

Diagonal state designs with reconfigurable real-time circuits

Yizhi Shen ^{1,*} Katherine Klymko,² Eran Rabani ^{3,4,5} Norm M. Tubman,⁶ Daan Camps ²
Roel Van Beeumen ¹ and Michael Lindsey ⁷

¹*Applied Mathematics and Computational Research Division, Lawrence Berkeley National Laboratory, Berkeley, California 94720, USA*

²*NERSC, Lawrence Berkeley National Laboratory, Berkeley, California 94720, USA*

³*Materials Sciences Division, Lawrence Berkeley National Laboratory, Berkeley, California 94720, USA*

⁴*Department of Chemistry, University of California, Berkeley, Berkeley, California 94720, USA*

⁵*The Sackler Center for Computational Molecular and Materials Science, Tel Aviv University, Tel Aviv 69978, Israel*

⁶*NASA Ames Research Center, Moffett Field, California 94035, USA*

⁷*Department of Mathematics, University of California, Berkeley, Berkeley, California 94720, USA*



(Received 27 September 2024; accepted 29 September 2025; published 15 January 2026)

Unitary designs are widely used in quantum computation, but in many practical settings it suffices to construct a diagonal state design generated with unitary gates diagonal in the computational basis. In this work, we introduce a simple and efficient diagonal state 3-design based on real-time evolutions under 2-local Hamiltonians. Our construction is inspired by the classical Girard-Hutchinson trace estimator in that it involves the stochastic preparation of many random-phase states. Though the exact Girard-Hutchinson states are not tractably implementable on a quantum computer, we can construct states that match the statistical moments of the Girard-Hutchinson states with real-time evolution. Importantly, our random states are all generated using the same Hamiltonians for real-time evolution, with the randomness arising solely from stochastic variations in the durations of the evolutions. In this sense, the circuit is fully reconfigurable and thus suited for near-term realizations on both digital and analog platforms. Moreover, we show how to extend our construction to achieve diagonal state designs of arbitrarily high order.

DOI: [10.1103/nb7c-d6kk](https://doi.org/10.1103/nb7c-d6kk)

I. INTRODUCTION

Unitary designs, which faithfully reproduce statistical moments of the Haar distribution, play an important role in quantum information science, with wide-ranging applications including channel benchmarking, state or process tomography, and quantum linear algebra [1–4]. For many problems, it suffices to consider the class of diagonal unitary designs, which consist solely of diagonal unitary operations [5,6]. In principle, constructing a diagonal design should simplify the resulting circuits. Moreover, the restriction to purely diagonal gates augments the feasibility of fault-tolerant, error-corrected implementations [7]. Despite their simplicity, diagonal designs can be highly useful in randomization tasks. Notably, their scrambling properties are sufficient for powerful tomographic probes that predict arbitrary state properties [8–11].

In this manuscript, we introduce a quantum algorithm for constructing a diagonal 3-design, which samples random states within a quantum many-body Hilbert space. To prepare these random states (i.e., wavefunctions), we make use of real-time evolutions under a fixed set of simple and commuting

auxiliary Hamiltonians, where only the evolution durations are randomized (and furthermore independent of the system size). By phase cancellation, the random states yield a desired stochastic resolution of identity. Notably, such randomized real-time evolutions, formally viewed as a sequence of commuting Pauli exponentials, enable a shallow implementation via gadget- or measurement-based rules [12–14]. For example, according to the phase gadget rule, each diagonal Pauli exponential can be decomposed into a single-qubit Z rotation and two ladders of cnot gates. Since our fixed auxiliary Hamiltonians are conveniently 2-local and only the evolution durations are randomized, we say that the circuit implementing our diagonal 3-design is *reconfigurable*. That is, across a variety of both digital and analog platforms, we construct a single hardware-native circuit designed for reuse over many samples.

Compared to other approaches for constructing state designs, the strengths of our approach are that it (1) generates random states through simple real-time evolutions whose durations can be randomized independently of the system size, (2) exactly attains the desired statistical moments while avoiding expensive handling of exponentially large Hilbert spaces, and (3) significantly enhances practical near-term quantum efficiency, since it eliminates the overhead required for approaches that implement a distinct circuit for each sampling instance.

The manuscript is organized as follows. In Sec. II, we start with an overview of unitary and diagonal unitary designs, highlighting the connections and disparities. We then expand

*Contact author: yizhis@lbl.gov

Published by the American Physical Society under the terms of the Creative Commons Attribution 4.0 International license. Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

on the intuition that real-time evolutions of randomized duration can fulfill the conditions of diagonal design. In Sec. III, we present a practical approach for constructing a diagonal design. We explicitly compute its moments and detail its reconfigurable circuit representations on both digital and analog platforms. In Sec. IV, we summarize and conclude.

The real-time construction introduced in Sec. III is well suited for state tomography, in particular for classical shadow protocols. Interestingly, recent ideas based on Hamiltonian-driven shadows [8–11] have demonstrated potential and permit native implementations on analog simulators. In particular, real-time evolution following a single random duration (discussed in detail within Sec. III B) can be employed to generate shadows as considered in Ref. [11], which assumes access to the ideal random diagonal ensemble. Our work reveals that this ensemble can in fact be sampled efficiently using several independent time evolutions of tractable duration.

II. REVIEW OF UNITARY AND DIAGONAL STATE DESIGNS

A unitary design is an ensemble of unitary operators $U \sim p$ drawn according to a distribution p that matches certain statistical moments of the Haar distribution over the unitary group. Specifically, a unitary d -design fulfills the defining property that for any quantum state $|\psi\rangle$,

$$\mathbb{E}_{U \sim p}[(U|\psi\rangle\langle\psi|U^\dagger)^{\otimes d}] = \mathbb{E}_{U \sim \text{Haar}}[(U|\psi\rangle\langle\psi|U^\dagger)^{\otimes d}]. \quad (1)$$

The matching property of Eq. (1) is valuable for a variety of tasks due to the prohibitive cost of explicitly sampling a random quantum circuit from the Haar distribution. In contrast, unitary designs offer a more feasible alternative as they are comparatively simpler to construct [2,15,16].

Meanwhile, *diagonal* unitary designs relax the requirement of matching the full Haar randomness. As its name suggests, a diagonal design involves the action of diagonal unitary operators $U \sim p_{\text{diag}}$ on some reference state [5,6]. To introduce the associated moment-matching property analogous to Eq. (1), we first consider the N -dimensional random-phase state $|\phi\rangle \in \mathbb{C}^N$,

$$|\phi\rangle = \sum_{\vec{n} \in \{0,1\}^Q} \phi_{\vec{n}} |\vec{n}\rangle = \frac{1}{\sqrt{N}} \sum_{\vec{n} \in \{0,1\}^Q} e^{-i\theta_{\vec{n}}} |\vec{n}\rangle, \quad (2)$$

where we allocate $Q = \lceil \log_2 N \rceil$ qubits to store the state, and $\theta_{\vec{n}} \sim \text{Uniform}(0, 2\pi)$ are independent and identically distributed random variables for all computational basis elements $\vec{n}$. Historically, the use of random-phase vectors $|\phi\rangle$ can be traced back to the seminal work of Girard and Hutchinson on stochastic trace estimation [17–19], for which the coefficients $\phi_{\vec{n}}$ are sampled independently and uniformly from $\{\pm 1\}$, i.e., the Rademacher distribution, on a classical computer. For this reason, throughout our manuscript, we refer to the state $|\phi\rangle$ following Eq. (2) as a classical or conventional Hutchinson state. Accordingly, a diagonal d -design is an ensemble of diagonal unitaries such that for some reference state $|\chi_0\rangle$, it holds that

$$\mathbb{E}_{U \sim p_{\text{diag}}}[(U|\chi_0\rangle\langle\chi_0|U^\dagger)^{\otimes d}] = \mathbb{E}[(|\phi\rangle\langle\phi|)^{\otimes d}], \quad (3)$$

where $|\phi\rangle$ on the right-hand side of Eq. (3) is understood to be a conventional Hutchinson state as in Eq. (2). We comment that it is not tractable to sample wavefunctions with independent components in the computational basis, such as the conventional Hutchinson state, as the cost grows exponentially in the system size.

The matching property prescribed above can be leveraged in computational routines essential for various quantum algorithms. Among the earliest applications is the one clean qubit model of computation [20], a computing paradigm targeting maximally mixed states. In particular, the state $\frac{1}{N}\mathbb{I}$ is stochastically simulated by uniformly sampling the computational basis $\{|\vec{n}\rangle\}_{n=0}^{N-1}$, which forms a 1-design. Moreover, the application of diagonal 2-designs to trace estimation matches the variance yielded by the conventional Hutchinson estimator, which is optimal among all estimators with independent components in the computational basis [19]. The connection between diagonal designs and trace estimation has not been previously observed to our knowledge. In addition, diagonal 3-designs can be exploited to perform accurate state tomography. This capability is crucial for recent Hamiltonian-driven shadows [8–11], which have demonstrated efficient prediction of arbitrary state observables on practical analog simulators.

To construct a state design, typically the scrambling circuits are composed randomly from some suitable pool of candidate gates. For example, the Hadamard, phase, and cnot gates combinatorially generate the Clifford group as a unitary 2-design, while single-qubit and controlled rotations [5] are sufficient to generate a diagonal unitary 2-design. These approaches hence necessitate the realization of a distinct circuit for each sampled random state. Despite encouraging theoretical guarantees on circuit preparation such as polynomial gate count [5,6,21], implementing these designs on near-term hardware would still be costly, since the generation of each random state requires executing a separate circuit compilation with varying gate composition and sequencing.

In our approach, we prioritize minimal quantum resource requirements for constructing a diagonal design. The central ingredient is the real-time evolution of a single, easily-prepared reference state for a random duration of time under an efficiently simulable Hamiltonian. Using this ingredient, we can generate random states achieving the matching identities [Eq. (3)] up to $d = 3$, later extending to the case $d \geq 4$. Importantly, our diagonal design is reconfigurable in the sense that we have described above (as it bypasses the repetitive synthesis and compilation of scrambling circuits), distinguishing itself from sample-and-assemble approaches. Furthermore, our construction is conceptually simple, relying only on commuting Pauli rotations that maximize circuit compression.

