



This is the accepted manuscript made available via CHORUS. The article has been published as:

Characterization of randomness in quantum circuits of continuous gate sets

Yosuke Mitsuhashi, Ryotaro Suzuki, Tomohiro Soejima, and Nobuyuki Yoshioka

Phys. Rev. A **111**, 052409 — Published 7 May 2025

DOI: [10.1103/PhysRevA.111.052409](https://doi.org/10.1103/PhysRevA.111.052409)

Characterization of Randomness in Quantum Circuits of Continuous Gate Sets

Yosuke Mitsuhashi,^{1,*} Ryotaro Suzuki,^{2,†} Tomohiro Soejima,^{3,‡} and Nobuyuki Yoshioka^{4,5,6,§}

¹*Department of Basic Science, University of Tokyo,
3-8-1 Komaba, Meguro-ku, Tokyo 153-8902, Japan*

²*Dahlem Center for Complex Quantum Systems,
Freie Universität Berlin, Berlin 14195, Germany*

³*Department of Physics, Harvard University, Cambridge, MA 02138, USA*

⁴*Department of Applied Physics, University of Tokyo,
7-3-1 Hongo, Bunkyo-ku, Tokyo 113-8656, Japan*

⁵*Quantum Computing Center, RIKEN Cluster for Pioneering Research (CPR), Wako-shi, Saitama 351-0198, Japan*

⁶*JST, PRESTO, 4-1-8 Honcho, Kawaguchi, Saitama, 332-0012, Japan*

In the accompanying paper of arXiv:2408.13472, we have established the method of characterizing the maximal order of asymptotic unitary designs generated by symmetric local random circuits, and have explicitly specified the order in the cases of $\mathbb{Z}_2$, $U(1)$, and $SU(2)$ symmetries. Here, we provide full details on the derivation of the main theorems for general symmetry and for concrete symmetries. Furthermore, we consider a general framework where we have access to a finite set of connected compact unitary subgroups, which includes symmetric local unitary gate sets.

I. INTRODUCTION

In quantum mechanics, symmetry plays a fundamental role in both constraining and enriching phenomena in wide range of spacial and dynamical sense. Early seminal example is represented by the Noether's theorem [1], which states that a global symmetry of a system results in a constrained dynamics that preserves a conserved charge. Symmetry also plays a crucial role in enriching physics, as represented in spontaneous symmetry breaking [2–5] and deconfined quantum criticality [6–8]. A prominent application in quantum information science is the protection of quantum memory by quantum error correction [9–12], in addition to the Eastin-Knill theorem that in turn puts restriction on a single error-correcting code to perform universal quantum computation [13].

Driven by the capability of quantum circuit models to capture various statistical physics phenomena, there is a surging interest in the interplay between symmetry and locality in quantum circuits. One primary example is the symmetry-protected topological order in quantum phases of matter, in which the presence/absence of constant-depth local symmetric quantum circuit is crucial for the definition [14–20]. Also, the interplay has been of interest to the statistical physics community which employs the quantum circuit model to describe discretized time evolution of local Hamiltonian to discover novel symmetry enriched phases in both static and dynamical ways [21–24].

The interplay between the symmetry and locality has shed light on a primary problem in quantum information science—the universality of symmetric local quantum circuits. Here the universality refers to the ability of a given set of local quantum gates to express arbitrary global unitary, and its practical significance is highlighted in the Solovay-Kitaev theorem which states that ϵ -close approximation of arbitrary unitary can be constructed from polylogarithmic number of universal gate sets [25, 26]. While the fundamental theory of quantum computing has established that universality can be achieved with a finite set of locally universal unitaries [27, 28], surprisingly it was shown recently that the representability of *symmetric* local circuit is restricted, i.e., does not satisfy universality [29]. It was later pointed out that some local circuits under symmetry constraints satisfy a property called the *semi-universality* [30–32], a weaker version of universality which ignores the tunability of relative phases between symmetry sectors [33].

The discovery of such a qualitative difference has further invoked question in terms of quantitative characterization, concretely in terms of the symmetric version of unitary t -design. Note that unitary design, representing a set of unitaries that reproduces the Haar measure up to the t th moment [34], has been a standard tool to understand the condition to perform various tasks in quantum information science including quantum advantage [35, 36], quantum tomography [37], randomized benchmarking [38], optimal quantum communication capacity [39], and chaotic dynamics [40]. While it is known that accumulation of non-symmetric local circuits allows us to generate unitary designs

* mitsuhashi@noneq.t.u-tokyo.ac.jp

† ryotaro.suzuki@fu-berlin.de

‡ tomohiro-soejima@g.harvard.edu

§ nyoshioka@ap.t.u-tokyo.ac.jp

up to arbitrary order [41–46], in symmetric cases the expressibility of the symmetric local unitaries remains unestablished. While there are existing attempts to characterize the design under $U(1)$ and $SU(d)$ symmetries [47, 48], we are lacking of integrated theory that provides the exact number of maximal order t achievable with symmetric local quantum circuits.

In an accompanying letter [49], we establish the method for general symmetric local quantum circuits that characterizes its expressibility in terms of symmetric unitary design. We have concretely shown that the necessary and sufficient condition of forming an asymptotic symmetric t -design is given by the nonexistence of a nontrivial integer solution of a certain linear equation specified by the symmetry and locality of the circuit. In this manuscript, we provide the full details of the derivation of the main theorems. The equivalence between asymptotic unitary designs and the nonexistence of a nontrivial integer solution can be intuitively understood as follows: Since we consider the situation where our accessible gate set is semi-universal, the difference between the expressibility of accessible gate set and that of the whole symmetric gate set appears only in the relative phases. Therefore, the distribution of a random circuit generated with some gate set is an asymptotic unitary t -design if and only if whenever we are given the sum of t relative phases, we can estimate the component of them, which can be equivalently expressed as the nonexistence of nontrivial integer solutions of a certain set of equations.

As for technical perspective, the core idea is to show the equivalence between the nonexistence of a nontrivial integer solution and the coincidence of the commutant of the t -fold allowed gate set and that of the t -fold symmetric unitary operators, which means that symmetric local quantum circuits are asymptotic unitary t -designs. When we prove the coincidence of the two commutants, we show the coincidence of the algebras of the t -fold allowed gate set of the t -fold symmetric unitary operators. On the other hand, when we prove the converse part, we explicitly construct an operator that commutes with all the t -fold allowed gates, but not with all the t -fold symmetric unitaries.

The remainder of this paper is organized as follows. In Sec. II, we introduce the preliminaries. In Sec. III, we present a theorem about the explicit order of unitary designs, which is applicable to general symmetries and general continuous gate sets. We also present the detailed results for the $\mathbb{Z}_2$, $U(1)$, and $SU(2)$ symmetries. Then, in Sec. IV, we present the proof of the general theorem. This is followed by Sec. V which gives the conclusion and discussion. For the completeness of our work, in Appendix A, we present the proof of the theorems about the concrete symmetries $\mathbb{Z}_2$, $U(1)$, and $SU(2)$. In Appendix B, we show technical lemmas used in the proofs of the main theorems.

II. PRELIMINARIES

The notations used in this paper are as follows: For a general Hilbert space $\mathcal{K}$, we denote the sets of all linear operators and all unitary operators on $\mathcal{K}$ by $\mathcal{L}(\mathcal{K})$ and $\mathcal{U}(\mathcal{K})$, respectively. As for the definition of the Lie algebra associated with a Lie group, we adopt the physical version, i.e., we define the Lie algebra as the tangent space at the identity divided by the imaginary unit i . We define $\mathbb{N} := \{n \in \mathbb{Z} \mid n > 0\}$ and $\mathbb{Z}_{\geq 0} := \{n \in \mathbb{Z} \mid n \geq 0\}$. For the sake of convenience, we define the sum and product over the empty set as 0 and 1, respectively.

We consider a circuit consisting of n qudits with a local dimension d , and we denote the associated Hilbert space by $\mathcal{H}$. For convenience, we denote the set of all linear operators and all unitary operators on the n qudits by $\mathcal{L}_n$ and $\mathcal{U}_n$, respectively, which are the same as $\mathcal{L}(\mathcal{H})$ and $\mathcal{U}(\mathcal{H})$. In the following, we give the notations about symmetry and the construction of random circuits. First, we explain the symmetry condition. By using the pair of a group G and its representation R on $\mathcal{H}$, we say that an operator $O \in \mathcal{L}(\mathcal{H})$ is (G, R) -symmetric if O commutes with $R(g)$ for all $g \in G$. We denote the set of all (G, R) -symmetric linear operators and unitary operators by $\mathcal{L}_{n,G,R}$ and $\mathcal{U}_{n,G,R}$, i.e.,

$$\mathcal{L}_{n,G,R} := \{L \in \mathcal{L}_n \mid [L, R(g)] = 0 \ \forall g \in G\}, \quad (1)$$

$$\mathcal{U}_{n,G,R} := \{U \in \mathcal{U}_n \mid [U, R(g)] = 0 \ \forall g \in G\}. \quad (2)$$

As examples of representations on multiqubit systems, we can take the following representations of three groups $\mathbb{Z}_2$, $U(1)$, and $SU(2)$ on n qubits:

$$R(g) = (Z^g)^{\otimes n} \text{ when } G = \mathbb{Z}_2 = \{0, 1\}, \quad (3)$$

$$R(e^{i\theta}) = (e^{i\theta Z})^{\otimes n} \text{ when } G = U(1), \quad (4)$$

$$R\left(e^{i(\theta_X X + \theta_Y Y + \theta_Z Z)}\right) = \left(e^{i(\theta_X X + \theta_Y Y + \theta_Z Z)}\right)^{\otimes n} \text{ when } G = SU(2), \quad (5)$$

where X , Y , and Z are the Pauli operators. We note that these representations R can be written as the tensor product of representation $T^{\otimes n}$ with a representation T on a single qubit.

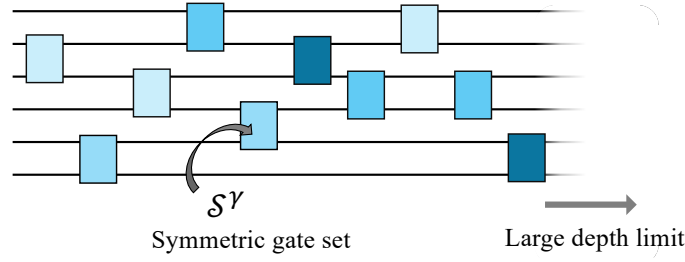


FIG. 1. Example of symmetric random circuits. We construct a random circuit by taking symmetric gate set $\mathcal{S}^\gamma$ with probability p^γ and randomly drawing a unitary operator from the gate set. This setup includes symmetric local random circuits when we consider the case when $\mathcal{S}^\gamma = \mathcal{U}_{n,G,R}^\gamma$ where γ denotes the locality of the gate set.

Next, we explain the construction of random circuits. We consider the case when the allowed gate set is expressed as a finite number of connected compact unitary subgroups of $\mathcal{U}_{n,G,R}$. We denote each connected compact subgroup by $\mathcal{S}^\gamma$ and the set of all possible γ by Γ . By using these gate set $\{\mathcal{S}^\gamma\}_{\gamma \in \Gamma}$, we consider the distribution

$$\zeta_{\{\mathcal{S}^\gamma\}_{\gamma \in \Gamma}} := \sum_{\gamma \in \Gamma} p^\gamma \mu_{\mathcal{S}^\gamma} \quad (6)$$

with the Haar measure $\mu_{\mathcal{S}^\gamma}$ on $\mathcal{S}^\gamma$ and $p^\gamma > 0$ satisfying $\sum_{\gamma \in \Gamma} p^\gamma = 1$. We note that the exact values of p^γ 's do not affect our results as long as $p^\gamma \neq 0$, as we explain later.

We note that this setup includes the random circuits consisting of symmetric and local gates as follows: We label n qudits as $1, 2, \dots$, and n , and for a subset of $\{1, 2, \dots, n\}$, we denote by $\mathcal{U}_{n,G,R}^\gamma$ the set of all unitary subgroup of $\mathcal{U}_{n,G,R}$ acting nontrivially on the qudits labeled by γ . For example, when we have access to all symmetric nearest-neighbor unitary operators in a one-dimensional chain with the open boundary condition, Γ is given by $\{\{1, 2\}, \{2, 3\}, \dots, \{n-1, n\}\}$, which is illustrated in Fig. 1.

In order to investigate randomness of the distribution $\zeta_{\{\mathcal{S}^\gamma\}_{\gamma \in \Gamma}}$ defined by Eq. (6), we use *asymptotic unitary designs* defined as follows:

Definition 1. (*Asymptotic symmetric unitary design.*) Let $n, t \in \mathbb{N}$, R be a unitary representation of a group G on $\mathcal{H}$, and ν be a distribution on $\mathcal{U}_{n,G,R}$. ν is an asymptotic (G, R) -symmetric unitary t -design if

$$\lim_{D \rightarrow \infty} (M_{t,\nu})^D = M_{t,\mu_{\mathcal{U}_{n,G,R}}}, \quad (7)$$

with the normalized Haar measure $\mu_{\mathcal{S}}$ on a compact Lie subgroup $\mathcal{S}$ of $\mathcal{U}_{n,G,R}$ and the t th-order moment operator of ν defined by

$$M_{t,\nu} := \int_{U \in \mathcal{U}_{n,G,R}} U^{\otimes t} \otimes U^{*\otimes t} d\nu(U). \quad (8)$$

This definition means that if a distribution ν is an asymptotic (G, R) -symmetric unitary t -design, the distribution of a circuit with infinite depth coincides with the Haar random distribution up to the t th moment. We use the term “asymptotic unitary design” because we only care about the asymptotic behavior of the distribution for deep circuits. We note that the distribution ν is an asymptotic unitary design if and only if for any $\epsilon > 0$, there exists $D_0 \in \mathbb{N}$ such that for any $D \geq D_0$, the D -fold convolution of ν is an ϵ -approximate unitary design.

In order to state the main theorem, we prepare the notion of semi-universality. If a gate set generates $\mathcal{U}_{n,G,R}$, it is called universal for $\mathcal{U}_{n,G,R}$. The semi-universality is a weaker version of the universality, defined as follows [33]:

Definition 2. (*Semi-universality.*) Let $n \in \mathbb{N}$, R be a representation of a group G , and $\mathcal{X}$ be a subset $\mathcal{U}_{n,G,R}$. $\mathcal{X}$ is semi-universal for $\mathcal{U}_{n,G,R}$ if

$$\langle \mathcal{X} \rangle \cdot Z(\mathcal{U}_{n,G,R}) = \mathcal{U}_{n,G,R}, \quad (9)$$

where $\langle \mathcal{X} \rangle$ is the group generated by the elements of $\mathcal{X}$, and $Z(\mathcal{U}_{n,G,R})$ is the center of $\mathcal{U}_{n,G,R}$, i.e., $Z(\mathcal{U}_{n,G,R}) := \{U \in \mathcal{U}_{n,G,R} \mid [U, V] = 0 \ \forall V \in \mathcal{U}_{n,G,R}\}$.

It is known in Refs. [30, 31] that the (G, R) -symmetric 2-local gate sets are semi-universal for $\mathcal{U}_{n,G,R}$ for $\mathbb{Z}_2$, $U(1)$, and $SU(2)$ symmetries given by Eqs. (3), (4), and (5) as long as Γ is *inseparable*. We say that Γ is inseparable in $\{1, 2, \dots, n\}$ if there is no pair of nontrivial subsets C_1 and C_2 of $\{1, 2, \dots, n\}$ that satisfy $C_1 \cap C_2 = \emptyset$, $C_1 \cup C_2 = \{1, 2, \dots, n\}$, and $\gamma \in C_1$ or $\gamma \in C_2$ for all $\gamma \in \Gamma$.

In order to present the condition for semi-universality more directly, we introduce the decomposition of symmetric operators. Every unitary representation R can be decomposed into irreducible representations, i.e., we can take an isomorphism

$$\mathcal{H} \cong \bigoplus_{\lambda \in \Lambda} \mathbb{C}^{r_\lambda} \otimes \mathbb{C}^{m_\lambda} \quad (10)$$

such that

$$R(g) = \sum_{\lambda \in \Lambda} F_\lambda(R_\lambda(g) \otimes I) F_\lambda^\dagger \quad \forall g \in G, \quad (11)$$

where Λ is the set of all labels λ for inequivalent irreducible representations appearing in R , R_λ 's are irreducible representations of G on $\mathbb{C}^{r_\lambda}$, m_λ is the multiplicity of the representation R_λ , and F_λ is the isometry from $\mathbb{C}^{r_\lambda} \otimes \mathbb{C}^{m_\lambda}$ to $\mathcal{H}$. By using Schur's lemma, every (G, R) -symmetric operator A can be written as

$$A = \sum_{\lambda \in \Lambda} F_\lambda(I \otimes A_\lambda) F_\lambda^\dagger \quad (12)$$

with some A_λ 's acting on $\mathbb{C}^{m_\lambda}$, which are uniquely determined for a (G, R) -symmetric operator $A \in \mathcal{L}_{n,G,R}$ on n qudits. By using this decomposition, $Z(\mathcal{U}_{n,G,R})$ can be explicitly written as

$$Z(\mathcal{U}_{n,G,R}) = \left\{ \sum_{\lambda \in \Lambda} F_\lambda(I \otimes e^{i\theta_\lambda} I) F_\lambda^\dagger \mid \theta_\lambda \in \mathbb{R} \quad \forall \lambda \in \Lambda \right\}. \quad (13)$$

We note that the semi-universality of $\mathcal{X}$ can be equivalently expressed as

$$\langle \mathcal{X} \rangle \supset \left\{ \sum_{\lambda \in \Lambda} F_\lambda(I \otimes U_\lambda) F_\lambda^\dagger \mid U_\lambda \in \text{SU}(m_\lambda) \quad \forall \lambda \in \Lambda \right\}. \quad (14)$$

It is trivial to see that Eq. (14) implies Eq. (9) by noting Eq. (13). The proof of the converse is as follows: We suppose that $\mathcal{X}$ satisfies Eq. (9). We take arbitrary $U \in \mathcal{U}_{n,G,R}$ in the form of $\sum_{\lambda \in \Lambda} F_\lambda(I \otimes U_\lambda) F_\lambda^\dagger$ with some $U_\lambda \in \text{SU}(m_\lambda)$. For each $\lambda \in \Lambda$, since $\text{SU}(m_\lambda)$ is a simple Lie group, we can take $U'_\lambda, U''_\lambda \in \text{SU}(m_\lambda)$ satisfying $U'^{-1}_\lambda U''^{-1}_\lambda U'_\lambda U''_\lambda = U_\lambda$. We define $U' := \sum_{\lambda \in \Lambda} F_\lambda(I \otimes U'_\lambda) F_\lambda^\dagger$ and $U'' := \sum_{\lambda \in \Lambda} F_\lambda(I \otimes U''_\lambda) F_\lambda^\dagger$. Since U' and U'' satisfy $U', U'' \in \mathcal{U}_{n,G,R}$, Eq. (9) implies that we can take $V', V'' \in \langle \mathcal{X} \rangle$ and $W', W'' \in Z(\mathcal{U}_{n,G,R})$ such that $U' = V'W'$ and $U'' = V''W''$. Then, by noting that W' and W'' commute with V', W', V'' , and W'' , we have $U = U'^{-1}U''^{-1}U'U'' = V'^{-1}V''^{-1}V'V'' \in \langle \mathcal{X} \rangle$.

In the following, we explain the relation between the (semi-)universality of the gate sets $\{\mathcal{S}^\gamma\}_{\gamma \in \Gamma}$ and asymptotic unitary designs of the distribution $\zeta_{\{\mathcal{S}^\gamma\}_{\gamma \in \Gamma}}$ generated by the gate set, which is shown in Fig. 2. First, if the distribution $\zeta_{\{\mathcal{S}^\gamma\}_{\gamma \in \Gamma}}$ defined by Eq. (6) is an asymptotic (G, R) -symmetric unitary 2-design, then the gate set $\bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma$ is semi-universal for $\mathcal{U}_{n,G,R}$. This can be proven by the combination of Theorem 16 in Ref. [50] and Lemma 1. When $\zeta_{\{\mathcal{S}^\gamma\}_{\gamma \in \Gamma}}$ is an asymptotic (G, R) -symmetric unitary 2-design, the commutant of $\{U^{\otimes 2} \mid \exists \gamma \in \Gamma \text{ s.t. } U \in \mathcal{S}^\gamma\}$ coincides with that of $\{U^{\otimes 2} \mid U \in \mathcal{U}_{n,G,R}\}$ by Lemma 1. This implies that the commutant of $\{A \otimes I + I \otimes A \mid \exists \gamma \in \Gamma \text{ s.t. } A \in \mathfrak{s}^\gamma\}$ coincides with that of $\{A \otimes I + I \otimes A \mid A \in \mathfrak{u}_{n,G,R}\}$, where $\mathfrak{s}^\gamma$ and $\mathfrak{u}_{n,G,R}$ is a Lie algebra of $\mathcal{S}^\gamma$ and $\mathcal{U}_{n,G,R}$, respectively. Then, Theorem 16 in Ref. [50] implies that $\bigcup_{\gamma \in \Gamma} \mathfrak{s}^\gamma$ generates $\mathfrak{u}_{n,G,R}$ up to $Z(\mathfrak{u}_{n,G,R})$ in the sense of Lie algebra, which implies the semi-universality of $\bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma$ for $\mathcal{U}_{n,G,R}$. We note that this statement holds only for gate sets consisting of connected compact groups, and not for discrete gate sets such as the Clifford group.

Second, if the gate set $\bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma$ is universal for $\mathcal{U}_{n,G,R}$ up to the global phase, then the distribution $\zeta_{\{\mathcal{S}^\gamma\}_{\gamma \in \Gamma}}$ is an asymptotic (G, R) -symmetric unitary t -design for all $t \in \mathbb{N}$, which directly follows from the same argument in the non-symmetric case [41]. Moreover, the converse is also true, as we explain below Theorem 1. Since the semi-universality reduces to the universality up to the global phase in the non-symmetric case, i.e., $G = \{I\}$, every class of

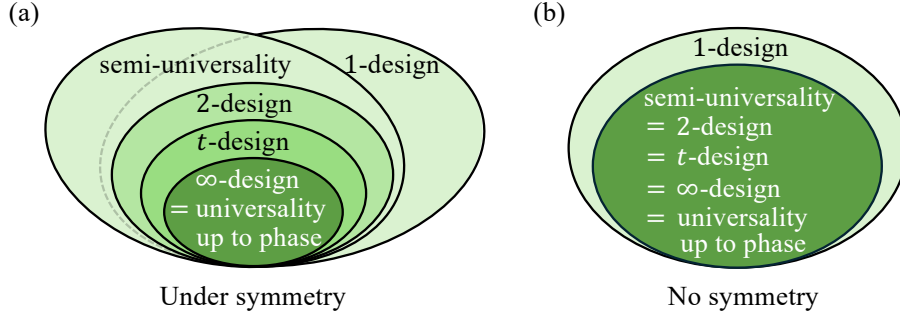


FIG. 2. Hierarchy of asymptotic unitary designs of random circuits and its relation with the (semi-)universality of the gate sets consisting of the circuits. (a) In the presence of symmetry, there is a rich structure of the classes of asymptotic unitary designs. Semi-universal gate sets are necessary to construct random circuits with 2-designs. Our main result is to establish a method to characterize the maximum order of unitary designs of the distribution for symmetric random circuits composed of semi-universal gate sets. (b) The relation between the universality and designs becomes rather trivial without symmetry.

distributions forming unitary t -designs coincides to the class of distributions forming unitary ∞ -designs. Thus, the inclusion relation in symmetric cases (Fig. 2 (a)) becomes much simpler in the non-symmetric case (Fig. 2 (b)).

Finally, we show that there are no nontrivial inclusion relations other than those stated above. Concretely, the semi-universality of the gate set $\bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma$ does not imply that the distribution $\zeta_{\{\mathcal{S}^\gamma\}_{\gamma \in \Gamma}}$ is an asymptotic (G, R) -symmetric unitary 2-design, and not even a 1-design. For example, when $n = 1$, $G = \mathbb{Z}_2$ and $R(g) = Z^g$ for $g \in \mathbb{Z}_2 = \{0, 1\}$, the gate set consisting only of the identity is semi-universal for $\mathcal{U}_{n, G, R}$, but is not an asymptotic unitary 1-design for $\mathcal{U}_{n, G, R}$. We also note that the distribution $\zeta_{\{\mathcal{S}^\gamma\}_{\gamma \in \Gamma}}$ being an asymptotic (G, R) -symmetric unitary 1-design does not imply the semi-universality of the gate set $\bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma$ for $\mathcal{U}_{n, G, R}$, and that the combination of these two conditions does not imply that the distribution $\zeta_{\{\mathcal{S}^\gamma\}_{\gamma \in \Gamma}}$ is an asymptotic (G, R) -symmetric unitary 2-design. For the proofs of the two statements above, we set $n = 2$, $G = \mathbb{Z}_2$, and $R(g) = (Z^g)^{\otimes 2}$ for $g \in \{0, 1\}$, and define the following four gate sets:

$$\mathcal{S}^1 := \{e^{i\theta X \otimes X}\}_{\theta \in \mathbb{R}}, \quad (15)$$

$$\mathcal{S}^2 := \{e^{i\theta Z \otimes Z}\}_{\theta \in \mathbb{R}}, \quad (16)$$

$$\mathcal{S}^3 := \{e^{i\theta Z \otimes I}\}_{\theta \in \mathbb{R}}, \quad (17)$$

$$\mathcal{S}^4 := \{e^{i\theta I \otimes Z}\}_{\theta \in \mathbb{R}}, \quad (18)$$

where I is the identity operator on a single qubit. When $\Gamma = \{1, 2, 3\}$, the distribution $\zeta_{\{\mathcal{S}^\gamma\}_{\gamma \in \Gamma}}$ is an asymptotic (G, R) -symmetric unitary 1-design by Lemma 1, but the gate set $\bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma$ is not semi-universal for $\mathcal{U}_{n, G, R}$, which can be confirmed by noting that $\langle \bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma \rangle = \{\sum_{\lambda \in \{0, 1\}} F_\lambda e^{i(-1)^\lambda \theta} U F_\lambda^\dagger \mid \theta \in \mathbb{R}, U \in \text{SU}(2)\}$, where F_λ is defined by $F_0 |j\rangle := |j\rangle \otimes |j\rangle$ and $F_1 |j\rangle := |j\rangle \otimes |1-j\rangle$ for $j \in \{0, 1\}$. When $\Gamma = \{1, 3, 4\}$, the distribution $\zeta_{\{\mathcal{S}^\gamma\}_{\gamma \in \Gamma}}$ is an asymptotic (G, R) -symmetric unitary 1-design by Lemma 1, and $\bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma$ is semi-universal for $\mathcal{U}_{n, G, R}$, but $\zeta_{\{\mathcal{S}^\gamma\}_{\gamma \in \Gamma}}$ is not an asymptotic unitary 2-design for $\mathcal{U}_{n, G, R}$ by Theorem 1. For the proof of the semi-universality, it is sufficient to confirm that the Lie algebras of $\mathcal{S}^\gamma$'s generate the Lie algebra $\mathfrak{u}_{n, G, R}$ of $\mathcal{U}_{n, G, R}$ up to $Z(\mathfrak{u}_{n, G, R})$ in the sense of Lie algebra.

III. MAIN RESULTS

First, we present the general result about the maximal order of asymptotic unitary designs, which is applicable to general symmetries. The following theorem corresponds to Theorem 2 of Ref. [49].

Theorem 1. (General result.) *Let $n, t \in \mathbb{N}$, R be a unitary representation of a group G on the Hilbert space $\mathcal{H}$ of n qudits, $\{\mathcal{S}^\gamma\}_{\gamma \in \Gamma}$ be the set of a finite number of connected compact subgroups of $\mathcal{U}_{n, G, R}$, and $\bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma$ be semi-universal. Then, the distribution $\zeta_{\{\mathcal{S}^\gamma\}_{\gamma \in \Gamma}}$ defined by Eq. (6) is an asymptotic (G, R) -symmetric unitary t -design if and only if there do not exist nontrivial integer solutions $\mathbf{x} = (x_\lambda)_{\lambda \in \Lambda} \in \mathbb{Z}^\Lambda$ satisfying*

$$\sum_{\lambda \in \Lambda} m_\lambda |x_\lambda| \leq 2t, \quad (19)$$

$$\sum_{\lambda \in \Lambda} m_{\lambda} x_{\lambda} = 0, \quad (20)$$

$$\sum_{\lambda \in \Lambda} v_{\lambda} x_{\lambda} = 0 \quad \forall \mathbf{v} \in \mathcal{V}, \quad (21)$$

where $\mathcal{V} := \text{span}_{\mathbb{R}}(\{\mathbf{f}(A) \mid \exists \gamma \in \Gamma \text{ s.t. } A \in \mathfrak{s}^{\gamma}\})$, $\mathfrak{s}^{\gamma}$ is the Lie algebra of $\mathcal{S}^{\gamma}$, and

$$\mathbf{f}(A) = (f_{\lambda}(A))_{\lambda \in \Lambda} := (\text{tr}(A_{\lambda}))_{\lambda \in \Lambda} \quad (22)$$

with A_{λ} determined from A by Eq. (12). Especially when $\mathcal{S}^{\gamma} = \mathcal{U}_{n,G,R}^{\gamma}$ and $R = T^{\otimes n}$ with some representation T of G on a single qudit, Eqs. (20) and (21) can be equivalently written as

$$\sum_{\lambda \in \Lambda} c_{\lambda} x_{\lambda} = 0 \quad \forall \mathbf{c} \in \mathcal{C}, \quad (23)$$

where $\mathcal{C}$ is defined by $\mathcal{C} := \{\mathbf{f}(A \otimes \mathbb{I}^{\otimes n-k}) \mid A \in \mathcal{L}_{k,G,T^{\otimes k}}\}$, and $k := \max_{\gamma \in \Gamma} \# \gamma$.

We give three remarks about this theorem. First, finding the condition on t for the nonexistence of nontrivial integer solutions of Eqs (19), (20), and (21) is equivalent to a simple integer optimization. In fact, the condition is explicitly expressed as

$$t < \min_{\mathbf{x} \in (\tilde{\mathcal{V}}^{\perp} \cap \mathbb{Z}^{\Lambda}) \setminus \{\mathbf{0}\}} \langle \mathbf{m}, \mathbf{x}^+ \rangle, \quad (24)$$

where

$$\mathbf{m} = (m_{\lambda})_{\lambda \in \Lambda}, \quad (25)$$

$$\mathbf{x}^+ = (x_{\lambda}^+)_{\lambda \in \Lambda} := ((|x_{\lambda}| + x_{\lambda})/2)_{\lambda \in \Lambda}, \quad (26)$$

$$\tilde{\mathcal{V}} := \text{span}_{\mathbb{R}}(\{\mathbf{m}\}) + \mathcal{V}, \quad (27)$$

and we use the standard inner product $\langle \mathbf{a}, \mathbf{b} \rangle := \sum_{\lambda \in \Lambda} a_{\lambda}^* b_{\lambda}$ for $\mathbf{a}, \mathbf{b} \in \mathbb{C}^{\Lambda}$. This can be understood by noting that Eq. (19), (20) and (21) are equivalent to $\langle \mathbf{m}, \mathbf{x}^+ \rangle \leq t$ and $\mathbf{x} \in \tilde{\mathcal{V}}^{\perp}$. When $\mathcal{S}^{\gamma} = \mathcal{U}_{n,G,R}^{\gamma}$ and $R = T^{\otimes n}$, by taking a basis of $\mathcal{C}$, Eq. (23) can be written as the set of $\dim(\mathcal{C})$ equations. We note that $\dim(\mathcal{C})$ is upper bounded by $\dim(\mathcal{L}_{k,G,T^{\otimes k}})$, which is independent of the qudit count n . Similarly to Eq. (24), the condition on t can be written as

$$t < \min_{\mathbf{x} \in (\mathcal{C}^{\perp} \cap \mathbb{Z}^{\Lambda}) \setminus \{\mathbf{0}\}} \langle \mathbf{m}, \mathbf{x}^+ \rangle. \quad (28)$$

Next, by using this theorem, we can confirm that $\zeta_{\{\mathcal{S}^{\gamma}\}_{\gamma \in \Gamma}}$ is an asymptotic unitary t -design for all $t \in \mathbb{N}$ if and only if $\bigcup_{\gamma \in \Gamma} \mathcal{S}^{\gamma}$ is universal for $\mathcal{U}_{n,G,R}$ up to the global phase. When $\bigcup_{\gamma \in \Gamma} \mathcal{S}^{\gamma}$ is universal for $\mathcal{U}_{n,G,R}$ up to the global phase, by Lemma 14, Eq. (20) and (21) have no nontrivial integer solution $\mathbf{x}$. Theorem 1 thus implies that $\zeta_{\{\mathcal{S}^{\gamma}\}_{\gamma \in \Gamma}}$ is an asymptotic unitary t -design for all $t \in \mathbb{N}$. On the other hand, when $\bigcup_{\gamma \in \Gamma} \mathcal{S}^{\gamma}$ is not universal for $\mathcal{U}_{n,G,R}$ up to the global phase, we can take $\mathbf{d} \in (\tilde{\mathcal{V}}^{\perp} \cap \mathbb{Z}^{\Lambda}) \setminus \{\mathbf{0}\}$ by Lemma 14, and define $t_0 := \langle \mathbf{m}, \mathbf{x}^+ \rangle$. Since $\mathbf{x} = \mathbf{d}$ is a nontrivial integer solution of Eqs. (20) and (21), any achievable order t is smaller than t_0 .

