when restricted to a one-dimensional (1D) chain of qubits with only nearest-neighbor interactions and a limited degree of control. This “Varying-Z” (VZ) model is defined by applying a series of Z-diagonal Hamiltonians in the presence of a constant and homogeneous (i.e., qubit-permutation-invariant) X-field requiring no individually addressed control. We consider the VZ model both on a general graph and in 1D. The latter is theoretically motivated by the question of the quantum computational power of 1D systems [6, 16] and experiments with 1D systems, such as chains of fluxonium qubits [17], and chains of transmons which were used in a prequel to Google’s quantum supremacy work [18]. The general VZ model is physically motivated by physical systems subject to always-on transverse fields, such as superconducting flux-qubit architectures [19–22] which experience a small but always-on X-field in a quantum annealing context [23].

The outline of this paper is as follows: in Sec. II we review the previous results on the universality and supremacy of 1D models. In Sec. III we define our model and in Sec. IV we demonstrate universality by reconstructing a universal gate set. In Sec. V we apply this universality result to generate distributions known to demonstrate quantum supremacy, and in Sec. VI we close with concluding remarks. Additional technical details are provided in the appendix.

II. BACKGROUND: UNIVERSALITY AND SUPREMACY VIA 1D MODELS

Universal Quantum Computation (UQC) is, informally, the ability to solve any problem that can be solved by any quantum computer, or more formally, the ability to approximate any unitary transformation to arbitrary accuracy in polynomial runtime [2, 3]. Quantum Supremacy (QS) is, also informally, the ability to solve problems that cannot be solved in the same amount of time by any classical computer [7]. More formally, QS is the ability to generate a probability distribution that cannot be efficiently approximated to arbitrary accuracy by any classical computer with access to randomness unless the polynomial hierarchy collapses, which is believed to be unlikely [10, 11]. A number of problems exist that are known to be solvable in theory by universal quantum computers but not classical computers, so a quantum computer’s universality implies its quantum supremacy [8, 9]. A brief further discussion of the complexity basis of supremacy is provided in Appendix A.

In recent years a number of alternative models of quantum computation have been proposed, with a variety of dimensionality, circuit depth, and homogeneity requirements needed to achieve universality. Here we restrict to considering models that are universal in 1D, and compare the models on their requirements needed to reproduce a depth $d$ universal gate set (UGS) based quantum circuit, as summarized in Table I. Let us now explain the gain achieved by the VZ model, by contrasting it with the other models featured in this table.

It is known that 1D gate-based quantum circuits can achieve QS in $O(n)$ depth [13, 14], so we can use 1D quantum circuits as a reference point to compare the runtime requirements of other universal models in achieving QS. One such model is the Quantum Approximate Op-
TABLE I. Table of various 1D models of universal quantum computation. Models are compared in terms of their requirements needed to reproduce the output distribution of a 1D circuit of \( n \) logical qubits and depth \( d \), to within total variation distance \( \epsilon \). The UQC and QS columns give the runtime required for universality and supremacy, respectively.

| Model                  | Inhomogeneity | Physical Qubits | UQC Runtime Scaling | QS Runtime Scaling | Reference |
|------------------------|---------------|----------------|---------------------|--------------------|-----------|
| QAOA Quantum Circuits  | Control Unit  | \( O(n\log(n)) \) | \( O(n^5d^2\epsilon^{-4}) \) | \( O(n^5\epsilon^{-4}) \) | [5]       |
| VZ Model               | \( Z \)       | \( 4n+2 \)     | \( O(nd) \)         | \( O(n^2) \)       | This work |
| Quantum Circuits       | \( X,Z \)     | \( n \)        | \( O(d) \)          | \( O(n) \)         | [6]       |

The VZ model reproduces a gate layer from a circuit in the gate model using a series of applied layers: gate layers corresponding to the application of a single time-independent Hamiltonian, which are natural to the VZ model. We refer to the gate layer being reproduced from applied layers as the effective layer. The VZ model all \( n \) qubits are initially prepared in the \( |+\rangle^\otimes n \) state and then acted upon by a series of applied unitary layers. These unitaries are generated by a series of Hamiltonians composed of two terms: a \( Z \)-diagonal term \( H^Z_l \) which varies by applied layer \( l \), and a constant, homogeneous \( X \)-field \( H^X \) which is independent of the layer. Each applied layer \( l \) is applied for time \( t_l \). Note that \( l \) plays the role of a discrete time index. We take the \( Z \)-Hamiltonians to be two-local between neighboring qubits located on the vertices \( i \in V \) of some underlying graph \( (V,\mathcal{E}) \), and with interactions \( w_{ij} \) on the edges \( (i,j) \in \mathcal{E} \) that are uniform in magnitude but can be turned on or off by edge. The \( l \)th Hamiltonian may be written as:

\[
H_l = H^Z_l + H^X
\]

\[
H^Z_l = a \sum_{i \in V} X_i
\]

\[
H^Z_l = b_l \sum_{(i,j) \in \mathcal{E}} w_{l,ij} Z_i Z_j + c_l \sum_{i \in V} v_{l,i} Z_i,
\]

where \( w_{l,ij} \in \{0,1\} \) and \( v_{l,i} \in \{0,1\} \) respectively switch the interactions and local fields on or off for the \( l \)th applied layer, and \( a > 0 \) is fixed throughout the circuit. The total number of qubits is \( n = |V| \).

Definition 2 (Varying-Z model). Starting from the initial state \( |+\rangle \equiv |+\rangle^\otimes n \), apply each Hamiltonian \( H_l \) for corresponding time \( t_l \), measure all the qubits in the \( Z \)-basis, and sample the final state.

The output probability distribution is given by:

\[
P(s) = |\langle s | \prod_l e^{-it_l H_l} |+\rangle|^2,
\]

where \( s \in \{0,1\}^n \).

Our main result is the following:

Theorem 1. The VZ model can simulate an arbitrary depth \( d \) quantum circuit on a graph of maximum degree operation, equivalent to a set of commuting gates applied in parallel in the circuit model.
Notably, any circuit on a graph of bounded degree, e.g., a 1D chain with $\Delta = 2$, may be simulated by the VZ model in depth $O(d)$. Given the universality of 1D quantum circuits, this has the immediate consequence: \textbf{Corollary 1.} \textit{The 1D VZ model is quantum computationally universal.}

Note that if $t_1$ or $a$ had a sufficient degree of inhomogeneity (i.e., dependence on the qubit index $i$), or if $a$ were allowed to vary by layer and vanish, we would have sufficient control to directly construct the single qubit UGS $\{W, T\}$, where $W = i e^{-i \frac{\pi}{\Delta} (X+Z)}$ is the Hadamard gate and $T = e^{-i \frac{\pi}{2} Z}$ is the $T$-gate. However, Theorem 1 shows that on graphs of bounded degree and perhaps in general, neither of these relaxations provides a benefit over the already asymptotically optimal depth scaling. In other words, replacing $X$-field control with a constant, always-on transverse field $H^x$ is sufficient for low-overhead universality, as long as the $Z$-diagonal Hamiltonian can be updated between successive applied gate layers. This is clearly a significant simplification in terms of control requirements over the standard UGS approach.

Note that the initial state $|\rangle$ is the ground state of $-H^x$, so it can be prepared by turning on this Hamiltonian and waiting for the system to relax into its ground state. It can also be prepared starting from the $|0\rangle^\otimes n$ state and applying the global Hadamard gate $W^\otimes n$, which is compatible with the VZ model since it requires no inhomogeneity of the $X$-field.

We remark that the VZ model resembles QAOA [24] to some extent. The main differences are the fact that in the VZ model the $X$-field is always on (whereas in QAOA one alternates between $H^z_i$ and $H^x$), and that in VZ model we assume that the $b$ and $c$ coefficients are $l$-dependent, whereas in QAOA they may vary by qubit but not by $l$ (see also Appendix B).