We note that scrambling induced by randomized Pauli rotations has also been considered in recent constructions of unitary designs [22,23]. The constructions exploit, for instance, either structured (cyclically sampling certain X and Z exponentials) [22] or exhaustive (blindly sampling all Pauli exponentials) [23] randomness to construct noncommuting rotations. While these approaches effectively generate *approximate* unitary designs, we emphasize that our work achieves *exact* diagonal state designs, which in turn can be built upon to synthesize unitary designs [24]. In Refs. [22,23], the circuit depths required to achieve an approximate unitary

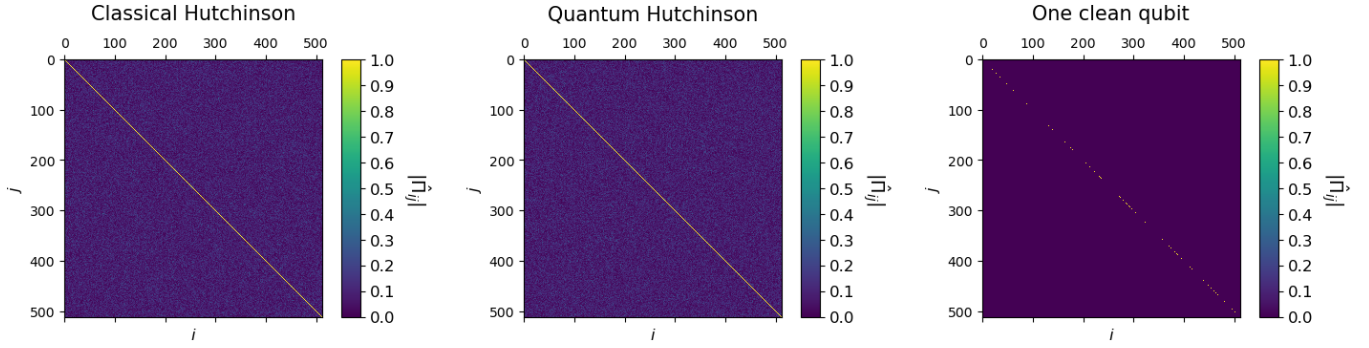


FIG. 1. Approximate resolution of identity $\hat{\Pi} = \frac{N}{K} \sum_{k=1}^K |\chi_k\rangle\langle\chi_k|$ constructed with $K = 10^2$ random states of various types. Left: Classical Hutchinson states. Center: Quantum Hutchinson states (this work). Right: Uniformly sampled computational basis, corresponding to the one clean qubit construction. Matrix elements $\hat{\Pi}_{ij}$ of the approximate identity operator are colored by their magnitudes. Color interpolates linearly from dark blue ($|\hat{\Pi}_{ij}| = 0$) to yellow ($|\hat{\Pi}_{ij}| = 1$). All three ensembles yield unbiased estimators in the infinite-sampling limit, but differ in variance. The figure visually demonstrates that the Hutchinson-based ensembles (left and center) can produce significantly smaller diagonal fluctuations than the uniform computational basis, highlighting the practical advantage of exact diagonal state d -designs ($d \geq 2$) in reducing estimator variance when approximating the identity operator.

d -design with an *additive error* ζ are $\mathcal{O}(d[Q - \log_2 \zeta])$ and $\mathcal{O}(d[Q - \log_2 \zeta] \log_2 Q)$, respectively, given all-to-all device connectivity. Instead, our approach achieves an exact diagonal state d -design using a circuit of depth $\mathcal{O}(Q^{r-1} \log_2 r / (r-1)!)$ with $r(d) = \lceil \log_2(d+1) \rceil$, as we show in Sec. III.

Hereafter, we refer to our random states, $|\chi\rangle = U|\chi_0\rangle$, as *quantum Hutchinson states*. To illustrate the different approaches described in this section and to motivate the quantum Hutchinson approach investigated in this work, we present an explicit comparison of classical Hutchinson, quantum Hutchinson, and one clean qubit approaches for the resolution of the identity, $\mathbb{E}[|\chi\rangle\langle\chi|] = \frac{1}{N}\mathbb{I}$, as shown in Fig. 1. It provides a visualization of how the quantum Hutchinson states achieve a high-fidelity approximation to the identity operator relative to one clean qubit states, given the same number of samples. This illuminates the relevance of an exact diagonal state d -design, particularly for $d \geq 2$, in formulating efficient stochastic estimators. Note the quantum and classical Hutchinson states exhibit nearly indistinguishable variances, though generating the latter at scale remains computationally demanding even on quantum devices.

III. MAIN RESULTS

A. Quantum Hutchinson state construction

In this section, we present the construction of our quantum Hutchinson states.

First, we prepare the initial state of our circuit, which is a uniform superposition of the Z -computational basis elements $\vec{n} \in \{0, 1\}^Q$:

$$|\chi_0\rangle = |+\rangle^{\otimes Q} = \frac{1}{\sqrt{N}} \sum_{\vec{n} \in \{0,1\}^Q} |\vec{n}\rangle, \quad (4)$$

with the use of $Q = \log_2 N$ Hadamard gates.

We evolve this initial state under the following diagonal Hamiltonian of spin-glass type:

$$G = \sum_{i \leq j}^Q \gamma_{ij} \Gamma_i \Gamma_j, \quad (5)$$

where $\Gamma_i = \frac{1-Z_i}{2}$ denotes the number operator acting on the qubit i , alternatively defined by $\Gamma_i|\vec{n}\rangle = n_i|\vec{n}\rangle$ and $\gamma_{ij} \sim \text{Uniform}(0, 2\pi)$ are independent and identically distributed random variables for all pairs of qubits $i \leq j$. We will evolve under G for one unit of time, and this action can be viewed as a sequence of real-time evolutions by all of the $\Gamma_i \Gamma_j$ (which all commute and hence do not introduce any Trotter error) for respective durations γ_{ij} . Our quantum Hutchinson states are thereby prepared as

$$|\chi\rangle = e^{-iG}|\chi_0\rangle = \prod_{i \leq j}^Q e^{-i\gamma_{ij} \Gamma_i \Gamma_j} |\chi_0\rangle, \quad (6)$$

with γ_{ij} sampled uniformly from the interval $[0, 2\pi]$. We will verify later that this construction indeed satisfies the matching properties up to $d = 3$.

For concreteness, we summarize the construction of our exact diagonal state 3-design in Algorithm 1 below.

B. Construction with a single random time

As a theoretical question, it is interesting to consider whether it is possible to construct a suitable quantum Hutchinson state as $|\chi\rangle = e^{-iGt}|\chi_0\rangle$, where G is a single fixed Hamiltonian and t is a single random time. In fact, as we show in Appendix A, it is possible to achieve this goal where G is taken to be a linear combination of the diagonal operators Γ_i and $\Gamma_i \Gamma_j$. However, the random time t must be exponentially

ALGORITHM 1. Diagonal state 3-design.

```

1: Input: System size  $Q$ 
2: Output: Random  $|\chi\rangle$  from a diagonal state 3-design
3:  $|\chi\rangle \leftarrow |+\rangle^{\otimes Q}$ 
4: for  $i = 1$  to  $Q$  do
5:   for  $j = i$  to  $Q$  do
6:      $\gamma_{ij} \sim \text{Uniform}(0, 2\pi)$ ,  $\Gamma_i = \frac{1-Z_i}{2}$  and  $\Gamma_j = \frac{1-Z_j}{2}$ ;
7:      $|\chi\rangle \leftarrow e^{-i\gamma_{ij} \Gamma_i \Gamma_j} |\chi\rangle$ ;
8:   end for
9: end for

```

long in the number of qubits Q . Ultimately it is convenient to view such a long real-time evolution as a sequence of individual real-time evolutions, whose durations are drawn from a different joint distribution than that of our main construction, according to the Hamiltonian components Γ_i and $\Gamma_i\Gamma_j$. From this point of view, the construction Eq. (6) emerges as a simpler alternative in which all the short random times are drawn independently. Moreover, the construction Eq. (6) enjoys the same hardware advantages of real-time evolution under a fixed set of elementary two-qubit Hamiltonians. Nonetheless, due to potential theoretical interest, we give further detail on the single-time construction in Appendix A, and we comment that in fact this work was initially motivated by this perspective.

C. Statistical properties

Now we show that the quantum Hutchinson state constructed in Eq. (6) is a diagonal 3-design.

Theorem 1. Consider the quantum Hutchinson and conventional Hutchinson states drawn randomly according to Eqs. (6) and (2), respectively. The moments of these two constructions match up to third order in the sense that, for $d \leq 3$,

$$\mathbb{E}[(|\chi\rangle\langle\chi|)^{\otimes d}] = \mathbb{E}[(|\phi\rangle\langle\phi|)^{\otimes d}]. \quad (7)$$

$$\mathbb{E}[(|\chi\rangle\langle\chi|)^{\otimes 1}] = \frac{1}{N} \sum_{\vec{m}, \vec{n}} \prod_{i \leq j}^Q \mathbb{E}[e^{i(n_i n_j - m_i m_j)\gamma}] |\vec{m}\rangle\langle\vec{n}| \quad (11)$$

$$= \frac{1}{N} \sum_{\vec{m}, \vec{n}} \prod_{i \leq j}^Q \delta_{n_i n_j, m_i m_j} |\vec{m}\rangle\langle\vec{n}| \quad (12)$$

$$= \frac{1}{N} \sum_{\substack{\vec{m}, \vec{n}: \\ \vec{m} \otimes \vec{m} = \vec{n} \otimes \vec{n}}} |\vec{m}\rangle\langle\vec{n}| \stackrel{(\text{Lemma 1})}{=} \mathbb{E}[(|\phi\rangle\langle\phi|)^{\otimes 1}], \quad (13)$$

$$\mathbb{E}[(|\chi\rangle\langle\chi|)^{\otimes 2}] = \frac{1}{N^2} \sum_{\vec{m}, \vec{m}', \vec{n}, \vec{n}'} \prod_{i \leq j}^Q \delta_{n_i n_j + n'_i n'_j, m_i m_j + m'_i m'_j} |\vec{m}\vec{m}'\rangle\langle\vec{n}\vec{n}'| \quad (14)$$

$$= \frac{1}{N^2} \sum_{\substack{\vec{m}, \vec{m}', \vec{n}, \vec{n}': \\ \vec{m} \otimes \vec{m} + \vec{m}' \otimes \vec{m}' = \vec{n} \otimes \vec{n} + \vec{n}' \otimes \vec{n}'}} |\vec{m}\vec{m}'\rangle\langle\vec{n}\vec{n}'| \stackrel{(\text{Lemma 1})}{=} \mathbb{E}[(|\phi\rangle\langle\phi|)^{\otimes 2}], \quad (15)$$

$$\mathbb{E}[(|\chi\rangle\langle\chi|)^{\otimes 3}] = \frac{1}{N^3} \sum_{\substack{\vec{m}, \vec{m}', \vec{m}'', \vec{n}, \vec{n}', \vec{n}'': \\ \vec{m} \otimes \vec{m} + \vec{m}' \otimes \vec{m}' + \vec{m}'' \otimes \vec{m}'' = \vec{n} \otimes \vec{n} + \vec{n}' \otimes \vec{n}' + \vec{n}'' \otimes \vec{n}''}} |\vec{m}\vec{m}'\vec{m}''\rangle\langle\vec{n}\vec{n}'\vec{n}''| \stackrel{(\text{Lemma 1})}{=} \mathbb{E}[(|\phi\rangle\langle\phi|)^{\otimes 3}]. \quad (16)$$

To arrive at Eqs. (13), (15), and (16) in the calculations, we have used the following lemma:

Lemma 1. For vectors $\vec{m}_1, \vec{m}_2, \vec{m}_3, \vec{n}_1, \vec{n}_2, \vec{n}_3 \in \{0, 1\}^Q$ and integer $1 \leq d \leq 3$, the matrix identity,

$$\sum_{i=1}^d \vec{m}_i \otimes \vec{m}_i = \sum_{i=1}^d \vec{n}_i \otimes \vec{n}_i \quad (17)$$

holds if and only if $(\vec{m}_1, \dots, \vec{m}_d) = \mathcal{P}_d(\vec{n}_1, \dots, \vec{n}_d)$ for some permutation $\mathcal{P}_d \in S_d$. Here, $\otimes$ is understood as the vector outer product so each term $\vec{m}_i \otimes \vec{m}_i$ can be viewed as a sym-

Proof. We first observe that the Hutchinson construction admits the statistical moments

$$\mathbb{E}[(|\phi\rangle\langle\phi|)^{\otimes 1}] = \frac{1}{N} \sum_{\vec{n}} |\vec{n}\rangle\langle\vec{n}|, \quad (8)$$

$$\mathbb{E}[(|\phi\rangle\langle\phi|)^{\otimes 2}] = \frac{1}{N^2} \sum_{\substack{\vec{m}, \vec{m}', \vec{n}, \vec{n}': \\ (\vec{m}, \vec{m}') = \mathcal{P}_2(\vec{n}, \vec{n}') \text{ for some } \mathcal{P}_2 \in S_2}} |\vec{m}\vec{m}'\rangle\langle\vec{n}\vec{n}'|, \quad (9)$$

$$\begin{aligned} \mathbb{E}[(|\phi\rangle\langle\phi|)^{\otimes 3}] \\ = \frac{1}{N^3} \sum_{\substack{\vec{m}, \vec{m}', \vec{m}'', \vec{n}, \vec{n}', \vec{n}'': \\ (\vec{m}, \vec{m}', \vec{m}'') = \mathcal{P}_3(\vec{n}, \vec{n}', \vec{n}'') \text{ for some } \mathcal{P}_3 \in S_3}} |\vec{m}\vec{m}'\vec{m}''\rangle\langle\vec{n}\vec{n}'\vec{n}''|, \end{aligned} \quad (10)$$

where the $\mathcal{P}_d \in S_d$ appearing in the summations above indicate permutations of d bitstrings. The vector equality constraints up to a permutation arise from the statistical independence of random phases $\theta_{\vec{n}}$ in Eq. (6).