Finally, we can compute the tight upper bound on the achievable order t by enumeration. When $\tilde{\mathcal{V}} = \mathbb{R}^{\Lambda}$, there does not exist an upper bound on t . In the following, we consider the case of $\tilde{\mathcal{V}} \neq \mathbb{R}^{\Lambda}$. In this case, by using the method above, we can take an upper bound t_0 , which is not necessarily tight. Then, Eq. (24) is equivalent to

$$t < \min \left\{ t_0, \min_{\mathbf{x} \in (\tilde{\mathcal{V}}^{\perp} \cap \mathbb{Z}^{\Lambda} \cap \mathcal{F}) \setminus \{\mathbf{0}\}} \langle \mathbf{m}, \mathbf{x}^+ \rangle \right\} \quad (29)$$

with a bounded region $\mathcal{F} := \{\mathbf{x} \in \mathbb{R}^{\Lambda} \mid |x_{\lambda}| < t_0/m_{\lambda} \quad \forall \lambda \in \Lambda\}$. For the proof of Eq. (29), it is sufficient to show that $\min_{\mathbf{x} \in \mathbb{Z}^{\Lambda} \setminus \mathcal{F}} \langle \mathbf{m}, \mathbf{x}^+ \rangle \geq t_0$ by noting that $[(\tilde{\mathcal{V}}^{\perp} \cap \mathbb{Z}^{\Lambda} \cap \mathcal{F}) \setminus \{\mathbf{0}\}] \cup (\mathbb{Z}^{\Lambda} \setminus \mathcal{F}) \supset (\tilde{\mathcal{V}}^{\perp} \cap \mathbb{Z}^{\Lambda}) \setminus \{\mathbf{0}\}$. For arbitrary $\mathbf{x} \in \mathbb{Z}^{\Lambda} \setminus \mathcal{F}$, we can take some $\lambda \in \Lambda$ such that $|x_{\lambda}| \geq t_0/m_{\lambda}$. We can suppose that $x_{\lambda} > 0$ without loss of generality, since $\mathbf{x} \in \mathbb{Z}^{\Lambda} \setminus \mathcal{F}$ implies $-\mathbf{x} \in \mathbb{Z}^{\Lambda} \setminus \mathcal{F}$. Then, we get $\langle \mathbf{m}, \mathbf{x}^+ \rangle \geq m_{\lambda} x_{\lambda} \geq t_0$.

In the following theorems, we consider the cases when $G = \mathbb{Z}_2$, $U(1)$ and $SU(2)$, and $\mathcal{S}^{\gamma}$ is given by the set $\mathcal{U}_{n,G,R}^{\gamma}$ of all (G, R) -symmetric unitary operators acting on the qubits represented by γ , and the locality of the gate set satisfies $\max_{\gamma \in \Gamma} \gamma = k$.

First, we present the result for the $\mathbb{Z}_2$ symmetry, which corresponds to the first result of Theorem 1 of Ref. [49].

Theorem 2. (Result for general locality k and general qubit count n under the $\mathbb{Z}_2$ symmetry.) Let $n, k, t \in \mathbb{N}$ satisfy $k \geq 2$ and $n \geq k + 1$, and R be a unitary representation of $G = \mathbb{Z}_2$ on n qubits defined by Eq. (3). Then, the distribution of the (G, R) -symmetric k -local random circuit is an asymptotic (G, R) -symmetric unitary t -design if and only if $t < 2^{n-1}$.

We note that the condition of t does not depend on the locality k , which is a feature different from the cases of $U(1)$ and $SU(2)$. We describe the proof of this theorem in Appendix A 1.

Next, we present the result for the $U(1)$ symmetry. For general locality k , we can give the maximal order of asymptotic unitary designs for sufficiently large n in the following theorem, which corresponds to the second part of Theorem 1 of Ref. [49].

Theorem 3. (Result for general locality k and sufficiently large qubit count n under the $U(1)$ symmetry.) Let $n, k, t \in \mathbb{N}$ satisfy $k \geq 2$ and $n \geq 2^k$, and R be a unitary representation of $G = U(1)$ on n qubits defined by Eq. (4). Then, the distribution of the (G, R) -symmetric k -local random circuit is an asymptotic (G, R) -symmetric unitary t -design if and only if

$$t < \frac{2^{\lfloor k/2 \rfloor}}{\lfloor k/2 \rfloor!} \prod_{\alpha=1}^{\lceil k/2 \rceil} (n - k + 2\alpha - 1). \quad (30)$$

We note that the condition $n \geq 2^k$ is needed only for the proof of the “if” part, i.e., for any $n \geq k + 1$, we can show that the distribution is not an asymptotic (G, R) -symmetric unitary t -design if t does not satisfy the condition above. We present the proof in Appendix A 2.

While the theorem above specifies the maximal order of unitary designs of the $U(1)$ -symmetric local random circuits for sufficiently many qubits, it does not guarantee that the bound is the same in the case of few qubits. As a result complementary to Theorem 3, we show the result for small locality $k = 2, 3$, and 4 in the following theorem.

Theorem 4. (Result for small locality k and general qubit count n under the $U(1)$ symmetry.) Let $n, t \in \mathbb{N}$, $k = 2, 3$ or 4, $n \geq k + 1$, and R be a unitary representation of $G = U(1)$ on n qubits defined by Eq. (4). Then, the distribution of the (G, R) -symmetric k -local random circuit is an asymptotic unitary t -design if and only if

$$\begin{cases} t < 2(n-1) & (\text{when } k = 2), \\ t < n(n-2) & (\text{when } k = 3), \\ t < 2(n-1)(n-3) & (\text{when } k = 4). \end{cases} \quad (31)$$

This theorem means that for the locality $k = 2, 3$, and 4, even in the case of few qubits, the maximal order of unitary designs is given by the same function of the number of qubits as in the many-qubit case. We note, however, that this does not hold for general locality. For example, when $n = 7$ and $k = 5$, we can confirm that the condition for t is given by $t < 64$, not by $t < 70$. In the proof of this theorem, we first check the range of n that satisfies the assumption in Lemma 7. For other n , we check the condition for the existence of nontrivial integer solutions for the equations in Lemma 5 one by one. We present the details in Appendix A 2.

Finally, we show the result for the case of $SU(2)$ symmetry. We present the result for general locality k for sufficiently large n in the following theorem, which corresponds to the third part of Theorem 1 of Ref. [49].

Theorem 5. (Result for general locality k and sufficiently large qubit count n under the $SU(2)$ symmetry.) Let $n, k, t \in \mathbb{N}$ satisfy $k \geq 2$ and $n \geq 2^{2(\lfloor k/2 \rfloor + 1)}$, and R be a unitary representation of $G = SU(2)$ on n qubits defined by Eq. (5). Then, the distribution of the (G, R) -symmetric k -local random circuit is an asymptotic (G, R) -symmetric unitary t -design if and only if

$$t < \frac{2^{\lfloor k/2 \rfloor}}{(\lfloor k/2 \rfloor + 1)!} \prod_{\alpha=1}^{\lfloor k/2 \rfloor + 1} (n - 2\alpha + 1). \quad (32)$$

Similarly to Theorem 3, the condition $n \geq 2^{2(\lfloor k/2 \rfloor + 1)}$ is needed only for the proof of the “if” part, and we can show that for any $k \geq 2(\lfloor k/2 \rfloor + 1)$, the distribution is not an asymptotic unitary t -design if t does not satisfy the condition above without the assumption. We present the proof in Appendix A 3.

While Theorem 5 gives the result for general locality k and sufficiently large n , it does not hold for small n . As a complementary result, we focus on the small locality $k = 2, 3$, and 4, and give the result for small n in the following theorem.

Theorem 6. (Result for small locality k and general qubit count n under the $SU(2)$ symmetry.) Let $n, t \in \mathbb{N}$, $k = 2, 3$, or 4 , $n \geq k + 1$, and R be a unitary representation of $G = SU(2)$ on n qubits defined by Eq. (5). Then, the distribution of the (G, R) -symmetric k -local random circuits is an asymptotic (G, R) -symmetric unitary t -designs if and only if

- when $k = 2$,

$$\begin{cases} t < \infty & \text{when } n = 3, \\ t < 10 & \text{when } n = 6, \\ t < 20 & \text{when } n = 7, 8, \\ t < (n-1)(n-3) & \text{when } n = 4, 5 \text{ or } n \geq 9. \end{cases} \quad (33)$$

- when $k = 3$,

$$\begin{cases} t < 10 & \text{when } n = 6, \\ t < 20 & \text{when } n = 7, 8, \\ t < (n-1)(n-3) & \text{when } n = 4, 5 \text{ or } n \geq 9. \end{cases} \quad (34)$$

- when $k = 4$,

$$\begin{cases} t < \infty & \text{when } n = 5, \\ t < 35 & \text{when } n = 8, \\ t < 90 & \text{when } n = 9, \\ t < 96 & \text{when } n = 10, \\ t < 192 & \text{when } n = 11, \\ t < 330 & \text{when } n = 12, \\ t < \frac{2}{3}(n-1)(n-3)(n-5) & \text{when } n = 6, 7 \text{ or } n \geq 13. \end{cases} \quad (35)$$

In the proof of this theorem, we check the range of n that satisfies the assumption in Lemma 11. For n that does not satisfy the assumptions, we check the equations one by one, which we present in Appendix A 3.

IV. PROOF OF THE GENERAL THEOREM (THEOREM 1)

In this section, we present the proof of Theorem 1. This proof consists of three parts. First, in Lemma 1, we rewrite the condition for forming unitary designs in terms of commutants. Next, in Lemma 2, we prove that the condition for the commutants is satisfied when Eqs. (19), (20), and (21) have no nontrivial integer solution. Finally, in Lemma 3, we prove the converse part, i.e., we prove that the condition for the commutants is not satisfied when Eqs. (19), (20), and (21) have a nontrivial integer solution.

First, we show that the necessary and sufficient condition for forming unitary t -designs can be described as a property of commutants of t -fold operators. This is a standard technique to deal with unitary designs.

Lemma 1. Let $t, n \in \mathbb{N}$, R be a unitary representation of a group G on $\mathcal{H}$, and $\{\mathcal{S}^\gamma\}_{\gamma \in \Gamma}$ be a finite set of connected compact Lie subgroups of $\mathcal{U}_{n,G,R}$. Then, $\zeta_{\{\mathcal{S}^\gamma\}_{\gamma \in \Gamma}}$ is an asymptotic (G, R) -symmetric unitary t -design if and only if

$$\text{Comm} \left(\Omega_t \left(\bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma \right) \right) = \text{Comm}(\Omega_t(\mathcal{U}_{n,G,R})), \quad (36)$$

where $\text{Comm}(\mathcal{X})$ is the set of operators commuting with all operators in $\mathcal{X}$, and

$$\Omega_t(U) := U^{\otimes t}. \quad (37)$$

Proof. By the definition of the moment operator and the definition of $\zeta_{\{\mathcal{S}^\gamma\}_{\gamma \in \Gamma}}$, we have

$$M_{t, \zeta_{\{\mathcal{S}^\gamma\}_{\gamma \in \Gamma}}} = \sum_{\gamma \in \Gamma} p^\gamma M_{t, \mathcal{S}^\gamma}. \quad (38)$$

By Lemma 15, $M_{t,\mathcal{S}^\gamma}$ is Hermitian and positive for all $\gamma \in \Gamma$. Thus $M_{t,\zeta_{\{\mathcal{S}^\gamma\}_{\gamma \in \Gamma}}}$ is also Hermitian and positive, and has the following spectral decomposition:

$$M_{t,\zeta_{\{\mathcal{S}^\gamma\}_{\gamma \in \Gamma}}} = \sum_{h \in H} h \Pi_{\{|\Psi\rangle \in \mathcal{H}^{\otimes 2t} \mid M_{t,\zeta_{\{\mathcal{S}^\gamma\}_{\gamma \in \Gamma}}} |\Psi\rangle = h |\Psi\rangle\}}, \quad (39)$$

where H is the set of eigenvalues of $M_{t,\zeta_{\{\mathcal{S}^\gamma\}_{\gamma \in \Gamma}}}$, and $\Pi_{\mathcal{K}}$ is the projection operator onto $\mathcal{K}$. Since $M_{t,\zeta_{\{\mathcal{S}^\gamma\}_{\gamma \in \Gamma}}}$ is a convex combination of projections, we have $H \subset [0, 1]$. Then, we have

$$\lim_{D \rightarrow \infty} \left(M_{t,\zeta_{\{\mathcal{S}^\gamma\}_{\gamma \in \Gamma}}} \right)^D = \lim_{D \rightarrow \infty} \sum_{h \in H} h^D \Pi_{\{|\Psi\rangle \in \mathcal{H}^{\otimes 2t} \mid M_{t,\zeta_{\{\mathcal{S}^\gamma\}_{\gamma \in \Gamma}}} |\Psi\rangle = h |\Psi\rangle\}} = \Pi_{\{|\Psi\rangle \in \mathcal{H}^{\otimes 2t} \mid M_{t,\zeta_{\{\mathcal{S}^\gamma\}_{\gamma \in \Gamma}}} |\Psi\rangle = |\Psi\rangle\}}. \quad (40)$$

We are going to show that

$$\{|\Psi\rangle \in \mathcal{H}^{\otimes 2t} \mid M_{t,\zeta_{\{\mathcal{S}^\gamma\}_{\gamma \in \Gamma}}} |\Psi\rangle = |\Psi\rangle\} = \bigcap_{\gamma \in \Gamma} E(\text{Comm}(\Omega_t(\mathcal{S}^\gamma))), \quad (41)$$

where $E : \mathcal{L}(\mathcal{H}^{\otimes t}) \rightarrow \mathcal{H}^{\otimes 2t}$ is defined by

$$E(K) := (K \otimes I) |\eta\rangle \quad \forall K \in \mathcal{L}(\mathcal{H}^{\otimes t}) \quad (42)$$

with

$$|\eta\rangle := \frac{1}{\sqrt{d^{tn}}} \sum_{j=1}^{d^{tn}} |j\rangle \otimes |j\rangle \quad (43)$$

and an orthonormal basis $\{|j\rangle\}_{j=1}^{d^{tn}}$ of $\mathcal{H}^{\otimes t}$. For the proof of the inclusion relation $\{|\Psi\rangle \in \mathcal{H}^{\otimes 2t} \mid M_{t,\zeta_{\{\mathcal{S}^\gamma\}_{\gamma \in \Gamma}}} |\Psi\rangle = |\Psi\rangle\} \supset \bigcap_{\gamma \in \Gamma} E(\text{Comm}(\Omega_t(\mathcal{S}^\gamma)))$, we take arbitrary $|\Psi\rangle \in \bigcap_{\gamma \in \Gamma} E(\text{Comm}(\Omega_t(\mathcal{S}^\gamma)))$. By Lemma 15, we have $M_{t,\mu_{\mathcal{S}^\gamma}} |\Psi\rangle = |\Psi\rangle$ for all $\gamma \in \Gamma$. By Eq. (38), we get $M_{t,\zeta_{\{\mathcal{S}^\gamma\}_{\gamma \in \Gamma}}} |\Psi\rangle = |\Psi\rangle$. For the proof of the inverse inclusion relation, we take arbitrary $|\Psi\rangle \in \mathcal{H}^{\otimes 2t}$ satisfying $M_{t,\zeta_{\{\mathcal{S}^\gamma\}_{\gamma \in \Gamma}}} |\Psi\rangle = |\Psi\rangle$. Then by Eq. (38), we have

$$\sum_{\gamma \in \Gamma} p^\gamma \langle \Psi | M_{t,\zeta_{\{\mathcal{S}^\gamma\}_{\gamma \in \Gamma}}} |\Psi\rangle = \langle \Psi | M_{t,\zeta_{\{\mathcal{S}^\gamma\}_{\gamma \in \Gamma}}} |\Psi\rangle = 1. \quad (44)$$

By noting that $\sum_{\gamma \in \Gamma} p^\gamma = 1$, $p^\gamma > 0$, and $\langle \Psi | M_{t,\zeta_{\{\mathcal{S}^\gamma\}_{\gamma \in \Gamma}}} |\Psi\rangle \in [0, 1]$ for all $\gamma \in \Gamma$, Eq. (44) implies that $\langle \Psi | M_{t,\zeta_{\{\mathcal{S}^\gamma\}_{\gamma \in \Gamma}}} |\Psi\rangle = 1$ for all $\gamma \in \Gamma$, which implies that $|\Psi\rangle \in E(\text{Comm}(\Omega_t(\mathcal{S}^\gamma)))$ by Lemma 15. Since this holds for $\gamma \in \Gamma$, we get $|\Psi\rangle \in \bigcap_{\gamma \in \Gamma} E(\text{Comm}(\Omega_t(\mathcal{S}^\gamma)))$. Thus we have shown Eq. (41). Since E is bijective, we have

$$\bigcap_{\gamma \in \Gamma} E(\text{Comm}(\Omega_t(\mathcal{S}^\gamma))) = E \left(\bigcap_{\gamma \in \Gamma} \text{Comm}(\mathcal{S}^\gamma) \right) = E \left(\text{Comm} \left(\bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma \right) \right). \quad (45)$$

By Eqs. (40) and (45), we have

$$\lim_{D \rightarrow \infty} \left(M_{t,\zeta_{\{\mathcal{S}^\gamma\}_{\gamma \in \Gamma}}} \right)^D = \Pi_{E(\text{Comm}(\bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma))}. \quad (46)$$

By Lemma 15, we have

$$M_{t,\mu_{\mathcal{U}_{n,G,R}}} = \Pi_{E(\text{Comm}(\Omega_t(\mathcal{U}_{n,G,R})))}. \quad (47)$$

By Eqs. (46) and (47), the distribution $\zeta_{\{\mathcal{S}^\gamma\}_{\gamma \in \Gamma}}$ is an asymptotic (G, R) -symmetric unitary t -design if and only if $E(\text{Comm}(\bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma)) = E(\text{Comm}(\Omega_t(\mathcal{U}_{n,G,R})))$, which is equivalent to Eq. (36) by the bijectivity of E . $\square$

Next, we show that the nonexistence of nontrivial integer solution of equations in Theorem 1 implies the commutant relation presented in Lemma 1.

Lemma 2. Let $n, t \in \mathbb{N}$, R be a unitary representation of a group G , $\{\mathcal{S}^\gamma\}_{\gamma \in \Gamma}$ be a finite set of connected compact Lie subgroup of $\mathcal{U}_{n,G,R}$, $\bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma$ be semi-universal for $\mathcal{U}_{n,G,R}$ and Eqs. (19) (20), and (21) do not have a nontrivial integer solution $(x_\lambda)_{\lambda \in \Lambda} \in \mathbb{Z}^\Lambda$. Then,

$$\text{Comm} \left(\Omega_t \left(\bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma \right) \right) = \text{Comm}(\Omega_t(\mathcal{U}_{n,G,R})), \quad (48)$$

where Ω_t is defined by Eq. (37).

Proof. We prove this lemma in three steps.

In the first step, we show that

$$\sum_{(\lambda, \alpha) \in \Xi} e^{i w_{\lambda, \alpha}} P_{\lambda, \alpha} \in \left\langle \bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma \right\rangle \quad \forall \mathbf{w} = (w_{\lambda, \alpha})_{(\lambda, \alpha) \in \Xi} \in \mathcal{W}, \quad (49)$$

where a set Ξ , a linear subspace $\mathcal{W}$ of $\mathbb{R}^\Xi$, and projections $P_{\lambda, \alpha}$ are defined by

$$\Xi := \{(\lambda, \alpha) \mid \lambda \in \Lambda, \alpha \in \{1, 2, \dots, m_\lambda\}\}, \quad (50)$$

$$\mathcal{W} := \Delta^{-1}(\mathcal{V}), \quad (51)$$

$$\Delta(\mathbf{w}) := (\Delta_\lambda(\mathbf{w}))_{\lambda \in \Lambda} \quad \forall \mathbf{w} \in \mathbb{R}^\Xi, \quad (52)$$

$$\Delta_\lambda(\mathbf{w}) := \sum_{\alpha=1}^{m_\lambda} w_{\lambda, \alpha} \quad \forall \mathbf{w} \in \mathbb{R}^\Xi, \quad (53)$$

$$\mathcal{V} := \mathbf{f} \left(\text{span} \left(\bigcup_{\gamma \in \Gamma} \mathfrak{s}^\gamma \right) \right), \quad (54)$$

$$P_{\lambda, \alpha} := F_\lambda(I \otimes |\alpha\rangle \langle \alpha|) F_\lambda^\dagger, \quad (55)$$

and $|\alpha\rangle$ is the α th basis vector of $\mathbb{C}^{m_\lambda}$. We take arbitrary $\mathbf{w} \in \mathcal{W}$. By the definition of $\mathcal{W}$, there exists $A \in \text{span}(\bigcup_{\gamma \in \Gamma} \mathfrak{s}^\gamma)$ such that

$$\left(\sum_{\alpha=1}^{m_\lambda} w_{\lambda, \alpha} \right)_{\lambda \in \Lambda} = \mathbf{f}(A). \quad (56)$$

Since $A \in \text{span}(\bigcup_{\gamma \in \Gamma} \mathfrak{s}^\gamma)$, A can be written as

$$A = \sum_{\gamma \in \Gamma} A^\gamma \quad (57)$$

with some $A^\gamma \in \mathfrak{s}^\gamma$. By noting that $A^\gamma \in \mathfrak{u}_{n,G,R}$, A^γ can be expressed as

$$A^\gamma = \sum_{\lambda \in \Lambda} F_\lambda(I \otimes A_\lambda^\gamma) F_\lambda^\dagger \quad (58)$$

with some $A_\lambda^\gamma \in \mathcal{L}(\mathbb{C}^{m_\lambda})$, which implies that

$$e^{-i A^\gamma} = \sum_{\lambda \in \Lambda} F_\lambda \left(I \otimes e^{-i A_\lambda^\gamma} \right) F_\lambda^\dagger. \quad (59)$$

By the definition of $P_{\lambda, \alpha}$, we have

$$\sum_{(\lambda, \alpha) \in \Xi} e^{i w_{\lambda, \alpha}} P_{\lambda, \alpha} = \sum_{\lambda \in \Lambda} F_\lambda \left[I \otimes \left(\sum_{\alpha=1}^{m_\lambda} e^{i w_{\lambda, \alpha}} |\alpha\rangle \langle \alpha| \right) \right] F_\lambda^\dagger. \quad (60)$$

By Eqs. (59) and (60), we get

$$\left(\sum_{(\lambda, \alpha) \in \Xi} e^{iw_{\lambda, \alpha}} P_{\lambda, \alpha} \right) \left(\prod_{\gamma \in \Gamma} e^{-iA^\gamma} \right) = \sum_{\lambda \in \Lambda} F_\lambda \left(I \otimes \left(\sum_{\alpha=1}^{m_\lambda} e^{iw_{\lambda, \alpha}} |\alpha\rangle \langle \alpha| \right) \left(\prod_{\gamma \in \Gamma} e^{-iA_\lambda^\gamma} \right) \right) F_\lambda^\dagger. \quad (61)$$

By plugging Eq. (58) into Eq. (57), we get

$$A = \sum_{\lambda \in \Lambda} F_\lambda \left(I \otimes \sum_{\gamma \in \Gamma} A_\lambda^\gamma \right) F_\lambda^\dagger, \quad (62)$$

which implies that

$$f_\lambda(A) = \text{tr} \left(\sum_{\gamma \in \Gamma} A_\lambda^\gamma \right) = \sum_{\gamma \in \Gamma} \text{tr}(A_\lambda^\gamma). \quad (63)$$

By Eqs. (56) and (61), we get

$$\sum_{\alpha=1}^{m_\lambda} w_{\lambda, \alpha} = \sum_{\gamma \in \Gamma} \text{tr}(A_\lambda^\gamma), \quad (64)$$

which implies that

$$\det \left(\left(\sum_{\alpha=1}^{m_\lambda} e^{iw_{\lambda, \alpha}} |\alpha\rangle \langle \alpha| \right) \left(\prod_{\gamma \in \Gamma} e^{-iA_\lambda^\gamma} \right) \right) = e^{i \sum_{\alpha=1}^{m_\lambda} w_{\lambda, \alpha}} \prod_{\gamma \in \Gamma} e^{-i \text{tr}(A_\lambda^\gamma)} = e^{i(\sum_{\alpha=1}^{m_\lambda} w_{\lambda, \alpha} - \sum_{\gamma \in \Gamma} \text{tr}(A_\lambda^\gamma))} = 1. \quad (65)$$

This means that the operator of the l.h.s. of Eq. (61) is in the form of $\sum_{\lambda \in \Lambda} F_\lambda (I \otimes U_\lambda) F_\lambda^\dagger$ with some $U_\lambda \in \text{SU}(m_\lambda)$. By using the semi-universality condition shown as Eq. (14), we have

$$\left(\sum_{(\lambda, \alpha) \in \Xi} e^{iw_{\lambda, \alpha}} P_{\lambda, \alpha} \right) \left(\prod_{\gamma \in \Gamma} e^{-iA^\gamma} \right) \in \left\langle \bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma \right\rangle. \quad (66)$$

Since $e^{-iA^\gamma} \in \mathcal{S}^\gamma$, we have

$$\left(\prod_{\gamma \in \Gamma} e^{-iA^\gamma} \right)^{-1} \in \left\langle \bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma \right\rangle. \quad (67)$$

By multiplying Eq. (66) and Eq. (67), we get Eq. (49).

In the second step, we show that

$$\mathcal{S}_t \left(\bigotimes_{l=1}^t P_{\lambda_l, \alpha_l} \right) \in \text{Alg} \left(\Omega_t \left(\left\langle \bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma \right\rangle \right) \right) \quad \forall (\lambda_1, \alpha_1), \dots, (\lambda_t, \alpha_t) \in \Xi, \quad (68)$$

where $\text{Alg}(\cdot)$ is the generated algebra over $\mathbb{C}$, and $\mathcal{S}_t$ is defined by

$$\mathcal{S}_t(A) := \frac{1}{t!} \sum_{\sigma \in \mathfrak{S}_t} V_\sigma A V_\sigma^\dagger. \quad (69)$$

with V_σ defined by

$$V_\sigma \left(\bigotimes_{\alpha=1}^m |\psi_\alpha\rangle \right) = \bigotimes_{\alpha=1}^m |\psi_{\sigma^{-1}(\alpha)}\rangle \quad (70)$$

for $\sigma \in \mathfrak{S}_m$. We define $z_{\lambda,\alpha} := \#\{s \in \{1, 2, \dots, t\} \mid (\lambda_s, \alpha_s) = (\lambda, \alpha)\}$. By using Lemma 16, we have

$$\mathcal{S}_t \left(\bigotimes_{s=1}^t P_{\lambda_s, \alpha_s} \right) = \mathcal{S}_t \left(\bigotimes_{(\lambda, \alpha) \in \Xi} P_{\lambda, \alpha}^{\otimes z_{\lambda, \alpha}} \right), \quad (71)$$

where we note that we do not have to specify the order in Ξ due to the property of $\mathcal{S}_t$. By Eq. (71), it is sufficient to show that $\mathcal{S}_t \left(\bigotimes_{(\lambda, \alpha) \in \Xi} P_{\lambda, \alpha}^{\otimes z_{\lambda, \alpha}} \right) \in \text{Alg} \left(\Omega_t \left(\bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma \right) \right)$. We take an arbitrary fixed basis of $\{\mathbf{q}_l\}_{l=1, \dots, L}$ of $\mathcal{W}$ and arbitrary $\theta_1, \dots, \theta_L \in \mathbb{R}$. Since $\sum_{l=1}^L \theta_l \mathbf{q}_l \in \mathcal{W}$, by Eq. (49), we have

$$\sum_{(\lambda, \alpha) \in \Xi} \exp \left(i \sum_{l=1}^L \theta_l q_{l, \lambda, \alpha} \right) P_{\lambda, \alpha} \in \left\langle \bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma \right\rangle, \quad (72)$$

which implies that

$$\left(\sum_{(\lambda, \alpha) \in \Xi} \exp \left(i \sum_{l=1}^L \theta_l q_{l, \lambda, \alpha} \right) P_{\lambda, \alpha} \right)^{\otimes t} \in \Omega_t \left(\left\langle \bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma \right\rangle \right). \quad (73)$$

By Lemma 16, we have

$$\begin{aligned} \left(\sum_{(\lambda, \alpha) \in \Xi} \exp \left(i \sum_{l=1}^L \theta_l q_{l, \lambda, \alpha} \right) P_{\lambda, \alpha} \right)^{\otimes t} &= \sum_{\mathbf{z}' \in \mathcal{Z}_t} \frac{t!}{\prod_{(\lambda, \alpha) \in \Xi} z'_{\lambda, \alpha}!} \mathcal{S}_t \left(\bigotimes_{(\lambda, \alpha) \in \Xi} \left(\exp \left(i \sum_{l=1}^L \theta_l q_{l, \lambda, \alpha} \right) P_{\lambda, \alpha} \right)^{\otimes z'_{\lambda, \alpha}} \right) \\ &= \sum_{\mathbf{z}' \in \mathcal{Z}_t} \frac{t!}{\prod_{(\lambda, \alpha) \in \Xi} z'_{\lambda, \alpha}!} \exp \left(i \sum_{l=1}^L \theta_l \sum_{(\lambda, \alpha) \in \Xi} z'_{\lambda, \alpha} q_{l, \lambda, \alpha} \right) \mathcal{S}_t \left(\bigotimes_{(\lambda, \alpha) \in \Xi} P_{\lambda, \alpha}^{\otimes z'_{\lambda, \alpha}} \right), \end{aligned} \quad (74)$$

where $\mathcal{Z}_t$ is defined by

$$\mathcal{Z}_t := \left\{ \mathbf{z}' \in (\mathbb{Z}_{\geq 0})^\Xi \mid \sum_{(\lambda, \alpha) \in \Xi} z'_{\lambda, \alpha} = t \right\}. \quad (75)$$

Eq. (74) implies that

$$\begin{aligned} &\lim_{\Theta \rightarrow \infty} \frac{1}{(2\Theta)^L} \int_{-\Theta}^{\Theta} d\theta_L \cdots \int_{-\Theta}^{\Theta} d\theta_1 \exp \left(-i \sum_{l=1}^L \theta_l \sum_{(\lambda, \alpha) \in \Xi} q_{l, \lambda, \alpha} z_{\lambda, \alpha} \right) \left(\sum_{(\lambda, \alpha) \in \Xi} \exp \left(i \sum_{l=1}^L \theta_l q_{l, \lambda, \alpha} \right) P_{\lambda, \alpha} \right)^{\otimes t} \\ &= \sum_{\mathbf{z}' \in \mathcal{Z}_t} \frac{t!}{\prod_{(\lambda, \alpha) \in \Xi} z'_{\lambda, \alpha}!} \prod_{l=1}^L \left(\lim_{\Theta \rightarrow \infty} \frac{1}{2\Theta} \int_{-\Theta}^{\Theta} \exp \left(i \theta_l \left(\sum_{(\lambda, \alpha) \in \Xi} q_{l, \lambda, \alpha} z'_{\lambda, \alpha} - \sum_{(\lambda, \alpha) \in \Xi} q_{l, \lambda, \alpha} z_{\lambda, \alpha} \right) \right) d\theta_l \right) \mathcal{S}_t \left(\bigotimes_{(\lambda, \alpha) \in \Xi} P_{\lambda, \alpha}^{\otimes z'_{\lambda, \alpha}} \right) \\ &= \sum_{\mathbf{z}' \in \mathcal{Z}_t} \frac{t!}{\prod_{(\lambda, \alpha) \in \Xi} z'_{\lambda, \alpha}!} \prod_{l=1}^L \delta_{\sum_{(\lambda, \alpha) \in \Xi} q_{l, \lambda, \alpha} z'_{\lambda, \alpha}, \sum_{(\lambda, \alpha) \in \Xi} q_{l, \lambda, \alpha} z_{\lambda, \alpha}} \mathcal{S}_t \left(\bigotimes_{(\lambda, \alpha) \in \Xi} P_{\lambda, \alpha}^{\otimes z'_{\lambda, \alpha}} \right). \end{aligned} \quad (76)$$

Since there do not exist nontrivial $(x_\lambda)_{\lambda \in \Lambda} \in \mathbb{Z}^\Lambda$ satisfying Eqs. (19), (20), and (21) by assumption, Lemma 17 implies that if $\sum_{(\lambda, \alpha) \in \Xi} z_{\lambda, \alpha} = \sum_{(\lambda, \alpha) \in \Xi} z'_{\lambda, \alpha} = t$ and $\sum_{(\lambda, \alpha) \in \Xi} w_{\lambda, \alpha} z_{\lambda, \alpha} = \sum_{(\lambda, \alpha) \in \Xi} w_{\lambda, \alpha} z'_{\lambda, \alpha}$ for all $(w_{\lambda, \alpha}) \in \mathcal{W}$, then we have $\mathbf{z} = \mathbf{z}'$. This can be rephrased as

$$\prod_{l=1}^L \delta_{\sum_{(\lambda, \alpha) \in \Xi} q_{l, \lambda, \alpha} z'_{\lambda, \alpha}, \sum_{(\lambda, \alpha) \in \Xi} q_{l, \lambda, \alpha} z_{\lambda, \alpha}} = \prod_{(\lambda, \alpha) \in \Xi} \delta_{z'_{\lambda, \alpha}, z_{\lambda, \alpha}}. \quad (77)$$

By Eqs. (76) and (77), we get

$$\begin{aligned} & \lim_{\Theta \rightarrow \infty} \frac{1}{(2\Theta)^L} \int_{-\Theta}^{\Theta} d\theta_L \cdots \int_{-\Theta}^{\Theta} d\theta_1 \exp \left(-i \sum_{l=1}^L \theta_l \sum_{(\lambda, \alpha) \in \Xi} q_{l, \lambda, \alpha} z_{\lambda, \alpha} \right) \left(\sum_{(\lambda, \alpha) \in \Xi} \exp \left(i \sum_{l=1}^L \theta_l q_{l, \lambda, \alpha} \right) P_{\lambda, \alpha} \right)^{\otimes t} \\ &= \frac{t!}{\prod_{(\lambda, \alpha) \in \Xi} z_{\lambda, \alpha}!} \mathcal{S}_t \left(\bigotimes_{(\lambda, \alpha) \in \Xi} P_{\lambda, \alpha}^{\otimes z_{\lambda, \alpha}} \right). \end{aligned} \quad (78)$$

By Eq. (73), the l.h.s. of Eq. (78) is an element of $\text{Alg}(\Omega_t(\langle \bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma \rangle))$. Thus Eq. (78) implies that $\mathcal{S}_t \left(\bigotimes_{\lambda, \alpha} P_{\lambda, \alpha}^{\otimes z_{\lambda, \alpha}} \right) \in \text{Alg}(\Omega_t(\langle \bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma \rangle))$. By combining this with Eq. (71), we get Eq. (68).