\textbf{Proof outline of Theorem 1.} Two-qubit gates are universal for quantum computation [3], and an arbitrary two-qubit gate can be produced with a constant number of single qubit unitaries and gates generated by ZZ interactions [27, 28], which we refer to as ZZ-gates. Thus, in order to reproduce an arbitrary quantum circuit, it is sufficient to demonstrate the ability to generate arbitrary single qubit unitaries and ZZ-gates. We will first demonstrate the ability to reproduce layers corresponding to arbitrary single qubit unitaries (Lemma 1) and then corresponding to ZZ-gates with arbitrary real coupling constants (Lemma 2). The technical challenge in proving these results is to deal with the fact the $X$-field is always on.

Each type of effective gate layer $G_L$ can be implemented using $l_{\text{max}}(L) \in O(1)$ applied layers of the VZ model, corresponding to the decomposition
\begin{equation}
G_L = \prod_{l=1}^{l_{\text{max}}(L)} e^{-it_l(H^x + H^z_l)}.
\end{equation}

As each effective layer can apply gates across all qubits in parallel, we will then analyze the decomposition of an arbitrary circuit into layers based on its UGS, and conclude that the circuit can be implemented in the VZ model with depth overhead proportional to the number of gates that may act on the same qubit within a single gate layer.

\section{Proof of Universality of the VZ Model}

In this section we provide a detailed proof of Theorem 1.

\subsection{Single-qubit gate layers}

Consider an effective gate layer $G_L$ corresponding to identical arbitrary single qubit unitaries $g_i$, $i \in \mathcal{V}$. Let $g_i$ apply a rotation by some angle $\gamma$ about some axis $\vec{r}$.

\textbf{Lemma 1.} \textit{The VZ model can implement an arbitrary effective single-qubit gate layer $G_L$ [Eq. (4)] in three applied layers.}

\textbf{Proof.} We will show that $G_L$ may be decomposed into a product of three applied unitary layers as
\begin{equation}
G_L = V^\otimes n \bigotimes_{i=1}^{n} U_i \left(V^\dagger\right)^{\otimes n} = \bigotimes_{i \in \mathcal{V}} V_i U_i V_i^\dagger,
\end{equation}

with
\begin{align}
U_i &= e^{-it(aX_i + cv_i Z_i)}, \quad v_i = 1 \text{ iff unitary } g_i \text{ is applied to qubit } i. \tag{6a} \\
V_i &= e^{-it' (aX_i + c' Z_i)}.
\end{align}

$V^\dagger$ may be implemented modulo $\pi$, and does not require changing the $X$-field strength $a$ (we suppress the $i$ subscript where convenient). The resulting effective and applied layers are depicted in Fig. 1.

Intuitively, we would like $U_i$ to implement a Bloch sphere rotation by $\gamma$ for qubits $i$ with $v_i = 1$ and by 0 otherwise, up to equivalence modulo $\pi$. $V$ and $V^\dagger$ effectively rotate the rotational axis of $U_i$ to point along the Bloch vector $\vec{r}$.
where we take \( \psi \in [0, \frac{\pi}{4}] \) and \( \alpha' \in [\frac{\pi}{8}, \frac{3\pi}{8}] \). From here it is straightforward to solve for \( c', t' \).

The resulting values of \( c, t, c', t' \), in Eq. (6) are

\[
\begin{align*}
t &= \frac{\pi}{a} \\
c &= \frac{a}{\pi} \sqrt{(\theta + \gamma)^2 - \pi^2} \\
t' &= \frac{\alpha' \sin(2\psi)}{a} \\
c' &= \frac{\alpha \cot(2\psi)}{a}
\end{align*}
\]

for \( \psi \) and \( \alpha' \) in Eq. (11). Substituting these values into Eq. (5) yields the desired \( G_L \).

We note that in the case that \( \phi = 0 \), Eq. (11) reduces to\( \psi = (\theta + \alpha)/2 \) and \( \alpha' = \pi/2 \). This case creates the \( T \) gate when \( (\theta, \gamma) = (0, \frac{\pi}{8}) \) and Hadamard gate when \( (\theta, \gamma) = (\frac{\pi}{8}, \frac{\pi}{4}) \) so it is in fact sufficient to construct a universal set of single-qubit gates. The benefit of having found a way to represent general single-qubit unitaries is theoretical completeness and the potential simplicity of other UGSs.

**B. ZZ coupling layers**

Now consider an effective two-qubit coupling layer \( G_L \) corresponding to ZZ-coupling gates \( g_{ij} = e^{-iCZ_iZ_j} \) with an arbitrary real coupling constant \( C > 0 \), and acting on some but not all pairs of qubits connected by edges in \( \mathcal{E} \).

Such a layer decomposes as

\[
G_L = \prod_{(i,j) \in \mathcal{E}} (g_{ij})^{w_{ij}} \quad w_{ij} \in \{0,1\}
\]

where \( w_{ij} = w_{ji} = 1 \) iff qubit \( i \) couples to qubit \( j \) and 0 otherwise. Again the question arises, how would we implement \( G_L \) using just the components of the VZ model?

We restrict to the case where each qubit experiences at most a single two-qubit gate (and no > 2-qubit gates) in a single timestep (we relax this restriction in Sec. IV C). I.e., we assume that each qubit couples to at most one of its neighbors at a time:

\[
\sum_j w_{ij} = \sum_i w_{ij} \in \{0,1\}
\]

\[
w_{ij} = 0 \text{ for } (i,j) \notin \mathcal{E}
\]

In this case we have the following lemma:

**Lemma 2.** The VZ model can implement a two-qubit coupling gate layer \( G_L \) [Eq. (13)] in at most 6 applied layers.

**Proof.** We show that this may be implemented in the VZ model using either three or six applied layers depending on whether there exist uncoupled qubits. Let \( S \subset \mathcal{V} \)

\[
\begin{align*}
\psi &= \frac{1}{2} \tan^{-1} \left( \frac{\cos(2\alpha) - \cos(2\theta)}{\sin(2\theta) \cos(2\theta) - \sin(2\alpha)} \right) \\
\alpha' &= \frac{1}{2} \sin^{-1} \left( \frac{\sin(2\theta) \sin(2\phi)}{\sin(2\psi - 2\alpha)} \right)
\end{align*}
\]
be the set of uncoupled qubits, i.e., qubits $i$ for which $w_{ij} = 0 \quad \forall j$, and set $X_S = \sum_{i \in S} X_i$. The implementation takes the form:

$$G_L = e^{-i\gamma X_S} e^{-itH^*U} e^{-it'H^*}$$

for

$$U = e^{-it(H^* + \sum_{(i,j) \in E} w_{ij} Z_i Z_j)}$$

and $e^{-i\gamma X_S}$ an auxiliary single qubit unitary layer, as defined in the previous subsection, acting on qubits in $S$. This $e^{-i\gamma X_S}$ cancels out the $X$-rotation uncoupled qubits experience while coupled qubits are being acted upon; in the case that all qubits are coupled it reduces to the identity. The decomposition into applied layers is depicted in Fig. 3.

The pairwise coupling assumption [Eq. (14)] allows use of the following two-qubit decomposition between qubits $i$ and $j$, derived in Appendix F:

$$e^{-it(a(X_i + X_j) + bZ_i Z_j)}$$

$$= e^{-i\beta(X_i + X_j)} e^{-iD_1 X_i X_j} e^{-iD_2 Y_i Y_j} e^{-iD_3 Z_i Z_j} e^{-i\beta(X_i + X_j)}$$

with

$$D_1 = 0$$

$$D_2 = \frac{1}{2} (bt - \omega)$$

$$D_3 = \frac{1}{2} (bt + \omega)$$

$$\omega = \sin^{-1}\left(\frac{b}{\sqrt{4a^2 + b^2}} \sin\left(t\sqrt{4a^2 + b^2}\right)\right)$$

$$\beta = \frac{s}{4} \cos^{-1}\left(\cos\left(t\sqrt{4a^2 + b^2}\right) \sec(\omega)\right) + \frac{\pi}{2}$$

where $s = \text{sign}(a \sin(\sqrt{4a^2 + b^2}t))$ and we pick $\omega \in [-\frac{\pi}{2}, \frac{\pi}{2}]$ and $\beta \in [0, \pi]$. Uncoupled qubits have $w_{ij} = 0 \quad \forall j$, and simply experience $e^{-i\omega t X}$, as shown in Fig. 3.