Next, we consider the quantum Hutchinson construction. Note that if $\gamma \sim \text{Uniform}(0, 2\pi)$, then for any integer k , the expectation $\mathbb{E}[e^{ik\gamma}]$ is 1 if $k = 0$, and 0 otherwise. This identity enables the computations:

metric matrix $\vec{m}_i^\top \vec{m}_i$, or equivalently a 2-tensor, with entries $(\vec{m}_i \otimes \vec{m}_i)_{ab} = m_{i,a} m_{i,b}$.

The proof of Lemma 1 is presented within Appendix B, where we also explain why the lemma does not apply to the case $d = 4$. This thus completes the proof of Theorem 1. It is worth noting that the exact same proof holds if we replace the uniform random sampling of time durations γ_{ij} over $(0, 2\pi)$ with a uniform sampling from the discrete set $\{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$ as can be confirmed by direct calculation. ■

Now, let us illustrate how Theorem 1 is applied to yield guarantees on our random states $|\chi\rangle$. First, the base

case $d = 1$, together with Eq. (8), establishes the stochastic resolution of identity, $\mathbb{E}[|\chi\rangle\langle\chi|] = \frac{1}{N}\mathbb{I}$, essential in many randomization tasks. Second, we examine the case $d = 2$. Theorem 1 in this case, combined with Eq. (9), implies that

$$\mathbb{E}[|\chi\rangle\langle\chi|^{\otimes 2}] = \left(\frac{1}{N} \sum_{\vec{n}} |\vec{n}\rangle\langle\vec{n}| \right)^{\otimes 2} + \frac{1}{N^2} \sum_{\vec{m} \neq \vec{n}} |\vec{m}\vec{n}\rangle\langle\vec{m}\vec{n}|, \quad (18)$$

recovering the well-known second moment of conventional Hutchinson states:

$$\mathbb{E}[|\langle\chi|A|\chi\rangle|^2] = |\mathbb{E}\langle\chi|A|\chi\rangle|^2 + \frac{1}{N^2} \sum_{\vec{m} \neq \vec{n}} |\langle\vec{m}|A|\vec{n}\rangle|^2, \quad (19)$$

where $A \in \mathbb{C}^{N \times N}$ and $\mathbb{E}\langle\chi|A|\chi\rangle = \frac{1}{N}\text{Tr}[A]$.

Alternatively, we can express the variance as

$$\mathbb{V}[\langle\chi|A|\chi\rangle] = \frac{1}{N^2} \sum_{\vec{m} \neq \vec{n}} |\langle\vec{m}|A|\vec{n}\rangle|^2 \leq \frac{1}{N^2} \|A\|_F^2, \quad (20)$$

where we have a succinct bound in terms of the Frobenius norm of the operator A . Note that the exact expression for the variance can often be reduced through a similarity transformation, for example, if A enjoys certain symmetries [25]. By Chebyshev's inequality, taking an empirical average over K randomly sampled states, we expect that with high probability

$$\left| \frac{1}{K} \sum_{k=1}^K \langle\chi_k|A|\chi_k\rangle - \frac{1}{N} \text{Tr}[A] \right| \leq \frac{1}{N} \|A\|_F \epsilon, \quad (21)$$

where $\epsilon = \mathcal{O}(\frac{1}{\sqrt{K}})$ independently of A . In this sense, we say that the fluctuations of the estimator for the normalized operator trace are on the order of $\frac{1}{N} \|A\|_F$.

Finally, we explore how our simple construction can be generalized naturally to higher-order diagonal designs by increasing the interaction locality in the Hamiltonian G . We focus on diagonal d -designs with $4 \leq d \leq 7$ as an illustrative example, while demonstrating that the underlying argument extends inductively to a general diagonal d -design as presented in Algorithm 2.

ALGORITHM 2. Diagonal state d -design.

```

1: Input: System size  $Q$ 
2: Output: Random  $|\chi\rangle$  from a diagonal state  $d$ -design
3:  $r \leftarrow \lceil \log_2(d+1) \rceil$ ;
4:  $|\chi\rangle \leftarrow |\chi_0\rangle = |+\rangle^{\otimes Q}$ ;
5: for  $i = 1$  to  $Q$  do
6:   for  $i_2 = i_1$  to  $Q$  do
7:      $\vdots$ 
8:   for  $i_r = i_{r-1}$  to  $Q$  do
9:      $\gamma_{i_1 i_2 \dots i_r} \sim \text{Uniform}(0, 2\pi)$ ;
10:     $\Gamma_i = \frac{1}{2}(1 - Z_i)$  for  $i = i_1, i_2, \dots, i_r$ ;
11:     $|\chi\rangle \leftarrow e^{-i\gamma_{i_1 i_2 \dots i_r} \Gamma_{i_1} \Gamma_{i_2} \dots \Gamma_{i_r}} |\chi\rangle$ ;
12:   end for
13: end for
14: end for

```

Corollary 1. The quantum Hutchinson states $|\chi\rangle = e^{-iG}|\chi_0\rangle$ generated by the following 3-local Hamiltonian,

$$G = \sum_{i \leq j \leq k}^Q \gamma_{ijk} \Gamma_i \Gamma_j \Gamma_k, \quad (22)$$

form a diagonal 7-design, provided that all the durations $\gamma_{ijk} \sim \text{Uniform}(0, 2\pi)$ or $\gamma_{ijk} \sim \text{Uniform}\{\frac{\pi}{4}f : f \in \mathbb{Z}_8\}$ are drawn independently. More generally, an r -local Ising Hamiltonian of the form

$$G = \sum_{i_1 \leq i_2 \leq \dots \leq i_r}^Q \gamma_{i_1 i_2 \dots i_r} \Gamma_{i_1} \Gamma_{i_2} \dots \Gamma_{i_r} \quad (23)$$

generates a diagonal d -design of order up to $d = 2^r - 1$, provided that $\gamma_{i_1 i_2 \dots i_r} \sim \text{Uniform}(0, 2\pi)$ or $\gamma_{i_1 i_2 \dots i_r} \sim \text{Uniform}\{\frac{2\pi}{d+1}f : f \in \mathbb{Z}_{d+1}\}$ are drawn independently.

The proof of Corollary 1 follows from Theorem 1 and is outlined in Appendix B. ■

D. Resource requirements

Having established that our construction realizes exact diagonal state d -designs, we now turn to the motivation and resource implications.

Exact state designs, beyond their approximate counterpart, are valuable in several contexts. In randomized benchmarking and certification protocols [26,27], perfect error cancellation hinges on averaging over exact designs. Substituting approximate designs introduces systematic errors that build up when the designs are repeatedly used within a single run of the protocols, which can ultimately spoil the outcome [28]. In observable prediction protocols under shadow tomography, moment-matching ensembles, including exact diagonal designs, often yield a closed-form inverse of the shadow channel for tractable classical processing [11,29]. By contrast, approximate designs can lead to complicated or unstable formal inverses, incurring unwanted bias.

In practice, the resource overhead of our exact diagonal state designs can be quantified explicitly. For a diagonal state 3-design, our construction uses Q one- and $\frac{Q(Q-1)}{2}$ two-qubit Pauli rotations, covering all qubit pairings, to implement the generating Hamiltonian. Each two-qubit Pauli rotation is equivalent to a single-qubit rotation conjugated by two cnot gates. More generally, a diagonal state d -design uses $\binom{Q+r-1}{r}$ Pauli rotations, corresponding to all r -qubit multisets. Each multiqubit rotation decomposes into a single-qubit rotation and at most $2(r-1)$ cnot gates arranged in two ladders. For a fixed $r \ll Q$, the quantum circuit depth thus scales as

$$D \leq \frac{\binom{Q}{r} \log_2 r}{Q/r} = \mathcal{O}(Q^{r-1} \log_2 r / (r-1)!), \quad (24)$$

while the total gate count is

$$N_{\text{gate}} \leq \underbrace{\binom{Q+r-1}{r}}_{\text{single-qubit}} + 2(r-1) \underbrace{\binom{Q+r-1}{r}}_{\text{CNOT}} \quad (25)$$

$$= \mathcal{O}(Q^r / (r-1)!), \quad (26)$$

where $\log_2 r$ reflects circuit depth arising from the binary-tree implementation of each cnot ladder [23].

E. Reconfigurability on digital platforms

Next, we examine the hardware requirements for our diagonal 3-design on a digital quantum platform. In particular, all quantum Hutchinson instances can be realized with a single reconfigurable quantum circuit.

Observe that by using $\Gamma_i \Gamma_j = \frac{1}{4}(1 - Z_i - Z_j + Z_i Z_j)$, the Hamiltonian G from Eq. (5) can be rewritten, up to a global phase, in terms of the Pauli Z operators as the Ising-type Hamiltonian,

$$G = \sum_{i < j}^Q h_{ij} Z_i Z_j + \sum_{i=1}^Q h_i Z_i, \quad (27)$$

with the Ising couplings and external field strengths given by $h_{ij} = \frac{\gamma_{ij}}{4}$ and $h_i = -\frac{\gamma_i}{2} - \sum_{j>i} \frac{\gamma_{ij}}{4}$. The unitary time evolution in the Z basis is hence a product of elementary diagonal gates:

$$e^{-iGt} = \left(\prod_{i \neq j}^Q e^{-ih_{ij} Z_i Z_j t} \right) \left(\prod_{i=1}^Q e^{-ih_i Z_i t} \right) \quad (28)$$

$$= \left(\prod_{i < j}^Q R_{zz}(4h_{ij}t | i, j) \right) \left(\bigotimes_{i=1}^Q R_z(2h_i t | i) \right), \quad (29)$$

where $R_z(\phi | i)$ and $R_{zz}(\phi | i, j)$ are one- and two-qubit Z rotations of angle ϕ , respectively. Each two-qubit rotation can be further unfolded as a cnot-conjugated one-qubit rotation:

$$R_{zz}(\phi | i, j) = C_x(i, j) R_z(\phi | j) C_x(i, j), \quad (30)$$

where the cnot, $C_x(i, j)$, acts on the control and target qubits (i, j) . Hence, the circuit can be efficiently synthesized using only one-qubit Z rotations and two-qubit cnot gates.