In the final step, we show Eq. (48). We take arbitrary $U \in Z(\mathcal{U}_{n, G, R})$. Then, U can be written as

$$U = \sum_{\lambda \in \Lambda} F_\lambda (I \otimes u_\lambda I) F_\lambda^\dagger = \sum_{(\lambda, \alpha) \in \Xi} u_\lambda P_{\lambda, \alpha} \quad (79)$$

with some $u_\lambda \in \mathbb{C}$. By the definitions of Ω_t and $\mathcal{S}_t$ and Eq. (79), we get

$$\begin{aligned} \Omega_t(U) &= U^{\otimes t} \\ &= \mathcal{S}_t(U^{\otimes t}) \\ &= \mathcal{S}_t \left(\sum_{(\lambda_1, \alpha_1), \dots, (\lambda_t, \alpha_t) \in \Xi} \bigotimes_{s=1}^t u_{\lambda_s} P_{\lambda_s, \alpha_s} \right) \\ &= \sum_{(\lambda_1, \alpha_1), \dots, (\lambda_t, \alpha_t) \in \Xi} \left(\prod_{s=1}^t u_{\lambda_s} \right) \mathcal{S}_t \left(\bigotimes_{s=1}^t P_{\lambda_s, \alpha_s} \right) \\ &\in \text{Alg} \left(\Omega_t \left(\left\langle \bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma \right\rangle \right) \right). \end{aligned} \quad (80)$$

Since this holds for all $U \in Z(\mathcal{U}_{n, G, R})$, we have

$$\Omega_t(Z(\mathcal{U}_{n, G, R})) \subset \text{Alg} \left(\Omega_t \left(\left\langle \bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma \right\rangle \right) \right). \quad (81)$$

By taking the commutant of the both sides, we get

$$\text{Comm}(\Omega_t(Z(\mathcal{U}_{n, G, R}))) \subset \text{Comm} \left(\text{Alg} \left(\Omega_t \left(\left\langle \bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma \right\rangle \right) \right) \right) = \text{Comm} \left(\Omega_t \left(\left\langle \bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma \right\rangle \right) \right). \quad (82)$$

Since $\bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma$ is semi-universal for $\mathcal{U}_{n, G, R}$, we have

$$\Omega_t \left(\left\langle \bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma \right\rangle \right) \cdot \Omega_t(Z(\mathcal{U}_{n, G, R})) = \Omega_t(\mathcal{U}_{n, G, R}). \quad (83)$$

By taking the commutant of this equation, we get

$$\text{Comm} \left(\Omega_t \left(\left\langle \bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma \right\rangle \right) \right) \cap \text{Comm}(\Omega_t(Z(\mathcal{U}_{n, G, R}))) = \text{Comm}(\Omega_t(\mathcal{U}_{n, G, R})). \quad (84)$$

By Eqs. (82) and (84), we get Eq. (48). $\square$

Finally, we show the converse of Lemma 2.

Lemma 3. *Let $n, t \in \mathbb{N}$, $\{\mathcal{S}^\gamma\}_{\gamma \in \Gamma}$ be a finite set of connected compact unitary subgroups of $\mathcal{U}_{n,G,R}$, and Eqs. (19), (20), and (21) have a nontrivial integer solution $\mathbf{x} \in \mathbb{Z}^\Lambda$. Then,*

$$\text{Comm} \left(\Omega_t \left(\bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma \right) \right) \neq \text{Comm}(\Omega_t(\mathcal{U}_{n,G,R})). \quad (85)$$

Proof. We prove this lemma in three steps.

In the first step, we show that

$$\omega_t(A) |\Phi(\mathbf{p})\rangle = \left(\sum_{\lambda \in \Lambda} m_\lambda \text{tr}(A_\lambda) \right) |\Phi(\mathbf{p})\rangle, \quad (86)$$

for all $A \in \mathfrak{u}_{n,G,R}$ and $\mathbf{p} \in (\mathbb{Z}_{\geq 0})^\Lambda$ satisfying $\sum_{\lambda \in \Lambda} m_\lambda p_\lambda = t$, where A_λ is defined by Eq. (12), and

$$|\Phi(\mathbf{p})\rangle := \bigotimes_{\lambda \in \Lambda} \left[F_\lambda^{\otimes m_\lambda} (|\psi_\lambda\rangle^{\otimes m_\lambda} \otimes |\chi(\mathbb{C}^{m_\lambda})\rangle) \right]^{\otimes p_\lambda}, \quad (87)$$

with arbitrarily chosen states $|\psi_\lambda\rangle \in \mathbb{C}^{r_\lambda}$ and

$$|\chi(\mathbb{C}^m)\rangle := \frac{1}{\sqrt{m!}} \sum_{\sigma \in \mathfrak{S}_m} \text{sgn}(\sigma) \bigotimes_{\alpha=1}^m |\sigma(\alpha)\rangle, \quad (88)$$

$$\omega_t(A) := \sum_{s=1}^t I^{\otimes s-1} \otimes A \otimes I^{\otimes t-s}. \quad (89)$$

By noting that $(O_1 \otimes I + I \otimes O_2)(|\phi_1\rangle \otimes |\phi_2\rangle) = (\alpha_1 + \alpha_2)(|\phi_1\rangle \otimes |\phi_2\rangle)$ when $O_j |\phi_j\rangle = \alpha_j |\phi_j\rangle$, for the proof of (86), it is sufficient to show that

$$\omega_{m_\lambda}(A) \left[F_\lambda^{\otimes m_\lambda} (|\psi_\lambda\rangle^{\otimes m_\lambda} \otimes |\chi(\mathbb{C}^{m_\lambda})\rangle) \right] = \text{tr}(A_\lambda) \left[F_\lambda^{\otimes m_\lambda} (|\psi_\lambda\rangle^{\otimes m_\lambda} \otimes |\chi(\mathbb{C}^{m_\lambda})\rangle) \right] \quad (90)$$

for all $\lambda \in \Lambda$. By the decomposition of A , we have

$$AF_\lambda = \sum_{\mu \in \Lambda} F_\mu (I \otimes A) F_\mu^\dagger F_\lambda. \quad (91)$$

By the definition of F_λ 's, we have

$$F_\mu^\dagger F_\lambda = \begin{cases} I & \text{if } \lambda = \mu \\ 0 & \text{if } \lambda \neq \mu. \end{cases} \quad (92)$$

By plugging Eq. (92) into Eq. (91), we get

$$AF_\lambda = F_\lambda (I \otimes A_\lambda). \quad (93)$$

By the definition of ω_{m_λ} and this equation, we get

$$\begin{aligned} \omega_{m_\lambda}(A) F_\lambda^{\otimes m_\lambda} &= \sum_{s=1}^{m_\lambda} F_\lambda^{\otimes s-1} \otimes AF_\lambda \otimes F_\lambda^{\otimes m_\lambda-s} \\ &= \sum_{s=1}^{m_\lambda} F_\lambda^{\otimes s-1} \otimes F_\lambda (I \otimes A_\lambda) \otimes F_\lambda^{\otimes m_\lambda-s} \\ &= F_\lambda^{\otimes m_\lambda} \omega_{m_\lambda}(I \otimes A_\lambda) \\ &= F_\lambda^{\otimes m_\lambda} (I^{\otimes m_\lambda} \otimes \omega_{m_\lambda}(A_\lambda)), \end{aligned} \quad (94)$$

which implies that

$$\omega_{m_\lambda}(A) \left[F_\lambda^{\otimes m_\lambda}(|\psi_\lambda\rangle^{\otimes m_\lambda} \otimes |\chi(\mathbb{C}^{m_\lambda})\rangle) \right] = F_\lambda^{\otimes m_\lambda}(|\psi_\lambda\rangle^{\otimes m_\lambda} \otimes \omega_{m_\lambda}(A_\lambda) |\chi(\mathbb{C}^{m_\lambda})\rangle). \quad (95)$$

By applying Lemma 18 to the r.h.s. of this equation, we get Eq. (90).

In the second step, we show that

$$\text{Comm} \left(\omega_t \left(\bigcup_{\gamma \in \Gamma} \mathfrak{s}^\gamma \right) \right) \neq \text{Comm}(\omega_t(\mathbf{u}_{n,G,R})). \quad (96)$$

For the proof of this, we construct an operator O such that $O \in \text{Comm}(\bigcup_{\gamma \in \Gamma} \mathfrak{s}^\gamma)$ and $O \notin \text{Comm}(\mathbf{u}_{n,G,R})$. By Lemma 17, we can take two different vectors $\mathbf{y}, \mathbf{y}' \in (\mathbb{Z}_{\geq 0})^\Lambda$ satisfying $\sum_{\lambda \in \Lambda} m_\lambda y_\lambda = \sum_{\lambda \in \Lambda} m_\lambda y'_\lambda \leq t$ and $\sum_{\lambda \in \Lambda} y_\lambda v_\lambda = \sum_{\lambda \in \Lambda} y'_\lambda v_\lambda$ for all $\mathbf{v} \in \mathbf{f}(\text{span}(\bigcup_{\lambda \in \Lambda} \mathfrak{s}^\gamma))$. We define O by

$$O := |\Phi(\mathbf{y})\rangle \langle \Phi(\mathbf{y}')| \otimes I^{\otimes u}, \quad (97)$$

where $u := t - \sum_{\lambda \in \Lambda} m_\lambda y_\lambda$. By Eq. (86), we have

$$[\omega_t(A), O] = \left(\sum_{\lambda \in \Lambda} y_\lambda \text{tr}(A_\lambda) - \sum_{\lambda \in \Lambda} y'_\lambda \text{tr}(A_\lambda) \right) O = 0 \quad \forall A \in \bigcup_{\gamma \in \Gamma} \mathfrak{s}^\gamma, \quad (98)$$

which means that $O \in \text{Comm}(\bigcup_{\gamma \in \Gamma} \mathfrak{s}^\gamma)$. Since we have $\mathbf{y}$ and $\mathbf{y}'$ are different, we can take $\kappa \in \Lambda$ such that $y_\kappa \neq y'_\kappa$. We define $\tilde{P}_\kappa := \sum_{\alpha=1}^{m_\kappa} P_{\kappa,\alpha}$. Then, we have $\tilde{P}_\kappa \in \mathbf{u}_{n,G,R}$, and Eq. (86) implies that

$$[\omega_t(\tilde{P}_\kappa), O] = (y_\mu \text{tr}(\tilde{P}_\kappa) - y'_\mu \text{tr}(\tilde{P}_\kappa)) O = m_\lambda (y_\kappa - y'_\kappa) O \neq 0, \quad (99)$$

which means that $O \notin \text{Comm}(\mathbf{u}_{n,G,R})$. Thus we have proven Eq. (85).

Finally, we show Eq. (85). We note that

$$\text{Comm} \left(\Omega_t \left(\bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma \right) \right) = \text{Comm} \left(\bigcup_{\gamma \in \Gamma} \Omega_t(\mathcal{S}^\gamma) \right) = \bigcap_{\gamma \in \Gamma} \text{Comm}(\Omega_t(\mathcal{S}^\gamma)), \quad (100)$$

$$\text{Comm} \left(\omega_t \left(\bigcup_{\gamma \in \Gamma} \mathfrak{s}^\gamma \right) \right) = \text{Comm} \left(\bigcup_{\gamma \in \Gamma} \omega_t(\mathfrak{s}^\gamma) \right) = \bigcap_{\gamma \in \Gamma} \text{Comm}(\omega_t(\mathfrak{s}^\gamma)). \quad (101)$$

By Lemma 19, we have

$$\text{Comm}(\Omega_t(\mathcal{S}^\gamma)) = \text{Comm}(\omega_t(\mathfrak{s}^\gamma)). \quad (102)$$

By Eqs. (100), (101), and (102), we get

$$\text{Comm} \left(\Omega_t \left(\bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma \right) \right) = \text{Comm} \left(\omega_t \left(\bigcup_{\gamma \in \Gamma} \mathfrak{s}^\gamma \right) \right). \quad (103)$$

By using Lemma 19 again, we have

$$\text{Comm}(\omega_t(\mathbf{u}_{n,G,R})) = \text{Comm}(\Omega_t(\mathcal{U}_{n,G,R})). \quad (104)$$

Eqs. (103) and (104) imply the equivalence between Eq. (96) and Eq. (85). $\square$

By combining the lemmas above, we get the proof of Theorem 1 as follows:

Proof of Theorem 1. The “if” part follows from the combination of Lemmas 1 and 2, and the “only if” part follows from the combination of Lemmas 1 and 3. When R can be written as $T^{\otimes n}$ with a single-qudit representation T , Eq. (20) is implied by Eq. (21), because $I \in \mathbf{u}_{n,G,R}^\gamma$ with some $\gamma \in \Gamma$ (actually for all $\gamma \in \Gamma$) and $f_\lambda(I) = m_\lambda$. By Lemma 20, Eq. (21) is equivalent to Eq. (23). By combining these two statements, we can confirm that Eqs. (20) and (21) are equivalent to Eq. (23). $\square$

V. CONCLUSION AND DISCUSSION

In this work, we have proposed a general method for calculating the maximal t such that the random circuits with a gate set of connected compact unitary subgroups form asymptotic symmetric unitary t -designs. In particular, we have explicitly identified the tight bound on the maximal achievable order of unitary designs of symmetric local random circuits in the cases of $\mathbb{Z}_2$, $U(1)$, and $SU(2)$ symmetries. Although we have focused on the above symmetries, our method is general and useful for calculating the maximal order of design for other symmetries as long as the gate set satisfies the semi-universality. On the other hand, symmetric random circuits that do not satisfy the semi-universality do not generate asymptotic symmetric unitary 2-designs. We can therefore show the maximal order of designs of arbitrary symmetric random circuits, once we know if a given gate set satisfies the semi-universality. In this sense, we have fully characterized the randomness of symmetric local random circuits.

Although we have only considered the local random circuit where we apply one gate at each time step, the maximal order of design is the same for a random circuit with other architectures, such as the brick-wall architecture, as long as the circuit cannot be separated into two independent parts and the representation is the tensor product of a single-qudit representation.

It is an important open problem to derive the rate to generate an asymptotic symmetric unitary t -design in symmetric local random circuits. Without any symmetry, it has been shown recently that local random circuits are unitary t -designs if the circuit depth is linear in t [51]. It would be interesting to ask if the t -dependence on the convergence rate is the same under a symmetry. Moreover, while n -qubit local random circuits without any symmetry have been shown to form unitary t -designs with a logarithmic depth in n [45], the situation is completely different under a symmetry: it is observed that symmetric circuits require superlinear depth in the case of $U(1)$ symmetry [48] and $SU(2)$ symmetry [47]. Therefore, it is desirable to characterize how the convergence rate depends on the qubit count n under general symmetry. In addition, we believe that our work will open up new directions for future research. In the proof of Lemma 3, we have found a conserved quantity on t -copy states which evolve under symmetric and local dynamics. To investigate the consequence of such conservation law for physical properties, such as thermalization and entanglement dynamics, would also be interesting.

ACKNOWLEDGEMENTS

The authors wish to thank Iman Marvian, Hiroyasu Tajima, Janek Denzler, and Zongping Gong for insightful discussions. Y.M. is supported by JSPS KAKENHI Grant No. JP23KJ0421. R.S. is supported by the BMBF (PhoQuant, Grant No. 13N16103). This research is funded in part by the Gordon and Betty Moore Foundation's EPiQS Initiative, Grant GBMF8683 to T.S. N.Y. wishes to thank JST PRESTO No. JPMJPR2119, JST ASPIRE Grant Number JPMJAP2316, and the support from IBM Quantum. This work was supported by JST Grant Number JPMJPF2221, JST ERATO Grant Number JPMJER2302, and JST CREST Grant Number JPMJCR23I4, Japan.

Note Added: During the preparation of this article, we became aware of independent work by Austin Hulse, Hanqing Liu, and Iman Marvian [52], which studies similar questions and was posted on arXiv concurrently with the present paper. Both have arrived at the same result on the maximal order of unitary designs under the $U(1)$ and $SU(2)$ symmetries. Ref. [52] has assumed conjectures about combinatorial identities, which are introduced as Eqs. (86) and (120) of the version 1 of their manuscript for the proof of general k -local cases. In our work, we have provided a proof that is independent of any conjectures.

-
- [1] E. Noether, Invariante variationsprobleme, *Nachr. Ges. Wiss. Gottingen* **1918**, 235 (1918).
 - [2] Y. Nambu, Axial vector current conservation in weak interactions, *Phys. Rev. Lett.* **4**, 380 (1960).
 - [3] Y. Nambu and G. Jona-Lasinio, Dynamical model of elementary particles based on an analogy with superconductivity. i, *Phys. Rev.* **122**, 345 (1961).
 - [4] J. Goldstone, Field theories with superconductor solutions, *Nuovo Cim.* **19**, 154 (1961).
 - [5] Y. Nambu, Nobel lecture: Spontaneous symmetry breaking in particle physics: A case of cross fertilization, *Rev. Mod. Phys.* **81**, 1015 (2009).
 - [6] T. Senthil, A. Vishwanath, L. Balents, S. Sachdev, and M. P. A. Fisher, Deconfined quantum critical points, *Science* **303**, 1490 (2004).
 - [7] T. Senthil, L. Balents, S. Sachdev, A. Vishwanath, and M. P. A. Fisher, Quantum criticality beyond the landau-ginzburg-wilson paradigm, *Phys. Rev. B* **70**, 144407 (2004).
 - [8] A. W. Sandvik, Evidence for deconfined quantum criticality in a two-dimensional heisenberg model with four-spin interactions, *Phys. Rev. Lett.* **98**, 227202 (2007).

- [9] P. W. Shor, Scheme for reducing decoherence in quantum computer memory, *Phys. Rev. A* **52**, R2493 (1995).
- [10] A. M. Steane, Error correcting codes in quantum theory, *Phys. Rev. Lett.* **77**, 793 (1996).
- [11] A. R. Calderbank and P. W. Shor, Good quantum error-correcting codes exist, *Phys. Rev. A* **54**, 1098 (1996).
- [12] M. A. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*. (Cambridge University Press, Cambridge, 2000).
- [13] B. Eastin and E. Knill, Restrictions on transversal encoded quantum gate sets, *Phys. Rev. Lett.* **102**, 110502 (2009).
- [14] X.-G. Wen, Topological orders and edge excitations in fractional quantum hall states, *Advances in Physics* **44**, 405 (1995).
- [15] C. L. Kane and E. J. Mele, Quantum spin hall effect in graphene, *Phys. Rev. Lett.* **95**, 226801 (2005).
- [16] M. Z. Hasan and C. L. Kane, Colloquium: Topological insulators, *Rev. Mod. Phys.* **82**, 3045 (2010).
- [17] M. Sato and Y. Ando, Topological superconductors: a review, *Rep. Prog. Phys.* **80**, 076501 (2017).
- [18] Z.-C. Gu and X.-G. Wen, Tensor-entanglement-filtering renormalization approach and symmetry-protected topological order, *Phys. Rev. B* **80**, 155131 (2009).
- [19] F. Pollmann, A. M. Turner, E. Berg, and M. Oshikawa, Entanglement spectrum of a topological phase in one dimension, *Phys. Rev. B* **81**, 064439 (2010).
- [20] X. Chen, Z.-C. Gu, Z.-X. Liu, and X.-G. Wen, Symmetry-protected topological orders in interacting bosonic systems, *Science* **338**, 1604 (2012).
- [21] Y. Bao, S. Choi, and E. Altman, Symmetry enriched phases of quantum circuits, *Annals of Physics* **435**, 168618 (2021).
- [22] A. Lavasani, Y. Alavirad, and M. Barkeshli, Measurement-induced topological entanglement transitions in symmetric random quantum circuits, *Nature Phys.* **17**, 342 (2021).
- [23] R. Morral-Yepes, F. Pollmann, and I. Lovas, Detecting and stabilizing measurement-induced symmetry-protected topological phases in generalized cluster models, *Phys. Rev. B* **108**, 224304 (2023).
- [24] J. Hauser, Y. Li, S. Vijay, and M. P. A. Fisher, Continuous symmetry breaking in adaptive quantum dynamics, *Phys. Rev. B* **109**, 214305 (2024).
- [25] A. Y. Kitaev, Quantum computations: algorithms and error correction, *Russ. Math. Surv.* **52**, 1191 (1997).
- [26] C. M. Dawson and M. A. Nielsen, The solovay-kitaev algorithm, *Quantum Info. Comput.* **6**, 81 (2006).
- [27] D. P. DiVincenzo, Two-bit gates are universal for quantum computation, *Phys. Rev. A* **51**, 1015 (1995).
- [28] S. Lloyd, Almost any quantum logic gate is universal, *Phys. Rev. Lett.* **75**, 346 (1995).
- [29] I. Marvian, Restrictions on realizable unitary operations imposed by symmetry and locality, *Nature Phys.* **18**, 283 (2022).
- [30] I. Marvian, Theory of quantum circuits with abelian symmetries, *Phys. Rev. Res.* **6**, 043292 (2024).
- [31] I. Marvian, H. Liu, and A. Hulse, Rotationally invariant circuits: Universality with the exchange interaction and two ancilla qubits, *Phys. Rev. Lett.* **132**, 130201 (2024).
- [32] A. Hulse, H. Liu, and I. Marvian, A framework for semi-universality: Semi-universality of 3-qudit $su(d)$ -invariant gates, *arXiv preprint arXiv:2407.21249* (2024).
- [33] J. Kempe, D. Bacon, D. P. DiVincenzo, and K. B. Whaley, Encoded universality from a single physical interaction, *Quantum Info. Comput.* **1**, 33 (2001).
- [34] 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).
- [35] S. Boixo, S. V. Isakov, V. N. Smelyanskiy, R. Babbush, N. Ding, Z. Jiang, M. J. Bremner, J. M. Martinis, and H. Neven, Characterizing quantum supremacy in near-term devices, *Nature Phys.* **14**, 595 (2018).
- [36] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. S. L. Brandao, D. A. Buell, B. Burkett, Y. Chen, Z. Chen, B. Chiaro, R. Collins, W. Courtney, A. Dunsworth, E. Farhi, B. Foxen, A. Fowler, C. Gidney, M. Giustina, R. Graff, K. Guerin, S. Habegger, M. P. Harrigan, M. J. Hartmann, A. Ho, M. Hoffmann, T. Huang, T. S. Humble, S. V. Isakov, E. Jeffrey, Z. Jiang, D. Kafri, K. Kechedzhi, J. Kelly, P. V. Klimov, S. Knysh, A. Korotkov, F. Kostritsa, D. Landhuis, M. Lindmark, E. Lucero, D. Lyakh, S. Mandrà, J. R. McClean, M. McEwen, A. Megrant, X. Mi, K. Michielsen, M. Mohseni, J. Mutus, O. Naaman, M. Neeley, C. Neill, M. Y. Niu, E. Ostby, A. Petukhov, J. C. Platt, C. Quintana, E. G. Rieffel, P. Roushan, N. C. Rubin, D. Sank, K. J. Satzinger, V. Smelyanskiy, K. J. Sung, M. D. Trevithick, A. Vainsencher, B. Villalonga, T. White, Z. J. Yao, P. Yeh, A. Zalcman, H. Neven, and J. M. Martinis, Quantum supremacy using a programmable superconducting processor, *Nature* **574**, 505 (2019).
- [37] H.-Y. Huang, R. Kueng, and J. Preskill, Predicting many properties of a quantum system from very few measurements, *Nature Phys.* **16**, 1050 (2020).
- [38] J. Emerson, R. Alicki, and K. Życzkowski, Scalable noise estimation with random unitary operators, *J. Opt. B: Quantum Semiclass. Opt.* **7**, S347 (2005).
- [39] F. Dupuis, M. Berta, J. Wullschleger, and R. Renner, One-shot decoupling, *Commun. Math. Phys.* **328**, 251 (2014).
- [40] D. A. Roberts and B. Yoshida, Chaos and complexity by design, *J. High Energy Phys.* **2017**, 121.
- [41] F. G. S. L. Brandão, A. W. Harrow, and M. Horodecki, Local random quantum circuits are approximate polynomial-designs, *Commun. Math. Phys.* **346**, 397 (2016).
- [42] J. Haferkamp, Random quantum circuits are approximate unitary t -designs in depth $O\left(nt^{5+o(1)}\right)$, *Quantum* **6**, 795 (2022).
- [43] S. Mittal and N. Hunter-Jones, Local random quantum circuits form approximate designs on arbitrary architectures, *arXiv preprint arXiv:2310.19355* (2023).
- [44] D. Belkin, J. Allen, S. Ghosh, C. Kang, S. Lin, J. Sud, F. Chong, B. Fefferman, and B. K. Clark, Approximate t -designs in generic circuit architectures, *arXiv preprint arXiv:2310.19783* (2024).
- [45] T. Schuster, J. Haferkamp, and H.-Y. Huang, Random unitaries in extremely low depth, *arXiv preprint arXiv:2407.07754* (2024).

- [46] N. LaRacunte and F. Leditzky, Approximate t -designs in generic circuit architectures, [arXiv preprint arXiv:2407.07876 \(2024\)](#).
- [47] Z. Li, H. Zheng, J. Liu, L. Jiang, and Z.-W. Liu, Designs from local random quantum circuits with $SU(d)$ symmetry, [PRX Quantum 5, 040349 \(2024\)](#).
- [48] S. N. Hearth, M. O. Flynn, A. Chandran, and C. R. Laumann, Unitary k -designs from random number-conserving quantum circuits, [arXiv preprint arXiv:2306.01035 \(2023\)](#).
- [49] Y. Mitsuhashi, R. Suzuki, T. Soejima, and N. Yoshioka, Unitary designs of symmetric local random circuits, [arXiv preprint arXiv:2408.13472 \(2024\)](#).
- [50] R. Zeier and Z. Zimborás, On squares of representations of compact lie algebras, [J. Math. Phys. 56, 081702 \(2015\)](#).
- [51] C.-F. Chen, J. Haah, J. Haferkamp, Y. Liu, T. Metger, and X. Tan, Incompressibility and spectral gaps of random circuits, [arXiv preprint arXiv:2406.07478 \(2024\)](#).
- [52] A. Hulse, H. Liu, and I. Marvian, Unitary designs from random symmetric quantum circuits, [arXiv preprint arXiv:2408.14463 \(2024\)](#).
- [53] A. W. Knap, *Lie Groups Beyond an Introduction*. 2nd ed. (Birkhäuser, Boston, 2002).

Appendix A: Proofs of the theorems for the concrete symmetries (Theorems 2, 3, 4, 5, and 6)

Before going into the concrete cases of symmetries, we prepare a simple useful lemma for general symmetries, which we use many times.

Lemma 4. *Let $n, t \in \mathbb{N}$, R be a unitary representation of a group G , Λ be the set of labels of irreducible representations appearing in the decomposition of R , $(x_\lambda)_{\lambda \in \Lambda}$ satisfy Eqs. (19) and (20), and Λ' be an arbitrary subset of Λ . Then, $|\sum_{\lambda \in \Lambda'} m_\lambda x_\lambda| \leq t$.*

Proof. By the triangle inequality, we have

$$\sum_{\lambda \in \Lambda} m_\lambda |x_\lambda| = \sum_{\lambda \in \Lambda'} m_\lambda |x_\lambda| + \sum_{\lambda \in \Lambda \setminus \Lambda'} m_\lambda |x_\lambda| \geq \left| \sum_{\lambda \in \Lambda'} m_\lambda x_\lambda \right| + \left| \sum_{\lambda \in \Lambda \setminus \Lambda'} m_\lambda x_\lambda \right|. \quad (\text{A1})$$

By Eq. (20), we have

$$\sum_{\lambda \in \Lambda \setminus \Lambda'} m_\lambda x_\lambda = - \sum_{\lambda \in \Lambda'} m_\lambda x_\lambda. \quad (\text{A2})$$

By plugging Eq. (A2) into Eq. (A1), we get

$$\sum_{\lambda \in \Lambda} m_\lambda |x_\lambda| \geq 2 \left| \sum_{\lambda \in \Lambda'} m_\lambda x_\lambda \right|. \quad (\text{A3})$$

By Eqs. (19) and (A3), we get $|\sum_{\lambda \in \Lambda'} m_\lambda x_\lambda| \leq t$. □

1. $\mathbb{Z}_2$ symmetry

In this section, we consider the representation R of $\mathbb{Z}_2$ defined by Eq. (3). Since $\bigcup_{\gamma \in \Gamma} \mathcal{U}_{n,G,R}^\gamma$ is semi-universal for $\mathcal{U}_{n,G,R}$ [30], we can use Theorem 1. We note that the representation R can be decomposed into two inequivalent irreducible representations $R_\lambda(g) := (-1)^{\lambda g}$ with $\lambda \in \Lambda := \{0, 1\}$ with multiplicity $m_\lambda = 2^{n-1}$, which corresponds to the spectral decomposition of $Z^{\otimes n}$. By using these results, we can easily derive the maximal order of asymptotic unitary designs under the $\mathbb{Z}_2$ symmetry presented as Theorem 2.