We restrict to the pure ZZ-coupling of Eq. (13) between qubits $i$ and $j$ by requiring that $D_2 = 0$ [to cancel the undesired $Y_i Y_j$ term in Eq. (17b)], and thus that

$$bt = \omega = D_3 \equiv D.$$  \hspace{1cm} (19)

For coupled pairs, we take $b \neq 0$ and solve for $t$ in terms of $D$. Namely, substituting Eq. (19) into Eq. (18d) we obtain

$$\text{sinc}(D) = \text{sinc}\left(\sqrt{4a^2t^2 + D^2}\right),$$  \hspace{1cm} (20)

where $\text{sinc}(x) \equiv \sin(x)/x$. 

![Image](image_url)
Achieving the desired magnitude of coupling in Eq. (13) up to an overall phase requires that $D = C \mod \pi$. As demonstrated in Appendix G, for every $C \in [0, \pi]$, there exists a $k \in \{0, 1, 2, 3\}$ such that when $D = C + k\pi$, Eq. (20) is numerically solvable for $at > 0$. Thus for any $C \in [0, \pi]$, we can pick this value of $k$ and corresponding numerical solution $t$, and set $b = D t^{-1} = (C + k\pi) t^{-1}$.

With these parameter choices and taking the product across all pairs of qubits, the overall action of $U$ becomes

$$e^{-it(H^x + b \sum_{i,j} w_{ij} Z_i Z_j)} = e^{-iatX_S} e^{-i\beta X_S} e^{-iC \sum_{i,j} w_{ij} Z_i Z_j} e^{-i\beta X_S},$$

up to an overall phase, for $X_S = \sum_{i \notin S} X_i$.

The effect of $\beta$ can be undone by a uniform $X$-rotation for time $at' = \pi - \beta$ before and after the coupling layer. This gives

$$e^{-it'H^x} e^{-it(H^x + b \sum_{i,j} w_{ij} Z_i Z_j)} e^{-it'H^x} = e^{-i(\pi - \beta) at} X_S e^{-iC w_{ij} Z_i Z_j},$$

In the case that $|S| = 0$, $X_S = 0$, and the result is pure $ZZ$ coupling of the desired magnitude $C$. In the case that some qubits are uncoupled, the extra rotation on those qubits can be undone with an auxiliary inhomogeneous $X$-rotation by angle $\gamma = 2\beta - at$. In this case we have

$$e^{-i\gamma X_S} e^{-it'H^x} e^{-it(H^x + b \sum_{i,j} w_{ij} Z_i Z_j)} e^{-it'H^x} = e^{-iC \sum_{i,j} w_{ij} Z_i Z_j}.$$ 

In either case, by picking parameters

$$t = \text{sinc}(C + k\pi) = \text{sinc}(\sqrt{4a^2 t^2 + (C + k\pi)^2})$$

$$b = (C + k\pi) t^{-1}$$

$$t' = (\pi - \beta) a^{-1}$$

$$\gamma = 2\beta - at,$$

the effective coupling layer is implemented in at most 6 applied layers.

Alternatively, if the coupling layer is preceded or succeeded by single qubit unitary layers acting nontrivially on the exact same set of qubits, the required $e^{-it'H^x}$ evolution may be absorbed into the single qubit unitary layers, and thus become effectively free, as long as the auxiliary $e^{-it X_S}$ has $\gamma$ tuned to compensate. Furthermore, if multiple effective $ZZ$-coupling layers share a set $S$ of uncoupled qubits, their auxiliary $X$-rotations will commute with all the $ZZ$-couplings, and thus can be combined into a single auxiliary unitary. Both of these methods may be used to implement SWAP gates more efficiently, as is done in Section V.

It is also worth mentioning that an effective layer of disjoint $e^{-i\frac{\pi}{2} Z \otimes Z}$ gates may be implemented in at most six applied layers, and one of disjoint CZ gates $e^{-i\frac{\pi}{4}(Z_1 \otimes Z_2 + Z_2 \otimes Z_1)}$ in at most eight by absorbing one of the $e^{-it'H^x}$ rotations into the single qubit effective layer. Either case is sufficient for universality in combination with arbitrary single qubit gates. Though universality can be achieved using just $C = \frac{\pi}{4}$, the fact that we demonstrated the ability under the VZ model to apply arbitrary (real) couplings is for more than just theoretical completeness, as it can reduce depth requirements.

### C. Depth Requirements

Naively, a depth $d$ quantum circuit on some graph could be implemented in the VZ model on the same graph in $O(nd)$ layers without parallelization, simply by viewing each gate as its own effective layer. While this is sufficient for universality, we can reduce the required depth by a factor of $n$ using parallelization in terms of a universal gate set, leading to Theorem 1.

**Proof of Theorem 1.** Say that a circuit has depth $d$ when written in terms of UGS $\mathcal{G}$, composed of gates that act only on nearest neighbor qubits in some underlying architecture described by a graph $(V, \mathcal{E})$. We can assume that $\mathcal{G}$ is composed of single-qubit unitaries and two-qubit $ZZ$-coupling, as any two-qubit gate can be decomposed into $O(1)$ gates of this form [27]. Then each effective layer of the original circuit can be viewed as at most $|\mathcal{G}|$
individual effective sublayers, each corresponding to the application of a single $g \in \mathcal{G}$ to some subset of the qubits (Fig. 4).

Consider an effective sublayer corresponding to a two-qubit coupling gate $g$. Within the sublayer, $g$ can act on an individual qubit $i$ once for each neighbor that qubit has. Because the decomposition used in Sec. IV B requires pairwise coupling of qubits, we must further decompose $g$ into an effective sublayer for each application of $g$ on $i$ (Fig. 5). The application of a single two-qubit coupling gate layer may require as many effective sublayers as the minimum edge coloring of the underlying graph $(\mathcal{V}, \mathcal{E})$. By Vizing’s theorem [29], this can be upper bounded by $\Delta + 1$, where $\Delta$ is the maximum degree of the graph. In case the graph is a grid based lattice of dimension $D$, this simply becomes the number of sublattices of paired qubits, which is $\Delta = 2D$.

After full sublayer decomposition, each effective sublayer corresponds either to a single-qubit unitary or ZZ-coupling on monogamously paired qubits, so it is of a form that can be implemented in the VZ model in $O(1)$ applied layers. An arbitrary quantum circuit of depth $d$ can then be represented in the VZ model in depth $O(d|\mathcal{G}|\Delta)$ on the same graph. In the case of a $D$-dimensional integer lattice $\mathbb{Z}^D$, this becomes $O(2d|\mathcal{G}|D)$.

For example to reproduce the effect of $\mathcal{G} = \{ W, T, e^{-i\pi \mathbb{Z} \otimes \mathbb{Z}} \}$ on a 1D chain of qubits, effective sublayers of $W$ and $T$ gates may each be implemented in three applied layers while $e^{-i\pi \mathbb{Z} \otimes \mathbb{Z}}$ requires up to 2 effective sublayers of at most 6 each, so each effective layer of the original circuit requires at most 18 applied layers of the VZ model to implement on the same graph.

By extending the 1D implementation of arbitrary IQP circuits used in Ref. [13] to more general circuits, one sees that 1D quantum circuits are universal with $O(n)$ depth overhead. Thus the 1D VZ model is capable of representing any depth-$d$ quantum circuit expressed in terms of UGS $\mathcal{G}$ on an arbitrary graph, in depth $O(nd|\mathcal{G}|)$. Interestingly, as a fully connected graph has $\Delta = n - 1$, in the worst case the 1D and same graph VZ models have the same asymptotic depth scaling.

Note that in Table I we state that an $O(d)$-depth 1D VZ model reproduces the output distribution of a 1D circuit of $n$ logical qubits and depth $d$; the extra $n$ prefactor overhead in the expression $O(nd|\mathcal{G}|)$ is incurred when going from an arbitrary graph to a 1D chain, or when generating SWAP gates.