Notably, the quantum Hutchinson state sampling only involves modification of the $\mathcal{O}(Q^2)$ rotation angles but does not involve replacement or reordering of any gates. Moreover, by exploiting gate commutation relations, we can bound both the gate count and circuit depth required to produce a quantum Hutchinson state (cf. Theorem 2 below). The circuit we have presented yields a naïve gate count scaling of $\mathcal{O}(Q^2)$, with $\frac{Q(Q+1)}{2} R_z$ gates and $Q(Q-1)$ cnot gates. While the implementation of this circuit is indeed feasible on devices with native all-to-all connectivity, we can slightly reduce the cnot gate count and moreover show that the circuit depth is $\mathcal{O}(Q)$.

Theorem 2. e^{-iG} can be implemented using a single circuit with depth no greater than $D = 9Q - 2$, where the circuit contains $\frac{Q(Q+1)}{2} R_z$ gates and at most $N_{\text{CNOT}} = \lfloor \frac{5Q^2 - 3Q - 2}{6} \rfloor$ cnot gates.

Proof. We exploit the commutation or rewriting rules for R_z and cnot gates,

$$C_x(j, k) R_{zz}(\phi | i, j) = R_{zz}(\phi | i, j) C_x(j, k), \quad (31)$$

$$C_x(i, j) C_x(j, k) C_x(i, k) = C_x(j, k) C_x(i, j), \quad (32)$$

where (i, j, k) indexes a triplet of distinct qubit registries. When combined, the rules help improve local compilation as

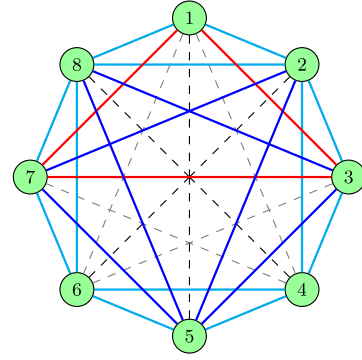
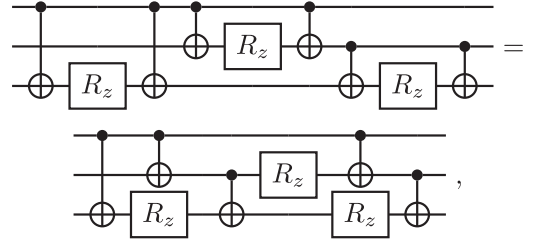


FIG. 2. Edge-disjoint triangles in a complete graph with $|\mathcal{V}| = Q = 8$ vertices. The colors distinguish triangles with different connectivities.

illustrated graphically below,



resulting in a reduction in both the gate count and circuit depth for a three-qubit block. Recall that each $R_{zz}(\phi | i, j)$ uniquely captures a two-body interaction $h_{ij} Z_i Z_j$ in G . So the overall resource reduction from our improved local compilation can be estimated by identifying the triplets or triangles (i, j, k) that lack shared edges in an all-to-all graph representing our Ising Hamiltonian. This is a topic deeply examined in graph theory and combinatorics [30–32]. In particular, we highlight the fact that in a complete graph, $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ with $|\mathcal{E}| = \frac{|\mathcal{V}|(|\mathcal{V}|-1)}{2}$, the maximal number of such edge-disjoint triangles is at least $N_a \geq \frac{(|\mathcal{V}|-1)(|\mathcal{V}|-2)}{6}$. For example, Fig. 2 shows the assembly of different three-qubit blocks in a eight-qubit complete graph, where a set of seven edge-disjoint triangles is highlighted. The number of ‘dangling’ edges untouched by the triangles is therefore bounded by $N_b \leq |\mathcal{E}| - 3N_a = Q - 1$, which gives a total cnot count of

$$N_{\text{CNOT}} \leq 5N_a + 2N_b. \quad (33)$$

Moreover, it is apparent that any two triangles commute with each other unless they share a common vertex. This observation allows us to bound the circuit depth,

$$D \leq 12 \left\lfloor \frac{Q}{2} \right\rfloor + 3N_b + 1, \quad (34)$$

where the first two terms in Eq. (34) account for the $\lfloor \frac{Q}{2} \rfloor$ layers of triangles with varying connectivities, as marked by the different colors in Fig. 2, and N_b layers of untouched dangling edges. We also include the layer of R_z gates that capture the external fields $\{h_i Z_i\}_{i=1}^Q$ in G .

(For the special cases $Q \equiv 1 \pmod{6}$ or $Q \equiv 3 \pmod{6}$, we saturate an optimal number of edge-disjoint triangles,

$N_a = \frac{Q(Q-1)}{6}$. This therefore implies a tighter bound of $N_{\text{CNOT}} \leq \frac{5Q^2-5Q}{6}$ and $D \leq 6Q + 1$ in these cases. ■

For higher-order diagonal designs generated via r -local Hamiltonian, a similar analysis allows us to establish that the scrambling circuit has depth $\mathcal{O}(Q^{r-1}/(r-1)!)$, where we recall $r = \lceil \log_2(d+1) \rceil$ as indicated in Sec. III C.

F. Reconfigurability on analog platforms

In this section, we proceed to investigate the hardware implementation of our diagonal 3-design on a dynamics-driven analog platform, where the construction based on the real-time evolution yields significant advantages. Our analysis primarily centers around systems of interacting neutral atoms undergoing Rydberg excitations [33,34]. Although our focus is specific, similar considerations can hold for other analog models.

Recall that a general Rydberg Hamiltonian takes the form

$$G_{\text{Rydberg}} = \sum_{i=1}^Q \Omega_i X_i + \sum_{i=1}^Q \Delta_i \Gamma_i + \sum_{i<j}^Q V_{ij} \Gamma_i \Gamma_j, \quad (35)$$

where Ω_i and Δ_i determine the local Rabi frequency and detuning, respectively, on the atomic site i , while $V_{ij} \propto \frac{1}{r_{ij}^6}$ sets the repulsive van der Waals interaction between sites i and j separated by a distance of r_{ij} . Therefore, our spin-glass Hamiltonian G is natively Rydberg with vanishing Rabi driving, $\Omega_i \equiv 0$.

In addition, preparation of the initial state can be accomplished by unit-time evolution under another Rydberg Hamiltonian of the form of Eq. (35), where $\Omega_i = -\frac{\Delta_i}{2} = -\frac{\pi}{2\sqrt{2}}$ and $V_{ij} \equiv 0$. This is the case because

$$|\chi_0\rangle = \bigotimes_{i=1}^Q e^{i\frac{\pi}{2\sqrt{2}}(X_i+Z_i)} |\vec{0}\rangle, \quad (36)$$

where physical ground state $|\vec{0}\rangle$ is the native atomic configuration.

The overall evolution that we require, including the preparation of $|\chi_0\rangle$ can therefore be produced using the time-dependent waveforms,

$$\begin{cases} (\Omega_i, \Delta_i) = \left(-\frac{\pi}{2\sqrt{2}}, \frac{\pi}{\sqrt{2}}\right), & \text{if } 0 \leq t \leq 1, \\ (\Omega_i, \Delta_i) = (0, \gamma_{ii}), & \text{if } 1 \leq t \leq 2, \end{cases} \quad (37)$$

prescribing piecewise-constant local Rabi drivings as well as detunings.

Moving forward, we discuss the simulation of the remaining pairwise coupling terms with physical interactions V_{ij} .

Naïvely, given positive weights $\gamma_{ij} \sim \text{Uniform}(0, 2\pi)$, we must choose the Q atomic positions $\vec{r}_i$ so that the resulting distances $r_{ij} = \|\vec{r}_i - \vec{r}_j\|_2$ satisfy $V_{ij}(r_{ij}) = \gamma_{ij}$. However, this embedding problem is NP-hard when Q exceeds the spatial dimension (which is 3 at most), and a solution does not exist in most cases.

Instead, we formulate an alternative approach by exploiting the commutation of the diagonal operators Γ_i . As a first attempt, we consider the decomposition $e^{-iGt} = \prod_{i<j} e^{-iG_{ij}t}$,

where

$$G_{ij} := \gamma_{ij} \Gamma_i \Gamma_j + \frac{1}{Q-1} (\gamma_{ii} \Gamma_i + \gamma_{jj} \Gamma_j), \quad (38)$$

which holds because $\Gamma_i = \Gamma_i \Gamma_i$ for each i . The regrouping of the Hamiltonian contributions suggests that we should achieve the analog evolution e^{-iGt} using $\frac{Q(Q-1)}{2}$ analog blocks $e^{-iG_{ij}t}$ each of which couples only a single pair of atoms, and between which atom positions are dynamically shuffled.

However, by considering a more sophisticated coupling within each analog block we can bring the block depth down to Q . Theorem 3 states this result and moreover quantifies the atom shuffling that we require between blocks in terms of the number of SWAP gates, each of which is realized as the physical swapping of a pair of atoms. In this construction, it is more convenient to work with simplified γ_{ij} that are sampled i.i.d. from the uniform distribution over the discrete set $\{0, \frac{2\pi}{3}, \frac{4\pi}{3}\}$. If γ is so distributed, then for any integer k , the expectation $\mathbb{E}[e^{ik\gamma}]$ is 1 if k is an integer multiple of 3, and 0 otherwise. Therefore, the variance equality from Theorem 1 holds just as well in this case.

Theorem 3. e^{-iG} can be implemented on a Rydberg simulator with at most Q analog blocks. Each of these analog blocks performs Rydberg evolution of time $\mathcal{O}(1)$ for a one-dimensional chain of Q Rydberg atoms. The circuit also involves a total of at most $N_{\text{SWAP}} = \frac{Q(Q-1)}{2}$ swap gates, i.e., the physical swaps of two atoms, which appear in between the analog blocks.

Proof. The use of the discrete couplings γ_{ij} allows us to restrict to only three physical distances $\Lambda_2 < \Lambda_1 < \Lambda_0$ such that $V_{ij}(\Lambda_2) = \frac{4\pi}{3}$, $V_{ij}(\Lambda_1) = \frac{2\pi}{3}$, and $V_{ij}(\Lambda_0) = 0$. This choice is possible due to the rapid decay of the van der Waals interaction.

We now invoke classic edge coloring results for a complete graph of Q vertices corresponding to the Q qubits. Specifically, the edges of this graph can be decorated with at most Q different colors so that no incident edges have the same color. In general, edge colorings can be assigned efficiently with $\mathcal{O}(\text{poly}(Q))$ run-time [35,36], but we make use of a very specific construction for the complete graph.

Without loss of generality, we assume that Q is even and use the following coloring scheme. We distribute $Q-1$ vertices evenly on a circle to create a regular polygon and locate the remaining vertex at the center of the circle, as illustrated in Fig. 3. Then, we assign a distinct color to each edge connecting a central-exterior vertex pair (as indicated by dashed lines in Fig. 3), and color the edges perpendicular to the central edge (as solid lines in Fig. 3). This assignment uses $\frac{|\mathcal{E}|}{|\mathcal{V}|/2} = Q-1$ colors to cover our complete graph.