Proof of Theorem 2. Since R can be written as $T^{\otimes n}$ with a single-qubit representation T , by using Theorem 1, we consider the condition on t such that Eqs. (19) and (23) do not have a nontrivial integer solution. Since m_λ is given by 2^{n-1} , Eq. (19) is equivalent to

$$2^{n-1}(|x_0| + |x_1|) \leq 2t. \quad (\text{A4})$$

Since every $A' \in \mathfrak{u}_{n,G,R}^\gamma$ can be decomposed into the direct sum $A_0 \oplus A_1$ with A_λ acting on the eigenspace of $Z^{\otimes k}$ with eigenvalue $(-1)^\lambda$, we have $f_\lambda(A) = 2^{n-k}(\text{tr}(A_0) + \text{tr}(A_1))$, which does not depend in λ . Thus Eq. (23) is equivalent to

$$x_0 + x_1 = 0. \quad (\text{A5})$$

By plugging Eq. (A5) into Eq. (A4), we get $2^n|x_0| \leq 2t$, which yields $2^{n-1}|x_0| \leq t$, which implies that Eqs. (19) and (23) have no nontrivial integer solution if and only if $t < 2^{n-1}$. $\square$

2. U(1) symmetry

In this section, we consider the representation R of $U(1)$ defined by Eq. (4). Similarly to the Z_2 symmetry, $\bigcup_{\gamma \in \Gamma} \mathcal{U}_{n,G,R}^\gamma$ is semi-universal for $\mathcal{U}_{n,G,R}$ [30], and thus we can use Theorem 1.

First, we explicitly present the conditions of Eqs. (19) and (23) in Theorem 1.

Lemma 5. *Let $n, k, t \in \mathbb{N}$, $2 \leq k \leq n-1$, and R be a unitary representation of $G = U(1)$ defined by Eq. (4). Then, the distribution of the (G, R) -symmetric k -local random circuit is an asymptotic (G, R) -symmetric unitary t -design if and only if there exists no nontrivial integer solution $\mathbf{x} = (x_\lambda)_{\lambda=0,\dots,n} \in \mathbb{Z}^{n+1}$ satisfying*

$$\sum_{\lambda=0}^n \binom{n}{\lambda} |x_\lambda| \leq 2t, \quad (\text{A6})$$

$$\sum_{\lambda=j}^{n-k+j} \binom{n-k}{\lambda-j} x_\lambda = 0 \quad \forall j \in \{0, 1, \dots, k\}. \quad (\text{A7})$$

Proof. Since the representation R defined by Eq. (4) is the tensor product of representation of a single-qudit representation, Theorem 1 implies that the condition for the distribution of (G, R) -symmetric k -local random circuits forming an asymptotic unitary t -design if and only if Eqs. (19) and (23) have no nontrivial integer solution. In the following, it is sufficient to show that Eqs. (19) and (23) are equivalent to Eqs. (A6) and (A7), respectively. The representation R can be decomposed into $n+1$ inequivalent irreducible representations, which are given by $R_\lambda(e^{i\theta}) = e^{i(n-2\lambda)\theta}$ for $\lambda \in \Lambda = \{0, 1, \dots, n\}$. Since each of the representations R_λ corresponds to the eigenvalue of $\sum_{j=1}^n \mathbf{I}^{\otimes j-1} \otimes Z \otimes \mathbf{I}^{\otimes n-j}$, we find that the multiplicity m_λ of R_λ is given by $\binom{n}{\lambda}$. Thus Eq. (19) is rewritten as Eq. (A6). We fix $\gamma \in \Gamma$ and consider (G, R) -symmetric k -local operators that act nontrivially on some fixed k qubits. We note that such operators can be written as a linear combination of operators in the form of $A_j \otimes \mathbf{I}^{\otimes n-k}$ with A_j acting only on the eigenspaces of the sum of the Pauli-Z operators on k qubits with eigenvalues $k-2j$ for $j = 0, 1, \dots, k$ and I acting on the rest $n-k$ qubits. Then, we have

$$f_\lambda(A_j \otimes \mathbf{I}^{\otimes n-k}) = \binom{n-k}{\lambda-j} \text{tr}(A_j), \quad (\text{A8})$$

and Eq. (23) is rewritten as Eq. (A7). $\square$

In the following, we present the explicit condition on t such that Eqs. (A6) and (A7) in Lemma 5 have no nontrivial integer solution. First, we give a sufficient condition in the following lemma.

Lemma 6. *Let $n, k \in \mathbb{N}$, $2 \leq k \leq n-1$, and R be a unitary representation of $G = U(1)$ defined by Eq. (4). Then, Eqs. (A6) and (A7) have a nontrivial integer solution $\mathbf{x} = (x_\lambda)_{\lambda=0,\dots,n} \in \mathbb{Z}^{n+1}$ if*

$$t \geq \frac{2^{\lfloor k/2 \rfloor}}{\left\lceil \frac{k}{2} \right\rceil!} \prod_{\alpha=1}^{\lceil k/2 \rceil} (n-k+2\alpha-1). \quad (\text{A9})$$

Proof. We define a vector $\mathbf{y}_{n,k} = (y_{n,k,\lambda})_{\lambda \in \Lambda} \in \mathbb{Z}^\Lambda$ by

$$y_{n,k,\lambda} := \frac{(-1)^\lambda}{(n-k-1)!} \prod_{\alpha=1}^{n-k-1} \left(\lambda - \left\lceil \frac{k}{2} \right\rceil - \alpha \right), \quad (\text{A10})$$

and we show that $\mathbf{y}_{n,k}$ is a nontrivial integer solution of Eqs. (A6) and (A7). By the definition of $\mathbf{y}_{n,k}$, we have

$$\begin{aligned} \sum_{\lambda=0}^n \binom{n-k}{\lambda-j} y_{n,k,\lambda} &= \sum_{\lambda=0}^n \binom{n-k}{\lambda-j} \frac{(-1)^\lambda}{(n-k-1)!} \prod_{\alpha=1}^{n-k-1} \left(\lambda - \left\lceil \frac{k}{2} \right\rceil - \alpha \right) \\ &= \sum_{\lambda=0}^n \binom{n-k}{\lambda-j} \frac{(-1)^\lambda}{(n-k-1)!} \left(\frac{d}{dz} \right)^{n-k-1} z^{\lambda - \lceil k/2 \rceil - 1} \Big|_{z=1} \end{aligned}$$

$$\begin{aligned}
&= \frac{(-1)^j}{(n-k-1)!} \left(\frac{d}{dz} \right)^{n-k-1} z^{j-\lceil k/2 \rceil - 1} \sum_{\lambda=0}^n \binom{n-k}{\lambda-j} (-z)^{\lambda-j} \Big|_{z=1} \\
&= \frac{(-1)^j}{(n-k-1)!} \left(\frac{d}{dz} \right)^{n-k-1} z^{j-\lceil k/2 \rceil - 1} (1-z)^{n-k} \Big|_{z=1} \\
&= 0,
\end{aligned} \tag{A11}$$

which implies that $\mathbf{y}_{n,k}$ is a nontrivial integer solution of Eq. (A7). The definition of $\mathbf{y}_{n,k}$ also implies that

$$\begin{aligned}
&\sum_{\lambda=0}^n \binom{n}{\lambda} |y_{n,k,\lambda}| \\
&= \sum_{\lambda=0}^n \binom{n}{\lambda} \frac{1}{(n-k-1)!} \prod_{\alpha=1}^{n-k-1} \left| \lambda - \left\lceil \frac{k}{2} \right\rceil - \alpha \right| \\
&= \sum_{\lambda=0}^{\lceil k/2 \rceil} \binom{n}{\lambda} \frac{1}{(n-k-1)!} \prod_{\alpha=1}^{n-k-1} \left(\alpha + \left\lceil \frac{k}{2} \right\rceil - \lambda \right) + \sum_{\lambda=n-k+\lceil k/2 \rceil}^n \binom{n}{\lambda} \frac{1}{(n-k-1)!} \prod_{\alpha=1}^{n-k-1} \left(\lambda - \left\lceil \frac{k}{2} \right\rceil - \alpha \right) \\
&= \sum_{\lambda=0}^{\lceil k/2 \rceil} \binom{n}{\lambda} \binom{n-k-1+\lceil k/2 \rceil - \lambda}{n-k-1} + \sum_{\lambda=n-k+\lceil k/2 \rceil}^n \binom{n}{\lambda} \binom{\lambda - \lceil k/2 \rceil - 1}{n-k-1}.
\end{aligned} \tag{A12}$$

We note that

$$\sum_{\lambda=n-k+\lceil k/2 \rceil}^n \binom{n}{\lambda} \binom{\lambda - \lceil k/2 \rceil - 1}{n-k-1} = \sum_{\lambda=n-\lfloor k/2 \rfloor}^n \binom{n}{\lambda} \binom{\lambda - k + \lfloor \frac{k}{2} \rfloor - 1}{n-k-1} = \sum_{\lambda=0}^{\lfloor k/2 \rfloor} \binom{n}{\lambda} \binom{n-k-1+\lfloor \frac{k}{2} \rfloor - \lambda}{n-k-1}. \tag{A13}$$

By plugging Eq. (A13) into Eq. (A12), we get

$$\sum_{\lambda=0}^n \binom{n}{\lambda} |y_{n,k,\lambda}| = \sum_{\lambda=0}^{\lceil k/2 \rceil} \binom{n}{\lambda} \binom{n-k-1+\lceil \frac{k}{2} \rceil - \lambda}{n-k-1} + \sum_{\lambda=0}^{\lfloor k/2 \rfloor} \binom{n}{\lambda} \binom{n-k-1+\lfloor \frac{k}{2} \rfloor - \lambda}{n-k-1}. \tag{A14}$$

We note that for any $j \geq 0$,

$$\sum_{\lambda=0}^j \binom{n}{\lambda} \binom{n-k-1+j-\lambda}{n-k-1} = \sum_{\lambda=0}^j \binom{n}{\lambda} \binom{n-k-1+j-\lambda}{j-\lambda} = a_{n,k,j}, \tag{A15}$$

where we define

$$a_{n,k,j} := \sum_{\lambda=0}^j \binom{n}{j-\lambda} \binom{n-k+\lambda-1}{\lambda} \tag{A16}$$

for $n, k, j \in \mathbb{Z}$ satisfying $0 \leq k \leq n-1$ and $j \geq 0$. By applying Eq. (A15) to Eq. (A14), we get

$$\sum_{\lambda=0}^n \binom{n}{\lambda} |y_{n,k,\lambda}| = a_{n,k,\lceil k/2 \rceil} + a_{n,k,\lfloor k/2 \rfloor} = 2 \cdot \frac{2^{\lfloor k/2 \rfloor}}{\lfloor \frac{k}{2} \rfloor!} \prod_{\alpha=1}^{\lfloor k/2 \rfloor} (n-k+2\alpha-1), \tag{A17}$$

where we used Lemma 25. Thus $\mathbf{y}_{n,k}$ is a nontrivial integer solution of Eqs. (A6) and (A7) when t satisfies Eq. (A9). $\square$

Next, we show that for sufficiently large n , the condition on t in Lemma 6 is a necessary condition for the equations in Lemma 5 having no nontrivial integer solution.

Lemma 7. *Let $n, k, t \in \mathbb{N}$, $2 \leq k \leq n-1$, R be a unitary representation of $G = \mathrm{U}(1)$ defined by Eq. (4), and $b_{n,j}$ defined for $j \in \mathbb{N}$ by*

$$b_{n,j} := \frac{2^{\lfloor j/2 \rfloor}}{\lfloor \frac{j}{2} \rfloor!} \prod_{\alpha=1}^{\lfloor j/2 \rfloor} (n-j+2\alpha-1) \tag{A18}$$

satisfy $b_{n,k} \leq \binom{n}{j}$ for all $j \in \{\lceil k/2 \rceil + 1, \lceil k/2 \rceil + 2, \dots, n - \lceil k/2 \rceil - 1\}$, and when k is odd, $b_{n,j}$ also satisfy $b_{n,k} \leq b_{n,k+1}$. Then, Eqs. (A6) and (A7) have no nontrivial integer solution $\mathbf{x} = (x_\lambda)_{\lambda=0,\dots,n} \in \mathbb{Z}^{n+1}$ if and only if $t < b_{n,k}$.

We note that the assumptions are satisfied when $n \geq 2^k$, as we show in Lemma 21.

Proof. We take arbitrary integer solution $\mathbf{x}$ of Eqs. (A6) and (A7), and show that $\mathbf{x} = \mathbf{0}$. When $t < b_{n,k}$, Eq. (A7) implies that

$$\sum_{\lambda=0}^n \binom{n}{\lambda} |x_\lambda| < 2b_{n,k}. \quad (\text{A19})$$

Before going into the detailed proof process, we note that the assumption of $b_{n,k} \leq b_{n,k+1}$ for odd k implies that $n \geq k+2$, because when k is odd and $n = k+1$, we have

$$b_{n,k} = \frac{2^{(k-1)/2}}{\left(\frac{k+1}{2}\right)!} \prod_{\alpha=1}^{(k+1)/2} 2\alpha = \frac{1}{2} \cdot \frac{2^{(k+1)/2}}{\left(\frac{k+1}{2}\right)!} \left(\prod_{\alpha=2}^{(k+1)/2} 2\alpha \right) \cdot 2 > \frac{2^{(k+1)/2}}{\left(\frac{k+1}{2}\right)!} \left(\prod_{\alpha=2}^{(k+1)/2} (2\alpha - 1) \right) = b_{n,k+1}, \quad (\text{A20})$$

which contradicts with $b_{n,k} \leq b_{n,k+1}$. By using Lemma 4 with $\Lambda' = \{\lambda\}$ for $\lambda \in \{\lceil k/2 \rceil + 1, \lceil k/2 \rceil + 2, \dots, n - \lceil k/2 \rceil - 1\}$, and the assumption of $b_{n,k} \leq \binom{n}{\lceil k/2 \rceil + 1}$, we have

$$x_\lambda = 0 \quad \forall \lambda \in \{\lceil k/2 \rceil + 1, \lceil k/2 \rceil + 2, \dots, n - \lceil k/2 \rceil - 1\}, \quad (\text{A21})$$

which means that $\mathbf{x}$ is in the space orthogonal to the space spanned by $\{\mathbf{w}_j\}_{j=0}^k$ and $\{\mathbf{v}_j\}_{j=\lceil k/2 \rceil + 1}^{n - \lceil k/2 \rceil - 1}$, where $\mathbf{w}_j := ((\binom{n-k}{\lambda-j}))_{\lambda \in \Lambda}$ for $j \in \{0, 1, \dots, k\}$ and $\mathbf{v}_j := (\delta_{\lambda,j})_{\lambda \in \Lambda}$ for $j \in \{\lceil k/2 \rceil + 1, \lceil k/2 \rceil + 2, \dots, n - \lceil k/2 \rceil - 1\}$. We note that these vectors are linearly independent, because we can show that $\sum_{j=0}^k p_j \mathbf{w}_j + \sum_{j=\lceil k/2 \rceil + 1}^{n - \lceil k/2 \rceil - 1} q_j \mathbf{v}_j = \mathbf{0}$ implies that $p_j = 0$ and $q_j = 0$ for all j by looking at the elements for $\lambda = 0, 1, \dots, \lceil k/2 \rceil, n, n-1, \dots, n - \lceil k/2 \rceil + 1, \lceil k/2 \rceil + 1, \lceil k/2 \rceil + 2, \dots, n - \lceil k/2 \rceil - 1$ in order. Since $n \geq k+1$ when k is even and from $n \geq k+2$ when k is odd, we have $\lceil k/2 \rceil \leq n - \lceil k/2 \rceil - 1$, which implies that the size of the set $\{\lceil k/2 \rceil + 1, \lceil k/2 \rceil + 2, \dots, n - \lceil k/2 \rceil - 1\}$ is given by $(n - \lceil k/2 \rceil - 1) - \lceil k/2 \rceil = n - 2\lceil k/2 \rceil - 1$. Thus the dimension of the linear space of $\mathbf{x}$ satisfying Eqs. (A6) and (A21) is given by $(n+1) - [(k+1) + (n - 2\lceil k/2 \rceil - 1)] = 2\lceil k/2 \rceil - k + 1$, which is 1 when k is even and 2 when k is odd.

When k is even, by noting that $\mathbf{y}_{n,k}$ satisfies Eqs. (A6) and (A21), $\mathbf{x}$ can be written as $\mathbf{x} = r\mathbf{y}_{n,k}$ with some $r \in \mathbb{R}$. Since $\mathbf{x}$ is an integer vector and $y_{n,k,\lceil k/2 \rceil} = (-1)^{n-k+\lceil k/2 \rceil-1}$, we have $r = x_{\lceil k/2 \rceil} / y_{n,k,\lceil k/2 \rceil} \in \mathbb{Z}$. By Eq. (A17), we have

$$\sum_{\lambda=0}^n \binom{n}{\lambda} |x_\lambda| = \sum_{\lambda=0}^n \binom{n}{\lambda} |ry_{n,k,\lambda}| = 2|r|b_{n,k}. \quad (\text{A22})$$

By plugging this into Eq. (A19), we get $|r| < 1$, which implies that $r = 0$. Thus Eqs. (A6) and (A7) have no nontrivial integer solution.

When k is odd, to prepare a basis of the linear space of $\mathbf{x}$ satisfying Eqs. (A6) and (A21), we define $\mathbf{y}'_{n,k} = (y'_{n,k,\lambda})_{\lambda \in \Lambda}$ by $y'_{n,k,\lambda} := y_{n,k,n-\lambda}$. We can see that $\mathbf{y}'_{n,k}$ is also a nontrivial integer solution of Eq. (A7) by considering the transformation of $\lambda \mapsto n-\lambda$ in Eq. (A11). We note that $\mathbf{y}_{n,k}$ and $\mathbf{y}'_{n,k}$ are linearly independent, which can be confirmed by $y_{n,k,\lceil k/2 \rceil} = (-1)^{\lceil k/2 \rceil + n - k - 1}$, $y_{n,k,\lceil k/2 \rceil + n - k - 1} = 0$, $y'_{n,k,\lceil k/2 \rceil} = 0$, and $y'_{n,k,\lceil k/2 \rceil + n - k - 1} = (-1)^{\lceil k/2 \rceil}$. Thus, $\mathbf{x}$ can be written as $\mathbf{x} = r\mathbf{y}_{n,k} + r'\mathbf{y}'_{n,k}$ with some $r, r' \in \mathbb{R}$. Since $\mathbf{x}$ is an integer vector, we have $r = x_{\lceil k/2 \rceil} / y_{n,k,\lceil k/2 \rceil} \in \mathbb{Z}$ and $r' = x_{\lceil k/2 \rceil + n - k - 1} / y_{n,k,\lceil k/2 \rceil + n - k - 1} \in \mathbb{Z}$. By Eq. (A21), we have

$$\sum_{\lambda=0}^n \binom{n}{\lambda} |x_\lambda| = \sum_{\lambda=0}^{\lceil k/2 \rceil} \binom{n}{\lambda} (|x_\lambda| + |x_{n-\lambda}|) = \sum_{\lambda=0}^{\lceil k/2 \rceil} \binom{n}{\lambda} (|ry_{n,k,\lambda} + r'y'_{n,k,\lambda}| + |ry'_{n,k,\lambda} + r'y_{n,k,\lambda}|), \quad (\text{A23})$$

where we used $x_{n-\lambda} = ry_{n,k,n-\lambda} + r'y'_{n,k,n-\lambda} = ry'_{n,k,\lambda} + r'y_{n,k,\lambda}$. By the triangle inequality, we have

$$\begin{aligned} \sum_{\lambda=0}^n \binom{n}{\lambda} |x_\lambda| &\geq \sum_{\lambda=0}^{\lceil k/2 \rceil} \binom{n}{\lambda} [(|r||y_{n,k,\lambda}| - |r'||y'_{n,k,\lambda}|) + (|r'||y_{n,k,\lambda}| - |r||y'_{n,k,\lambda}|)] \\ &= (|r| + |r'|) \sum_{\lambda=0}^{\lceil k/2 \rceil} \binom{n}{\lambda} (|y_{n,k,\lambda}| - |y'_{n,k,\lambda}|). \end{aligned} \quad (\text{A24})$$

For $\lambda \in \{0, 1, \dots, \lceil k/2 \rceil\}$, we have

$$\begin{aligned} |y_{n,k,\lambda}| &= \frac{1}{(n-k-1)!} \prod_{\alpha=1}^{n-k-1} \left(\alpha + \left\lceil \frac{k}{2} \right\rceil - \lambda \right), \\ |y'_{n,k,\lambda}| &= \frac{1}{(n-k-1)!} \prod_{\alpha=1}^{n-k-1} \left(\alpha - 1 + \left\lceil \frac{k}{2} \right\rceil - \lambda \right) = \frac{1}{(n-k-1)!} \prod_{\alpha=0}^{n-k-2} \left(\alpha + \left\lceil \frac{k}{2} \right\rceil - \lambda \right), \end{aligned} \quad (\text{A25})$$

which imply that

$$\begin{aligned} |y_{n,k,\lambda}| - |y'_{n,k,\lambda}| &= \frac{1}{(n-k-2)!} \prod_{\alpha=1}^{n-k-2} \left(\alpha + \left\lceil \frac{k}{2} \right\rceil - \lambda \right) \\ &= \frac{1}{[n-(k+1)-1]!} \prod_{\alpha=1}^{n-(k+1)-1} \left(\alpha + \left\lceil \frac{k+1}{2} \right\rceil - \lambda \right) \\ &= |y_{n,k+1,\lambda}|. \end{aligned} \quad (\text{A26})$$

By plugging Eq. (A26) into Eq. (A24), we get

$$\sum_{\lambda=0}^n \binom{n}{\lambda} |x_\lambda| \geq (|r| + |r'|) \sum_{\lambda=0}^{\lceil k/2 \rceil} \binom{n}{\lambda} |y_{n,k+1,\lambda}| = (|r| + |r'|) \cdot \frac{1}{2} \sum_{\lambda=0}^n \binom{n}{\lambda} |y_{n,k+1,\lambda}|, \quad (\text{A27})$$

where we used $y_{n,k+1,\lambda} = 0$ for all $\lambda \in \{\lceil k/2 \rceil + 1, \lceil k/2 \rceil + 2, \dots, n - \lceil k/2 \rceil - 1\}$ and $|y_{n,k+1,\lambda}| = |y_{n,k+1,n-\lambda}|$ for all $\lambda \in \{0, 1, \dots, \lceil k/2 \rceil\}$ in the equality. By plugging Eq. (A17) into Eq. (A27)

$$\sum_{\lambda=0}^n \binom{n}{\lambda} |x_\lambda| = (|r| + |r'|) b_{n,k+1} \geq (|r| + |r'|) b_{n,k}, \quad (\text{A28})$$

where we used the assumption of $b_{n,k} \leq b_{n,k+1}$ in the second inequality. By Eqs. (A19) and (A28), we have $|r| + |r'| < 2$, which means $r = 0$ or $r' = 0$. In both cases, we have

$$\sum_{\lambda=0}^n \binom{n}{\lambda} |x_\lambda| = \sum_{\lambda=0}^n \binom{n}{\lambda} |r y_{n,k,\lambda} + r' y_{n,k,n-\lambda}| = \sum_{\lambda=0}^n \binom{n}{\lambda} (|r| |y_{n,k,\lambda}| + |r'| |y_{n,k,n-\lambda}|) = (|r| + |r'|) \cdot 2b_{n,k}, \quad (\text{A29})$$

where we used Eq. (A17) in the last equality. By Eqs. (A19) and (A29), we get $|r| + |r'| < 1$, which implies that $r = r' = 0$. We can therefore conclude that Eqs. (A6) and (A7) have no nontrivial integer solution when $t < b_{n,k}$. $\square$

By using the lemmas above, we can prove Theorem 3 as follows:

Proof of Theorem 3. In Lemma 5, we have explicitly rewritten the equations in Theorem 1 in the U(1) case. When t does not satisfy Eq. (30), by Lemma 6, there exists a nontrivial integer solution for all $n \geq k + 1$. When t satisfies Eq. (30), by Lemma 7, there exists no nontrivial integer solution under a certain assumption about n and k , which are guaranteed when $n \geq 2^k$ by Lemma 21. $\square$

By directly considering the condition on t such that Eqs. (A6) and (A7) in Lemma 5 have no nontrivial integer solution for the region of n that does not satisfy the assumption in Lemma 7, we can prove Theorem 4.

Proof of Theorem 4. By Lemma 5, the distribution of the (G, R) -symmetric k -local random circuit forming an asymptotic unitary t -design if and only if Eqs. (A6) and (A7) have no nontrivial integer solution. We note that $b_{n,k}$ defined by Eq. (A18) satisfies $b_{n,2} = 2(n-1)$, $b_{n,3} = n(n-2)$, and $b_{n,4} = 2(n-1)(n-3)$. Since we have proven the existence of a nontrivial integer solution when t satisfies Eq. (31) by Lemma 6, it is sufficient to show the nonexistence of a nontrivial integer solution of Eqs. (A6) and (A7) when t does not satisfy Eq. (31).

First, we consider the case when $k = 2$. We can confirm that the assumption in Lemma 7 holds for all $n \geq 3$. When $n \geq 4$, for any $j \in \{2, 3, \dots, n-2\}$, we have

$$\binom{n}{j} \geq \binom{n}{2} = \frac{n}{4} b_{n,2} \geq b_{n,2}, \quad (\text{A30})$$

and this trivially holds when $n = 3$, because the set $\{2, 3, \dots, n-2\}$ is empty. By Lemma 7, Eqs. (A6) and (A7) have no nontrivial integer solution for all $n \geq 3$.

Next, we consider the case when $k = 3$. We can confirm that the assumptions in Lemma 7 hold for $n = 5$ and $n \geq 7$. As for the first assumption, when $n \geq 7$, we have for any $j \in \{3, 4, \dots, n-3\}$,

$$\binom{n}{j} \geq \binom{n}{3} = \frac{n-1}{6} b_{n,3} \geq b_{n,3}, \quad (\text{A31})$$

and this trivially holds when $n = 5$, because the set $\{3, 4, \dots, n-3\}$ is empty. As for the second assumption, we have

$$b_{n,4} = b_{n,3} + (n-1)(n-5) + 1 \geq b_{n,3}. \quad (\text{A32})$$

By Lemma 7, Eqs. (A6) and (A7) have no nontrivial integer solution when $n = 5$ or $n \geq 7$. Thus, we have only to check the cases of $n = 4$ and 6 in the following.

- When $n = 4$, Eqs. (A6) and (A7) are explicitly written as

$$|x_0| + 4|x_1| + 6|x_2| + 4|x_3| + |x_4| \leq 2t, \quad (\text{A33})$$

$$x_j + x_{j+1} = 0 \quad \forall j \in \{0, 1, 2, 3\}. \quad (\text{A34})$$

We show that these equations have no nontrivial integer solution for $t < 8$. We take an arbitrary integer solution $\mathbf{x}$. Eq. (A7) implies $x_j = (-1)^j x_0$ for all $j \in \{1, 2, 3, 4\}$. By plugging this into Eq. (A6), we get $16|x_0| \leq 2t < 16$, which implies $x_0 = 0$. We thus have $\mathbf{x} = \mathbf{0}$, which implies that Eqs. (A6) and (A7) have no nontrivial integer solution.

- When $n = 6$, Eqs. (A6) and (A7) are explicitly written as

$$|x_0| + 6|x_1| + 15|x_2| + 20|x_3| + 15|x_4| + 6|x_5| + |x_6| \leq 2t, \quad (\text{A35})$$

$$x_j + 3x_{j+1} + 3x_{j+2} + x_{j+3} = 0 \quad \forall j \in \{0, 1, 2, 3\}. \quad (\text{A36})$$

We show that these equations have no nontrivial integer solution for $t < 24$. We take an arbitrary integer solution $\mathbf{x}$. We define $y_j := x_j + x_{6-j}$ for $j = 0, 1$, and 2. By Eq. (A7), we have $y_0 = 9y_2 + 16x_3$ and $y_1 = -4y_2 - 6x_3$. By Lemma 4, we have $|y_2| \leq 1$ and $|x_3| \leq 1$. We thus have $(y_2, x_3) = \pm(1, 1), \pm(0, 1), \pm(-1, 1), \pm(1, 0)$, or $(0, 0)$, which implies $\sum_{j=0}^6 \binom{6}{j} |x_j| \geq |y_0| + 6|y_1| + 15|y_2| + 20|x_3| = 120, 72, 54, 48$, or 0, respectively, where we used the triangle inequality. By combining this with Eq. (A6), we get $\mathbf{x} = \mathbf{0}$. We can therefore conclude that Eqs. (A6) and (A7) have no nontrivial integer solution.

Finally, we consider the case when $k = 4$. We can confirm that the assumption in Lemma 7 holds for $n = 5$ and $n \geq 11$. When $n \geq 11$, for any $j \in \{3, 4, \dots, n-3\}$, we have

$$\binom{n}{j} \geq \binom{n}{3} = b_{n,3} + \frac{(n-1)[(n-3)(n-11)+3]}{6} \geq b_{n,3}, \quad (\text{A37})$$

and this trivially holds when $n = 5$, because the set $\{3, 4, \dots, n-3\}$ is empty. By Lemma 7, Eqs. (A6) and (A7) have no nontrivial integer solution when $n = 5$ or $n \geq 11$. Thus, we have only to check the cases of $n = 6, 7, 8, 9$, and 10 in the following.

- When $n = 6$, Eqs. (A6) and (A7) are explicitly written as

$$|x_0| + 6|x_1| + 15|x_2| + 20|x_3| + 15|x_4| + 6|x_5| + |x_6| \leq 2t, \quad (\text{A38})$$

$$x_j + 2x_{j+1} + x_{j+2} = 0 \quad \forall j \in \{0, 1, 2, 3, 4\}. \quad (\text{A39})$$

We show that these equations have no nontrivial integer solution for $t < 30$. We take an arbitrary integer solution $\mathbf{x}$. We define $y_j := x_j + x_{n-j}$ for $j = 0, 1$, and 2. By Eq. (A7), we have $y_0 = -2x_3$, $y_1 = 2x_3$, and $y_2 = -2x_3$, which imply that $64|x_3| = |y_0| + 6|y_1| + 15|y_2| + 20|x_3| \leq \sum_{j=0}^6 \binom{6}{j} |x_j| \leq 2t < 60$. We thus get $y_0 = y_1 = y_2 = x_3 = 0$. By Eq. (A7), we have $x_0 = -x_6 = 3x_2$ and $x_1 = -x_5 = -2x_2$. By noting that $60|x_2| = \sum_{j=0}^6 \binom{6}{j} |x_j| \leq 2t < 60$, we get $\mathbf{x} = \mathbf{0}$. We can therefore conclude that Eqs. (A6) and (A7) have no nontrivial integer solution.