The 1D case is also interesting in its own right: it is known that 1D $O(n)$ depth universal quantum circuits anticoncentrate [30] and can generate distributions that cannot be efficiently classically simulated [13]. In the next section, we provide a circuit distribution that demonstrates this, and analyze the depth overhead required to implement it in the VZ model.

![FIG. 5. (a) An example of an effective coupling sublayer $L$ of a 1D circuit, in which the coupling gate $g$ is applied across all qubits, rather than restricted to pairwise coupling. (b) The sublayer $L$ implemented as two effective coupling sublayers, each with pairwise coupling.]

### V. DEMONSTRATING QUANTUM SUPREMACY

#### A. Homogeneous X-field

In this section we apply the previous results towards demonstration of quantum supremacy.

**Corollary 2.** The 1D VZ model can generate a distribution in $O(n)$ depth that cannot be approximately simulated by a classical computer in the worst case.

The proof follows from Theorem 1 and the distribution generated in Refs. [8, 13], in which it is shown that no classical computer can efficiently sample from a distribution approximating the one in question. Here we detail the distribution and account for the exact overhead introduced from generating it in the VZ, rather than gate-based model of quantum computation. This distribution was proposed in Ref. [8] and is the output distribution of an Instantaneous Quantum Polynomial-time (IQP) model with long range interactions:

$$P_{\text{IQP}}(s) = \langle s | H^{\otimes n} e^{-i C_z} | + \rangle, \quad (25)$$

where

$$C_z = w_{ij} Z_i Z_j + v_i Z_i, \quad w_{ij}, v_i \in \left\{ \frac{1}{8} k\pi \right\}_{k=0}^7, \quad (26)$$

with $w_{ij}$ and $v_i$ chosen uniformly at random from their domains and $s$ a string in the $Z$ basis.

In the VZ model we can generate the distribution of Eq. (25) using a modified version of the circuit design
FIG. 6. The \( n = 4 \) case of a 1D \( O(n) \)-depth circuit capable of generating the distribution in Eq. (25) via alternating layers of ZZ coupling and SWAP gates. It is equivalent to that of Ref. [13], but composed of Hadamard gates (\( W \)), SWAP gates, and Z-diagonal gates of the form \( e^{i v_i Z_i} \) and \( e^{i w_{ij} Z_i Z_j} \), denoted by their degree of rotation \( v_i \) or \( w_{ij} \). In this design qubits effectively act as particles moving past each other in 1D, and after \( n \) layers each qubit has a chance to interact with each other qubit once. As Z-diagonal gates commute, multiple interactions between any pair of qubits can be implemented as a single interaction. Thus, this 1D depth \( O(n) \) circuit is sufficient to implement the circuit implied by Eq. (25).

FIG. 7. (a) The first two layers of an example circuit with arbitrarily chosen \( w_{ij} \) and \( v_i \). Z-diagonal gates are denoted by their degree of rotation. (b) The same two layers rewritten as effective sublayers which can be implemented in the VZ model. For example, the gate corresponding to \( v_2 = \frac{5 \pi}{8} \) in (a) is decomposed into \( \frac{\pi}{2} \) and \( \frac{\pi}{8} \) gates in (b), with the \( \frac{\pi}{8} \) gate shifted so that it is executed in parallel with the other \( \frac{\pi}{8} \) gate from (a) to form a sublayer.

of Ref. [13], as is depicted in Fig. 6. The depth overhead of implementing this circuit in the VZ model is affected by choice of UGS. Rather than implementing each term in \( C_Z \) as an independent single qubit or coupling gate [Fig. 7(a)], we break each layer of single qubit and coupling gates into three effective sublayers by using the binary decomposition

\[
v_i = \frac{4\pi}{8} a_i + \frac{2\pi}{8} b_i + \frac{\pi}{8} c_i \quad a_i, b_i, c_i \in \{0, 1\}
\]  

(27)

and implementing each \( a, b, c \) as its own sublayer. Each ZZ coupling layer is decomposed into three sublayers with an equivalent decomposition on \( w_{ij} \) [Fig. 7(b)]. A SWAP gate may be implemented by decomposition into a product of Hadamard gates and single-qubit and two-qubit Z-diagonal gates (Fig. 8).

Using the methods of Sec. III, each sublayer of Fig. 7(b) corresponding to a single qubit gate can be implemented in three applied layers, and thus the set of all single qubit gates requires nine applied layers using the decomposition of Eq. (27). Similarly, each coupling layer requires 18 applied layers, or \( 18n \) in total between the \( n \) ZZ-coupling layers. In implementation of the SWAP layer [Fig. 8(c)], we combine adjacent single qubit unitary layers acting nontrivially on the same qubits. The result is that a SWAP gate requires only five effective single qubit unitary layers, or 15 applied layers. We further combine the \( e^{-it' H^z} \) rotations needed for coupling layers into the adjacent single qubit unitary layers; all but one \( e^{-it' H^z} \) rotation can be absorbed this way. All the auxiliary \( e^{-i\gamma X_S} \) rotations can be combined, so the set of three effective ZZ-coupling layers requires only four applied layers to implement if every qubit is coupled (\( |S| = 0 \)), or seven otherwise. In total, each of the \( n \) effective SWAP layers requires either 19 or 22 applied layers, depending on whether the SWAP gates span every qubit or not. When \( n \) is even, half of the SWAP layers act on all qubits, but for odd \( n \) every layer has uncoupled qubits, so in general the total overhead for the SWAP gate layers is at most \( 22n \). Summing the \( 18n \) applied layers for ZZ-coupling, \( 22n \) applied layers for SWAP gates, nine applied layers for single-qubit gates, and final all-qubit Hadamard, the
entire circuit can be implemented in $40n + 10$ applied layers.

These calculations assume a noiseless computation model. The presence of noise can reduce fidelity of an output distribution of a circuit to the point that it no longer demonstrates quantum supremacy (see, e.g., Ref. [31] for a discussion of this in the context of random circuit sampling), but for this distribution even a simple repetition code with $O(\ln(n))$ repetitions is sufficient to regain supremacy [32]. The universality of the VZ model allows it to perform this repetition code efficiently, in contrast to methods of demonstrating QS which are not universal, and thus not necessarily able to correct for the effects of decoherence.

### B. Alternating X-field

In this section we consider a slight modification of the VZ model in which the X-field can be turned off for half the qubits at a time – either those of even or odd index. This modification reduces the depth required to apply the SWAP gate while still being easier to implement than the full circuit model, and thus reduces total depth required to demonstrate quantum supremacy. We still use the homogeneous X-field method for implementing the ZZ-coupling layers. For even $n$, in each SWAP layer the SWAP gates alternate between acting pairwise on one sub-lattice such that they cover all of the qubits, and acting pairwise on the other sub-lattice such that there are two unaffected qubits at the boundaries of the qubit chain. For odd $n$ every sub-lattice acted on by SWAP gates has a single unaffected qubit. Cases with unaffected qubits require more layers to cancel the X-rotations these boundary qubits experience while the other qubits are being swapped, which we will discuss it at the end of this subsection.