Let $\{\mathcal{E}_i\}_{i=1}^{Q-1}$ be a partition of the edge set $\mathcal{E}$,

$$\bigsqcup_{i=1}^{Q-1} \mathcal{E}_i = \mathcal{E}, \quad (39)$$

resulting from the coloring scheme above. Our analog evolution can thus be achieved using $Q-1$ blocks,

$$e^{-iG} = \prod_{k=1}^{Q-1} e^{-iG_k} = \prod_{k=1}^{Q-1} \prod_{(i,j) \in \mathcal{E}_k} e^{-iG_{ij}}, \quad (40)$$

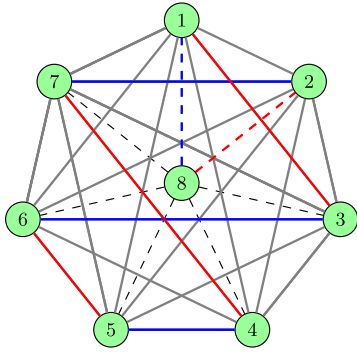


FIG. 3. Edge-coloring of a complete graph with $|\mathcal{V}| = Q = 8$ vertices. The colors partition all the edges into $(Q - 1)$ groups. Each group represents a unique atom configuration consisting of disjoint doublets. For purpose of visualization, we highlight two of the colored groups (red and blue, respectively).

where the Hamiltonian G_k for each analog block only includes interactions between atom dimers that share the same color assignment. The block Hamiltonian G_k can be embedded onto a one-dimensional lattice with variable lattice spacing Λ_0 , Λ_1 , and Λ_2 as sketched in Fig. 4. To change the dimer configuration from G_k to G_{k+1} , we permute $Q/2$ vertices on the lattice since we can redistribute them to pair with the remaining half of the vertices. For example, the pairing $(3, 1) \mapsto (3, 6)$ in Fig. 4 from red to blue leaves the vertex 3 untouched. Such a permutation can canonically be written as a sequence of at most $\frac{Q}{2} - 1$ elementary transpositions. A transposition of the two vertices i and j corresponds to the physical swapping of two atom positions. Such atom swaps upon the application of each analog block are shown schematically in Fig. 4. We notice that each set of $\frac{Q}{2}$ distinctly colored edges can be paired with one of the exterior edges $(1, 2), (2, 3), \dots$, etc. Since our graph of polygon exhibits a discrete rotational symmetry along its exterior edges, all the $|\mathcal{V}|$ edges can be decorated as we cycle through the exterior edges. Accordingly, we employ

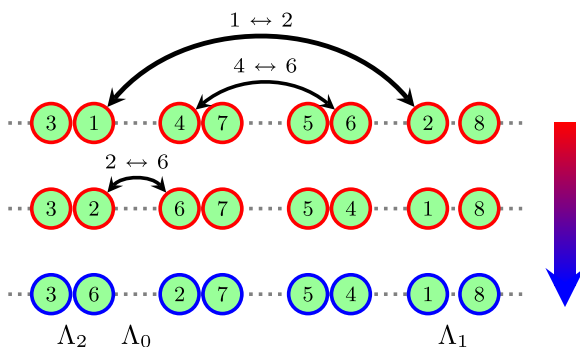


FIG. 4. Embedding of the edge-colored graph onto a one-dimensional chain of interacting neutral atoms with $|\mathcal{V}| = Q = 8$ qubits. Each color, assigned on a subset of $Q/2$ edges, designates a dimer pairing of the vertices, which is reconfigured after each analog block e^{-iG_k} . The swapping involved in one such dimer reconfiguration (red to blue as in Fig. 3) is illustrated from top to bottom. The black bent arrows indicate the sequence of vertex transpositions needed to transition from the old to the new color assignment.

a total of $Q - 1$ different permutations throughout the whole analog evolution.

Finally, we remark that the complementary case of odd Q can be adapted readily from the even case, if we introduce an additional, auxiliary vertex to the graph. Combining the two cases, we thereby need at most $N_{\text{SWAP}} = Q(\frac{Q+1}{2} - 1) = \frac{Q(Q-1)}{2}$ to bridge the Q analog blocks. ■

Meanwhile, analog devices with local qubit connectivities, commonly a nearest-neighbor topology, are also capable of simulating e^{-iG} with a similar resource cost. For nearest-neighbor devices, the identification of the graph Hamiltonian paths [37,38], for example, enables us to decompose the evolution into $\mathcal{O}(Q)$ analog blocks [39].

IV. CONCLUSION

In this work, we introduce a real-time diagonal design that is efficiently implementable on near-term hardware. Leveraging time evolution under Ising-type Hamiltonians that can be conveniently realized on digital and analog quantum platforms, we construct randomized “quantum Hutchinson” states. We show that our quantum Hutchinson states match the moments that would be achieved by conventional Hutchinson states in an exponentially high-dimensional space, though the latter can not be efficiently realized with quantum resources. Furthermore, we discuss how to implement the real-time states using a single reconfigurable circuit, whose compilation across different stochastic runs remains unchanged up to the durations of the real-time evolutions. The hardware-adapted implementation suits state-of-the-art digital and analog platforms.

ACKNOWLEDGMENTS

This work was funded by the U.S. Department of Energy (DOE) under Contract No. DE-AC02-05CH11231, through the Office of Science, Office of Advanced Scientific Computing Research (ASCR) Exploratory Research for Extreme-Scale Science (Y.S., K.K., D.C., R.V.B.). This research used resources of the National Energy Research Scientific Computing Center (NERSC), a U.S. Department of Energy Office of Science User Facility located at Lawrence Berkeley National Laboratory, operated under Contract No. DE-AC02-05CH11231. E.R. acknowledges support from the Center for Computational Study of Excited-State Phenomena in Energy Materials (C2SEP) at the Lawrence Berkeley National Laboratory, which is funded by the U.S. Department of Energy, Office of Science, Basic Energy Sciences, Materials Sciences and Engineering Division, under Contract No. DE-AC02-05CH11231, as part of the Computational Materials Sciences Program. N.M.T. is grateful for support from NASA Ames Research Center. This material is based upon work supported by the U.S. Department of Energy, Office of Science, National Quantum Information Science Research Centers, Superconducting Quantum Materials and Systems Center (SQMS) under the Contract No. DE-AC02-07CH11359 and by the U.S. Department of Energy, Office of Science, Accelerated Research in Quantum Computing Centers, Quantum Utility through Advanced Computational

Quantum Algorithms, Grant No. DE-SC0025572. M.L. also acknowledges support from a Sloan Research Fellowship.

APPENDIX A: CONSTRUCTION OF DIAGONAL DESIGN WITH A SINGLE RANDOM TIME

Here, we detail the construction, indicated in Sec. III B, achieving a suitable quantum Hutchinson state with a single random time and a fixed Hamiltonian G .

First, for arbitrary G , consider the full spectral decomposition

$$G = \sum_{n=0}^{N-1} \lambda_n |n^G\rangle\langle n^G|, \quad (\text{A1})$$

with eigenpairs $(\lambda_n, |n^G\rangle)_{n=0}^{N-1}$.

Let us examine the dynamics on an initial state that is a uniform superposition in the G basis, namely, $|\chi^G\rangle := \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} |n^G\rangle$. For a time $t \in \mathbb{R}$, we denote the corresponding time-evolved state by $|\chi(t)\rangle = e^{-iGt} |\chi^G\rangle$. We will view $|\chi(t)\rangle$ as a random state by randomly sampling *only* the time t from a suitable scalar distribution with probability density $p(t)$. Taking an expectation $\mathbb{E}$ over the time randomness, we arrive at the operator identity,

$$\mathbb{E}[|\chi(t)\rangle\langle\chi(t)|] = \frac{1}{N} \sum_{n,m=0}^{N-1} \mathbb{E}[e^{i(\lambda_n - \lambda_m)t}] |m^G\rangle\langle n^G| \quad (\text{A2})$$

$$= \frac{1}{N} (\mathbb{I} + \mathbb{B}), \quad (\text{A3})$$

where the operator $\mathbb{B}$ is a bias in the resolution of identity, which we will show can be made zero or extremely small. [Note that in our main construction of Eq. (6), the resolution of identity is always exactly unbiased].

In the G basis, $\mathbb{B}$ takes the form

$$\mathbb{B} = \sum_{n \neq m}^{N-1} \varphi_t(\Delta_{mn}) |m^G\rangle\langle n^G|, \quad (\text{A4})$$

where $\Delta_{mn} = \lambda_n - \lambda_m$ denote the G -eigenvalue differences and $\varphi_t(s) := \mathbb{E}[e^{ist}]$ denotes the characteristic function of the distribution $p(t)$.

A suitable choice of $p(t)$ can effectively control the bias. For example, a Gaussian distribution $p(t) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-t^2/2\sigma^2}$ yields $\varphi_t(\Delta_{mn}) = e^{-\Delta_{mn}^2\sigma^2/2}$. As σ increases, the bias gets exponentially suppressed. Alternatively, the bias from the fat-tailed distribution $p(t) = \frac{1}{\pi t^2/\sigma} \sin^2(t/\sigma)$ completely vanishes for large σ . In either case, we observe from Eq. (A4) that a nondegenerate G spectrum, i.e., in which $\Delta_{mn} \neq 0$ for all $m \neq n$, is essential to approximately fulfill the stochastic resolution of identity bias, since indeed $\varphi_t(0) = 1$ always.

In addition to guaranteeing the stochastic resolution of identity, we also want our Hutchinson-type estimator to have an ideal variance. Then, for a given operator A whose trace we seek, we can compute the variance of our estimator as

$$\mathbb{V}[\langle\chi(t)|A|\chi(t)\rangle] = \sum_{m \neq n} \sum_{m' \neq n'} A_{mn}^* A_{m'n'} \varphi_t(\Delta_{m'n'}^{mn}), \quad (\text{A5})$$

where again the expectation is taken with respect to the distribution $p(t)$ for t and A_{mn} are the matrix elements of A in the G basis. This variance will match the idealized Hutchinson variance,

$$\sum_{m \neq n} |A_{mn}|^2, \quad (\text{A6})$$

if all the nontrivial differences of eigenvalue differences, denoted $\Delta_{m'n'}^{mn} = \Delta_{mn} - \Delta_{m'n'}$, where $(m, n) \neq (m', n')$ and $(m, m') \neq (n, n')$, are nonzero and the characteristic function is suitably constructed as outlined above.

To make things more concrete, we consider G that is diagonal in the Z basis, so $|\chi_0\rangle = |\chi^G\rangle = |+\rangle^{\otimes Q}$. As a first attempt, we use the operator G_1 with an equispaced spectrum $\lambda_n = n$, where $n = 0, \dots, N-1$. In fact G_1 can be tractably constructed on the quantum computer with $Q = \log_2 N$ qubits in terms of the one-qubit number operators as

$$G_1 = \sum_{k=1}^Q 2^{k-1} \Gamma_k. \quad (\text{A7})$$

Although the spectrum of G_1 is nondegenerate, the differences of eigenvalue differences are highly degenerate, hence the variance of the resulting Hutchinson-type estimator is severely suboptimal.

In order to recover performance of the classic Hutchinson estimator, we are motivated to ask following question: Can we find a simple parametric form of the G spectrum $\{\lambda_n\}$ such that the resulting “excitations” $\{\Delta_{mn}\}_{m \neq n}$ are all distinct from one another? This same question motivates the theory of Golomb rulers in number theory [40–42].