- When $n = 7$, Eqs. (A6) and (A7) are explicitly written as

$$|x_0| + 7|x_1| + 21|x_2| + 35|x_3| + 35|x_4| + 21|x_5| + 7|x_6| + |x_7| \leq 2t, \quad (\text{A40})$$

$$x_{j+0} + 3x_{j+1} + 3x_{j+2} + x_{j+3} = 0 \quad \forall j \in \{0, 1, 2, 3, 4\}. \quad (\text{A41})$$

We show that these equations have no nontrivial integer solution for $t < 48$. We take an arbitrary integer solution $\mathbf{x}$. We define $y_j := x_j + x_{n-j}$ for $j = 0, 1, 2$, and 3 . By Eq. (A7), we have $y_0 = -7y_3$, $y_1 = 5y_3$, and $y_2 = -3y_3$, which imply that $140|y_3| = |y_0| + 7|y_1| + 21|y_2| + 35|y_3| \leq \sum_{j=0}^7 \binom{7}{j} |x_j| \leq 2t < 96$, where we used the triangle inequality. We thus get $y_0 = y_1 = y_2 = y_3 = 0$. By noting that $21|x_2| + 35|x_3| = (21|x_2| + 35|x_3| + 35|x_4| + 21|x_5|)/2 < 48$, we have $(x_2, x_3) = \pm(0, 1)$, $\pm(1, 0)$, $\pm(2, 0)$, or $(0, 0)$, which implies $\sum_{j=0}^7 \binom{7}{j} |x_j| = 108, 96, 192$, or 0 , respectively. By combining this with Eq. (A6), we get $\mathbf{x} = \mathbf{0}$. We can therefore conclude that Eqs. (A6) and (A7) have no nontrivial integer solution.

- When $n = 8$, Eqs. (A6) and (A7) are explicitly written as

$$|x_0| + 8|x_1| + 28|x_2| + 56|x_3| + 70|x_4| + 56|x_5| + 28|x_6| + 8|x_7| + |x_8| \leq 2t, \quad (\text{A42})$$

$$x_{j+0} + 4x_{j+1} + 6x_{j+2} + 4x_{j+3} + x_{j+4} = 0 \quad \forall j \in \{0, 1, 2, 3, 4\}. \quad (\text{A43})$$

We show that these equations have no nontrivial integer solution for $t < 70$. We take an arbitrary integer solution $\mathbf{x}$. By Lemma 4, we have $x_4 = 0$. We define $y_j := x_j + x_{n-j}$ for $j = 0, 1, 2$, and 3 . By Eq. (A7), we have $y_0 = -16y_3$, $y_1 = 9y_3$, and $y_2 = -4y_3$, which imply that $256|y_3| = \sum_{j=0}^3 \binom{8}{j} |y_j| = \sum_{j=0}^8 \binom{8}{j} |x_j| \leq 2t < 140$. We thus get $y_0 = y_1 = y_2 = y_3 = 0$. By noting that $28|x_2| + 56|x_3| = (28|x_2| + 56|x_3| + 56|x_5| + 28|x_6|)/2 \leq t < 70$, we have $(x_2, x_3) = \pm(0, 1)$, $\pm(1, 0)$, $\pm(2, 0)$, $(0, 0)$, which implies $\sum_{j=0}^8 \binom{8}{j} |x_j| = 224, 140, 280$, or 0 , respectively. By combining this with Eq. (A6), we get $\mathbf{x} = \mathbf{0}$. We can therefore conclude that Eqs. (A6) and (A7) have no nontrivial integer solution.

- When $n = 9$, Eqs. (A6) and (A7) are explicitly written as

$$|x_0| + 9|x_1| + 36|x_2| + 84|x_3| + 126|x_4| + 126|x_5| + 84|x_6| + 36|x_7| + 9|x_8| + |x_9| \leq 2t, \quad (\text{A44})$$

$$x_{j+0} + 5x_{j+1} + 10x_{j+2} + 10x_{j+3} + 5x_{j+4} + x_{j+5} = 0 \quad \forall j \in \{0, 1, 2, 3, 4\}. \quad (\text{A45})$$

We show that these equations have no nontrivial integer solution for $t < 96$. We take an arbitrary integer solution $\mathbf{x}$. By Lemma 4, we have $x_4 = x_5 = 0$. We define $y_j := x_j + x_{n-j}$ for $j = 0, 1, 2$, and 3 . By Eq. (A7), we have $y_0 = -30y_3$, $y_1 = 14y_3$, and $y_2 = -5y_3$, which imply $420|y_3| = \sum_{j=0}^3 \binom{9}{j} |y_j| \leq \sum_{j=0}^9 \binom{9}{j} |x_j| \leq 2t < 192$. We thus get $y_0 = y_1 = y_2 = y_3 = 0$. By noting that $36|x_2| + 84|x_3| = (36|x_2| + 84|x_3| + 84|x_6| + 36|x_7|)/2 \leq t$, we have $(x_2, x_3) = \pm(0, 1)$, $\pm(1, 0)$, $\pm(2, 0)$, or $(0, 0)$, which implies $\sum_{j=0}^9 \binom{9}{j} |x_j| = 400, 192, 384$, or 0 , respectively. By combining this with Eq. (A6), we get $\mathbf{x} = \mathbf{0}$. We can therefore conclude that Eqs. (A6) and (A7) have no nontrivial integer solution.

- When $n = 10$, Eqs. (A6) and (A7) are explicitly written as

$$|x_0| + 10|x_1| + 45|x_2| + 120|x_3| + 210|x_4| + 252|x_5| + 210|x_6| + 120|x_7| + 45|x_8| + 10|x_9| + |x_{10}| \leq 2t, \quad (\text{A46})$$

$$x_{j+0} + 6x_{j+1} + 15x_{j+2} + 20x_{j+3} + 15x_{j+4} + 6x_{j+5} + x_{j+6} = 0 \quad \forall j \in \{0, 1, 2, 3, 4\}. \quad (\text{A47})$$

We show that these equations have no nontrivial integer solution for $t < 126$. We take an arbitrary integer solution $\mathbf{x}$. By Lemma 4, we have $x_4 = x_5 = x_6 = 0$. We define $y_j := x_j + x_{n-j}$ for $j = 0, 1, 2$, and 3 . By Eq. (A7), we have $y_0 = -50y_3$, $y_1 = 20y_3$, and $y_2 = -6y_3$, which imply $640|y_3| = \sum_{j=0}^3 \binom{10}{j} |y_j| \leq \sum_{j=0}^{10} \binom{10}{j} |x_j| \leq 2t < 252$. We thus get $y_0 = y_1 = y_2 = y_3 = 0$. By noting that $45|x_2| + 120|x_3| = (45|x_2| + 120|x_3| + 120|x_7| + 45|x_8|)/2 \leq t$, we have $(x_2, x_3) = \pm(0, 1)$, $\pm(1, 0)$, $\pm(2, 0)$, $(0, 0)$, which implies $\sum_{j=0}^{10} \binom{10}{j} |x_j| = 648, 252, 504$, or 0 , respectively. By combining this with Eq. (A6), we get $\mathbf{x} = \mathbf{0}$. We can therefore conclude that Eqs. (A6) and (A7) have no nontrivial integer solution. $\square$

3. SU(2) symmetry

In this section, we consider the representation R of $\text{SU}(2)$ defined by Eq. (5). Since $\bigcup_{\gamma \in \Gamma} \mathcal{U}_{n,G,R}^\gamma$ is semi-universal for $\mathcal{U}_{n,G,R}$ [31], we can use the result of Theorem 1. By noting that R can be written as $T^{\otimes n}$ with a representation

T on a single qubit, we consider the condition for Eqs. (19) and (23) having no nontrivial integer solutions. Since R can be irreducibly decomposed into spin- λ representations with $\lambda \in \{n/2, n/2 - 1, \dots, n/2 - \lfloor n/2 \rfloor\}$, we use this λ as the index for the irreducible representation appearing in R , i.e., Λ in Theorem 1 is given by

$$\Lambda = \{n/2, n/2 - 1, \dots, n/2 - \lfloor n/2 \rfloor\}. \quad (\text{A48})$$

As a preparation, we derive a property about $f_\lambda(Q_\sigma)$, where Q_σ is the permutation operator that brings the j th qubit to the $\sigma(j)$ th qubit.

Lemma 8. *Let $n \in \mathbb{N}$, R be a unitary representation of $G = \text{SU}(2)$ on n qubits defined by Eq. (5), Λ be given by Eq. (A48), $\lambda \in \Lambda$, $\sigma \in \mathfrak{S}_n$ be decomposed as $\sigma = \sigma_1 \sigma_2 \cdots \sigma_L$ with p_l -cycles $\sigma_l \in \mathfrak{S}_n$ nontrivially acting on disjoint subsets of $\{1, 2, \dots, n\}$, and $\tilde{f}_\lambda$ be defined by*

$$\tilde{f}_\lambda(A) := \sum_{\kappa \in \Lambda, \kappa \geq \lambda} f_\kappa(A) \quad \forall A \in \mathcal{L}_{n,G,R}. \quad (\text{A49})$$

Then,

$$\tilde{f}_\lambda(I) = \binom{n}{\frac{n}{2} - \lambda}, \quad (\text{A50})$$

$$\tilde{f}_\lambda(Q_\sigma) = \sum_{q_1, q_2, \dots, q_L \in \{0,1\}} \binom{n - \sum_{l=1}^L p_l}{\frac{n}{2} - \lambda - \sum_{l=1}^L q_l p_l}. \quad (\text{A51})$$

We note that a p -cycle means a permutation σ that nontrivially acts only on p elements $j_1, j_2, \dots, j_p$ and satisfies $\sigma(j_1) = j_2, \sigma(j_2) = j_3, \dots, \sigma(j_p) = j_1$.

Proof. We take an orthonormal basis $\{|\lambda, \mu, \alpha\rangle\}_{\mu \in \{\lambda, \lambda-1, \dots, -\lambda\}, \alpha \in \{1, 2, \dots, m_\lambda\}}$ of the spin- λ representation space such that

$$[(X^{\text{tot}})^2 + (Y^{\text{tot}})^2 + (Z^{\text{tot}})^2] |\lambda, \mu, \alpha\rangle = 4\lambda(\lambda + 1) |\lambda, \mu, \alpha\rangle, \quad (\text{A52})$$

$$Z^{\text{tot}} |\lambda, \mu, \alpha\rangle = 2\mu |\lambda, \mu, \alpha\rangle, \quad (\text{A53})$$

where X^{tot} , Y^{tot} , and Z^{tot} are the sum of all the Pauli operators on the n qubits, and α is the index for degeneracy. We can take orthonormal bases $\{|\mu\rangle\}$ and $\{|\alpha\rangle\}$ of the representation space and the multiplicity space such that

$$F_\lambda(|\mu\rangle \otimes |\alpha\rangle) = |\lambda, \mu, \alpha\rangle. \quad (\text{A54})$$

Thus, for any $\lambda, \kappa \in \Lambda$ satisfying $\lambda \leq \kappa$, we have

$$\begin{aligned} \sum_{\alpha \in \{1, 2, \dots, m_\kappa\}} \langle \kappa, \lambda, \alpha | A | \kappa, \lambda, \alpha \rangle &= \sum_{\alpha \in \{1, 2, \dots, m_\kappa\}} \sum_{\kappa' \in \Lambda} (\langle \lambda | \otimes \langle \alpha |) F_\kappa^\dagger F_{\kappa'} (I \otimes A_{\kappa'}) F_{\kappa'}^\dagger F_\kappa (|\lambda\rangle \otimes |\alpha\rangle) \\ &= \sum_{\alpha \in \{1, 2, \dots, m_\kappa\}} (\langle \lambda | \otimes \langle \alpha |) (I \otimes A_\kappa) (|\lambda\rangle \otimes |\alpha\rangle) \\ &= \text{tr}(A_\kappa) \\ &= f_\kappa(A), \end{aligned} \quad (\text{A55})$$

where we used $F_\kappa^\dagger F_{\kappa'}$ is the identity when $\kappa = \kappa'$ and otherwise 0 in the second equality. By the definition of $\tilde{f}_\lambda$, we get

$$\tilde{f}_\lambda(Q_\sigma) = \sum_{\kappa \in \Lambda, \kappa \geq \lambda} \sum_{\alpha \in \{1, 2, \dots, m_\kappa\}} \langle \kappa, \lambda, \alpha | Q_\sigma | \kappa, \lambda, \alpha \rangle. \quad (\text{A56})$$

We note that $\{|\kappa, \lambda, \alpha\rangle\}_{\kappa \geq \lambda, \alpha \in \{1, 2, \dots, m_\kappa\}}$ is an orthonormal basis of the eigenspace of Z^{tot} with eigenvalue 2λ , and we can also take another orthonormal basis $\{|a_1 a_2 \cdots a_n\rangle\}_{(a_1, a_2, \dots, a_n) \in S_\lambda}$, where $S_\lambda := \{(a_1, a_2, \dots, a_n) \in \{0, 1\}^n \mid \#\{j \in \{1, 2, \dots, n\} \mid a_j = 1\} = n/2 - \lambda\}$, and $|a_1 a_2 \cdots a_n\rangle$ is the tensor product of the eigenvectors $|a\rangle$ of the single-qubit Pauli-Z operators satisfying $Z|0\rangle = (-1)^a |a\rangle$. By the basis transformation, we can rewrite Eq. (A56) as

$$\tilde{f}_\lambda(Q_\sigma) = \sum_{(a_1, a_2, \dots, a_n) \in S_\lambda} \langle a_1 a_2 \cdots a_n | Q_\sigma | a_1 a_2 \cdots a_n \rangle$$

$$\begin{aligned}
&= \sum_{(a_1, a_2, \dots, a_n) \in S_\lambda} \langle a_{\sigma(1)} a_{\sigma(2)} \cdots a_{\sigma(n)} | a_1 a_2 \cdots a_n \rangle \\
&= \#\{(a_1, a_2, \dots, a_n) \in S_\lambda \mid a_{\sigma(j)} = a_j \ \forall j \in \{1, 2, \dots, n\}\}.
\end{aligned} \tag{A57}$$

When σ is the identity, Eq. (A57) implies that

$$\tilde{f}_\lambda(I) = \#S_\lambda = \binom{n}{\frac{n}{2} - \lambda}. \tag{A58}$$

When σ is decomposed into disjoint cycles $\{\sigma_l\}_{l=1}^L$, we take disjoint subsets $D_1, D_2, \dots, D_L$ of $\{1, 2, \dots, L\}$ such that σ_l nontrivially acts on D_l for all $l \in \{1, 2, \dots, L\}$. Since σ_l is a p_l -cycle, $\#D_l = p_l$. The condition $a_{\sigma(j)} = a_j \ \forall j \in \{1, 2, \dots, n\}$ means that a_j must be identical for every element j in D_l . When $a_j = q_l$ for all $j \in D_l$ with some $q_l \in \{0, 1\}$, the number of strings $(a_1, a_2, \dots, a_n) \in S_\lambda$ is $\binom{n - \sum_{l=1}^L p_l}{\frac{n}{2} - \lambda - \sum_{l=1}^L q_l p_l}$. By summing them up over all $q_1, q_2, \dots, q_L \in \{0, 1\}$, we get Eq. (A51). $\square$

By using Lemma 8, we give the explicit expression of Eqs. (19) and (23) in Theorem 1. The following lemma is the counterpart of Lemma 5 in the SU(2) case.

Lemma 9. *Let $n, k, t \in \mathbb{N}$, R be a unitary representation of $G = \text{SU}(2)$ defined by Eq. (5), and Λ be given by Eq. (A48). Then, the distribution of the (G, R) -symmetric k -local random circuit is an asymptotic (G, R) -symmetric unitary t -design if and only if there exists no nontrivial integer solution $\mathbf{x} = (x_\lambda)_{\lambda \in \Lambda} \in \mathbb{Z}^\Lambda$ satisfying*

$$\sum_{\lambda \in \Lambda} \left(\binom{n}{\frac{n}{2} - \lambda} - \binom{n}{\frac{n}{2} - \lambda - 1} \right) |x_\lambda| \leq 2t, \tag{A59}$$

$$\sum_{\lambda \in \Lambda} \left(\binom{n-2j}{\frac{n}{2} - j - \lambda} - \binom{n-2j}{\frac{n}{2} - j - \lambda - 1} \right) x_\lambda = 0 \ \forall j \in \left\{ 0, 1, 2, \dots, \left\lfloor \frac{k}{2} \right\rfloor \right\}. \tag{A60}$$

Proof. Since R is a tensor product of representation on a single qubit, Theorem 1 implies that the distribution of (G, R) -symmetric k -local random circuit is an asymptotic unitary t -design if and only if Eqs. (19) and (23) have no nontrivial integer solution. Thus it is sufficient to show that Eqs. (19) and (23) are equivalent to Eqs. (A59) and (A60), respectively. By Lemma 8, we have

$$m_\lambda = f_\lambda(I) = \tilde{f}_\lambda(I) - \tilde{f}_{\lambda+1}(I) = \binom{n}{\frac{n}{2} - \lambda} - \binom{n}{\frac{n}{2} - \lambda - 1}. \tag{A61}$$

Thus Eq. (19) is equivalent to Eq. (A59).

In the following, we show the equivalence between Eq. (23) and Eq. (A60). By the Schur-Weyl duality, every (G, R) -symmetric operator $A \in \mathcal{L}_{k, G, R}$ can be written as a linear combination of the permutation operators Q_σ 's with permutations $\sigma \in \mathfrak{S}_k$, where Q_σ is the operator that brings the j th qubit to $\sigma(j)$ th qubit. Thus Eq. (23) is equivalent to

$$\sum_{\lambda \in \Lambda} f_\lambda(Q_\sigma \otimes I^{\otimes n-k}) x_\lambda = 0 \ \forall \sigma \in \mathfrak{S}_k. \tag{A62}$$

First, we show that Eq. (A60) implies Eq. (A62). We note that the permutation σ nontrivially acting on at most k elements can be written as $\sigma = \sigma_1 \sigma_2 \cdots \sigma_L$ with some disjoint p_l -cycles satisfying $\sum_{l=1}^L p_l = k$. By Lemma 8, we have

$$\begin{aligned}
\tilde{f}_\lambda(Q_\sigma \otimes I^{\otimes n-k}) &= \sum_{q_1, q_2, \dots, q_L \in \{0, 1\}} \binom{n-k}{\frac{n}{2} - \lambda - \sum_{l=1}^L q_l p_l} \\
&= \frac{1}{2} \sum_{q_1, q_2, \dots, q_L \in \{0, 1\}} \left(\binom{n-k}{\frac{n}{2} - \lambda - \sum_{l=1}^L q_l p_l} + \binom{n-k}{\frac{n}{2} - \lambda - \sum_{l=1}^L (1 - q_l) p_l} \right) \\
&= \frac{1}{2} \sum_{q_1, q_2, \dots, q_L \in \{0, 1\}} \left(\binom{n-k}{\frac{n}{2} - \lambda - \sum_{l=1}^L q_l p_l} + \binom{n-k}{\frac{n}{2} - \lambda - k + \sum_{l=1}^L q_l p_l} \right) \\
&= \sum_{j=0}^k u_j \left(\binom{n-k}{\frac{n}{2} - \lambda - j} + \binom{n-k}{\frac{n}{2} - \lambda - k + j} \right)
\end{aligned}$$

$$= \sum_{j=0}^{\lfloor k/2 \rfloor} \tilde{u}_j \left(\binom{n-k}{\frac{n}{2}-\lambda-j} + \binom{n-k}{\frac{n}{2}-\lambda-k+j} \right), \quad (\text{A63})$$

where u_j is defined by

$$u_j := \frac{1}{2} \# \left\{ (q_1, q_2, \dots, q_L) \in \{0, 1\}^L \mid \sum_{l=1}^L q_l p_l = j \right\} \quad (\text{A64})$$

for $j \in \{0, 1, \dots, k\}$, and $\tilde{u}_j$ is defined by $\tilde{u}_j := u_j + u_{k-j}$ for $j \in \{0, 1, \dots, (k-1)/2\}$ when k is odd, and $\tilde{u}_j := u_j + u_{k-j}$ for $j \in \{0, 1, \dots, k/2 - 1\}$ and $\tilde{u}_{k/2} := u_{k/2}$ when k is even. By Lemma 26, for any $\lambda \in \Lambda$, we can take $(v_{j,l})_{j,l \in \{0,1,\dots,\lfloor k/2 \rfloor\}} \in \mathbb{R}^{(\lfloor k/2 \rfloor + 1)^2}$ such that

$$\binom{n-k}{\frac{n}{2}-\lambda-j} + \binom{n-k}{\frac{n}{2}-\lambda-k+j} = \sum_{l=0}^{\lfloor k/2 \rfloor} v_{j,l} \binom{n-2l}{\frac{n}{2}-\lambda-l}. \quad (\text{A65})$$

By plugging Eq. (A65) into Eq. (A63), we get

$$\tilde{f}_\lambda(Q_\sigma \otimes \mathbb{I}^{\otimes n-k}) = \sum_{l=0}^{\lfloor k/2 \rfloor} \sum_{j=0}^{\lfloor k/2 \rfloor} \tilde{u}_j v_{j,l} \binom{n-2l}{\frac{n}{2}-\lambda-l}, \quad (\text{A66})$$

which implies

$$f_\lambda(Q_\sigma \otimes \mathbb{I}^{\otimes n-k}) = \tilde{f}_\lambda(Q_\sigma \otimes \mathbb{I}^{\otimes n-k}) - \tilde{f}_{\lambda+1}(Q_\sigma \otimes \mathbb{I}^{\otimes n-k}) = \sum_{l=0}^{\lfloor k/2 \rfloor} \sum_{j=0}^{\lfloor k/2 \rfloor} \tilde{u}_j v_{j,l} \left(\binom{n-2l}{\frac{n}{2}-l-\lambda} - \binom{n-2l}{\frac{n}{2}-l-\lambda-1} \right). \quad (\text{A67})$$

Thus Eq. (A60) implies Eq. (A62).

Next, we show that Eq. (A62) implies Eq. (A60). By Lemma 27, for any $\lambda \in \Lambda$, we can take $(w_{j,l})_{j,l \in \{0,1,\dots,\lfloor k/2 \rfloor\}} \in \mathbb{R}^{(\lfloor k/2 \rfloor + 1)^2}$ such that for any $j \in \{0, 1, \dots, \lfloor k/2 \rfloor\}$,

$$\binom{n-2j}{\frac{n}{2}-\lambda-j} = \sum_{l=0}^{\lfloor k/2 \rfloor} w_{j,l} \left(\binom{n-l}{\frac{n}{2}-\lambda} + \binom{n-l}{\frac{n}{2}-\lambda-l} \right). \quad (\text{A68})$$

For each $l \in \{1, 2, \dots, \lfloor k/2 \rfloor\}$, we take some l -cycle ζ_l . By Lemma 8, we have

$$\tilde{f}_\lambda(I) = \binom{n}{\frac{n}{2}-\lambda}, \quad \tilde{f}_\lambda(Q_{\zeta_l} \otimes \mathbb{I}^{\otimes n-k}) = \binom{n-l}{\frac{n}{2}-\lambda} + \binom{n-j}{\frac{n}{2}-\lambda-l}. \quad (\text{A69})$$

By using Eq. (A69), we can rewrite Eq. (A68) as

$$\binom{n-2j}{\frac{n}{2}-\lambda-j} = 2w_{j,0}\tilde{f}_\lambda(I) + \sum_{l=1}^{\lfloor k/2 \rfloor} w_{j,l}\tilde{f}_\lambda(Q_{\zeta_l} \otimes \mathbb{I}^{\otimes n-k}), \quad (\text{A70})$$

which implies that

$$\begin{aligned} \binom{n-2j}{\frac{n}{2}-\lambda-j} - \binom{n-2j}{\frac{n}{2}-\lambda-j-1} &= 2w_{j,0}(\tilde{f}_\lambda(I) - \tilde{f}_{\lambda+1}(I)) + \sum_{l=1}^{\lfloor k/2 \rfloor} w_{j,l}(\tilde{f}_\lambda(Q_{\zeta_l} \otimes \mathbb{I}^{\otimes n-k}) - \tilde{f}_{\lambda+1}(Q_{\zeta_l} \otimes \mathbb{I}^{\otimes n-k})) \\ &= 2w_{j,0}f_\lambda(I) + \sum_{l=1}^{\lfloor k/2 \rfloor} w_{j,l}f_\lambda(Q_{\zeta_l} \otimes \mathbb{I}^{\otimes n-k}). \end{aligned} \quad (\text{A71})$$

Thus Eq. (A62) implies Eq. (A60). $\square$

In the following, we consider the condition on t for Eqs. (A59) and (A60) in Lemma 9 having no nontrivial integer solution. First, we present a sufficient condition for the existence of nontrivial integer solution. The following lemma is the counterpart of Lemma 6 in the $SU(2)$ case.

Lemma 10. *Let $n, k \in \mathbb{N}$, $k \geq 2$, $n \geq 2(\lfloor k/2 \rfloor + 1)$, and R be a unitary representation of $G = SU(2)$ defined by Eq. (5). Then, Eqs. (A59) and (A60) have a nontrivial integer solution if*

$$t \geq \frac{2^{\lfloor k/2 \rfloor}}{(\lfloor \frac{k}{2} \rfloor + 1)!} \prod_{\alpha=1}^{\lfloor k/2 \rfloor + 1} (n - 2\alpha + 1). \quad (\text{A72})$$

We exclude the case $n = k + 1$ with even k in this lemma. In that case, the equations have no nontrivial integer solution for all $t \in \mathbb{N}$.

Proof. We define $\mathbf{y} = (y_\lambda)_{\lambda \in \Lambda}$ by

$$y_\lambda := (-1)^{n/2-\lambda} \left(\lambda + \frac{n}{2} - \lfloor \frac{k}{2} \rfloor - 1 \right) \left(\lambda - \frac{n}{2} + \lfloor \frac{k}{2} \rfloor + 1 \right), \quad (\text{A73})$$

and show that $\mathbf{y}$ is a nontrivial integer solution of Eqs. (A59) and (A60). By the definition of $\mathbf{y}$, we can show that $\mathbf{y}$ satisfies Eqs. (A59) as follows:

$$\begin{aligned} & \sum_{\lambda \in \{n/2, n/2-1, \dots, n/2-\lfloor k/2 \rfloor-1\}} \left(\binom{n-2j}{\frac{n}{2}-j-\lambda} - \binom{n-2j}{\frac{n}{2}-j-\lambda-1} \right) y_\lambda \\ &= (-1)^{\lfloor k/2 \rfloor + 1} \sum_{\kappa=0}^{\lfloor k/2 \rfloor + 1} \left(\binom{n-2j}{\lfloor \frac{k}{2} \rfloor - j + 1 - \kappa} - \binom{n-2j}{\lfloor \frac{k}{2} \rfloor - j - \kappa} \right) \cdot (-1)^\kappa \binom{n-2\lfloor \frac{k}{2} \rfloor - 2 + \kappa}{\kappa} \\ &= (-1)^{\lfloor k/2 \rfloor + 1} \sum_{\kappa=0}^{\lfloor k/2 \rfloor + 1} \left(\binom{n-2j}{\lfloor \frac{k}{2} \rfloor - j + 1 - \kappa} - \binom{n-2j}{\lfloor \frac{k}{2} \rfloor - j - \kappa} \right) \cdot (-1)^\kappa \binom{n-2\lfloor \frac{k}{2} \rfloor - 2 + \kappa}{\kappa} \\ &= (-1)^{\lfloor k/2 \rfloor + 1} \left(\binom{2\lfloor \frac{k}{2} \rfloor - 2j + 1}{\lfloor \frac{k}{2} \rfloor - j + 1} - \binom{2\lfloor \frac{k}{2} \rfloor - 2j + 1}{\lfloor \frac{k}{2} \rfloor - j} \right) \\ &= 0, \end{aligned} \quad (\text{A74})$$

where the second equality can be confirmed by comparing the coefficients of $z^{\lfloor k/2 \rfloor - j + 1}$ in both sides of $(1-z)(1+z)^{n-2j} \cdot (1+z)^{-(n-2\lfloor k/2 \rfloor - 1)} = (1-z)(1+z)^{2\lfloor k/2 \rfloor - 2j + 1}$. The definition of $\mathbf{y}$ (Eq. (A73)) also implies that

$$\begin{aligned} & \sum_{\lambda \in \{n/2, n/2-1, \dots, n/2-\lfloor k/2 \rfloor-1\}} \left(\binom{n}{\frac{n}{2}-\lambda} - \binom{n}{\frac{n}{2}-\lambda-1} \right) |y_\lambda| \\ &= \sum_{\kappa=0}^{\lfloor k/2 \rfloor + 1} \left(\binom{n}{\lfloor \frac{k}{2} \rfloor + 1 - \kappa} - \binom{n}{\lfloor \frac{k}{2} \rfloor - \kappa} \right) \binom{n-2\lfloor \frac{k}{2} \rfloor - 2 + \kappa}{\kappa} \\ &= \sum_{\kappa=0}^{\lfloor k/2 \rfloor + 1} \binom{n}{\lfloor \frac{k}{2} \rfloor + 1 - \kappa} \binom{n-2\lfloor \frac{k}{2} \rfloor - 1 + \kappa}{\kappa} \\ &= a_{n, 2(\lfloor k/2 \rfloor + 1), \lfloor k/2 \rfloor + 1} \\ &= \frac{2^{\lfloor k/2 \rfloor + 1}}{(\lfloor \frac{k}{2} \rfloor + 1)!} \prod_{\alpha=1}^{\lfloor k/2 \rfloor + 1} (n - 2\alpha + 1) \end{aligned} \quad (\text{A75})$$

where the second equality can be confirmed by comparing the coefficients of $z^{\lfloor k/2 \rfloor + 1}$ in both sides of $(1-z)(1+z)^n \cdot (1-z)^{-(n-2\lfloor k/2 \rfloor - 1)} = (1+z)^n / (1-z)^{n-2\lfloor k/2 \rfloor - 2}$, and the third and fourth equalities follow from the definition of $a_{n,k,j}$ (Eq. (A16)) and Lemma 24, respectively. Thus $\mathbf{y}$ is a nontrivial integer solution of Eqs. (A59) and (A60) if t satisfies Eq. (A72). $\square$

Next, we show that for sufficiently large n , the condition on t presented in Lemma 10 is necessary for Eqs. (A59) and (A60) in Lemma 9 having no nontrivial integer solution. The following lemma is the counterpart of Lemma 11 in the $SU(2)$ case.

Lemma 11. Let $n, k \in \mathbb{N}$, $k \geq 2$, $n \geq 2(\lfloor k/2 \rfloor + 1)$, R be a unitary representation of $G = \text{SU}(2)$ defined by Eq. (5), and $c_{n,k}$ defined by

$$c_{n,k} := \frac{2^{\lfloor k/2 \rfloor}}{(\lfloor \frac{k}{2} \rfloor + 1)!} \prod_{\alpha=1}^{\lfloor k/2 \rfloor + 1} (n - 2\alpha + 1) \quad (\text{A76})$$

satisfy $c_{n,k} \leq \binom{n}{j+1} - \binom{n}{j}$ for all $j \in \{\lfloor k/2 \rfloor + 1, \lfloor k/2 \rfloor + 2, \dots, \lfloor n/2 \rfloor - 1\}$. Then, Eqs. (A59) and (A60) have no nontrivial integer solution if and only if $t < c_{n,k}$.

We note that the condition on n and k is satisfied when $n \geq 2^{2(\lfloor k/2 \rfloor + 1)}$, as we show in Lemma 23.