In the alternating X-field method, instead of implementing the SWAP gate as three CNOT gates as in Fig. 8(a), we use different building blocks: ZZ-coupling layers with nonzero X-fields on either only the even or only the odd qubits, as shown in Fig. 9. First we start from one of these coupling layers with X-fields on only the even qubits. We can write the action of this layer as

$$U = \prod_{i=\text{odd}} e^{-it(aX_{i+1} + bZ_{i}Z_{i+1})}$$

for appropriately chosen $b$. Consider just the two-qubit gate acting on the first and second qubits; it has the following block-diagonal structure:

$$U_{12} = e^{-it(aX_{2} + bZ_{1}Z_{2})} = \begin{bmatrix} U_{1} & 0 \\ 0 & U_{2} \end{bmatrix}$$

where $0$ is the $2 \times 2$ zero-matrix, and we can further decompose

$$U_{1} = e^{i\gamma Y} e^{-i\gamma X} e^{-i\alpha Y}, \quad U_{2} = e^{-i\alpha Y} e^{-i\gamma X} e^{i\alpha Y},$$

where

$$\alpha = \frac{1}{2} \cos^{-1}\left(\frac{a}{\sqrt{a^2 + b^2}}\right),$$

$$\gamma = t \sqrt{a^2 + b^2}.$$  \hfill (31a)

If we set $b = a$ and $t = \frac{\pi}{2\sqrt{2n}}$, then $U_{1} = -iW$, and $U_{1}^{\dagger}U_{2} = \tilde{Y}$, where $\tilde{Y} = ZX = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. Thus for this choice of $b$ and $t$,

$$U_{12} = -i(I \otimes W)C\tilde{Y}_{12}$$

where $C\tilde{Y}_{12}$ is the controlled $\tilde{Y}$ gate. Similar to the ZZ-coupling gates (recall the discussion in Sec. IV B), this operation leads to a net $X$-rotation on uncoupled qubits which still experience an X-field, which then must be undone by an extra single-qubit unitary following the SWAP layer.
Defining the above building block $U_{12}$, the total circuit required for a SWAP gate will be:

$$C = U_{12} W_1 W_2 U_{21} U_{12} W_2$$

$$= i(W_2 C Y_{12}) W_1 W_2 (W_1 C Y_{21})(W_2 C Y_{12}) W_2$$

The product of $W_1 W_2$ needs just one effective single qubit gate layer in total, and any effect on uncoupled qubits can be incorporated into the extra single-qubit unitary $e^{-i\gamma X_s}$ on these qubits following the SWAP layer. Since the last $W_2$ requires three single qubit gate layers, the total number of required layers for implementing the above decomposition is seven.

Defining $\tilde{Y} = -Y = XZ$ and using the equality $W_2 C Y_{12} = C \tilde{Y}_{12} W_2$, we can simplify the above expression as below:

$$C = i W_2 C \tilde{Y}_{12} W_1 W_2 W_1 C \tilde{Y}_{21} W_2 C \tilde{Y}_{12} W_2$$

$$= i C \tilde{Y}_{12} W_2 W_1 W_2 W_1 C \tilde{Y}_{21} C \tilde{Y}_{12} W_2$$

$$= i C \tilde{Y}_{12} C Y_{21} C Y_{12}$$

$$= i C X_{12} C Z_{12} C Z_{21} C X_{12} C X_{12} C Z_{12}$$

$$= i C X_{12} C X_{21} C X_{12} C Z_{12}$$

$$= i \text{SWAP}_{12} C Z_{12}$$

$$= i C Z_{21} \text{SWAP}_{12}.$$  

This is the required SWAP gate up to $C Z_{21}$. This unwanted $C Z_{21}$ can be written as a product of single qubit $Z$-diagonal gates and $Z Z$-couplings, and can in fact be incorporated into the existing single qubit and coupling gates already in the overall circuit, simply by shifting the values of $w_{12}$, $v_1$, and $v_2$ by $\frac{\pi}{2}$. These $v_i$ and $w_{ij}$ parameters are chosen from a uniform distribution over the full range of multiples of $\frac{\pi}{2}$ mod $\pi$, so the shift by $\frac{\pi}{2}$ does not affect the distribution. This makes the $CZ$ gate effectively free to include.

In this construction a SWAP gate layer spanning all qubits can be implemented in seven applied layers. In the case of unwrapped qubits, an unwrapped qubit experiences a different net $X$-rotation depending on whether it is of even or odd qubit index. As there are at most two values of unwanted $X$-rotation after the SWAP layer, these can be undone in at most two single-qubit effective layers, or six applied layers. This brings the total number of applied layers to implement a single effective SWAP layer to seven if every qubit is swapped, 10 if there is a single unwrapped qubit, or at most 13 otherwise.

For even $n$ the model alternates between SWAP layers with zero and two unwrapped qubits, so the set of all SWAP layers requires $7 + 13 + \cdots + 10n$ applied layers. For odd $n$, every SWAP layer has a single unwrapped qubit, so the SWAP layers require a total of $10n$ applied layers – the same as in the even $n$ case. Including $18n$ applied layers of $Z Z$-coupling gates and 10 of single qubit gates and Hadamards, the total number of applied layers required to reach supremacy becomes $28n+10$ (recall that the cost was $40n+10$ in the case of a fully homogeneous $X$-field).

VI. CONCLUSIONS

Minimalism is both a sound engineering design principle and a desirable feature of theoretical models. By minimalism we mean a reduction in the consumption of some or more precious resources, or the reliance on a small set of assumptions. This work is an attempt to be minimalistic about the resources and assumptions underlying both implementations and models of universal quantum computation and quantum supremacy. From a practical perspective, spatially homogeneous or global control can be a significant advantage over individualized or local control, since the latter typically involves additional control wires or lasers, each of which is another source of noise and decoherence. From a theoretical perspective, it is interesting to investigate the computational power of fully or partially translationally invariant models in low dimensions.

In accordance with this perspective we have studied the power of a minimalistic model that assumes spatially homogeneous $X$-field control but spatially inhomogeneous $Z$-field control [Eq. (1)]. We have shown that this “VZ model” can be used to demonstrate quantum supremacy even in 1D, and is furthermore universal for quantum computation. The overhead required to implement the circuit model with a standard universal gate set using the 1D VZ model is constant in system size and is significantly lower than the universal version of QAOA (see Table I). We are unaware of any model of quantum computation with a higher degree of homogeneity that achieves the same asymptotic depth scaling as the VZ model.

Perhaps the most immediate application of the VZ model would be a demonstration of quantum supremacy in the IQP setting, which we have shown here can be implemented in at most $40n+10$ layers of control pulses, for a circuit of width $n$. This model may be the next to be used for a quantum supremacy demonstration, now that this has been done using random circuit sampling [15] and boson sampling [33]. Such a demonstration within the VZ model would be particularly viable using flux qubits [20–22], where leaving a constant and homogeneous $X$-field on while locally controlling only $Z$-fields and interactions is both simpler and less prone to noise than also controlling the $X$-field.
ACKNOWLEDGMENTS

We thank Paolo Zanardi for many insightful discussions. This research was sponsored by the Army Research Office and was accomplished under Grant Number W911NF-20-1-0075. This research is also based upon work (partially) supported by the Office of the Director of National Intelligence (ODNI), Intelligence Advanced Research Projects Activity (IARPA) and the Defense Advanced Research Projects Agency (DARPA), via the U.S. Army Research Office contract W911NF-17-C-0050. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the ODNI, IARPA, DARPA, ARO, or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright annotation thereon. This work is partially supported by a DOE/HEP QuantISED program grant, QC-CFP/Quantum Machine Learning and Quantum Computation Frameworks (QCCFP-QMLQCF) for HEP, Grant No. DE-SC0019219.

Appendix A: Complexity basis of quantum supremacy

Bounded-error Probabilistic Polynomial-time (BPP) is the computational complexity class of problems that a classical computer, with access to true randomness, can solve with high probability in time polynomial in input size. It can be viewed as the class of problems that is realistic for a classical computer to solve. Bounded-error Quantum Polynomial-time (BQP) is the equivalent class for quantum computers. It is widely believed that BQP ≠ BPP, due to a hypothetical tool called postselection. Postselection is the ability to select the results of randomness after completing all computations. The classes associated with BPP and BQP when the computer has access to postselection are referred to as PostBPP and PostBQP. While PostBPP is known to be within the third level of the polynomial hierarchy, a hierarchy representing a generalization of the P vs NP distinction, it is known by Toda’s and Aaronson’s theorems that Post-BQP in fact contains the entire polynomial hierarchy as a subset [10, 34]. If BQP=BPP, then postBQP=PostBPP, and the entire polynomial hierarchy would be contained within its third level, a situation referred to as collapse of the polynomial hierarchy. This is conjectured to not happen for the same reason it is believed that P ≠ NP.

The output of problems in BQP takes the form of distributions that one samples from. Because we cannot take infinite samples in practice, we cannot perfectly calculate the distribution that a practical quantum computer is sampling from. Verifying that a problem has been solved relies on anticoncentration of the output distribution [12, 32]: the outcome probabilities must be sufficiently spread across all possible outcomes of measurements, so that there is a nonvanishing signal-to-noise ratio for at least a constant fraction of all possible outcomes.