The simplest explicit specification of a Golomb ruler is the sequence

$$\lambda_n = Nn^2 + n, \quad 0 \leq n \leq N-1, \quad (\text{A8})$$

where $\min_{m \neq n} |\Delta_{mn}| = \Delta_{01} = N+1$. It is convenient to normalize our sequence of G eigenvalues, $\lambda_n = \frac{N}{N+1}n^2 + \frac{1}{N+1}n$, so that the minimal excitation is 1: $\min_{m \neq n} |\Delta_{mn}| = 1$.

We can construct a Hamiltonian G_2 achieving this spectrum in terms of G_1 :

$$G_2 = \frac{N}{N+1} G_1^2 + \frac{1}{N+1} G_1 \quad (\text{A9})$$

$$= \sum_{i \neq j}^Q h_{ij} Z_i Z_j + \sum_{i=1}^Q h_i Z_i + \text{const.}, \quad (\text{A10})$$

for suitably defined Ising-type interactions h_{ij} and field strengths h_i .

For an appropriate choice of time randomness, e.g., $p(t) = \frac{1}{\pi t^2/\sigma} \sin^2(t/\sigma)$ with $\sigma > 1$, the exact variance of the conventional Hutchinson estimator is therefore recovered.

Note, however, that the parameters h_{ij} and h_i are exponentially large in the number Q of qubits. In order to construct gates implementing time evolution by G of duration t for a random time $t \sim p(t)$, we would need to compute th_{ij} and th_i modulo 2π to a high precision. This is in principle possible but would require extended-precision arithmetic as the number of qubits grows. Since time evolution by G would best be achieved by running separate time evolutions by the component terms of the Hamiltonian (whose durations are only

significant modulo 2π), we recover an approach similar to our main construction Eq. (6). Although the simplicity of Eq. (6) is to be preferred, it is interesting to observe the connection.

APPENDIX B: PROOF OF LEMMA AND COROLLARY

1. Proof of Lemma 1

Proof. We first note that the matrix identity,

$$\sum_{i=1}^d \vec{m}_i \otimes \vec{m}_i = \sum_{i=1}^d \vec{n}_i \otimes \vec{n}_i, \quad (\text{B1})$$

implies the vector identity,

$$\sum_{i=1}^d \vec{m}_i = \sum_{i=1}^d \vec{n}_i, \quad (\text{B2})$$

when restricted to the diagonal. In the $d = 1$ case, $\vec{m}_1 = \vec{n}_1$ holds trivially from Eq. (B2).

For the case $d = 2$, we make the following observation from Eq. (B2): If $\vec{m}_1 = \vec{n}_1$, it must follow that $\vec{m}_2 = \vec{n}_2$. Hence, we can assume that $\vec{m}_1 \neq \vec{n}_1$, and it remains only to show that $\vec{m}_1 = \vec{n}_2$ or $\vec{n}_1 = \vec{m}_2$, because in either case Eq. (B2) then immediately indicates $(\vec{m}_1, \vec{m}_2) = (\vec{n}_2, \vec{n}_1)$. By the assumption of $\vec{m}_1 \neq \vec{n}_1$, there exists some index $a \in \{1, \dots, Q\}$ such that either $(m_{1,a}, n_{1,a}) = (0, 1)$ or $(m_{1,a}, n_{1,a}) = (1, 0)$. In these respective cases, Eq. (B2) then implies the component identity $(m_{2,a}, n_{2,a}) = (1, 0)$ or $(m_{2,a}, n_{2,a}) = (0, 1)$, respectively. By taking the a th column of Eq. (B1), we obtain

$$m_{1,a}\vec{m}_1 + m_{2,a}\vec{m}_2 = n_{1,a}\vec{n}_1 + n_{2,a}\vec{n}_2. \quad (\text{B3})$$

Accordingly, we must have either $\vec{n}_1 = \vec{m}_2$ or $\vec{m}_1 = \vec{n}_2$ as was to be shown.

Finally, we turn to the case $d = 3$, where we can apply our previous results inductively. First, we observe that if $\vec{m}_1 = \vec{n}_1$, then by Eq. (B1) and our proof in the case $d = 2$, it follows that $(\vec{m}_2, \vec{m}_3) = \mathcal{P}_2(\vec{n}_2, \vec{n}_3)$ for a suitable permutation $\mathcal{P}_2$.

Hence, we can assume that $\vec{m}_1 \neq \vec{n}_1$, so there exists an index $a \in \{1, \dots, Q\}$ such that $(m_{1,a}, n_{1,a}) = (0, 1)$ or $(m_{1,a}, n_{1,a}) = (1, 0)$. Without loss of generality, we focus on the case $(m_{1,a}, n_{1,a}) = (1, 0)$, since similar arguments hold for the complementary case $(m_{1,a}, n_{1,a}) = (0, 1)$ due to the binary symmetry.

The a th component of the vector identity Eq. (B2) then reads as

$$1 + m_{2,a} + m_{3,a} = n_{2,a} + n_{3,a}. \quad (\text{B4})$$

Among $m_{2,a}, m_{3,a}, n_{2,a}, n_{3,a} \in \{0, 1\}$, this equation is solved only by the following choices:

$$(m_{2,a}, m_{3,a}, n_{2,a}, n_{3,a}) = \begin{cases} (0, 0, 1, 0) \\ (0, 0, 0, 1) \\ (1, 0, 1, 1) \\ (0, 1, 1, 1) \end{cases}. \quad (\text{B5})$$

Once again taking the a th column of Eq. (B1), observe that the first two cases indicate $\vec{m}_1 = \vec{n}_2$ and $\vec{m}_1 = \vec{n}_3$, respectively. Either way, we can again reduce to the case $d = 2$.

Then, it remains only to consider the last two cases from Eq. (B5). Taking the a th column of Eq. (B1), these two cases imply that $\vec{m}_1 + \vec{m}_2 = \vec{n}_2 + \vec{n}_3$ and $\vec{m}_1 + \vec{m}_3 = \vec{n}_2 + \vec{n}_3$,

respectively. But from Eq. (B2), we must obtain $\vec{m}_3 = \vec{n}_1$ and $\vec{m}_2 = \vec{n}_1$, respectively. Either way, we once again reduce to the case $d = 2$, and the proof is complete. ■

We remark that these combinatorial arguments do not extend to $d \geq 4$, because the list of cases analogous to Eq. (B5) no longer allows a full reduction to the cases $d \leq 3$. For example, under our assumption $(m_{1,a}, n_{1,a}) = (1, 0)$, the relevant component-wise identity for $d = 4$,

$$1 + m_{2,a} + m_{3,a} + m_{4,a} = n_{2,a} + n_{3,a} + n_{4,a}, \quad (\text{B6})$$

admits many solutions, including the particular choice of $(m_{2,a}, m_{3,a}, m_{4,a}, n_{2,a}, n_{3,a}, n_{4,a}) = (1, 0, 0, 1, 1, 0)$. Now evaluating the a th column of Eq. (B1) with this solution, we arrive at the identities $\vec{m}_1 + \vec{m}_2 = \vec{n}_2 + \vec{n}_3$ and $\vec{m}_3 + \vec{m}_4 = \vec{n}_1 + \vec{n}_4$. However, these two vector identities do not necessarily imply the condition $(\vec{m}_1, \vec{m}_2) = \mathcal{P}_2(\vec{n}_2, \vec{n}_3)$ or $(\vec{m}_3, \vec{m}_4) = \mathcal{P}_2(\vec{n}_1, \vec{n}_4)$. A concrete instance to explicitly verify, even for $Q = 3$, is given by

$$\begin{cases} \vec{m}_1 = (1, 0, 0) \\ \vec{m}_2 = (0, 1, 0) \\ \vec{m}_3 = (0, 0, 1) \\ \vec{m}_4 = (1, 1, 1) \end{cases}, \quad \begin{cases} \vec{n}_1 = (1, 0, 1) \\ \vec{n}_2 = (0, 0, 0) \\ \vec{n}_3 = (1, 1, 0) \\ \vec{n}_4 = (0, 1, 1) \end{cases}, \quad (\text{B7})$$

where $(\vec{m}_1, \dots, \vec{m}_4) \neq \mathcal{P}_4(\vec{n}_1, \dots, \vec{n}_4)$ for $\mathcal{P}_4 \in S_4$. This confirms that the lemma does not hold for $d = 4$.

2. Proof of Corollary 1

Proof. For any $k \in \mathbb{Z}$, if $\gamma \sim \text{Uniform}\{\frac{2\pi}{d+1}f : f \in \mathbb{Z}_{d+1}\}$, then the expectation

$$\mathbb{E}[e^{ik\gamma}] = \begin{cases} 1, & k \in (d+1)\mathbb{Z} \\ 0, & \text{otherwise} \end{cases} \quad (\text{B8})$$

is nonzero only if k is an integer multiple of $d+1$. Under our construction,

$$k = \sum_{i=1}^d \left[\prod_{a \in \mathcal{A}} m_{i,a} - \prod_{a \in \mathcal{A}} n_{i,a} \right], \quad (\text{B9})$$

for a subset $\mathcal{A} \subseteq \{1, \dots, Q\}$ with $|\mathcal{A}| = r$. Since $|k| \leq d$, the expectation remains nonvanishing only if $k = 0$, thus replicating the statistics of $\gamma \sim \text{Uniform}(0, 2\pi)$.

Let us first examine the 3-local Hamiltonian G defined in Eq. (22) with $r = 3$. Consequently, the statistical moments of the quantum Hutchinson state generated under this Hamiltonian can be computed as

$$\mathbb{E}[|\chi\rangle\langle\chi|^{\otimes d}] = \frac{1}{N^d} \sum_{\{\vec{m}_i, \vec{n}_i\}_{i=1}^d}^{\text{restricted}} |\{\vec{m}_i\}\rangle\langle\{\vec{n}_i\}|, \quad (\text{B10})$$

where the summation on the right-hand side is restricted to terms satisfying

$$\sum_{i=1}^d \vec{m}_i \otimes \vec{m}_i \otimes \vec{m}_i = \sum_{i=1}^d \vec{n}_i \otimes \vec{n}_i \otimes \vec{n}_i, \quad (\text{B11})$$

with $\otimes$ understood as a general Kronecker product such that each $\vec{m}_i \otimes \vec{m}_i \otimes \vec{m}_i$ can be equivalently viewed as a 3-tensor with entries $(\vec{m}_i \otimes \vec{m}_i \otimes \vec{m}_i)_{abc} = m_{i,a}m_{i,b}m_{i,c}$. We notice that Eq. (B11) immediately implies the matrix and vector identities Eqs. (B1) and (B2) from Lemma 1. Our first goal is to

establish that Eq. (B11) for $1 \leq d \leq 4$ holds precisely if and only if $(\vec{m}_1, \dots, \vec{m}_d) = \mathcal{P}_d(\vec{n}_1, \dots, \vec{n}_d)$ for some $\mathcal{P}_d \in \mathcal{S}_d$.

In the case $d = 1$, $\vec{m}_1 = \vec{n}_1$ holds trivially from exactly Eq. (B2) as in Appendix B 1.

In the cases $d = 2$ and $d = 3$, we assume as usual that $\vec{m}_1 \neq \vec{n}_1$ where $(m_{1,a}, n_{1,a}) = (1, 0)$ for some qubit index $a \in \{1, \dots, Q\}$. We can then derive desired conclusions in these cases solely from the lower-rank equalities Eqs. (B1) and (B2), following the proof of Theorem 1.