Proof. We take arbitrary integer solution $\mathbf{x}$ of Eqs. (A59) and (A60), and show that $\mathbf{x} = \mathbf{0}$ when $t < c_{n,k}$. By Lemma 4 and the assumption that $c_{n,k} \leq \binom{n}{\lfloor k/2 \rfloor + 1}$ for $j = \lfloor k/2 \rfloor + 1$ and $\lfloor n/2 \rfloor - 1$, we have

$$x_\lambda = 0 \quad \forall \lambda \in \left\{ \frac{n}{2} - \left\lfloor \frac{k}{2} \right\rfloor - 2, \frac{n}{2} - \left\lfloor \frac{k}{2} \right\rfloor - 3, \dots, \frac{n}{2} - \left\lfloor \frac{n}{2} \right\rfloor \right\}, \quad (\text{A77})$$

By noting that $\binom{n-2j}{n/2-j-\lambda} - \binom{n-2j}{n/2-j-\lambda-1} = 0$ when $\lambda > n/2 - j$, we can see that the linear space of $\mathbf{x}$ satisfying Eqs. (A60) and (A77) is 1-dimensional. By Eq. (A74), $\mathbf{y}$ defined by Eq. (A73) is a nontrivial solution of Eq. (A60) and we can directly confirm that $\mathbf{y}$ also satisfies Eq. (A77). Thus $\mathbf{x}$ can be written as $\mathbf{x} = r\mathbf{y}$ with some $r \in \mathbb{R}$. Since $\mathbf{x}$ is an integer vector and $y_{n/2-\lfloor k/2 \rfloor-1} = (-1)^{\lfloor k/2 \rfloor + 1}$, we have $r = x_{n/2-\lfloor k/2 \rfloor-1}/y_{n/2-\lfloor k/2 \rfloor-1} \in \mathbb{Z}$. By Eq. (A75), we have

$$\sum_{\lambda \in \{n/2, n/2-1, \dots, n/2-\lfloor k/2 \rfloor-1\}} \left(\binom{n}{\frac{n}{2} - \lambda} - \binom{n}{\frac{n}{2} - \lambda - 1} \right) |x_\lambda| = 2|r|c_{n,k}. \quad (\text{A78})$$

When $t < c_{n,k}$, Eq. (A60) implies that

$$\sum_{\lambda \in \{n/2, n/2-1, \dots, n/2-\lfloor k/2 \rfloor-1\}} \left(\binom{n}{\frac{n}{2} - \lambda} - \binom{n}{\frac{n}{2} - \lambda - 1} \right) |x_\lambda| < 2c_{n,k}. \quad (\text{A79})$$

By plugging Eq. (A78) into Eq. (A79), we get $r = 0$, which implies that Eqs. (A59) and (A60) have no nontrivial integer solution when $t < c_{n,k}$. $\square$

By using the lemmas above, we can prove Theorem 5 as follows:

Proof of Theorem 5. In Lemma 9, we have explicitly rewritten the equations in Theorem 1 in the $\text{SU}(2)$ case. When t does not satisfy Eq. (32), by Lemma 10, there exists a nontrivial integer solution for all $k \geq 2(\lfloor k/2 \rfloor + 1)$. When t satisfies Eq. (32), by Lemma 11, there exists no nontrivial integer solution under a certain assumption about n and k , which is guaranteed when $n \geq 2^{2(\lfloor k/2 \rfloor + 1)}$ by Lemma 23. $\square$

For the proof of Theorem 6, we directly consider the condition on t such that Eqs. (A59) and (A60) have no nontrivial integer solution for the region of n where we cannot use Lemma 11.

Proof of Theorem 6. By Lemma 9, the distribution of the (G, R) -symmetric k -local random circuit forming an asymptotic unitary t -design if and only if Eqs. (A59) and (A60) have no nontrivial integer solution.

First, we consider the case when $k = 2$ or $k = 3$. Since Eqs. (A59) and (A60) are the same when $k = 2$ and when $k = 3$, it is sufficient to consider the case when $k = 2$. We note that the common assumption $n \leq 2(\lfloor k/2 \rfloor + 1)$ in Lemmas 10 and 11 is satisfied when $n \geq 4$. We also note that when $n = 4, 5$, or $n \geq 11$, the other assumption in Lemma 10 holds, i.e.,

$$(n-1)(n-3) \leq \binom{n}{j+1} - \binom{n}{j} \quad \forall j \in \left\{ 2, 3, \dots, \left\lfloor \frac{n}{2} \right\rfloor - 1 \right\}. \quad (\text{A80})$$

By combining Lemmas 10 and 11, we get the conclusion. The proof of Eq. (A80) is as follows: When $n = 4$ or 5 , since the set $\{2, 3, \dots, \lfloor n/2 \rfloor - 1\}$ is empty, Eq. (A80) trivially holds. When $n \geq 11$, it is sufficient to show that

$\binom{n}{j+1} - \binom{n}{j} \geq (n-1)(n-3)$ only for $j = 2$ and $j = \lfloor n/2 \rfloor - 1$ by Lemma 22. For the proof of the case of $j = 2$, we have

$$\binom{n}{3} - \binom{n}{2} = n(n-1) \cdot \frac{n-5}{6} \geq (n-1)(n-3) \cdot 1 = (n-1)(n-3). \quad (\text{A81})$$

For the proof of the case of $j = \lfloor n/2 \rfloor - 1$, when $n = 11$, we can directly confirm that

$$\binom{n}{\lfloor \frac{n}{2} \rfloor} - \binom{n}{\lfloor \frac{n}{2} \rfloor - 1} = \binom{11}{5} - \binom{11}{4} = 132 \geq 80 = (11-1)(11-3) = (n-1)(n-3). \quad (\text{A82})$$

When $n \geq 12$, we have

$$\begin{aligned} \binom{n}{\lfloor \frac{n}{2} \rfloor} - \binom{n}{\lfloor \frac{n}{2} \rfloor - 1} &= \frac{n(n-1)(n-2)(n-3)}{5!} \left(\prod_{\alpha=6}^{\lfloor n/2 \rfloor} \frac{n-2\lfloor \frac{n}{2} \rfloor + 2 + \alpha}{\alpha} \right) \left(n-2\lfloor \frac{n}{2} \rfloor + 1 \right) \\ &\geq \frac{12 \cdot (n-1) \cdot 10 \cdot (n-3)}{120} \\ &= (n-1)(n-3). \end{aligned} \quad (\text{A83})$$

For $n = 3, 6, 7, 8, 9$, and 10 , we get the conclusion by explicitly writing down the equations in Lemma 9.

- When $n = 3$, Eq. (A60) is explicitly rewritten as

$$x_{3/2} + 2x_{1/2} = 0, \quad (\text{A84})$$

$$x_{3/2} = 0, \quad (\text{A85})$$

which implies that $x_{3/2} = x_{1/2} = 0$. Therefore, Eqs. (A59) and (A60) do not have a nontrivial solution for all $t \in \mathbb{N}$.

- When $n = 6$. Eqs. (A59) and (A60) are explicitly written as

$$|x_3| + 5|x_2| + 9|x_1| + 5|x_0| \leq 2t, \quad (\text{A86})$$

$$x_3 + 5x_2 + 9x_1 + 5x_0 = 0, \quad (\text{A87})$$

$$x_2 + 3x_1 + 2x_0 = 0. \quad (\text{A88})$$

If $t \geq 10$, Eqs. (A59) and (A60) have a nontrivial integer solution $(x_3, x_2, x_1, x_0) = (1, -1, 1, -1)$. If $t < 10$, any integer solution $\mathbf{x}$ satisfies $|x_1| \leq 1$ and $|x_0| \leq 1$ by Lemma 4. We thus have $(x_1, x_0) = \pm(1, 1), \pm(1, 0), \pm(0, 1), \pm(1, -1)$, or $(0, 0)$, which implies $|x_3| + 5|x_2| + 9|x_1| + 5|x_0| = 50, 30, 20, 20$, or 0 , respectively. By combining this with Eq. (A59), we get $\mathbf{x} = \mathbf{0}$. We can therefore conclude that Eqs. (A59) and (A60) have no nontrivial integer solution.

- When $n = 7$. Eqs. (A59) and (A60) are explicitly written as

$$|x_{7/2}| + 6|x_{5/2}| + 14|x_{3/2}| + 14|x_{1/2}| \leq 2t, \quad (\text{A89})$$

$$x_{7/2} + 6x_{5/2} + 14x_{3/2} + 14x_{1/2} = 0, \quad (\text{A90})$$

$$x_{5/2} + 4x_{3/2} + 5x_{1/2} = 0. \quad (\text{A91})$$

If $t \geq 20$, Eqs. (A59) and (A60) have a nontrivial integer solution $(x_{7/2}, x_{5/2}, x_{3/2}, x_{1/2}) = (6, -1, -1, 1)$. If $t < 20$, any integer solution $\mathbf{x}$ satisfies $|x_{3/2}| \leq 1$ and $|x_{1/2}| \leq 1$ by Lemma 4. We thus have $(x_{3/2}, x_{1/2}) = \pm(1, 1), \pm(1, 0), \pm(0, 1), \pm(1, -1)$, or $(0, 0)$, which implies $|x_{7/2}| + 6|x_{5/2}| + 14|x_{3/2}| + 14|x_{1/2}| = 108, 48, 60, 40$, or 0 , respectively. By combining this with Eq. (A59), we get $\mathbf{x} = \mathbf{0}$.

- When $n = 8$. Eqs. (A59) and (A60) are explicitly written as

$$|x_4| + 7|x_3| + 20|x_2| + 28|x_1| + 14|x_0| \leq 2t, \quad (\text{A92})$$

$$x_4 + 7x_3 + 20x_2 + 28x_1 + 14x_0 = 0, \quad (\text{A93})$$

$$x_3 + 5x_2 + 9x_1 + 5x_0 = 0. \quad (\text{A94})$$

If $t \geq 20$, Eqs. (A59) and (A60) have a nontrivial integer solution $(x_4, x_3, x_2, x_1, x_0) = (6, 0, -1, 0, 1)$. If $t < 20$, any integer solution $\mathbf{x}$ satisfies $x_2 = x_1 = 0$ and $|x_0| \leq 1$ by Lemma 4. We thus have $x_4 = 21x_0$ and $x_3 = -5x_0$, which implies $|x_4| + 7|x_3| + 14|x_0| = 70|x_0|$. By combining this with Eq. (A59), we get $\mathbf{x} = \mathbf{0}$.

- When $n = 9$. Eqs. (A59) and (A60) are explicitly written as

$$|x_{9/2}| + 8|x_{7/2}| + 27|x_{5/2}| + 48|x_{3/2}| + 42|x_{1/2}| \leq 2t, \quad (\text{A95})$$

$$x_{9/2} + 8x_{7/2} + 27x_{5/2} + 48x_{3/2} + 42x_{1/2} = 0, \quad (\text{A96})$$

$$x_{7/2} + 6x_{5/2} + 14x_{3/2} + 14x_{1/2} = 0. \quad (\text{A97})$$

If $t \geq 48$, the existence of nontrivial integer solution of Eqs. (A59) and (A60) have been proven in Lemma . If $t < 48$, any integer solution $\mathbf{x}$ satisfies $x_{3/2} = 0$, $|x_{5/2}| \leq 1$, and $|x_{1/2}| \leq 1$ by Lemma 4. We thus have $(x_{5/2}, x_{1/2}) = \pm(1, 1), \pm(1, 0), \pm(0, 1), \pm(1, -1)$, or $(0, 0)$, which implies $|x_{9/2}| + 8|x_{7/2}| + 27|x_{5/2}| + 48|x_{3/2}| + 42|x_{1/2}| = 320, 96, 224, 182$, or 0 , respectively. By combining this with Eq. (A59), we get $\mathbf{x} = \mathbf{0}$.

- When $n = 10$. Eqs. (A59) and (A60) are explicitly written as

$$|x_5| + 9|x_4| + 35|x_3| + 75|x_2| + 90|x_1| + 42|x_0| \leq 2t, \quad (\text{A98})$$

$$x_5 + 9x_4 + 35x_3 + 75x_2 + 90x_1 + 42x_0 = 0, \quad (\text{A99})$$

$$x_4 + 7x_3 + 20x_2 + 28x_1 + 14x_0 = 0. \quad (\text{A100})$$

If $t \geq 63$, the existence of nontrivial integer solution of Eqs. (A59) and (A60) have been proven in Lemma . If $t < 63$, any integer solution $\mathbf{x}$ satisfies $x_2 = x_1 = 0$, $|x_3| \leq 1$, and $|x_0| \leq 1$ by Lemma 4. We thus have $(x_3, x_1) = \pm(1, 1), \pm(1, 0), \pm(0, 1), \pm(1, -1)$, or $(0, 0)$, which implies $|x_5| + 9|x_4| + 35|x_3| + 75|x_2| + 90|x_1| + 42|x_0| = 378, 126, 252, 196$, or 0 , respectively. By combining this with Eq. (A59), we get $\mathbf{x} = \mathbf{0}$.

Next, we consider the case when $k = 4$. We note that when $n = 6, 7$, or $n \geq 18$, the assumption in Lemma 11 holds, i.e.,

$$\frac{2}{3}(n-1)(n-3)(n-5) \leq \binom{n}{j+1} - \binom{n}{j} \quad \forall j \in \left\{3, 4, \dots, \left\lfloor \frac{n}{2} \right\rfloor - 1\right\}. \quad (\text{A101})$$

Thus we can use Lemma 11, and by combining it with lemma 10, we get the conclusion. The proof of Eq. (A101) is as follows: When $n = 6$ or 7 , since the set $\{3, 4, \dots, \lfloor n/2 \rfloor - 1\}$ is empty, Eq. (A101) trivially holds. When $n \geq 18$, by Lemma 22, it is sufficient to show that $\binom{n}{j+1} - \binom{n}{j} \geq 2(n-1)(n-3)(n-5)/3$ only for $j = 3$ and $j = \lfloor n/2 \rfloor - 1$. For the proof of the case of $j = 3$, we have

$$\begin{aligned} \binom{n}{4} - \binom{n}{3} &= \frac{n(n-1)(n-2)(n-7)}{24} \\ &= \frac{2}{3}(n-1) \cdot \frac{n-2}{16} \cdot n(n-7) \\ &\geq \frac{2}{3}(n-1) \cdot 1 \cdot (n-3)(n-5) \\ &= \frac{2}{3}(n-1)(n-3)(n-5). \end{aligned} \quad (\text{A102})$$

For the proof of $j = \lfloor n/2 \rfloor - 1$, we have

$$\begin{aligned} \binom{n}{\lfloor \frac{n}{2} \rfloor} - \binom{n}{\lfloor \frac{n}{2} \rfloor - 1} &= \frac{n(n-1)(n-2)(n-3)(n-4)(n-5)}{7!} \left(\prod_{\alpha=8}^{\lfloor n/2 \rfloor} \frac{n-2\lfloor \frac{n}{2} \rfloor + 2 + \alpha}{\alpha} \right) \left(n - 2\lfloor \frac{n}{2} \rfloor + 1 \right) \\ &\geq \frac{18 \cdot (n-1) \cdot 16 \cdot (n-3) \cdot 14 \cdot (n-5)}{7!} \\ &= \frac{4}{5}(n-1)(n-3)(n-5) \\ &\geq \frac{2}{3}(n-1)(n-3)(n-5). \end{aligned} \quad (\text{A103})$$

In the following, we confirm the results for $n = 5, 8, 9, \dots, 17$ by explicitly writing down the equations in Lemma 9.

- When $n = 5$, Eq. (A60) is explicitly written as

$$x_{5/2} + 4x_{3/2} + 5x_{1/2} = 0, \quad (\text{A104})$$

$$x_{3/2} + 2x_{1/2} = 0, \quad (\text{A105})$$

$$x_{1/2} = 0, \quad (\text{A106})$$

which implies that $x_{5/2} = x_{3/2} = x_{1/2} = 0$. Therefore, Eqs. (A59) and (A60) do not have a nontrivial solution for all $t \in \mathbb{N}$.

- When $n = 8$, Eqs. (A59) and (A60) are explicitly written as

$$|x_4| + 7|x_3| + 20|x_2| + 28|x_1| + 14|x_0| \leq 2t, \quad (\text{A107})$$

$$x_4 + 7x_3 + 20x_2 + 28x_1 + 14x_0 = 0, \quad (\text{A108})$$

$$x_3 + 5x_2 + 9x_1 + 5x_0 = 0, \quad (\text{A109})$$

$$x_2 + 3x_1 + 2x_0 = 0. \quad (\text{A110})$$

If $t \geq 35$, Eqs. (A59) and (A60) have a nontrivial integer solution $(x_4, x_3, x_2, x_1, x_0) = (1, -1, 1, -1, 1)$. If $t < 35$, any integer solution $\mathbf{x}$ satisfies $|x_2| \leq 1$, $|x_1| \leq 1$, and $|x_0| \leq 2$ by Lemma 4. We thus have $(x_2, x_1, x_0) = \pm(1, 1, -2)$, $\pm(1, -1, 1)$, or $(0, 0, 0)$, which implies $|x_4| + 7|x_3| + 20|x_2| + 28|x_1| + 14|x_0| = 112, 70$, or 0 , respectively. By combining this with Eq. (A59), we get $\mathbf{x} = \mathbf{0}$. We can therefore conclude that Eqs. (A59) and (A60) have no nontrivial integer solution.

- When $n = 9$, Eqs. (A59) and (A60) are explicitly written as

$$|x_{9/2}| + 8|x_{7/2}| + 27|x_{5/2}| + 48|x_{3/2}| + 42|x_{1/2}| \leq 2t, \quad (\text{A111})$$

$$x_{9/2} + 8x_{7/2} + 27x_{5/2} + 48x_{3/2} + 42x_{1/2} = 0, \quad (\text{A112})$$

$$x_{7/2} + 6x_{5/2} + 14x_{3/2} + 14x_{1/2} = 0, \quad (\text{A113})$$

$$x_{5/2} + 4x_{3/2} + 5x_{1/2} = 0. \quad (\text{A114})$$

If $t \geq 90$, Eqs. (A59) and (A60) have a nontrivial integer solution $(x_{9/2}, x_{7/2}, x_{5/2}, x_{3/2}, x_{1/2}) = (-15, 6, -1, -1, 1)$. If $t < 90$, any integer solution $\mathbf{x}$ satisfies $|x_{5/2}| \leq 3$, $|x_{3/2}| \leq 1$, and $|x_{1/2}| \leq 2$ by Lemma 4. We thus have $(x_{5/2}, x_{3/2}, x_{1/2}) = \pm(-1, 1, -1)$ or $(0, 0, 0)$, which implies $|x_{9/2}| + 8|x_{7/2}| + 27|x_{5/2}| + 48|x_{3/2}| + 42|x_{1/2}| = 180$ or 0 , respectively. By combining this with Eq. (A59), we get $\mathbf{x} = \mathbf{0}$.

- When $n = 10$, Eqs. (A59) and (A60) are explicitly written as

$$|x_5| + 9|x_4| + 35|x_3| + 75|x_2| + 90|x_1| + 42|x_0| \leq 2t, \quad (\text{A115})$$

$$x_5 + 9x_4 + 35x_3 + 75x_2 + 90x_1 + 42x_0 = 0, \quad (\text{A116})$$

$$x_4 + 7x_3 + 20x_2 + 28x_1 + 14x_0 = 0, \quad (\text{A117})$$

$$x_3 + 5x_2 + 9x_1 + 5x_0 = 0. \quad (\text{A118})$$

If $t \geq 96$, Eqs. (A59) and (A60) have a nontrivial integer solution $(x_5, x_4, x_3, x_2, x_1, x_0) = (-21, 6, 0, -1, 0, 1)$. If $t < 96$, any integer solution $\mathbf{x}$ satisfies $|x_3| \leq 2$, $|x_2| \leq 1$, $|x_1| \leq 1$, $|x_0| \leq 2$ by Lemma 4. We thus have $(x_3, x_2, x_1, x_0) = \pm(1, -1, 1, -1)$, $\pm(1, 0, 1, -2)$, $\pm(0, 1, 0, -1)$, or $(0, 0, 0, 0)$, which implies $|x_5| + 9|x_4| + 35|x_3| + 75|x_2| + 90|x_1| + 42|x_0| = 256, 294, 192$, or 0 , respectively. By combining this with Eq. (A59), we get $\mathbf{x} = \mathbf{0}$.

- When $n = 11$, Eqs. (A59) and (A60) are explicitly written as

$$|x_{11/2}| + 10|x_{9/2}| + 44|x_{7/2}| + 110|x_{5/2}| + 165|x_{3/2}| + 132|x_{1/2}| \leq 2t, \quad (\text{A119})$$

$$x_{11/2} + 10x_{9/2} + 44x_{7/2} + 110x_{5/2} + 165x_{3/2} + 132x_{1/2} = 0, \quad (\text{A120})$$

$$x_{9/2} + 8x_{7/2} + 27x_{5/2} + 48x_{3/2} + 42x_{1/2} = 0, \quad (\text{A121})$$

$$x_{7/2} + 6x_{5/2} + 14x_{3/2} + 14x_{1/2} = 0. \quad (\text{A122})$$

If $t \geq 192$, Eqs. (A59) and (A60) have a nontrivial integer solution $(x_{11/2}, x_{9/2}, x_{7/2}, x_{5/2}, x_{3/2}, x_{1/2}) = (27, -6, 0, 0, 1, -1)$. If $t < 192$, any integer solution $\mathbf{x}$ satisfies $|x_{7/2}| \leq 4$, $|x_{5/2}| \leq 1$, $|x_{3/2}| \leq 1$, and $|x_{1/2}| \leq 1$ by Lemma 4. We thus have $(x_{7/2}, x_{5/2}, x_{3/2}, x_{1/2}) = \pm(0, 0, 1, -1)$ or $(0, 0, 0, 0)$, which implies $|x_{11/2}| + 10|x_{9/2}| + 44|x_{7/2}| + 110|x_{5/2}| + 165|x_{3/2}| + 132|x_{1/2}| = 384$ or 0 , respectively. By combining this with Eq. (A59), we get $\mathbf{x} = \mathbf{0}$.

- When $n = 12$, Eqs. (A59) and (A60) are explicitly written as

$$|x_6| + 11|x_5| + 54|x_4| + 154|x_3| + 275|x_2| + 297|x_1| + 132|x_0| \leq 2t, \quad (\text{A123})$$

$$x_6 + 11x_5 + 54x_4 + 154x_3 + 275x_2 + 297x_1 + 132x_0 = 0, \quad (\text{A124})$$

$$x_5 + 9x_4 + 35x_3 + 75x_2 + 90x_1 + 42x_0 = 0, \quad (\text{A125})$$

$$x_4 + 7x_3 + 20x_2 + 28x_1 + 14x_0 = 0. \quad (\text{A126})$$

If $t \geq 330$, Eqs. (A59) and (A60) have a nontrivial integer solution $(x_6, x_5, x_4, x_3, x_2, x_1, x_0) = (33, -6, 0, 0, 0, 1, -2)$. If $t < 330$, any integer solution $\mathbf{x}$ satisfies $m_\lambda|x_\lambda| < 330$ for all $\lambda \in \{0, 1, 2, 3, 4\}$ and $|m_\lambda x_\lambda + m_\kappa x_\kappa| < 330$ for all $\lambda, \kappa \in \{0, 1, 2, 3, 4\}$ satisfying $\lambda \neq \kappa$ by Lemma 4. We thus have $(x_6, x_5, x_4, x_3, x_2, x_1, x_0) = \pm(132, -28, 0, 2, 0, 0, -1)$, $\pm(33, -6, 0, 0, 0, 1, -2)$, $\pm(34, -7, 1, -1, 1, 0, -1)$, or $(0, 0, 0, 0, 0, 0, 0)$, which implies $|x_6| + 11|x_5| + 54|x_4| + 154|x_3| + 275|x_2| + 297|x_1| + 132|x_0| = 880, 660, 726$, or 0 , respectively. By combining this with Eq. (A59), we get $\mathbf{x} = \mathbf{0}$.

- When $n = 13$, Eqs. (A59) and (A60) are explicitly written as

$$|x_{13/2}| + 12|x_{11/2}| + 65|x_{9/2}| + 208|x_{7/2}| + 429|x_{5/2}| + 572|x_{3/2}| + 429|x_{1/2}| \leq 2t, \quad (\text{A127})$$

$$x_{13/2} + 12x_{11/2} + 65x_{9/2} + 208x_{7/2} + 429x_{5/2} + 572x_{3/2} + 429x_{1/2} = 0, \quad (\text{A128})$$

$$x_{11/2} + 10x_{9/2} + 44x_{7/2} + 110x_{5/2} + 165x_{3/2} + 132x_{1/2} = 0, \quad (\text{A129})$$

$$x_{9/2} + 8x_{7/2} + 27x_{5/2} + 48x_{3/2} + 42x_{1/2} = 0. \quad (\text{A130})$$

If $t \geq 640$, Lemma 10 implies that Eqs. (A59) and (A60) have a nontrivial integer solution. If $t < 640$, any integer solution $\mathbf{x}$ satisfies $m_\lambda|x_\lambda| < 640$ for all $\lambda \in \{1/2, 3/2, 5/2, 7/2, 9/2\}$ and $|m_\lambda x_\lambda + m_\kappa x_\kappa| < 640$ for all $\lambda, \kappa \in \{1/2, 3/2, 5/2, 7/2, 9/2\}$ satisfying $\lambda \neq \kappa$ by Lemma 4. By these conditions and Eq. (A60) in the case of $j = 2$, we get $x_{1/2} = x_{3/2} = x_{5/2} = x_{7/2} = x_{9/2} = 0$. By plugging this into Eq. (A60) in the cases of $j = 0$ and 1 , we get $\mathbf{x} = \mathbf{0}$.

- When $n = 14$, Eqs. (A59) and (A60) are explicitly written as

$$|x_7| + 13|x_6| + 77|x_5| + 273|x_4| + 637|x_3| + 1001|x_2| + 1001|x_1| + 429|x_0| \leq 2t, \quad (\text{A131})$$

$$x_7 + 13x_6 + 77x_5 + 273x_4 + 637x_3 + 1001x_2 + 1001x_1 + 429x_0 = 0, \quad (\text{A132})$$

$$x_6 + 11x_5 + 54x_4 + 154x_3 + 275x_2 + 297x_1 + 132x_0 = 0, \quad (\text{A133})$$

$$x_5 + 9x_4 + 35x_3 + 75x_2 + 90x_1 + 42x_0 = 0. \quad (\text{A134})$$

If $t \geq 858$, Lemma 10 implies that Eqs. (A59) and (A60) have a nontrivial integer solution. If $t < 858$, any integer solution $\mathbf{x}$ satisfies $m_\lambda|x_\lambda| < 640$ for all $\lambda \in \{0, 1, 2, 3, 4, 5\}$ and $|m_\lambda x_\lambda + m_\kappa x_\kappa| < 640$ for all $\lambda, \kappa \in \{0, 1, 2, 3, 4, 5\}$ satisfying $\lambda \neq \kappa$ by Lemma 4. By these conditions and Eq. (A60) in the case of $j = 2$, we get $x_0 = x_1 = x_2 = x_3 = x_4 = x_5 = 0$. By plugging this into Eq. (A60) in the cases of $j = 0$ and 1 , we get $\mathbf{x} = \mathbf{0}$.

- When $n = 15$, Eqs. (A59) and (A60) are explicitly written as

$$|x_{15/2}| + 14|x_{13/2}| + 90|x_{11/2}| + 350|x_{9/2}| + 910|x_{7/2}| + 1638|x_{5/2}| + 2002|x_{3/2}| + 1430|x_{1/2}| \leq 2t, \quad (\text{A135})$$

$$x_{15/2} + 14x_{13/2} + 90x_{11/2} + 350x_{9/2} + 910x_{7/2} + 1638x_{5/2} + 2002x_{3/2} + 1430x_{1/2} = 0, \quad (\text{A136})$$

$$x_{13/2} + 12x_{11/2} + 65x_{9/2} + 208x_{7/2} + 429x_{5/2} + 572x_{3/2} + 429x_{1/2} = 0, \quad (\text{A137})$$

$$x_{11/2} + 10x_{9/2} + 44x_{7/2} + 110x_{5/2} + 165x_{3/2} + 132x_{1/2} = 0. \quad (\text{A138})$$

If $t \geq 1120$, Lemma 10 implies that Eqs. (A59) and (A60) have a nontrivial integer solution. If $t < 1120$, any integer solution $\mathbf{x}$ satisfies $x_{5/2} = x_{3/2} = x_{1/2} = 0$, $|x_{11/2}| \leq 12$, $|x_{9/2}| \leq 3$, and $|x_{7/2}| \leq 1$ by Lemma 4. By these conditions and Eq. (A60), we get $(x_{11/2}, x_{9/2}, x_{7/2}) = \pm(-10, 1, 0)$ or $(0, 0, 0)$, which implies $|x_{15/2}| + 14|x_{13/2}| + 90|x_{11/2}| + 350|x_{9/2}| + 910|x_{7/2}| + 1638|x_{5/2}| + 2002|x_{3/2}| + 1430|x_{1/2}| = 2240$ or 0 , respectively. By combining this with Eq. (A59), we get $\mathbf{x} = \mathbf{0}$.

- When $n = 16$, Eqs. (A59) and (A60) are explicitly written as

$$|x_8| + 15|x_7| + 104|x_6| + 440|x_5| + 1260|x_4| + 2548|x_3| + 3640|x_2| + 3432|x_1| + 1430|x_0| \leq 2t, \quad (\text{A139})$$

$$x_8 + 15x_7 + 104x_6 + 440x_5 + 1260x_4 + 2548x_3 + 3640x_2 + 3432x_1 + 1430x_0 = 0, \quad (\text{A140})$$

$$x_7 + 13x_6 + 77x_5 + 273x_4 + 637x_3 + 1001x_2 + 1001x_1 + 429x_0 = 0, \quad (\text{A141})$$

$$x_6 + 11x_5 + 54x_4 + 154x_3 + 275x_2 + 297x_1 + 132x_0 = 0. \quad (\text{A142})$$

If $t \geq 1430$, Lemma 10 implies that Eqs. (A59) and (A60) have a nontrivial integer solution. If $t < 1430$, any integer solution $\mathbf{x}$ satisfies $x_3 = x_2 = x_1 = x_0 = 0$, $|x_6| \leq 13$, $|x_5| \leq 3$, and $|x_4| \leq 1$ by Lemma 4. By these conditions and Eq. (A60), we get $(x_6, x_5, x_4) = \pm(-11, 1, 0)$ or $(0, 0, 0)$, which implies $|x_8| + 15|x_7| + 104|x_6| + 440|x_5| + 1260|x_4| + 2548|x_3| + 3640|x_2| + 3432|x_1| + 1430|x_0| = 2860$ or 0, respectively. By combining this with Eq. (A59), we get $\mathbf{x} = \mathbf{0}$.

- When $n = 17$, Eqs. (A59) and (A60) are explicitly written as

$$|x_{17/2}| + 16|x_{15/2}| + 119|x_{13/2}| + 544|x_{11/2}| + 1700|x_{9/2}| + 3808|x_{7/2}| + 6188|x_{5/2}| + 7072|x_{3/2}| + 4862|x_{1/2}| \leq 2t, \quad (\text{A143})$$

$$x_{17/2} + 16x_{15/2} + 119x_{13/2} + 544x_{11/2} + 1700x_{9/2} + 3808x_{7/2} + 6188x_{5/2} + 7072x_{3/2} + 4862x_{1/2} = 0, \quad (\text{A144})$$

$$x_{15/2} + 14x_{13/2} + 90x_{11/2} + 350x_{9/2} + 910x_{7/2} + 1638x_{5/2} + 2002x_{3/2} + 1430x_{1/2} = 0, \quad (\text{A145})$$

$$x_{13/2} + 12x_{11/2} + 65x_{9/2} + 208x_{7/2} + 429x_{5/2} + 572x_{3/2} + 429x_{1/2} = 0. \quad (\text{A146})$$

If $t \geq 1792$, Lemma 10 implies that Eqs. (A59) and (A60) have a nontrivial integer solution. If $t < 1792$, any integer solution $\mathbf{x}$ satisfies $x_{7/2} = x_{5/2} = x_{3/2} = x_{1/2} = 0$, $|x_{13/2}| \leq 15$, $|x_{11/2}| \leq 3$, and $|x_{9/2}| \leq 1$ by Lemma 4. By these conditions and Eq. (A60), we get $(x_{13/2}, x_{11/2}, x_{9/2}) = \pm(-12, 1, 0)$ or $(0, 0, 0)$, which implies $|x_{17/2}| + 16|x_{15/2}| + 119|x_{13/2}| + 544|x_{11/2}| + 1700|x_{9/2}| + 3808|x_{7/2}| + 6188|x_{5/2}| + 7072|x_{3/2}| + 4862|x_{1/2}| = 3584$ or 0, respectively. By combining this with Eq. (A59), we get $\mathbf{x} = \mathbf{0}$. □

Appendix B: Technical lemmas

In this appendix, we show several lemmas used in the proof of the main statements.