Appendix B: QAOA vs the VZ model

In QAOA [24] one considers a Hamiltonian of the form

\[ H(t) = a(t)H^X + d(t)H^Z \]

(B1a)

\[ H^X = \sum_{i \in \mathcal{V}} X_i \]

(B1b)

\[ H^Z = \sum_{(i,j) \in \mathcal{E}} b_{ij} Z_i Z_j + \sum_{i \in \mathcal{V}} c_i Z_i, \]

(B1c)

for \( n \) qubits occupying the vertices \( \mathcal{V} \) of a graph \( \mathcal{G} = (\mathcal{V}, \mathcal{E}) \). The parameters \( b_{ij} \) and \( c_i \) are controllable longitudinal local field and coupling constants, respectively, and \( a(t) \) and \( d(t) \) are time-dependent control functions. Note that \( H_l \) [Eq. (1)] is an instance of \( H(t) \), for each fixed \( l \) and \( t \).

The level-\( p \) QAOA produces an approximation \( C^*_p \) to the optimal value of the classical cost function represented by \( H^Z \):

\[ U(\beta, \gamma) = e^{-i\beta H^X} e^{-i\gamma H^Z} \]

(B2a)

\[ |\psi(\gamma, \beta)\rangle = \left( \prod_{k=1}^p U(\beta_k, \gamma_k) \right) |+\rangle \]

(B2b)

\[ C^*_p = \min_{\gamma, \beta} \langle \psi(\gamma, \beta) | H^Z | \psi(\gamma, \beta) \rangle \]

(B2c)

where \( \gamma = (\gamma_1, ..., \gamma_p), \beta = (\beta_1, ..., \beta_p) \) are the angles that parameterize the circuit. Various heuristic methods for choosing these angles have been considered, and for small values of \( p = O(1) \) the optimization can be done exactly [35].

The VZ model (Def. 2) differs from QAOA in that the alternating sequence of unitaries always includes \( H^X \), unlike the QAOA sequence given in Eq. (B2a). It also differs in that in QAOA the \( H^Z \) Hamiltonian is fixed, while in the VZ model we assume that the \( b,c,w \), and \( v \) coefficients in Eq. (1) are controllable from layer to layer, which would be equivalent to making \( b \) and \( c \) time-dependent in Eq. (B1c).

Appendix C: Depth Scaling of QAOA Universality

Here we analyze the required depth of the QAOA model used in Ref. [5] to reproduce a 1D circuit to within a given total variation distance error \( \epsilon \). This model of QAOA uses co-irrationality of terms in a Z-diagonal Hamiltonian \( H^Z \) to reproduce a translationally invariant gate layer \( U \) composed of a tensor product of one to two
qubit gates across all qubits. The evolution time needed to reproduce a specific gate layer such that

$$\|e^{-itH} - U\| \leq \epsilon'$$

\(t \in O(\epsilon^{-4})\), where \(\| \cdot \|\) is the operator norm.

The BCQA method applies individually addressed gates by using SWAP gates to effectively walk a certain qubit, dubbed the control unit, across the chain until it is adjacent to a qubit being acted on [25], then performing controlled gates. It thus requires \(O(n)\) depth to implement a single gate. Assuming the ability to parallelize, a 1D circuit of depth \(d\) with \(O(nd)\) gates will then require \(O(nd)\) depth BCQA to reproduce. In the QAOA implementation this becomes \(O(nd\epsilon^{-4})\), but we would like to bound runtime in terms of total variation distance \(\epsilon\) of the output distribution, not operator norm error \(\epsilon'\) of each individual gate.

For a target BCQA protocol \(C = \prod_{i=1}^{nd} U_i\), we can write the QAOA approximation as \(C' = \prod_{i=1}^{nd} (U_i + \delta_i)\), where \(\delta_i\) is the error of the \(i^{th}\) gate layer, such that \(\|\delta_i\| \leq \epsilon'\) \(\forall i\). Let \(\Delta \equiv C' - C\). Then the operator norm error of the complete QAOA implementation becomes

$$\|\Delta\| = \|\prod_{i=1}^{nd} (U_i + \delta_i) - \prod_{i=1}^{nd} U_i\|$$

$$= \|\sum_{i=1}^{nd} U_{ni} \cdots U_{i+1} \delta_i U_{i-1} \cdots U_1 + \cdots\|$$

$$\leq \sum_{i=1}^{nd} \|\delta_i\| + \sum_{i,k=1}^{nd} \|\delta_i \delta_k\| + \cdots$$

$$\in O(nd\epsilon').$$

Thus the total variation distance between the target BCQA and applied QAOA circuits becomes

$$\sum_{s} |P'(s) - P(s)| \leq \text{Tr}[|C'\rangle\langle 0|C'^\dagger - C\rangle\langle 0|C^\dagger|]$$

$$\in O(nd\epsilon')$$

where \(s\) represents a bitstring, the first inequality comes from bounding the total variation distance by the trace-norm distance,\(^1\) the third inequality from properties of the operator and trace norms,\(^2\) and in the last line we assumed that \(\epsilon' < 1/(nd)\).

Suppose we wish to approximate a circuit to total variation distance \(O(\epsilon)\). Then assuming the worst case bound in Eq. (C3), we must have \(\epsilon' \sim \frac{\epsilon}{nd}\). In this case the total runtime of the QAOA circuit is \(O(nd\epsilon^{-4}) = O(n^3d^4\epsilon^{-4})\).

### Appendix D: Failure of the Euler angles construction to generate single-qubit gates in the VZ model

We can define \(\text{su}(2)\) generators in the VZ model:

$$\tilde{X} = \cos(\alpha)X + \sin(\alpha)Z, \quad \tilde{Z} = -\sin(\alpha)X + \cos(\alpha)Z.$$  

(D1)

It is simple to check that this pair satisfies the \(\text{su}(2)\) commutation relations along with \(Y\) (e.g. \([\tilde{Z}, \tilde{X}] = 2iY\), etc.). From here we can construct any \(\text{SU}(2)\) single-qubit gate using the standard Euler angles construction:

$$g(\phi, \theta, \psi) = U^x(\phi)U^z(\theta)U^x(\psi) =$$

$$\begin{bmatrix}
\cos(\theta)e^{-i(\psi+\phi)} & -i\sin(\theta)e^{-i(\psi-\phi)} \\
-i\sin(\theta)e^{i(\psi-\phi)} & \cos(\theta)e^{i(\psi+\phi)}
\end{bmatrix},$$

(D2a)

where the angles take values within the intervals \(\theta \in [0, \pi/2], \phi \in [0, \pi], \psi \in [0, 2\pi]\) (mod \(\pi\)), and where \(U^x(\varphi) = \exp(-i\varphi \tilde{X})\) and \(U^z(\varphi) = \exp(-i\varphi \tilde{Z})\). This approach is certainly feasible for an applied layer in which all qubits undergo the same single-qubit gate. However, it fails when at least one qubit (but not all) in an applied layer is idle, since in the Euler angle construction the only way to generate the identity gate is to choose the angles as

$$\{\theta = 0, \psi = 2\pi - \phi\} \mod \pi.$$  

(D3)

The problem is that fixing \(\theta = 0\) restricts the ability to generate an arbitrary single-qubit gate on the non-idle qubits. I.e., suppose that the applied layer includes one idle and another non-idle qubit requiring the pure \(\tilde{X}\)-rotation \(g_2(0, \theta, 0) = g(\phi, \theta, 2\pi - \phi)\) with \(\theta > 0\). It is not possible to implement both gates without restricting generality within the same time-interval (applied layer) since this limits the allowed values of \(\theta\). Namely, for a layer of duration \(t\), on the one hand we would need \(t \cos \alpha = k\pi\) and \(t \sin \alpha = k\pi\) for the idle qubit (using \(\theta = k\pi\) with integer \(k\) instead of \(\theta = 0\)), but on the other hand we would also need \(t \cos \alpha = \theta\) and \(t \sin \alpha = \theta\) for the non-idle qubit, thus forcing \(\theta\) to be a multiple of \(\pi\).

\[^1\] \(\sum_s |P'(s) - P(s)|\) \(\leq \text{Tr}[|\rho' - \rho|]\), where \(P(s) = \text{Tr}[|s\rangle\langle s| \rho]\), with \(\rho = C\rangle\langle 0|C^\dagger\), and the inequality follows since the trace norm distance is the maximum of \(\frac{1}{2} \sum_s |\text{Tr}(E_s |\rho' - \rho|)|\) over all possible generalized measurements \(E_s\), which includes the projective measurement \(|s\rangle\langle s|\) [36].