For the interesting case $d = 4$, we once again examine the assumption $(m_{1,a}, n_{1,a}) = (1, 0)$. Let us take the a th slice (column-depth slice) of the tensor identity Eq. (B11) by fixing the first tensor index, i.e.,

$$\sum_{i=1}^4 m_{i,a} \vec{m}_i \otimes \vec{m}_i = \sum_{i=1}^4 n_{i,a} \vec{n}_i \otimes \vec{n}_i, \quad (\text{B12})$$

with possible choices,

$$(m_{2,a}, m_{3,a}, m_{4,a}, n_{2,a}, n_{3,a}, n_{4,a}) = \begin{cases} (0, 0, 0, 1, 0, 0) \\ (0, 0, 0, 0, 1, 0) \\ (0, 0, 0, 0, 0, 1) \\ (1, 0, 0, 1, 1, 0) \\ (1, 0, 0, 1, 0, 1) \\ (1, 0, 0, 0, 1, 1) \\ (0, 1, 0, 1, 1, 0) \\ (0, 1, 0, 1, 0, 1) \\ (0, 1, 0, 0, 1, 1) \\ (0, 0, 1, 1, 1, 0) \\ (0, 0, 1, 1, 0, 1) \\ (0, 0, 1, 0, 1, 1) \\ (1, 1, 0, 1, 1, 1) \\ (1, 0, 1, 1, 1, 1) \\ (0, 1, 1, 1, 1, 1) \end{cases}. \quad (\text{B13})$$

Now, we realize that Theorem 1 can be directly applied to all the choices above, allowing us to conclude the proof for $d = 4$.

We next establish that these quantum Hutchinson states indeed form a diagonal 7-design, based on what we have derived thus far. For $5 \leq d \leq 7$, we want to show

$$\sum_{i=1}^d \vec{m}_i^{\otimes r} = \sum_{i=1}^d \vec{n}_i^{\otimes r} \iff (\vec{m}_i)_{i=1}^d = \mathcal{P}_d((\vec{n}_i)_{i=1}^d), \quad (\text{B14})$$

where $\vec{m}_i^{\otimes r}$ is shorthand for the r -fold Kronecker product of $\vec{m}_i$ with itself. When $d = 5$, our starting assumption of $(m_{1,a}, n_{1,a}) = (1, 0)$ essentially yields two complementary 2-tensor identities upon restricting the first index of the 3-tensor identity,

$$\sum_{i \in \mathcal{I}_\alpha} \vec{m}_i^{\otimes 2} = \sum_{j \in \mathcal{J}_\alpha} \vec{n}_j^{\otimes 2}, \quad \alpha = 1, 2, \quad (\text{B15})$$

where $|\mathcal{I}_\alpha| = |\mathcal{J}_\alpha| \geq 1$ by Eq. (B2), and meanwhile $\mathcal{I}_1 \cup \mathcal{I}_2 = \mathcal{J}_1 \cup \mathcal{J}_2 = \{1, 2, 3, 4, 5\}$ form disjoint partitions. We observe that if $2 \leq |\mathcal{I}_1| \leq 3$, then Theorem 1 immediately implies $(\vec{m}_i)_{i \in \mathcal{I}_\alpha} = \mathcal{P}_{|\mathcal{I}_\alpha|}((\vec{n}_j)_{j \in \mathcal{J}_\alpha})$. Hence, it suffices to consider the remaining cases, where we assume $|\mathcal{I}_1| = 1$ without loss of generality (otherwise we simply exchange the members $\mathcal{I}_1 \leftrightarrow \mathcal{I}_2$). In this case, the 2-tensor identity over $\mathcal{I}_1$ and $\mathcal{J}_1$

trivially implies $\vec{m}_{\mathcal{I}_1} = \vec{m}_{\mathcal{J}_1}$, which, when combined with the left-hand side (LHS) of Eq. (B14), further implies that

$$\sum_{i \in \mathcal{I}_2} \vec{m}_i^{\otimes 3} = \sum_{j \in \mathcal{J}_2} \vec{n}_j^{\otimes 3}. \quad (\text{B16})$$

However, we can now use our result for $d = 4$ since $|\mathcal{I}_2| = |\mathcal{J}_2| = 4$, which allows us to conclude for $d = 5$ [thus, now Eq. (B14) is valid when $1 \leq d \leq 5$]. For $d = 6$, we almost repeat the same analysis, except that we need to consider the cases where $|\mathcal{I}_1| = 1$ and $|\mathcal{I}_2| = 2$. If $|\mathcal{I}_1| = 1$, then we can directly invoke the updated $d = 5$ result to conclude. If $|\mathcal{I}_1| = 2$, the relevant 2-tensor identity over $\mathcal{I}_1$ and $\mathcal{J}_1$ leads to a 3-tensor identity of the form Eq. (B16) over $\mathcal{I}_2$ and $\mathcal{J}_2$ with $|\mathcal{I}_2| = |\mathcal{J}_2| = 4$, allowing us to fully conclude for $d = 6$. Finally for $d = 7$, we encounter the additional nontrivial case of $|\mathcal{I}_1| = 3$ and $|\mathcal{I}_2| = 4$. Once again, the relevant 2-tensor identity over $\mathcal{I}_1$ and $\mathcal{J}_1$ helps us deduce a 3-tensor identity of the form Eq. (B16) over $\mathcal{I}_2$ and $\mathcal{J}_2$ with $|\mathcal{I}_2| = |\mathcal{J}_2| = 4$, which therefore concludes the proof for $4 \leq d \leq 7$. At this point, we can already see why such argument breaks down for $d = 8$: The case $|\mathcal{I}_1| = |\mathcal{I}_2| = 4$ exhausts the utility of our 2-tensor (low-rank) identities, which only provide us information if $|\mathcal{I}_1| \leq 3$ or $|\mathcal{I}_2| \leq 3$.

This completes the argument for $r = 2$ and motivates the introduction of higher-rank tensor identities for achieving higher design orders d by considering higher interaction locality $r > 3$.

In general, for $r > 3$, we want to establish the identity

$$\sum_{i=1}^d \vec{m}_i^{\otimes r} = \sum_{i=1}^d \vec{n}_i^{\otimes r} \iff (\vec{m}_i)_{i=1}^d = \mathcal{P}_d((\vec{n}_i)_{i=1}^d), \quad (\text{B17})$$

for all $d = 1, \dots, 2^r - 1$.

Assume that the equation on the LHS of Eq. (B17) holds, i.e.,

$$\sum_{i=1}^d \vec{m}_i^{\otimes r} = \sum_{i=1}^d \vec{n}_i^{\otimes r}. \quad (\text{B18})$$

Then, in particular,

$$\sum_{i=1}^d \vec{m}_i^{\otimes(r-1)} = \sum_{i=1}^d \vec{n}_i^{\otimes(r-1)}. \quad (\text{B19})$$

By induction on r , for any $d = 1, \dots, 2^{r-1} - 1$, it follows that

$$(\vec{m}_i)_{i=1}^d = \mathcal{P}_d((\vec{n}_i)_{i=1}^d). \quad (\text{B20})$$

Therefore, we can assume without loss of generality that $d \geq 2^{r-1}$.

Let us then extend the validity of Eq. (B17) for increasingly large d , starting with the case $d = 2^{r-1}$. We may assume without loss of generality that $\vec{m}_i \neq \vec{n}_i$ for some $i \in \{1, \dots, d\}$. (Otherwise, we can reduce to the case of $d < 2^{r-1}$.) Then, there exists a qubit index $a \in \{1, \dots, Q\}$ such that $m_{i,a} \neq n_{i,a}$. Upon reordering the i indices and exchanging the roles of $\vec{m}$ and $\vec{n}$, we may simply assume that $m_{1,a} = 1$ and $n_{1,a} = 0$.

By considering the $(a, \dots, \text{ath})$ entry of Eq. (B18) of r -index tensors, we deduce that

$$\sum_{i=1}^d m_{i,a} = \sum_{i=1}^d n_{i,a}. \quad (\text{B21})$$

Since $(m_{1,a}, n_{1,a}) = (1, 0)$, Eq. (B21) implies that there must exist some $j \neq 1$ such that $(m_{j,a}, n_{j,a}) = (0, 1)$. Let

$$\mathcal{I}_1 = \{i : m_{i,a} = 1\}, \quad (\text{B22a})$$

$$\mathcal{J}_1 = \{i : n_{i,a} = 1\}. \quad (\text{B22b})$$

We note that $1 \leq |\mathcal{I}_1| = |\mathcal{J}_1| \leq d - 1 = 2^{r-1} - 1$ (although the sets $\mathcal{I}_1$ and $\mathcal{J}_1$ need not be identical).

Equation (B18) is an equation of two r -index tensors. Now, we consider the equation of $(r - 1)$ -index tensors induced by setting the first index of both sides to be a :

$$\sum_{i \in \mathcal{I}_1} \tilde{m}_i^{\otimes(r-1)} = \sum_{i \in \mathcal{J}_1} \tilde{n}_i^{\otimes(r-1)}. \quad (\text{B23})$$

Since both sides are sums over at most $2^{r-1} - 1$ terms, we deduce by induction that

$$(\tilde{m}_i)_{i \in \mathcal{I}_1} = \mathcal{P}_{|\mathcal{J}_1|}((\tilde{n}_i)_{i \in \mathcal{J}_1}). \quad (\text{B24})$$

[Henceforth, we will adopt the shorthand $(\tilde{m}_i)_{\mathcal{I}_1}$ for, e.g., the LHS of the last equation].

Moreover, Eq. (B24) immediately implies that

$$\sum_{i \in \mathcal{I}_1} \tilde{m}_i^{\otimes r} = \sum_{i \in \mathcal{J}_1} \tilde{n}_i^{\otimes r}. \quad (\text{B25})$$

Combining this with Eq. (B18), we obtain

$$\sum_{i \in \mathcal{I}_2} \tilde{m}_i^{\otimes r} = \sum_{i \in \mathcal{J}_2} \tilde{n}_i^{\otimes r}, \quad (\text{B26})$$

where

$$\mathcal{I}_2 = \{i : m_{i,a} = 0\}, \quad (\text{B27a})$$

$$\mathcal{J}_2 = \{i : n_{i,a} = 0\}, \quad (\text{B27b})$$

with $1 \leq |\mathcal{I}_2| = |\mathcal{J}_2| \leq 2^{r-1} - 1$ (since $|\mathcal{I}_1| + |\mathcal{I}_2| = |\mathcal{J}_1| + |\mathcal{J}_2| = d$). Thus, applying induction once again, we arrive at the decomposition

$$((\tilde{m}_i)_{\mathcal{I}_1}, (\tilde{m}_i)_{\mathcal{I}_2}) = (\mathcal{P}_{|\mathcal{J}_1|}((\tilde{n}_i)_{\mathcal{J}_1}), \mathcal{P}_{|\mathcal{J}_2|}((\tilde{n}_i)_{\mathcal{J}_2})), \quad (\text{B28})$$

which verifies Eq. (B17) for the case $d = 2^{r-1}$.