For the proofs of Lemmas 13 and 14, we prepare a basic property of a compact abelian matrix Lie group.

Lemma 12. *Let $l \in \mathbb{N}$, $\mathcal{Y}$ be a linear subspace of $\mathbb{R}^l$, $H := \exp(i \cdot \text{diag}(\mathcal{Y}))$ be compact. Then, the Lie algebra $\mathfrak{h}$ of H is $\text{diag}(\mathcal{Y})$.*

Proof. Since H is a Lie subgroup of $\exp(i \cdot \text{diag}(\mathbb{R}^l))$, and the Lie algebra of $\exp(i \cdot \text{diag}(\mathbb{R}^l))$ is $\text{diag}(\mathbb{R}^l)$, the Lie algebra $\mathfrak{h}$ of H is a subset of $\text{diag}(\mathbb{R}^l)$. Thus, $\mathfrak{h}$ is given by $\mathfrak{h} = \{A \in \text{diag}(\mathbb{R}^l) \mid \forall \theta \in \mathbb{R} \exp(i\theta A) \in \exp(i \cdot \text{diag}(\mathcal{Y}))\}$, and it is sufficient to show that $\mathfrak{h} = \text{diag}(\mathcal{Y})$. Since $\mathfrak{h} \supset \text{diag}(\mathcal{Y})$ is trivial, we show that $\mathfrak{h} \subset \text{diag}(\mathcal{Y})$ in the following. We take arbitrary $A \in \mathfrak{h}$. Then, for any $\theta \in \mathbb{R}$, $\exp(i\theta A) \in \exp(i \cdot \text{diag}(\mathcal{Y}))$. When we define $\mathbf{a} := \text{diag}^{-1}(A)$, it can be equivalently expressed as $\theta \mathbf{a} = \mathbf{y} + 2\pi \mathbf{c}$ with some $\mathbf{y} \in \mathcal{Y}$ and $\mathbf{c} \in \mathbb{Z}^l$. We decompose $\mathbf{a}$ as $\mathbf{a} = \mathbf{b} + \mathbf{b}^\perp$ with some $\mathbf{b} \in \mathcal{Y}$ and $\mathbf{b}^\perp \in \mathcal{Y}^\perp$. By taking the inner product of $\theta \mathbf{a}$ and $\mathbf{b}^\perp$, we have $\theta \|\mathbf{b}^\perp\|^2 = 2\pi \langle \mathbf{c}, \mathbf{b}^\perp \rangle$. Since we can take such $\mathbf{c} \in \mathbb{Z}^l$ for all $\theta \in \mathbb{R}$, we get $\{\theta \|\mathbf{b}^\perp\|^2 \mid \theta \in \mathbb{R}\} \subset \{2\pi \langle \mathbf{c}, \mathbf{b}^\perp \rangle \mid \mathbf{c} \in \mathbb{Z}^l\}$. Since the r.h.s. of this is countable, the l.h.s. is also countable. We therefore get $\|\mathbf{b}^\perp\| = 0$, which implies that $\mathbf{a} \in \mathcal{Y}$, i.e., $A \in \text{diag}(\mathcal{Y})$. □

By using the lemma above, we show properties of the group of relative phases for the proof of Lemma 14.

Lemma 13. *Let $n \in \mathbb{N}$, R be a unitary representation of a group G , Λ be the set of the labels of the inequivalent irreducible representations appearing in R , Γ be a finite set, $\mathcal{S}^\gamma$ be a connected compact subgroup of $\mathcal{U}_{n,G,R}$ for all $\gamma \in \Gamma$, h be a function $\mathcal{L}_{n,G,R}$ to $\mathbb{C}^{\Lambda \times \Lambda}$ defined by*

$$h(A) := \text{diag}((\det(A_\lambda))_{\lambda \in \Lambda}) \quad \forall A \in \mathcal{L}_{n,G,R} \quad (\text{B1})$$

with A_λ determined by Eq. (12), and $\tilde{\mathcal{V}}$ be defined by Eq. (27). Then, $h(\langle \bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma \rangle) = \exp(i \cdot \text{diag}(\tilde{\mathcal{V}}))$, and there exist some $J \in \mathbb{N}$ and some orthogonal basis $\{\mathbf{v}_j\}_{j \in \{1,2,\dots,J\}}$ of $\tilde{\mathcal{V}}$ such that $\mathbf{v}_j \in \mathbb{Q}^\Lambda$ for all $j \in \{1,2,\dots,J\}$.

Proof. First, we show that $h(\langle \bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma \rangle) = \exp(i \cdot \text{diag}(\tilde{\mathcal{V}}))$. Since h satisfies $h(AB) = h(BA)$ for all $A, B \in \mathcal{L}_{n,G,R}$, we have $h(\langle \bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma \rangle) = h(\mathcal{T})$, where $\mathcal{T} := \{e^{i\theta} \prod_{\gamma \in \Gamma} U^\gamma \mid \theta \in \mathbb{R}, U^\gamma \in \mathcal{S}^\gamma \forall \gamma \in \Gamma\}$. Thus, it is sufficient to show that

$$h(\mathcal{T}) = \exp(i \cdot \text{diag}(\tilde{\mathcal{V}})). \quad (\text{B2})$$

We note that for any $\theta \in \mathbb{R}$ and $A^\gamma \in \mathfrak{s}^\gamma$, we have

$$\begin{aligned}
h \left(e^{i\theta} \prod_{\gamma \in \Gamma} e^{iA^\gamma} \right) &= \text{diag} \left(\left(\det \left(e^{i\theta} \prod_{\gamma \in \Gamma} e^{iA_\lambda^\gamma} \right) \right)_{\lambda \in \Lambda} \right) \\
&= \text{diag} \left(\left(e^{i\theta m_\lambda} \prod_{\gamma \in \Gamma} e^{i \text{tr}(A_\lambda^\gamma)} \right)_{\lambda \in \Lambda} \right) \\
&= \exp \left(i \cdot \text{diag} \left(\left(\theta m_\lambda + \sum_{\gamma \in \Gamma} \text{tr}(A_\lambda^\gamma) \right)_{\lambda \in \Lambda} \right) \right) \\
&= \exp \left(i \cdot \text{diag} \left(\theta \mathbf{m} + \sum_{\gamma \in \Gamma} \mathbf{f}(A^\gamma) \right) \right), \tag{B3}
\end{aligned}$$

where A_λ^γ is defined by $A^\gamma = \sum_{\lambda \in \Lambda} F_\lambda(\text{id}(\mathbb{C}^{r_\lambda}) \otimes A_\lambda^\gamma) F_\lambda^\dagger$. For the proof of $h(\mathcal{T}) \subset \exp(i \cdot \text{diag}(\tilde{\mathcal{V}}))$, for any $U \in \mathcal{T}$, we can take some $\theta \in \mathbb{R}$ and $U^\gamma \in \mathcal{S}^\gamma$ such that $U = e^{i\theta} \prod_{\gamma \in \Gamma} U^\gamma$. For each $\gamma \in \Gamma$, since $\mathcal{S}^\gamma$ is connected and compact, we can take A^γ such that $e^{iA^\gamma} = U^\gamma$. By Eq. (B3), we have

$$h(U) = h \left(e^{i\theta} \prod_{\gamma \in \Gamma} e^{iA^\gamma} \right) = \exp \left(i \cdot \text{diag} \left(\theta \mathbf{m} + \sum_{\gamma \in \Gamma} \mathbf{f}(A^\gamma) \right) \right) \in \exp(i \cdot \text{diag}(\tilde{\mathcal{V}})). \tag{B4}$$

For the proof of $h(\mathcal{T}) \supset \exp(i \cdot \text{diag}(\tilde{\mathcal{V}}))$, we take arbitrary $\mathbf{v} \in \tilde{\mathcal{V}}$. By the definition of $\tilde{\mathcal{V}}$, we can take some $\theta \in \mathbb{R}$ and $A^\gamma \in \mathfrak{s}^\gamma$ such that $\mathbf{v} = \theta \mathbf{m} + \sum_{\gamma \in \Gamma} \mathbf{f}(A^\gamma)$. By Eq. (B3), we have

$$\exp(i \cdot \text{diag}(\mathbf{v})) = \exp \left(i \cdot \text{diag} \left(\theta \mathbf{m} + \sum_{\gamma \in \Gamma} \mathbf{f}(A^\gamma) \right) \right) = h \left(e^{i\theta} \prod_{\gamma \in \Gamma} e^{iA^\gamma} \right) \in h(\mathcal{T}). \tag{B5}$$

By Eqs. (B4) and (B5), we get Eq. (B2).

Next, we show that there exist some $J \in \mathbb{N}$ and some orthogonal basis $\{\mathbf{v}_j\}_{j=1}^J$ of $\tilde{\mathcal{V}}$ such that $\mathbf{v}_j \in \mathbb{Q}^\Lambda$. Since $\mathcal{T}$ is a finite product of compact set, $\mathcal{T}$ is compact. The continuity of h implies that $h(\mathcal{T})$ is compact. By the construction of h and $\mathcal{T}$, $h(\mathcal{T})$ is an abelian Lie group. By Corollary 1.103 of Ref. [53], $h(\mathcal{T})$ is isomorphic to a torus $\exp(i \cdot \text{diag}(\mathbb{R}^J))$ with some $J \in \mathbb{N}$, where J is the dimension of a torus. We take an isomorphism ϕ from $\exp(i \cdot \text{diag}(\mathbb{R}^J))$ to $h(\mathcal{T})$. By Eq. (B2), ϕ gives an isomorphism from $\exp(i \cdot \text{diag}(\mathbb{R}^J))$ to $\exp(i \cdot \text{diag}(\tilde{\mathcal{V}}))$. By Lemma 12, the Lie algebras of these two Lie groups are $\text{diag}(\mathbb{R}^J)$ and $\text{diag}(\tilde{\mathcal{V}})$, respectively. Thus, the derivative $d\phi$ of ϕ at the identity gives an isomorphism from $\text{diag}(\mathbb{R}^J)$ to $\text{diag}(\tilde{\mathcal{V}})$. We denote the standard basis of $\mathbb{R}^J$ by $\{\mathbf{u}_j\}_{j=1}^J$, and define $\tilde{\mathbf{u}}_j \in \mathbb{R}^\Lambda$ by $\text{diag}(\tilde{\mathbf{u}}_j) := d\phi(\text{diag}(\mathbf{u}_j))$ for all $j \in \{1, 2, \dots, J\}$. Then, $\{\tilde{\mathbf{u}}_j\}_{j=1}^J$ is a basis of $\tilde{\mathcal{V}}$. By noting that $\exp(i2\pi \cdot \text{diag}(\tilde{\mathbf{u}}_j)) = \phi(\exp(i2\pi \cdot \text{diag}(\mathbf{u}_j))) = I$, we have $\tilde{\mathbf{u}}_j \in \mathbb{Z}^\Lambda$. We get an orthogonal basis $\{\mathbf{v}_j\}_{j \in \{1, 2, \dots, J\}}$ of $\tilde{\mathcal{V}}$ by the Gram-Schmidt orthogonalization, i.e., $\mathbf{v}_j := \tilde{\mathbf{u}}_j - \sum_{j'=1}^{j-1} (\langle \mathbf{v}_{j'}, \tilde{\mathbf{u}}_j \rangle / \|\mathbf{v}_{j'}\|^2) \mathbf{v}_{j'}$, and the basis vectors satisfy $\mathbf{v} \in \mathbb{Q}^\Lambda$ for all $j \in \{1, 2, \dots, J\}$. $\square$

By using the two lemmas above, we show the equivalent conditions to the universality of the gate set. We use the following lemma in the explanation below Theorem 1.

Lemma 14. *Let $n \in \mathbb{N}$, R be a unitary representation of a group G on n qudits, Λ be the set of the labels of the inequivalent irreducible representations appearing in R , Γ be a finite set, $\mathcal{S}^\gamma$ be a connected compact subgroup of $\mathcal{U}_{n,G,R}$ for all $\gamma \in \Gamma$, $\bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma$ be semi-universal for $\mathcal{U}_{n,G,R}$, and $\tilde{\mathcal{V}}$ be defined by Eq. (27). Then, the following three statements are equivalent:*

$$(i) \bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma \text{ is universal for } \mathcal{U}_{n,G,R} \text{ up to the global phase}, \tag{B6}$$

$$(ii) \tilde{\mathcal{V}} = \mathbb{R}^\Lambda, \tag{B7}$$

$$(iii) \tilde{\mathcal{V}}^\perp \cap \mathbb{Z}^\Lambda = \{\mathbf{0}\}. \tag{B8}$$

Proof. First, we prove that $(i) \iff (ii)$. We note that (i) is equivalent to

$$\left\langle \{e^{i\theta}I\}_{\theta \in \mathbb{R}} \cup \bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma \right\rangle \supset \left\{ \sum_{\lambda \in \Lambda} F_\lambda (I \otimes U_\lambda) F_\lambda^\dagger \mid U_\lambda \in \mathrm{U}(m_\lambda) \ \forall \lambda \in \Lambda \right\}. \quad (\text{B9})$$

Since $\bigcup_{\gamma \in \mathcal{S}^\gamma}$ is semi-universal for $\mathcal{U}_{n,G,R}$, the group $\{e^{i\theta}I\}_{\theta \in \mathbb{R}} \cup \bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma$ is also semi-universal for $\mathcal{U}_{n,G,R}$, which can be expressed as

$$\left\langle \{e^{i\theta}I\}_{\theta \in \mathbb{R}} \cup \bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma \right\rangle \supset \left\{ \sum_{\lambda \in \Lambda} F_\lambda (I \otimes U_\lambda) F_\lambda^\dagger \mid U_\lambda \in \mathrm{SU}(m_\lambda) \ \forall \lambda \in \Lambda \right\}, \quad (\text{B10})$$

as we have shown in Eq. (14). By comparing Eqs. (B9) and (B10), (i) is equivalent to $h(\langle \{e^{i\theta}I\}_{\theta \in \mathbb{R}} \cup \bigcup_{\gamma \in \Gamma} \mathcal{S}^\gamma \rangle) = \exp(i \cdot \text{diag}(\mathbb{R}^\Lambda))$, which can be equivalently written as

$$\exp(i \cdot \text{diag}(\tilde{\mathcal{V}})) = \exp(i \cdot \text{diag}(\mathbb{R}^\Lambda)). \quad (\text{B11})$$

by Lemma 13. It is thus sufficient to show that Eq. (B11) $\iff (ii)$. Since the Lie algebras of $\exp(i \cdot \text{diag}(\tilde{\mathcal{V}}))$ and $\exp(i \cdot \text{diag}(\mathbb{R}^\Lambda))$ are $\text{diag}(\tilde{\mathcal{V}})$ and $\text{diag}(\mathbb{R}^\Lambda)$, respectively by Lemma 12, taking the Lie algebras of the both sides of Eq. (B11) gives the proof of Eq. (B11) $\implies (ii)$. The converse $(ii) \implies$ Eq. (B11) is trivial.

Next, we prove that $(ii) \iff (iii)$. The proof of $(ii) \implies (iii)$ is trivial, because (ii) implies $\tilde{\mathcal{V}}^\perp = \{\mathbf{0}\}$. In the following, we show that $(iii) \implies (ii)$. We suppose that (ii) does not hold. Then, we can take some $\mathbf{e}_l \notin \tilde{\mathcal{V}}$ from the standard basis $\{\mathbf{e}_j\}_{j=1}^J$ of $\tilde{\mathcal{V}}$. By Lemma 13, we can take an orthogonal basis $\{\mathbf{v}_j\}_{j=1}^J$ of $\tilde{\mathcal{V}}$ such that $\mathbf{v}_j \in \mathbb{Q}^\Lambda$ for all $j \in \{1, 2, \dots, J\}$. By using this basis, we define $\tilde{\mathbf{d}} := \mathbf{e}_l - \sum_{j=1}^J \langle \mathbf{v}_j, \mathbf{e}_l \rangle / \|\mathbf{v}_j\|^2 \mathbf{v}_j \in \mathbb{Q}^\Lambda \setminus \{\mathbf{0}\}$. We can take some $\alpha \in \mathbb{Q} \setminus \{0\}$ such that $\alpha \tilde{\mathbf{d}} \in \mathbb{Z}^\Lambda$. Then, $\mathbf{d} := \alpha \tilde{\mathbf{d}}$ satisfies $\mathbf{d} \in (\tilde{\mathcal{V}}^\perp \cap \mathbb{Z}^\Lambda) \setminus \{\mathbf{0}\}$. $\square$

For the proof of Lemma 1, we show that the moment operator defined by Eq. (8) is a projection.

Lemma 15. *Let $n, t \in \mathbb{N}$ and $\mathcal{X}$ be a compact unitary subgroup of $\mathcal{U}_n$. Then,*

$$M_{t, \mu_{\mathcal{X}}} = \Pi_{E(\text{Comm}(\Omega_t(\mathcal{X})))}. \quad (\text{B12})$$

where E is defined by Eq. (42), i.e.,

$$E(K) := (K \otimes I) |\eta\rangle \ \forall K \in \mathcal{L}(\mathcal{H}^{\otimes n}), \quad (\text{B13})$$

$$|\eta\rangle := \frac{1}{\sqrt{d^{tn}}} \sum_{j=1}^{d^{tn}} |j\rangle \otimes |j\rangle, \quad (\text{B14})$$

and $\{|j\rangle\}_{j=1}^{d^{tn}}$ is an orthonormal basis of $\mathcal{H}^{\otimes t}$.

Proof. First, we show that $M_{t, \mu_{\mathcal{X}}}$ is a projection. By Corollary 8.31 of Ref. [53], the compactness of $\mathcal{X}$ implies that $\mathcal{X}$ is unimodular, and thus $\mu_{\mathcal{X}}$ is also a right-invariant Haar measure. Then, we have

$$M_{t, \mu_{\mathcal{X}}} = \int_{U \in \mathcal{X}} U^{\otimes t} \otimes U^{*\otimes t} d\mu_{\mathcal{X}}(U) = \int_{U \in \mathcal{X}} (U^\dagger)^{\otimes t} \otimes (U^\dagger)^{* \otimes t} d\mu_{\mathcal{X}}(U) = M_{t, \mu_{\mathcal{X}}}^\dagger. \quad (\text{B15})$$

Since $\mu_{\mathcal{X}}$ is left-invariant, we have

$$\begin{aligned} M_{t, \mu_{\mathcal{X}}}^2 &= \left(\int_{V \in \mathcal{X}} V^{\otimes t} \otimes V^{*\otimes t} d\mu_{\mathcal{X}}(V) \right) \left(\int_{U \in \mathcal{X}} U^{\otimes t} \otimes U^{*\otimes t} d\mu_{\mathcal{X}}(U) \right) \\ &= \int_{V \in \mathcal{X}} \int_{U \in \mathcal{X}} (VU)^{\otimes t} \otimes (VU)^{* \otimes t} d\mu_{\mathcal{X}}(U) d\mu_{\mathcal{X}}(V) \\ &= \int_{V \in \mathcal{X}} \int_{U \in \mathcal{X}} U^{\otimes t} \otimes U^{*\otimes t} d\mu_{\mathcal{X}}(U) d\mu_{\mathcal{X}}(V) \\ &= \int_{U \in \mathcal{X}} U^{\otimes t} \otimes U^{*\otimes t} d\mu_{\mathcal{X}}(U) \end{aligned}$$

$$= M_{t, \mu_{\mathcal{X}}}. \quad (\text{B16})$$

These two relations imply that $M_{t, \mu_{\mathcal{X}}}$ is a projection.

Next, we show that the projection space is $E(\text{Comm}(\Omega_t(\mathcal{X})))$. We note that

$$(U^{\otimes t} \otimes U^{*\otimes t})(L \otimes I) |\eta\rangle = (U^{\otimes t} \otimes U^{*\otimes t})(L \otimes I)(U^{\otimes t} \otimes U^{*\otimes t})^\dagger |\eta\rangle = (U^{\otimes t} L U^{\dagger \otimes t} \otimes I) |\eta\rangle. \quad (\text{B17})$$

By taking the Haar integral for $U \in \mathcal{X}$, we get

$$M_{t, \mu_{\mathcal{X}}}(L \otimes I) |\eta\rangle = \left[\left(\int_{U \in \mathcal{X}} U^{\otimes t} L U^{\dagger \otimes t} d\mu_{\mathcal{X}}(U) \right) \otimes I \right] |\eta\rangle. \quad (\text{B18})$$

For the proof of $\{|\Psi\rangle \in \mathcal{H}^{\otimes 2t} \mid M_{t, \mu_{\mathcal{X}}} |\Psi\rangle = |\Psi\rangle\} \supset E(\text{Comm}(\Omega_t(\mathcal{X})))$, we take arbitrary $|\Psi\rangle \in E(\text{Comm}(\Omega_t(\mathcal{X})))$. Then, $|\Psi\rangle$ can be written as $|\Psi\rangle = (L \otimes I) |\eta\rangle$ with some $L \in \text{Comm}(\Omega_t(\mathcal{X}))$. Thus, by using Eq. (B18), we get

$$M_{t, \mu_{\mathcal{X}}} |\Psi\rangle = M_{t, \mu_{\mathcal{X}}}(L \otimes I) |\eta\rangle = \left[\left(\int_{U \in \mathcal{X}} U^{\otimes t} L U^{\dagger \otimes t} d\mu_{\mathcal{X}}(U) \right) \otimes I \right] |\eta\rangle = (L \otimes I) |\eta\rangle = |\Psi\rangle. \quad (\text{B19})$$

For the proof of $\{|\Psi\rangle \in \mathcal{H}^{\otimes 2t} \mid M_{t, \mu_{\mathcal{X}}} |\Psi\rangle = |\Psi\rangle\} \subset E(\text{Comm}(\Omega_t(\mathcal{X})))$, we take arbitrary $|\Psi\rangle \in \mathcal{H}^{\otimes 2t}$ satisfying $M_{t, \mu_{\mathcal{X}}} |\Psi\rangle = |\Psi\rangle$. We take $L \in \mathcal{L}(\mathcal{H}^{\otimes t})$ such that $|\Psi\rangle = (L \otimes I) |\eta\rangle$. Then, we have

$$M_{t, \mu_{\mathcal{X}}}(L \otimes I) |\eta\rangle = (L \otimes I) |\eta\rangle. \quad (\text{B20})$$

By Eqs. (B18) and (B20), we get

$$\left[\left(\int_{U \in \mathcal{X}} U^{\otimes t} L U^{\dagger \otimes t} d\mu_{\mathcal{X}}(U) \right) \otimes I \right] |\eta\rangle = (L \otimes I) |\eta\rangle, \quad (\text{B21})$$

which implies that

$$\int_{U \in \mathcal{X}} U^{\otimes t} L U^{\dagger \otimes t} d\mu_{\mathcal{X}}(U) = L. \quad (\text{B22})$$

Then, by the left invariance of $\mu_{\mathcal{X}}$, we have

$$V^{\otimes t} L V^{\dagger \otimes t} = \int_{U \in \mathcal{X}} (VU)^{\otimes t} L (VU)^{\dagger \otimes t} d\mu_{\mathcal{X}}(U) = \int_{U \in \mathcal{X}} U^{\otimes t} L U^{\dagger \otimes t} d\mu_{\mathcal{X}}(U) = L \quad \forall V \in \mathcal{X}, \quad (\text{B23})$$

which means that $L \in \text{Comm}(\Omega_t(\mathcal{X}))$. Thus, we have proven that $|\Psi\rangle \in E(\text{Comm}(\Omega_t(\mathcal{X})))$. $\square$

For the second step of the proof of Lemma 2, we prepare the properties of $\mathcal{S}_t$ defined by Eq. (69).

Lemma 16. *Let $t \in \mathbb{N}$, $\mathcal{S}_t$ be defined by Eq. (69), $\sigma \in \mathfrak{S}_t$, V_σ be defined by Eq. (70), Ξ be a finite set, $L_1, L_2, \dots, L_t \in \mathcal{L}(\mathcal{H})$, and $O_\xi \in \mathcal{L}(\mathcal{H})$ for all $\xi \in \Xi$. Then,*

$$\mathcal{S}_t(L_1 \otimes L_2 \otimes \dots \otimes L_t) = \mathcal{S}_t(L_{\sigma(1)} \otimes L_{\sigma(2)} \otimes \dots \otimes L_{\sigma(t)}), \quad (\text{B24})$$

$$\left(\sum_{\xi \in \Xi} O_\xi \right)^{\otimes t} = \sum_{\mathbf{z} \in \mathcal{Z}_t} \frac{t!}{\prod_{\xi \in \Xi} z_\xi!} \mathcal{S}_t \left(\bigotimes_{\xi \in \Xi} O_\xi^{\otimes z_\xi} \right), \quad (\text{B25})$$

where $\mathcal{Z}_t$ is defined by Eq. (75), i.e.,

$$\mathcal{Z}_t := \left\{ \mathbf{z}' \in (\mathbb{Z}_{\geq 0})^\Xi \mid \sum_{(\lambda, \alpha) \in \Xi} z'_{\lambda, \alpha} = t \right\}. \quad (\text{B26})$$

Proof. By the definition of $\mathcal{S}_t$, we directly get Eq. (B24) as follows:

$$\mathcal{S}_t(L_1 \otimes L_2 \otimes \dots \otimes L_t) = \frac{1}{t!} \sum_{\sigma' \in \mathfrak{S}_t} V_{\sigma'} V_\sigma (L_{\sigma(1)} \otimes L_{\sigma(2)} \otimes \dots \otimes L_{\sigma(t)}) V_\sigma^\dagger V_{\sigma'}^\dagger$$

$$\begin{aligned}
&= \frac{1}{t!} \sum_{\sigma' \in \mathfrak{S}_t} V_{\sigma'\sigma} (L_{\sigma(1)} \otimes L_{\sigma(2)} \otimes \cdots \otimes L_{\sigma(t)}) V_{\sigma'\sigma}^\dagger \\
&= \frac{1}{t!} \sum_{\sigma' \in \mathfrak{S}_t} V_{\sigma'} (L_{\sigma(1)} \otimes L_{\sigma(2)} \otimes \cdots \otimes L_{\sigma(t)}) V_{\sigma'}^\dagger \\
&= \mathcal{S}_t (L_{\sigma(1)} \otimes L_{\sigma(2)} \otimes \cdots \otimes L_{\sigma(t)}).
\end{aligned} \tag{B27}$$

In the following, we show Eq. (B25). By the definition of $\mathcal{S}_t$, we have

$$\left(\sum_{\xi \in \Xi} O_\xi \right)^{\otimes t} = \mathcal{S}_t \left(\left(\sum_{\xi \in \Xi} O_\xi \right)^{\otimes t} \right) = \sum_{\xi \in \Xi^t} \mathcal{S}_t \left(\bigotimes_{\zeta \in \Xi} O_\zeta^{c_\zeta(\xi)} \right), \tag{B28}$$

where c is a map from Ξ^t to $\mathcal{Z}_t$, and the ζ component c_ζ of c is defined by

$$c_\zeta(\xi) := \#(\{u \mid \xi_u = \zeta\}). \tag{B29}$$

By noting that the inside of the summation of the r.h.s. of Eq. (B28) is given by $c(\xi)$, we can change the summation index as follows:

$$\sum_{\xi \in \Xi^t} \mathcal{S}_t \left(\bigotimes_{\zeta \in \Xi} O_\zeta^{c_\zeta(\xi)} \right) = \sum_{z \in \mathcal{Z}_t} \#(c^{-1}(z)) \mathcal{S}_t \left(\bigotimes_{\zeta \in \Xi} O_\zeta^{z_\zeta} \right). \tag{B30}$$

By considering the combinatorial interpretation of the multinomial coefficients, we have

$$\#(c^{-1}(z)) = \frac{t!}{\prod_{\zeta \in \Xi} z_\zeta}. \tag{B31}$$

By plugging Eq. (B31) into Eq. (B30), we get Eq. (B25). $\square$

We prepare a lemma about the condition for the existence of solutions of Eqs. (19), (20), and (21). We use (iii) $\implies$ (i) in the second step of the proof of Lemma 2, and (i) $\implies$ (ii) in the second step of the proof of the Lemma 3.

Lemma 17. *Let $t \in \mathbb{N}$, Λ be a finite set, $m_\lambda \in \mathbb{N}$ for all $\lambda \in \Lambda$, $\Xi := \{(\lambda, \alpha) \mid \lambda \in \Lambda, \alpha \in \{1, 2, \dots, m_\lambda\}\}$, $\mathcal{V}$ be a linear subspace of $\mathbb{R}^\Lambda$, and $\mathcal{W} := \Delta^{-1}(\mathcal{V})$, where $\Delta : \mathbb{R}^\Xi \rightarrow \mathbb{R}^\Lambda$ is defined by Eq. (52), i.e.,*

$$\Delta(\mathbf{w}) = (\Delta_\lambda(\mathbf{w}))_{\lambda \in \Lambda} \quad \forall \mathbf{w} \in \mathbb{R}^\Xi \tag{B32}$$

with $\Delta_\lambda : \mathbb{R}^\Xi \rightarrow \mathbb{R}$ defined by

$$\Delta_\lambda(\mathbf{w}) = \sum_{\alpha=1}^{m_\lambda} w_{\lambda, \alpha} \quad \forall \mathbf{w} \in \mathbb{R}^\Xi. \tag{B33}$$

Then, the following three statements are equivalent:

(i) There exists $\mathbf{x} = (x_\lambda)_{\lambda \in \Lambda} \in \mathbb{Z}^\Lambda$ such that

$$\mathbf{x} \neq \mathbf{0}, \tag{B34}$$

$$\sum_{\lambda \in \Lambda} m_\lambda |x_\lambda| \leq 2t, \tag{B35}$$

$$\sum_{\lambda \in \Lambda} m_\lambda x_\lambda = 0, \tag{B36}$$

$$\sum_{\lambda \in \Lambda} v_\lambda x_\lambda = 0 \quad \forall \mathbf{v} = (v_\lambda)_{\lambda \in \Lambda} \in \mathcal{V}. \tag{B37}$$

(ii) There exist $\mathbf{y} = (y_\lambda)_{\lambda \in \Lambda}, \mathbf{y}' = (y'_\lambda)_{\lambda \in \Lambda} \in (\mathbb{Z}_{\geq 0})^\Lambda$ such that

$$\mathbf{y} \neq \mathbf{y}', \tag{B38}$$

$$\sum_{\lambda \in \Lambda} m_\lambda y_\lambda = \sum_{\lambda \in \Lambda} m_\lambda y'_\lambda \leq t, \quad (\text{B39})$$

$$\sum_{\lambda \in \Lambda} v_\lambda y_\lambda = \sum_{\lambda \in \Lambda} v_\lambda y'_\lambda \quad \forall \mathbf{v} = (v_\lambda)_{\lambda \in \Lambda} \in \mathcal{V}. \quad (\text{B40})$$

(iii) There exist $\mathbf{z} = (z_{\lambda,\alpha})_{(\lambda,\alpha) \in \Xi}$, $\mathbf{z}' = (z'_{\lambda,\alpha})_{(\lambda,\alpha) \in \Xi} \in (\mathbb{Z}_{\geq 0})^\Xi$ such that

$$\mathbf{z} \neq \mathbf{z}', \quad (\text{B41})$$

$$\sum_{(\lambda,\alpha) \in \Xi} z_{\lambda,\alpha} = \sum_{(\lambda,\alpha) \in \Xi} z'_{\lambda,\alpha} \leq t, \quad (\text{B42})$$

$$\sum_{(\lambda,\alpha) \in \Xi} w_{\lambda,\alpha} z_{\lambda,\alpha} = \sum_{(\lambda,\alpha) \in \Xi} w_{\lambda,\alpha} z'_{\lambda,\alpha} \quad \forall \mathbf{w} = (w_{\lambda,\alpha})_{(\lambda,\alpha) \in \Xi} \in \mathcal{W}. \quad (\text{B43})$$

Proof. First, we show (i) $\implies$ (ii). We suppose that we can take $\mathbf{x} \in \mathbb{Z}^\Lambda$ satisfying Eqs. (B34), (B35), (B36), and (B37). We define $\mathbf{y}, \mathbf{y}' \in (\mathbb{Z}_{\geq 0})^\Lambda$ by

$$y_\lambda := \frac{|x_\lambda| + x_\lambda}{2}, \quad (\text{B44})$$

$$y'_\lambda := \frac{|x_\lambda| - x_\lambda}{2}, \quad (\text{B45})$$

which implies that $y_\lambda - y'_\lambda = x_\lambda$. Thus Eq. (B38), the equality in Eq. (B39), and Eq. (B40) directly follow from Eqs. (B34), (B36), and (B37), respectively. The inequality in Eq. (B39) can be shown as follows:

$$\sum_{\lambda \in \Lambda} m_\lambda y_\lambda = \frac{1}{2} \left(\sum_{\lambda \in \Lambda} m_\lambda y_\lambda + \sum_{\lambda \in \Lambda} m_\lambda y'_\lambda \right) = \frac{1}{2} \sum_{\lambda \in \Lambda} m_\lambda (y_\lambda + y'_\lambda) = \frac{1}{2} \sum_{\lambda \in \Lambda} m_\lambda |x_\lambda| \leq t. \quad (\text{B46})$$

Next, we show (ii) $\implies$ (iii). We suppose that we can take $\mathbf{y}, \mathbf{y}' \in (\mathbb{Z}_{\geq 0})^\Lambda$ satisfying Eqs. (B38), (B39) and (B40). We define $\mathbf{z}, \mathbf{z}' \in (\mathbb{Z}_{\geq 0})^\Xi$ by $z_{\lambda,\alpha} := y_\lambda$ and $z'_{\lambda,\alpha} := y'_\lambda$ for all $(\lambda, \alpha) \in \Xi$. Then, Eq. (B41) directly follows from Eq. (B38). We note that

$$\sum_{(\lambda,\alpha) \in \Xi} z_{\lambda,\alpha} = \sum_{\lambda \in \Lambda} \sum_{\alpha=1}^{m_\lambda} y_\lambda = \sum_{\lambda \in \Lambda} m_\lambda y_\lambda, \quad (\text{B47})$$

$$\sum_{(\lambda,\alpha) \in \Xi} w_{\lambda,\alpha} z_{\lambda,\alpha} = \sum_{\lambda \in \Lambda} \left(\sum_{\alpha=1}^{m_\lambda} w_{\lambda,\alpha} \right) y_\lambda = \sum_{\lambda \in \Lambda} \Delta_\lambda(\mathbf{w}) y_\lambda, \quad (\text{B48})$$

and in the same way, we can show that $\sum_{(\lambda,\alpha) \in \Xi} z'_{\lambda,\alpha} = \sum_{\lambda \in \Lambda} m_\lambda y'_\lambda$ and $\sum_{(\lambda,\alpha) \in \Xi} w_{\lambda,\alpha} z'_{\lambda,\alpha} = \sum_{\lambda \in \Lambda} \Delta_\lambda(\mathbf{w}) y'_\lambda$. Since $\Delta(\mathbf{w}) \in \mathcal{V}$, Eqs. (B42) and (B43) directly follow from Eqs. (B39) and (B40).