\(^2\) \(|\text{Tr}(AB)| \leq \|A\|\|B\|\|1\| [37, 38].\)
Appendix E: Proof of Eq. (11)

In this appendix our goal is to show that we can decompose a desired arbitrary single-qubit rotation

\[ g = e^{-i\gamma' \hat{x}} \]

where \( \hat{x} = (\sin(2\theta) \cos(2\phi), \sin(2\theta) \sin(2\phi), \cos(2\theta)) \), as \( g = VUV^\dagger \), where

\[ U = e^{-i\gamma' (\cos(2\alpha)Z + \sin(2\alpha)X)} \]

\[ V = e^{-i\alpha' (\cos(2\psi)Z + \sin(2\psi)X)} \]

Our second goal is to derive the values of \( \alpha' \) and \( \psi \) given in Eq. (11). In Eq. (9a) we take \( \gamma' = \pi + \gamma \). However, the results of this proof do not depend on specific choice of \( \gamma' \), aside from implicit dependence hidden in \( \alpha \) or other parameters.

Defining the adjoint group action as \( \text{Ad}_g(B) = gBg^{-1} \) and using the fact that

\[ \text{Ad}_A(e^B) = e^{ABA^\dagger} \]

for any unitary \( A \) and operator \( B \), and that

\[ \text{Ad}_e^\alpha Y (Z) = \cos(2\theta)Z + \sin(2\theta)X, \]

and similar identities obtained by cycling \( X \), \( Y \) and \( Z \), we may rewrite

\[ U = \text{Ad}_e^\alpha Y (e^{-i\gamma' Z}) \]

\[ V = \text{Ad}_e^\alpha Y (e^{-i\alpha' Z}) \]

Then setting \( u = 2\alpha - 2\psi \), we see that:

\[ VUV^\dagger = \text{Ad}_e^\alpha Y (\text{Ad}_{e^{-i\alpha' Z}} (\text{Ad}_{e^{-(u-\psi)} (e^{-i\gamma' Z})}))) \]

\[ = \text{Ad}_e^\alpha Y (\text{Ad}_{e^{-i\alpha' Z}} (e^{-i\gamma' \cos(u)Z + \sin(u)X})) \]

\[ = \text{Ad}_e^\alpha Y e^{-i\gamma' \cos(u)Z + \sin(u)X \cos(2\alpha')X - \sin(2\alpha')Y}) \]

\[ = e^{-i\gamma' (v_x X + v_y Y + v_z Z)} \]

where in the final line

\[ v_x = \cos(u) \sin(2\psi) + \sin(u) \cos(2\alpha') \cos(2\psi) \]

\[ v_y = -\sin(u) \sin(2\alpha') \]

\[ v_z = \cos(u) \cos(2\psi) - \sin(u) \cos(2\alpha') \sin(2\psi) \]

Using the representation of the desired gate \( g \) as in Eq. (11), this gives a system of three equations:

\[ v_x = r_x \]

\[ \sin(2\theta) \cos(2\phi) = \cos(u) \sin(2\psi) + \sin(u) \cos(2\alpha') \cos(2\psi) \]

\[ \sin(2\alpha') = \sin(2\alpha) + \sin(u) \cos(2\psi) \cos(2\alpha') - 1, \]

and \( v_y = r_y \)

\[ \sin(2\theta) \sin(2\phi) = -\sin(u) \sin(2\alpha') \]

and \( v_z = r_z \)

\[ \cos(2\theta) = \cos(u) \cos(2\psi) - \sin(u) \cos(2\alpha') \sin(2\psi) \]

\[ \sin(2\alpha') = \sin(2\alpha) - \sin(u) \sin(2\psi)(\cos(2\alpha') - 1). \]

The existence of a solution of these three equations for \( \alpha \), \( \alpha' \) and \( \psi \) proves that \( g \) can be written as \( VUV^\dagger \) as claimed.

Eq. (E9) immediately reduces to

\[ \sin(2\alpha') = -\frac{\sin(2\theta) \sin(2\phi)}{\sin(u)} \]

while Eqs. (E8) and (E10) can be combined into

\[ \tan(2\psi) = \frac{\cos(2\alpha) - \cos(2\theta)}{\sin(2\theta) \cos(2\phi) - \sin(2\alpha)}. \]

Thus, we have the values of \( \alpha' \) and \( \psi \) given in Eq. (11), up to a choice of the range of \( \tan^{-1} \) and \( \sin^{-1} \).

Appendix F: Two qubit coupling decomposition

The form of the decomposition in Eq. (17) is motivated by Ref. [39]; any \( U \in SU(4) \) can be decomposed as:

\[ U = k_1 e^{-i\left(D_1(X\otimes X) + D_2(Y\otimes Y) + D_3(Z\otimes Z)\right)} k_2 \]

where \( k_1, k_2 \in SU(2) \otimes SU(2) \) and \( D_1, D_2, D_3 \in \mathbb{R} \). To write \( U_{ij} = e^{-it(a(X_i + X_j) + bZ_i Z_j)} \) in this form we first diagonalize \( h_{ij} = a(X_i + X_j) + bZ_i Z_j \) and obtain its eigenvalues \( \{\epsilon_i\} \) and eigenstates \( \{|\epsilon_i\rangle\} \). Then we can obtain \( U_{ij} \) as \( \sum_{i} e^{-it\epsilon_i} |\epsilon_i\rangle \langle \epsilon_i| \). If we decompose \( U_{ij} \) in the Pauli basis, we can show that it has the following form:

\[ U_{ij} = P_{00} I + P_{01} X_i + P_{10} X_i + P_{11} X_i X_j + P_{22} Y_j + P_{33} Z_i Z_j \]

(F2)

with other terms equal to zero. From this form we see that we do not need to consider the most general form of a single qubit gate for \( k_1 \) and \( k_2 \). Instead we start from the following ansatz, which we will show to be sufficient:

\[ e^{-i\beta(X_i + X_j)} e^{-iD_1 X_i X_j} e^{-iD_2 Y_j} e^{-iD_3 Z_j} e^{-i\beta(X_i + X_j)} \]

(F3)

With this ansatz, the problem becomes solving the following equality:

\[ e^{-i\beta(X_i + X_j)} e^{-iD_1 X_i X_j} e^{-iD_2 Y_j} e^{-iD_3 Z_j} e^{-i\beta(X_i + X_j)} \]

(F4a)

\[ = e^{-i\beta(X_i + X_j)} e^{-iD_1 X_i X_j} e^{-iD_2 Y_j} e^{-iD_3 Z_j} e^{-i\beta(X_i + X_j)} \]

(F4b)

This requires solving 16 coupled equations, each for one element of a 4 x 4 matrix. To simplify the task we represent both sides of Eq. (F4) in the “magic basis” defined
in Ref. [40] as:

\[ |\phi_1\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad |\phi_2\rangle = \frac{i}{\sqrt{2}}(|00\rangle - |11\rangle) \quad |\phi_3\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \quad |\phi_4\rangle = \frac{i}{\sqrt{2}}(|01\rangle + |10\rangle). \]  

\[ \text{(F5a)} \]

In this basis both matrices are sparse, and can be equated term by term to solve for the given parameters. Also, the non-local part of the right hand side of Eq. (F4b), \( e^{-iD_1X_3}e^{-iD_2Y_1}e^{-iD_3Z_2} \), is diagonal in the magic basis. The following matrix changes the basis from the computational basis to the magic basis:

\[ Q = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i & 0 & 0 \\ 0 & 0 & 1 & i \\ 0 & 0 & -1 & i \\ 1 & -i & 0 & 0 \end{bmatrix}. \]  

\[ \text{(F6)} \]