Next, we consider the case $d = 2^{r-1} + 1$. As before, we assume $m_{1,a} = 1$ and $n_{1,a} = 0$ for some $a \in \{1, \dots, Q\}$; otherwise we can reduce to the previous case of $d = 2^{r-1}$. Following the same reasoning through Eqs. (B21), (B22a), and (B22b), we likewise obtain Eq. (B23), this time with $1 \leq |\mathcal{I}_1| \leq d - 1 = 2^{r-1}$.

If $|\mathcal{I}_1| < 2^{r-1}$, again we recover $(\tilde{m}_i)_{\mathcal{I}_1} = \mathcal{P}_{|\mathcal{J}_1|}((\tilde{n}_i)_{\mathcal{J}_1})$ just as in Eq. (B24). This implies Eq. (B25), and thereby Eq. (B26) with $|\mathcal{I}_2| \leq d - 1 = 2^{r-1}$. Then, by induction on the sets $\mathcal{I}_2$ and $\mathcal{J}_2$, we can deduce $(\tilde{m}_i)_{\mathcal{I}_2} = \mathcal{P}_{|\mathcal{J}_2|}((\tilde{n}_i)_{\mathcal{J}_2})$ and accordingly Eq. (B17) for $d = 2^{r-1} + 1$.

If instead $|\mathcal{I}_1| = 2^{r-1}$, we have $|\mathcal{I}_2| = d - |\mathcal{I}_1| = 1$ and additionally, by Eqs. (B23) and (B19),

$$\sum_{i \in \mathcal{I}_2} \tilde{m}_i^{\otimes(r-1)} = \sum_{i \in \mathcal{J}_2} \tilde{n}_i^{\otimes(r-1)}. \quad (\text{B29})$$

This identity implies via induction that $(\tilde{m}_i)_{\mathcal{I}_2} = \mathcal{P}_{|\mathcal{J}_2|}((\tilde{n}_i)_{\mathcal{J}_2})$ and hence Eq. (B26), which further implies Eq. (B25). By induction on the size of the sets $\mathcal{I}_1$ and $\mathcal{J}_1$, we then deduce $(\tilde{m}_i)_{\mathcal{I}_1} = \mathcal{P}_{|\mathcal{J}_1|}((\tilde{n}_i)_{\mathcal{J}_1})$, so that Eq. (B28) again holds. This verifies Eq. (B17) for $d = 2^{r-1} + 1$.

We can continue increasing d and employing the same proof strategy [essentially Eqs. (B19) and (B23), and our inductive hypothesis] iteratively, until we encounter the possibility that both $|\mathcal{I}_1| \geq 2^{r-1}$ and $|\mathcal{I}_2| \geq 2^{r-1}$. That is, we proceed unless the sizes of these subsets exceed the threshold where the supporting $(r - 1)$ -tensor identity no longer applies directly. Concretely, this allows us to reach $d = 2^r - 1$, as desired. ■

-
- [1] P. Hayden, D. Leung, P. W. Shor, and A. Winter, Randomizing quantum states: Constructions and applications, *Commun. Math. Phys.* **250**, 371 (2004).
- [2] C. Dankert, R. Cleve, J. Emerson, and E. Livine, Exact and approximate unitary 2-designs and their application to fidelity estimation, *Phys. Rev. A* **80**, 012304 (2009).
- [3] H.-Y. Huang, R. Kueng, and J. Preskill, Predicting many properties of a quantum system from very few measurements, *Nat. Phys.* **16**, 1050 (2020).
- [4] A. A. Mele, Introduction to Haar measure tools in quantum information: A beginner's tutorial, *Quantum* **8**, 1340 (2024).
- [5] Y. Nakata and M. Murao, Diagonal-unitary 2-design and their implementations by quantum circuits, *Int. J. Quantum Inf.* **11**, 1350062 (2013).
- [6] Y. Nakata, M. Koashi, and M. Murao, Generating a state t -design by diagonal quantum circuits, *New J. Phys.* **16**, 053043 (2014).
- [7] P. Aliferis, F. Brito, D. P. DiVincenzo, J. Preskill, M. Steffen, and B. M. Terhal, Fault-tolerant computing with biased-noise superconducting qubits: A case study, *New J. Phys.* **11**, 013061 (2009).
- [8] H.-Y. Hu and Y.-Z. You, Hamiltonian-driven shadow tomography of quantum states, *Phys. Rev. Res.* **4**, 013054 (2022).
- [9] M. C. Tran, D. K. Mark, W. W. Ho, and S. Choi, Measuring arbitrary physical properties in analog quantum simulation, *Phys. Rev. X* **13**, 011049 (2023).
- [10] M. McGinley and M. Fava, Shadow tomography from emergent state designs in analog quantum simulators, *Phys. Rev. Lett.* **131**, 160601 (2023).
- [11] Z. Liu, Z. Hao, and H.-Y. Hu, Predicting arbitrary state properties from single Hamiltonian quench dynamics, *Phys. Rev. Res.* **6**, 043118 (2024).
- [12] A. Cowtan, S. Dilkes, R. Duncan, W. Simmons, and S. Sivarajah, Phase gadget synthesis for shallow circuits, in *Proceedings 16th International Conference on Quantum Physics and Logic (QPL 2019)*, edited by B. Coecke and M. Leifer, Electronic Proceedings in Theoretical Computer Science (Chapman University, Orange, CA, 2019), Vol. 318, pp. 213–228.

- [13] D. Litinski, A game of surface codes: Large-scale quantum computing with lattice surgery, *Quantum* **3**, 128 (2019).
- [14] I. Mofic and A. Paler, On the constant depth implementation of Pauli exponentials, [arXiv:2408.08265](#).
- [15] D. Gross, K. Audenaert, and J. Eisert, Evenly distributed unitaries: On the structure of unitary designs, *J. Math. Phys.* **48**, 052104 (2007).
- [16] A. W. Harrow, A. Hassidim, and S. Lloyd, Quantum algorithm for linear systems of equations, *Phys. Rev. Lett.* **103**, 150502 (2009).
- [17] A. Girard, A fast ‘Monte-Carlo cross-validation’ procedure for large least squares problems with noisy data, *Numer. Math.* **56**, 1 (1989).
- [18] M. F. Hutchinson, A stochastic estimator of the trace of the influence matrix for Laplacian smoothing splines, *Commun. Stat.–Simul. Comput.* **19**, 433 (1990).
- [19] T. Iitaka and T. Ebisuzaki, Random phase vector for calculating the trace of a large matrix, *Phys. Rev. E* **69**, 057701 (2004).
- [20] E. Knill and R. Laflamme, Power of one bit of quantum information, *Phys. Rev. Lett.* **81**, 5672 (1998).
- [21] R. Cleve, D. Leung, L. Liu, and C. Wang, Near-linear constructions of exact unitary 2-designs, *Quantum Inf. Comput.* **16**, 721 (2016).
- [22] Y. Nakata, C. Hirche, M. Koashi, and A. Winter, Efficient quantum pseudorandomness with nearly time-independent Hamiltonian dynamics, *Phys. Rev. X* **7**, 021006 (2017).
- [23] J. Haah, Y. Liu, and X. Tan, Efficient approximate unitary designs from random Pauli rotations, in *Proceedings of the 2024 IEEE 65th Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE Computer Society, Los Alamitos, CA, 2024), pp. 463–475.
- [24] T. Metger, A. Poremba, M. Sinha, and H. Yuen, Simple constructions of linear-depth t -designs and pseudorandom unitaries, in *Proceedings of the 2024 IEEE 65th Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE Computer Society, Los Alamitos, CA, 2024), pp. 485–492.
- [25] R. V. Mishmash, T. P. Gujarati, M. Motta, H. Zhai, G. Kin-Lic Chan, and A. Mezzacapo, Hierarchical Clifford transformations to reduce entanglement in quantum chemistry wave functions, *J. Chem. Theory Comput.* **19**, 3194 (2023).
- [26] E. Magesan, J. M. Gambetta, and J. Emerson, Scalable and robust randomized benchmarking of quantum processes, *Phys. Rev. Lett.* **106**, 180504 (2011).
- [27] E. Magesan, J. M. Gambetta, and J. Emerson, Characterizing quantum gates via randomized benchmarking, *Phys. Rev. A* **85**, 042311 (2012).
- [28] Y. Nakata, D. Zhao, T. Okuda, E. Bannai, Y. Suzuki, S. Tamiya, K. Heya, Z. Yan, K. Zuo, S. Tamate, Y. Tabuchi, and Y. Nakamura, Quantum circuits for exact unitary t -designs and applications to higher-order randomized benchmarking, *PRX Quantum* **2**, 030339 (2021).
- [29] Q. Zhang, D. Qin, Z. You, F. Xu, J. Eisert, and Y. Zhou, Robust and efficient estimation of global quantum properties under realistic noise, [arXiv:2507.13237](#).
- [30] J. Spencer, Maximal consistent families of triples, *J. Comb. Theory* **5**, 1 (1968).
- [31] E. F. Assmus and J. D. Key, *Designs and their Codes*, *Cambridge Tracts in Mathematics* (Cambridge University Press, Cambridge, 1992).
- [32] T. Feder and C. S. Subi, Packing edge-disjoint triangles in given graphs, *Electron. Colloq. Comput. Complex.*, TR12-013 (2012).
- [33] H. Bernien, S. Schwartz, A. Keesling, H. Levine, A. Omran, H. Pichler, S. Choi, A. S. Zibrov, M. Endres, M. Greiner, V. Vuletić, and M. D. Lukin, Probing many-body dynamics on a 51-atom quantum simulator, *Nature (London)* **551**, 579 (2017).
- [34] D. Bluvstein, H. Levine, G. Semeghini, T. T. Wang, S. Ebadi, M. Kalinowski, A. Keesling, N. Maskara, H. Pichler, M. Greiner, V. Vuletić, and M. D. Lukin, A quantum processor based on coherent transport of entangled atom arrays, *Nature (London)* **604**, 451 (2022).
- [35] Z. Baranyai, On the factorization of the complete uniform hypergraphs, in *Infinite and Finite Sets*, edited by A. Hajnal, R. Rado, and V. T. Sós, *Colloq. Math. Soc. J. Bolyai* Vol. 10 (North-Holland, Amsterdam, 1975), pp. 91–107.
- [36] *Topics in Chromatic Graph Theory, Encyclopedia of Mathematics and its Applications*, edited by L. W. Beineke and R. J. Wilson (Cambridge University Press, Cambridge, 2015).
- [37] B. Alspach, J.-C. Bermond, and D. Sotteau, Decomposition into cycles I: Hamilton decompositions, in *Cycles and Rays* (Springer, Netherlands, Dordrecht, 1990), pp. 9–18.
- [38] R. Glebov, Z. Luria, and B. Sudakov, The number of Hamiltonian decompositions of regular graphs, *Isr. J. Math.* **222**, 91 (2017).
- [39] A. Galicia, B. Ramon, E. Solano, and M. Sanz, Enhanced connectivity of quantum hardware with digital-analog control, *Phys. Rev. Res.* **2**, 033103 (2020).
- [40] S. Sidon, Ein Satz über Trigonometrische Polynome und Seine Anwendung in der Theorie der Fourier-Reihen, *Math. Ann.* **106**, 536 (1932).
- [41] S. W. Golomb, How to number a graph, in *Graph Theory and Computing* (Academic Press, New York, 1972), pp. 23–37.
- [42] K. Drakakis, A review of the available construction methods for Golomb rulers, *Adv. Math. Commun.* **3**, 235 (2009).