Using \( Q \) we can write any matrix \( U \in SU(4) \) in the magic basis as:

\[ U_{\text{mag}} = \sum_{i,j} (Q^\dagger U Q)_{ij} |\phi_j\rangle \langle \phi_i| \]  

\[ \text{(F7)} \]

The ansatz defined in Eq. (F4b) takes the following form in this basis:

\[ \begin{bmatrix} u_{11} & 0 & 0 & u_{14} \\ 0 & u_{22} & 0 & 0 \\ 0 & 0 & u_{33} & 0 \\ u_{41} & 0 & 0 & u_{44} \end{bmatrix}, \]  

\[ \text{(F8)} \]

where

\[ u_{11} = \frac{1}{2} e^{-i(D_1+D_2+D_3)}(e^{2iD_2}(\cos(4\beta) - 1) + e^{2iD_3}(\cos(4\beta) + 1)) \]  

\[ u_{14} = e^{-iD_1} \sin(4\beta) \cos(D_2 - D_3) \]  

\[ u_{22} = e^{i(D_1-D_2-D_3)} \]  

\[ u_{33} = e^{i(D_1+D_2+D_3)} \]  

\[ u_{41} = -e^{-iD_1} \sin(4\beta) \cos(D_2 - D_3) \]  

\[ u_{44} = \frac{1}{2} e^{-i(D_1+D_2+D_3)}(e^{2iD_2}(\cos(4\beta) - 1) + e^{2iD_3}(\cos(4\beta) + 1)). \]  

\[ \text{(F9)} \]

The unitary defined in Eq. (F4a) takes the same form as shown in Eq. (F8) in the magic basis, such that:

\[ u_{11} = \cos \left( t \sqrt{4a^2 + b^2} \right) - \frac{i b \sin \left( t \sqrt{4a^2 + b^2} \right)}{\sqrt{4a^2 + b^2}} \]  

\[ u_{14} = \frac{2a \sin \left( t \sqrt{4a^2 + b^2} \right)}{\sqrt{4a^2 + b^2}} \]  

\[ u_{22} = e^{-ibt} \]  

\[ u_{33} = e^{ibt} \]  

\[ u_{41} = -\frac{2a \sin \left( t \sqrt{4a^2 + b^2} \right)}{\sqrt{4a^2 + b^2}} \]  

\[ u_{44} = \cos \left( t \sqrt{4a^2 + b^2} \right) + \frac{i b \sin \left( t \sqrt{4a^2 + b^2} \right)}{\sqrt{4a^2 + b^2}}. \]  

\[ \text{(F10)} \]

Equating Eq. (F9) and Eq. (F10) line by line, we obtain Eq. (18).

**Appendix G: Numerical solutions for the sinc function**

In this appendix we show that for every value of \( C \in [0, \pi] \), there exists a \( k \in \{0, 1, 2, 3\} \) such that the equation:

\[ \text{sinc}(\sqrt{x^2 + (C + k\pi)^2}) = \text{sinc}(C + k\pi) \]  

\[ \text{(G1)} \]

has a solution for some real \( x \) [where \( x = 2at \) in Eq. (20)]. This equation is transcendental and cannot be solved analytically. However, for a given pair of \((C, k)\), numerical methods can approximately solve Eq. (G1) in the domain \( x > 0 \) or determine that no solution exists. We checked the solvability of Eq. (G1) for \( C \in [0, \pi] \) and \( k = 0, 1, 2, 3 \) to determine the minimum range of \( k \) needed to make Eq. (G1) solvable for all \( C \). The results of this numerical determination are plotted in Fig. 10, from which one can see that \( k \in \{0, 1, 2, 3\} \) is sufficient.
FIG. 10. Values of $C$ and $k$ for which Eq. (G1) can be solved for $x > 0$. Color is included for visibility. For each value of $C$, at least one value of $k$ leads to a solution.

[1] J. Preskill, Quantum 2, 79 (2018).
[2] D. Deutsch, Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences, Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences 400, 97 (1985).
[3] D. P. DiVincenzo, Physical Review A 51, 1015 (1995).
[4] S. Lloyd, Physical Review Letters 75, 346 (1995).
[5] S. Lloyd, “Quantum approximate optimization is computationally universal,” (2018), arXiv:1812.11075 [quant-ph].
[6] R. Raussendorf, Physical Review A 72 (2005).
[7] J. Preskill, Quantum 2, 79 (2018).
[8] M. J. Bremner, A. Montanaro, and D. J. Shepherd, Physical Review A 51, 1015 (1995).
[9] S. Lloyd, Physical Review Letters 75, 346 (1995).
[10] S. Lloyd, “Quantum approximate optimization is computationally universal,” (2018), arXiv:1812.11075 [quant-ph].
[11] R. Raussendorf, Physical Review A 72 (2005).
[12] J. Preskill, Quantum 2, 79 (2018).
[13] M. J. Bremner, A. Montanaro, and D. J. Shepherd, Physical Review Letters 117 (2016).
[14] E. Farhi and A. W. Harrow, “Quantum supremacy through the quantum approximate optimization algorithm,” (2019), arXiv:1602.07674 [quant-ph].
[15] S. Aaronson, A. Montanaro, and D. J. Shepherd, Physical Review A 51, 1015 (1995).
[16] S. Lloyd, Physical Review Letters 75, 346 (1995).
lin, W. DeGottardi, D. J. Clarke, J. R. Melford, J. D. Strand, M. J. A. Stoutimore, S. Novikov, D. G. Ferguson, D. Lidar, K. M. Zick, and A. J. Przybysz, PRX Quantum 1, 020314 (2020).

[23] E. Mozgunov and D. A. Lidar, “Quantum adiabatic theorem for unbounded Hamiltonians, with applications to superconducting circuits,” (2020), arXiv:2011.08116 [quant-ph].

[24] E. Farhi, J. Goldstone, and S. Gutmann, “A quantum approximate optimization algorithm,” (2014), arXiv:1411.4028 [quant-ph].

[25] S. C. Benjamin, Phys. Rev. Lett. 88, 017904 (2001).

[26] M. E. Morales, J. Biamonte, and Z. Zimborás, Quantum Information Processing 19, 1 (2020).

[27] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, Physical Review A 52, 3457 (1995).

[28] M. A. Nielsen and I. L. Chuang, Quantum computation and quantum information (Cambridge University Press, 2010).

[29] V. Vizing, Diskret. Analiz 3, 25 (1964).

[30] D. Hangleiter, J. Bermejo-Vega, M. Schwarz, and J. Eisert, Quantum 2, 65 (2018).

[31] A. Zlokapa, S. Boixo, and D. Lidar, “Boundaries of quantum supremacy via random circuit sampling,” (2020), arXiv:2005.02464 [quant-ph].

[32] M. J. Bremner, A. Montanaro, and D. J. Shepherd, Quantum 1, 8 (2017).

[33] H.-S. Zhong, H. Wang, Y.-H. Deng, M.-C. Chen, L.-C. Peng, Y.-H. Luo, J. Qin, D. Wu, X. Ding, Y. Hu, P. Hu, X.-Y. Yang, W.-J. Zhang, H. Li, Y. Li, X. Jiang, L. Gan, G. Yang, L. You, Z. Wang, L. Li, N.-L. Liu, C.-Y. Lu, and J.-W. Pan, Science, eabe8770 (2020).

[34] S. Toda, SIAM J. Comput. 20, 865 (1991).

[35] M. Szegedy, “What do QAOA energies reveal about graphs?” (2019), arXiv:1912.12277 [quant-ph].

[36] D. Lidar and T. Brun, eds., Quantum Error Correction (Cambridge University Press, Cambridge, UK, 2013).

[37] R. Bhatia, Matrix Analysis, Graduate Texts in Mathematics No. 169 (Springer-Verlag, New York, 1997).

[38] D. A. Lidar, P. Zanardi, and K. Khodjasteh, Phys. Rev. A 78, 012308 (2008).

[39] J. Zhang, J. Vala, S. Sastry, and K. B. Whaley, Physical Review A 67 (2003).

[40] S. Hill and W. K. Wootters, Physical Review Letters 78, 5022 (1997).