Finally, we show (iii) $\implies$ (i). We suppose that we can take $\mathbf{z}, \mathbf{z}' \in (\mathbb{Z}_{\geq 0})^\Xi$ satisfying Eq. (B41), (B42), and (B43). We take arbitrary $\mu \in \Lambda$ and $\beta, \beta' \in \{1, 2, \dots, m_\mu\}$. By noting that $\mathbf{w} \in \mathcal{W}$ when $w_{\lambda,\alpha} := \delta_{\lambda,\mu}(\delta_{\alpha,\beta} - \delta_{\alpha,\beta'})$, Eq. (B43) implies that $z_{\mu,\beta} - z_{\mu,\beta'} = z'_{\mu,\beta} - z'_{\mu,\beta'}$, which yields $z_{\mu,\beta} - z'_{\mu,\beta} = z_{\mu,\beta'} - z'_{\mu,\beta'}$. Since this holds for all $\beta, \beta' \in \{1, 2, \dots, m_\mu\}$, $z_{\lambda,\alpha} - z'_{\lambda,\alpha}$ is independent of α . Thus we can define $\mathbf{x} \in \mathbb{Z}^\Lambda$ such that

$$x_\lambda = z_{\lambda,\alpha} - z'_{\lambda,\alpha} \quad \forall \alpha \in \{1, 2, \dots, m_\lambda\}, \lambda \in \Lambda. \quad (\text{B49})$$

By this relation, Eq. (B34) follows from Eq. (B41). By using Eqs. (B49) and (B42), we get Eq. (B35) as follows:

$$\sum_{\lambda \in \Lambda} m_\lambda |x_\lambda| = \sum_{(\lambda,\alpha) \in \Xi} |x_\lambda| = \sum_{(\lambda,\alpha) \in \Xi} |z_{\lambda,\alpha} - z'_{\lambda,\alpha}| \leq \sum_{(\lambda,\alpha) \in \Xi} (z_{\lambda,\alpha} + z'_{\lambda,\alpha}) = \sum_{(\lambda,\alpha) \in \Xi} z_{\lambda,\alpha} + \sum_{(\lambda,\alpha) \in \Xi} z'_{\lambda,\alpha} \leq 2t, \quad (\text{B50})$$

where we used the triangle inequality in the first inequality. Similarly, by using Eqs. (B49) and (B42), we get Eq. (B36) as follows:

$$\sum_{\lambda \in \Lambda} m_\lambda x_\lambda = \sum_{(\lambda,\alpha) \in \Xi} x_\lambda = \sum_{(\lambda,\alpha) \in \Xi} (z_{\lambda,\alpha} - z'_{\lambda,\alpha}) = \sum_{(\lambda,\alpha) \in \Xi} z_{\lambda,\alpha} - \sum_{(\lambda,\alpha) \in \Xi} z'_{\lambda,\alpha} = 0. \quad (\text{B51})$$

For any $\lambda \in \Lambda$, we arbitrarily take $\beta_\lambda \in \{1, 2, \dots, m_\lambda\}$. For any $\mathbf{v} \in \mathcal{V}$, by noting that $\mathbf{w} \in \mathcal{W}$ when $w_{\lambda,\alpha} := v_\lambda \delta_{\alpha,\beta_\lambda}$, Eq. (B43) implies that $\sum_{\lambda \in \Lambda} z_{\lambda,\beta_\lambda} v_\lambda = \sum_{\lambda \in \Lambda} z'_{\lambda,\beta_\lambda} v_\lambda$, which implies Eq. (B37). $\square$

For the first step of the proof of Lemma 3, we show the property of the totally antisymmetric state.

Lemma 18. Let $m \in \mathbb{N}$, A be a linear operator on $\mathbb{C}^m$ and $|\chi(\mathbb{C}^m)\rangle$ and ω_m be defined by Eqs. (88) and (89), respectively, i.e.,

$$|\chi(\mathbb{C}^m)\rangle := \frac{1}{\sqrt{m!}} \sum_{\sigma \in \mathfrak{S}_m} \text{sgn}(\sigma) \bigotimes_{\alpha=1}^m |\sigma(\alpha)\rangle, \quad (\text{B52})$$

$$\omega_t(A) := \sum_{s=1}^t I^{\otimes s-1} \otimes A \otimes I^{\otimes t-s}. \quad (\text{B53})$$

Then,

$$\omega_m(A) |\chi(\mathbb{C}^m)\rangle = \text{tr}(A) |\chi(\mathbb{C}^m)\rangle. \quad (\text{B54})$$

Proof. By using V_σ defined by Eq. (70), we have

$$|\chi(\mathbb{C}^m)\rangle = \frac{1}{\sqrt{m!}} \sum_{\sigma \in \mathfrak{S}_m} \text{sgn}(\sigma) V_{\sigma^{-1}} \left(\bigotimes_{\alpha=1}^m |\alpha\rangle \right). \quad (\text{B55})$$

This implies that

$$\omega_m(A) |\chi(\mathbb{C}^m)\rangle = \frac{1}{\sqrt{m!}} \sum_{\sigma \in \mathfrak{S}_m} \text{sgn}(\sigma) \omega_m(A) V_{\sigma^{-1}} \left(\bigotimes_{\alpha=1}^m |\alpha\rangle \right) = \frac{1}{\sqrt{m!}} \sum_{\sigma \in \mathfrak{S}_m} \text{sgn}(\sigma) V_{\sigma^{-1}} \omega_m(A) \left(\bigotimes_{\alpha=1}^m |\alpha\rangle \right). \quad (\text{B56})$$

We note that

$$\begin{aligned} \omega_m(A) \left(\bigotimes_{\alpha=1}^m |\alpha\rangle \right) &= \sum_{\beta=1}^m (I^{\otimes \beta} \otimes A \otimes I^{\otimes m-\beta}) \left[\left(\bigotimes_{\alpha=1}^{\beta-1} |\alpha\rangle \right) \otimes |\beta\rangle \otimes \left(\bigotimes_{\alpha=\beta+1}^m |\alpha\rangle \right) \right] \\ &= \sum_{\beta=1}^m \sum_{\beta'=1}^m \left(\bigotimes_{\alpha=1}^{\beta-1} |\alpha\rangle \right) \otimes a_{\beta',\beta} |\beta'\rangle \otimes \left(\bigotimes_{\alpha=\beta+1}^m |\alpha\rangle \right) \\ &= \sum_{\beta=1}^m \sum_{\beta'=1}^m \frac{I + V_{\tau_{\beta,\beta'}^{-1}}}{2} \left[\left(\bigotimes_{\alpha=1}^{\beta-1} |\alpha\rangle \right) \otimes a_{\beta',\beta} |\beta'\rangle \otimes \left(\bigotimes_{\alpha=\beta+1}^m |\alpha\rangle \right) \right], \end{aligned} \quad (\text{B57})$$

where $a_{\beta',\beta} := \langle \beta' | A | \beta \rangle$, and $\tau_{\beta,\beta'}$ is the transposition between β and β' . By plugging Eq. (B57) into Eq. (B56), we get

$$\omega_m(A) |\chi(\mathbb{C}^m)\rangle = \frac{1}{\sqrt{m!}} \sum_{\beta=1}^m \sum_{\beta'=1}^m \left(\sum_{\sigma \in \mathfrak{S}_m} \text{sgn}(\sigma) V_{\sigma^{-1}} \frac{I + V_{\tau_{\beta,\beta'}^{-1}}}{2} \right) \left[\left(\bigotimes_{\alpha=1}^{\beta-1} |\alpha\rangle \right) \otimes a_{\beta',\beta} |\beta'\rangle \otimes \left(\bigotimes_{\alpha=\beta+1}^m |\alpha\rangle \right) \right]. \quad (\text{B58})$$

We note that

$$\begin{aligned} \sum_{\sigma \in \mathfrak{S}_m} \text{sgn}(\sigma) V_{\sigma^{-1}} \frac{I + V_{\tau_{\beta,\beta'}^{-1}}}{2} &= \sum_{\sigma \in \mathfrak{S}_m} \frac{1}{2} \left(\text{sgn}(\sigma) V_{\sigma^{-1}} + \text{sgn}(\tau_{\beta,\beta'}) \text{sgn}(\tau_{\beta,\beta'} \sigma) V_{(\tau_{\beta,\beta'} \sigma)^{-1}} \right) \\ &= \sum_{\sigma \in \mathfrak{S}_m} \frac{1 + \text{sgn}(\tau_{\beta,\beta'})}{2} \text{sgn}(\sigma) V_{\sigma^{-1}} \\ &= \delta_{\beta,\beta'} \sum_{\sigma \in \mathfrak{S}_m} \text{sgn}(\sigma) V_{\sigma^{-1}}. \end{aligned} \quad (\text{B59})$$

By plugging Eq. (B59) into Eq. (B58), we get

$$\omega_m(A) |\chi(\mathbb{C}^m)\rangle = \frac{1}{\sqrt{m!}} \sum_{\beta=1}^m \sum_{\beta'=1}^m \delta_{\beta,\beta'} \sum_{\sigma \in \mathfrak{S}_m} \text{sgn}(\sigma) V_{\sigma^{-1}} \left[\left(\bigotimes_{\alpha=1}^{\beta-1} |\alpha\rangle \right) \otimes a_{\beta',\beta} |\beta'\rangle \otimes \left(\bigotimes_{\alpha=\beta+1}^m |\alpha\rangle \right) \right]$$

$$\begin{aligned}
&= \frac{1}{\sqrt{m!}} \sum_{\beta=1}^m \sum_{\sigma \in \mathfrak{S}_m} \text{sgn}(\sigma) V_{\sigma^{-1}} \left[\left(\bigotimes_{\alpha=1}^{\beta-1} |\alpha\rangle \right) \otimes a_{\beta,\beta} |\beta\rangle \otimes \left(\bigotimes_{\alpha=\beta+1}^m |\alpha\rangle \right) \right] \\
&= \left(\sum_{\beta=1}^m a_{\beta,\beta} \right) \left[\frac{1}{\sqrt{m!}} \sum_{\sigma \in \mathfrak{S}_m} \text{sgn}(\sigma) V_{\sigma^{-1}} \left(\bigotimes_{\alpha=1}^m |\alpha\rangle \right) \right].
\end{aligned} \tag{B60}$$

By Eqs. (B55) and (B60), we get Eq. (B54). $\square$

For the third step of the proof of Lemma 3, we show that the commutant of a Lie group is the same as that of its associated Lie algebra.

Lemma 19. *Let $n, t \in \mathbb{N}$, $\mathcal{S}$ be a connected compact Lie subgroup of $\mathcal{U}_n$ and $\mathfrak{s}$ be its associated Lie algebra. Then,*

$$\text{Comm}(\Omega_t(\mathcal{S})) = \text{Comm}(\omega_t(\mathfrak{s})). \tag{B61}$$

Proof. First, we show that $\text{Comm}(\Omega_t(\mathcal{S})) \subset \text{Comm}(\omega_t(\mathfrak{s}))$. We take arbitrary $L \in \text{Comm}(\Omega_t(\mathcal{S}))$. For any $A \in \mathfrak{s}$ and $\theta \in \mathbb{R}$, we have $e^{i\theta A} \in \mathcal{S}$, which implies that $e^{i\theta \omega_t(A)} = \Omega_t(e^{i\theta A}) \in \Omega_t(\mathcal{S})$. Thus we have $[L, e^{i\theta A}] = 0$. By taking the derivative at $\theta = 0$, we get $[L, A] = 0$. Since this holds for all $A \in \mathfrak{s}$, we have $L \in \text{Comm}(\mathfrak{s})$.

Next, we show that $\text{Comm}(\Omega_t(\mathcal{S})) \supset \text{Comm}(\omega_t(\mathfrak{s}))$. We take arbitrary $L \in \text{Comm}(\omega_t(\mathfrak{s}))$. Since $\mathcal{S}$ is connected and compact, every $U \in \mathcal{S}$ can be written as $U = e^{iA}$ with some $A \in \mathfrak{s}$. Thus we have $[L, \Omega_t(U)] = [L, e^{i\omega_t(A)}] = 0$. Since this holds for all $U \in \mathcal{S}$, we get $L \in \text{Comm}(\Omega_t(\mathcal{S}))$. $\square$

We show that in Theorem 1, Eq. (21) is equivalent to Eq. (23) in a spacial case.

Lemma 20. *Let $n \in \mathbb{N}$, T be a unitary representation of a group G on a single qudit, $R = T^{\otimes n}$, Λ be the set of the labels of the inequivalent irreducible representations appearing in R , $\mathbf{f}$ be defined by Eq. (22), Γ be a set of subsets of $\{1, 2, \dots, n\}$, $k := \max_{\gamma \in \Gamma} \#\gamma$, $\mathcal{V} := \text{span}_{\mathbb{R}}(\{\mathbf{f}(A) \mid \exists \gamma \in \Gamma \text{ s.t. } A \in \mathbf{u}_{n,G,R}^\gamma\})$, $\mathcal{C} := \{\mathbf{f}(A \otimes \mathbb{I}^{\otimes n-k}) \mid A \in \mathcal{L}_{k,G,T^{\otimes k}}\}$, and $\mathbf{x} \in \mathbb{Z}^\Lambda$. Then, $\sum_{\lambda \in \Lambda} v_\lambda x_\lambda = 0$ for all $\mathbf{v} \in \mathcal{V}$ is equivalent to $\sum_{\lambda \in \Lambda} c_\lambda x_\lambda = 0$ for all $\mathbf{c} \in \mathcal{C}$.*

Proof. For any $\gamma \in \Gamma$, we can take some qudit permutation operator P such that the map $\mathcal{E}_{\gamma,P} : \mathbf{u}_{\#\gamma,G,T^{\otimes \#\gamma}} \rightarrow \mathbf{u}_{n,G,T^{\otimes n}}^\gamma$ defined by $\mathcal{E}_{\gamma,P}(A) := P(A \otimes \mathbb{I}^{\otimes n-\#\gamma})P^\dagger$ is a bijection. Since R is given by $T^{\otimes n}$, we have $P \in \mathcal{U}_{n,G,R}$, which implies that P can be written as $P = \sum_{\lambda \in \Lambda} F_\lambda(I \otimes P_\lambda)F_\lambda^\dagger$ with some $P_\lambda \in \mathcal{U}(\mathcal{M}_\lambda)$. $B := A \otimes \mathbb{I}^{\otimes n-\#\gamma}$ can also be written as $B = \sum_{\lambda \in \Lambda} F_\lambda(I \otimes B_\lambda)F_\lambda^\dagger$ with some $B \in \mathcal{L}(\mathbb{C}^{m_\lambda})$. Then, we have $\mathbf{f}(\mathcal{E}_{\gamma,P}(A)) = (\text{tr}(P_\lambda B_\lambda P_\lambda^\dagger))_{\lambda \in \Lambda} = (\text{tr}(B_\lambda))_{\lambda \in \Lambda} = \mathbf{f}(A \otimes \mathbb{I}^{\otimes n-\#\gamma})$. By taking the range of this equation over $A \in \mathbf{u}_{\#\gamma,G,T^{\otimes \#\gamma}}$, we get $\{\mathbf{f}(A) \mid A \in \mathbf{u}_{n,G,T^{\otimes n}}^\gamma\} = \{\mathbf{f}(A \otimes \mathbb{I}^{\otimes n-\#\gamma}) \mid A \in \mathbf{u}_{\#\gamma,G,T^{\otimes \#\gamma}}\}$, which implies that $\mathcal{V} = \{\mathbf{f}(A \otimes \mathbb{I}^{\otimes n-k}) \mid A \in \mathbf{u}_{k,G,T^{\otimes k}}\}$. Since we have $\mathcal{L}_{k,G,T^{\otimes k}} = \mathbf{u}_{k,G,T^{\otimes k}} + i\mathbf{u}_{k,G,T^{\otimes k}}$, it holds that $\mathcal{C} = \mathcal{V} + i\mathcal{V}$. Thus, $\sum_{\lambda \in \Lambda} v_\lambda x_\lambda = 0$ for all $\mathbf{v} \in \mathcal{V}$ is equivalent to $\sum_{\lambda \in \Lambda} c_\lambda x_\lambda = 0$ for all $\mathbf{c} \in \mathcal{C}$. $\square$

We give a rough sufficient condition for the assumptions in Lemma 6.

Lemma 21. *Let $n, k \in \mathbb{N}$ satisfy $k \geq 2$ and $n \geq 2^k$, and $b_{n,j}$ be defined by Eq. (A18), i.e.,*

$$b_{n,j} := \frac{2^{\lfloor j/2 \rfloor}}{\lfloor \frac{j}{2} \rfloor!} \prod_{\alpha=1}^{\lfloor j/2 \rfloor} (n - j + 2\alpha - 1). \tag{B62}$$

Then, $b_{n,k} \leq \binom{n}{\lfloor k/2 \rfloor + 1}$. Moreover, when k is odd, $b_{n,k} \leq b_{n,k+1}$.

Proof. For the proof of $b_{n,k} \leq \binom{n}{\lfloor k/2 \rfloor + 1}$, it is sufficient to show that

$$2^{\lfloor k/2 \rfloor} \left(\left\lceil \frac{k}{2} \right\rceil + 1 \right) \prod_{\alpha=1}^{\lfloor k/2 \rfloor} (n - k + 2\alpha - 1) \leq \prod_{\alpha=1}^{\lfloor k/2 \rfloor + 1} (n - \alpha + 1). \tag{B63}$$

First, we consider the case when k is even. The product part in the definition of $b_{n,k}$ is upper bounded as

$$\prod_{\alpha=1}^{\lfloor k/2 \rfloor} (n - k + 2\alpha - 1) = \prod_{\alpha=1}^{k/2} (n - k + 2\alpha - 1)$$

$$\begin{aligned}
&= \prod_{\alpha=2}^{(k/2)+1} \left[n - k + 2 \left(\frac{k}{2} + 2 - \alpha \right) - 1 \right] \\
&= \prod_{\alpha=2}^{\lceil k/2 \rceil + 1} [n - \alpha + 1 - (\alpha - 2)] \\
&\leq \prod_{\alpha=2}^{\lceil k/2 \rceil + 1} (n - \alpha + 1).
\end{aligned} \tag{B64}$$

By the assumption that $n \geq 2^k$, we get

$$\left(\left\lceil \frac{k}{2} \right\rceil + 1 \right) 2^{\lfloor k/2 \rfloor} \leq 2^{\lceil k/2 \rceil} 2^{\lfloor k/2 \rfloor} = 2^k \leq n. \tag{B65}$$

By multiplying Eqs. (B64) and (B65), we get Eq. (B63).

Next, we consider the case when k is odd. We note that Eq. (B63) is equivalent to

$$2^{\lfloor k/2 \rfloor} \left(\left\lceil \frac{k}{2} \right\rceil + 1 \right) \prod_{\alpha=1}^{\lceil k/2 \rceil - 1} (n - k + 2\alpha - 1) \leq \prod_{\alpha=2}^{\lceil k/2 \rceil + 1} (n - \alpha + 1), \tag{B66}$$

because the term for $\alpha = \lceil k/2 \rceil$ in the l.h.s. and the term for $\alpha = 1$ in the r.h.s. in Eq. (B63) are both equal to n . By noting that $k - 1$ is even, we can substitute $n \mapsto n - 1$ and $k \mapsto k - 1$ in Eq. (B64). Then, the product part in the l.h.s. of Eq. (B66) is upper bounded as

$$\begin{aligned}
\prod_{\alpha=1}^{\lceil k/2 \rceil - 1} (n - k + 2\alpha - 1) &= \prod_{\alpha=1}^{\lceil (k-1)/2 \rceil} [(n-1) - (k-1) + 2\alpha - 1] \\
&\leq \prod_{\alpha=2}^{\lceil (k-1)/2 \rceil + 1} [(n-1) - \alpha + 1] \\
&= \prod_{\alpha=2}^{\lceil k/2 \rceil} [n - (\alpha + 1) + 1] \\
&= \prod_{\alpha=3}^{\lceil k/2 \rceil + 1} (n - \alpha + 1).
\end{aligned} \tag{B67}$$

By the assumption that $n \geq 2^k$ and $\lceil k/2 \rceil \geq 2$, we get

$$\left(\left\lceil \frac{k}{2} \right\rceil + 1 \right) 2^{\lfloor k/2 \rfloor} = \left(\left\lceil \frac{k}{2} \right\rceil + 2 \right) 2^{\lfloor k/2 \rfloor} - 2^{\lfloor k/2 \rfloor} \leq 2 \left\lceil \frac{k}{2} \right\rceil 2^{\lfloor k/2 \rfloor} - 1 \leq 2^{\lceil k/2 \rceil} 2^{\lfloor k/2 \rfloor} - 1 = 2^k - 1 \leq n - 1. \tag{B68}$$

By multiplying Eqs. (B67) and (B68), we get Eq. (B66). For the proof of $b_{n,k} \leq b_{n,k+1}$, it is sufficient to show that

$$\prod_{\alpha=1}^{(k+1)/2} (n - 2\alpha + 2) \leq 2 \prod_{\alpha=1}^{(k+1)/2} (n - 2\alpha + 1). \tag{B69}$$

We note that

$$\prod_{\alpha=2}^{(k+1)/2} (n - 2\alpha + 2) = \prod_{\alpha=1}^{(k+1)/2 - 1} (n - 2(\alpha + 1) + 2) \leq \prod_{\alpha=1}^{(k+1)/2 - 1} (n - 2\alpha + 1). \tag{B70}$$

By the assumption of $n \geq 2^k$, we have

$$n = 2(n - k) - (n - 2^k) - (2^k - 2k) \leq 2(n - k). \tag{B71}$$

By multiplying Eqs. (B70) and (B71), we get Eq. (B69). $\square$

We prepare a lemma making it easier to check whether the assumption in Lemma 11 holds or not.

Lemma 22. *Let $n, a, b \in \mathbb{Z}$ and $0 \leq a \leq b \leq n/2 - 1$. Then,*

$$\binom{n}{j+1} - \binom{n}{j} \geq \min \left\{ \binom{n}{a+1} - \binom{n}{a}, \binom{n}{b+1} - \binom{n}{b} \right\} \quad (\text{B72})$$

for all $j \in \{a, a+1, \dots, b\}$.

Proof. We note that

$$\left(\binom{n}{j+1} - \binom{n}{j} \right) - \left(\binom{n}{j} - \binom{n}{j-1} \right) = \binom{n}{j-1} \frac{(n-2j)^2 - (n+2)}{j(j+1)}. \quad (\text{B73})$$

for all $j \in \mathbb{Z}$ satisfying $1 \leq j \leq n/2 - 1$. The r.h.s. is positive at $j = 1$ and negative at $j = n/2 - 1$, and monotonically decreases as j increases. We can thus take $k \in \{a, a+1, \dots, b\}$ such that the value of Eq. (B73) is positive when $j < k$ and non-positive when $j \geq k$. This means that $\binom{n}{j+1} - \binom{n}{j}$ is increasing while $j \leq k$ and nonincreasing while $k \leq j$. Therefore $\binom{n}{j+1} - \binom{n}{j}$ takes the minimum value at $j = a$ or $j = b$. $\square$

By using the lemma above, we give a rough sufficient condition for the assumption in Lemma 11. The following lemma is the counterpart of Lemma 21 in the SU(2) case.

Lemma 23. *Let $n, k \in \mathbb{N}$ satisfy $k \geq 2$ and $n \geq 2^{2(\lfloor k/2 \rfloor + 1)}$, and $c_{n,k}$ be defined by Eq. (A76), i.e.,*

$$c_{n,k} := \frac{2^{\lfloor k/2 \rfloor}}{(\lfloor \frac{k}{2} \rfloor + 1)!} \prod_{\alpha=1}^{\lfloor k/2 \rfloor + 1} (n - 2\alpha + 1). \quad (\text{B74})$$

Then, $c_{n,k} \leq \binom{n}{j+1} - \binom{n}{j}$ for all $j \in \{\lfloor k/2 \rfloor + 1, \lfloor k/2 \rfloor + 2, \dots, \lfloor n/2 \rfloor - 1\}$.

Proof. By Lemma 22, it is sufficient to show that $c_{n,k} \leq \binom{n}{j+1} - \binom{n}{j}$ only for $j = \lfloor k/2 \rfloor + 1$ and $\lfloor n/2 \rfloor - 1$. First, we prove that $c_{n,k} \leq \binom{n}{j+1} - \binom{n}{j}$ in the case of $j = \lfloor k/2 \rfloor + 1$. We note that

$$\begin{aligned} \binom{n}{\lfloor \frac{k}{2} \rfloor + 2} - \binom{n}{\lfloor \frac{k}{2} \rfloor + 1} &= \frac{n - 2\lfloor \frac{k}{2} \rfloor - 3}{(\lfloor \frac{k}{2} \rfloor + 2)!} \left(\prod_{\alpha=1}^{\lfloor k/2 \rfloor + 1} (n - \alpha + 1) \right) \\ &\geq \frac{n - 2\lfloor \frac{k}{2} \rfloor - 3}{(\lfloor \frac{k}{2} \rfloor + 2)!} \prod_{\alpha=1}^{\lfloor k/2 \rfloor + 1} (n - 2\alpha + 1) \\ &= \frac{n - 2\lfloor \frac{k}{2} \rfloor - 3}{(\lfloor \frac{k}{2} \rfloor + 2)2^{\lfloor k/2 \rfloor}} c_{n,k}. \end{aligned} \quad (\text{B75})$$

Since n satisfies $n \geq 2^{2(\lfloor k/2 \rfloor + 1)}$, we have

$$\begin{aligned} \left(\left\lfloor \frac{k}{2} \right\rfloor + 2 \right) 2^{\lfloor k/2 \rfloor} &= \left[\left(\left\lfloor \frac{k}{2} \right\rfloor + 1 \right) + 1 \right] \left(2^{\lfloor k/2 \rfloor} + 2 \right) - 2 \left\lfloor \frac{k}{2} \right\rfloor - 4 \\ &\leq 2^{\lfloor k/2 \rfloor + 1} \cdot \left(2^{\lfloor k/2 \rfloor} + 2^{\lfloor k/2 \rfloor} \right) - 2 \left\lfloor \frac{k}{2} \right\rfloor - 3 \\ &= 2^{2(\lfloor k/2 \rfloor + 1)} - 2 \left\lfloor \frac{k}{2} \right\rfloor - 3 \\ &\leq n - 2 \left\lfloor \frac{k}{2} \right\rfloor - 3. \end{aligned} \quad (\text{B76})$$

By Eqs. (B75) and (B76), we get $c_{n,k} \leq \binom{n}{\lfloor k/2 \rfloor + 2} - \binom{n}{\lfloor k/2 \rfloor + 1}$.

Next, we prove the inequality in the case of $j = \lfloor n/2 \rfloor - 1$. When n is even, we note that

$$\binom{n}{\lfloor \frac{n}{2} \rfloor} - \binom{n}{\lfloor \frac{n}{2} \rfloor - 1} = \frac{1}{(\frac{n}{2})!} \prod_{\alpha=-1}^{n/2-3} (n - \alpha - 1)$$

$$\begin{aligned}
&= \frac{2(n-2)}{\left(\frac{n}{2}-1\right)!} (n-1) \prod_{\alpha=2}^{n/2-3} (n-\alpha-1) \\
&\geq \frac{2(n-2)}{\left(\left\lfloor \frac{k}{2} \right\rfloor + 3\right)! \left(\frac{n}{2}\right)^{n/2-\lfloor k/2 \rfloor - 4}} (n-1) \left(\prod_{\alpha=2}^{\lfloor k/2 \rfloor + 1} (n-\alpha-1) \right) \left(\frac{n}{2}\right)^{n/2-\lfloor k/2 \rfloor - 4} \\
&\geq \frac{2(n-2)}{\left(\left\lfloor \frac{k}{2} \right\rfloor + 3\right)!} (n-1) \prod_{\alpha=2}^{\lfloor k/2 \rfloor + 1} (n-2\alpha+1) \\
&= \frac{2(n-2)}{\left(\left\lfloor \frac{k}{2} \right\rfloor + 3\right)!} \prod_{\alpha=1}^{\lfloor k/2 \rfloor + 1} (n-2\alpha+1) \\
&= \frac{n-2}{\left(\left\lfloor \frac{k}{2} \right\rfloor + 2\right) \left(\left\lfloor \frac{k}{2} \right\rfloor + 3\right) 2^{\lfloor k/2 \rfloor - 1}} c_{n,k}.
\end{aligned} \tag{B77}$$

Since n satisfies $n \geq 2^{2(\lfloor k/2 \rfloor + 1)}$, we have

$$\begin{aligned}
\left(\left\lfloor \frac{k}{2} \right\rfloor + 2\right) \left(\left\lfloor \frac{k}{2} \right\rfloor + 3\right) 2^{\lfloor k/2 \rfloor - 1} &= \left(\left\lfloor \frac{k}{2} \right\rfloor + 2\right) \left(\left\lfloor \frac{k}{2} \right\rfloor + 4\right) 2^{\lfloor k/2 \rfloor - 1} - \left(\left\lfloor \frac{k}{2} \right\rfloor + 2\right) 2^{\lfloor k/2 \rfloor - 1} \\
&\leq 2^{\lfloor k/2 \rfloor + 3} \cdot 2^{\lfloor k/2 \rfloor - 1} - 2 \\
&= 2^{2(\lfloor k/2 \rfloor + 1)} - 2 \\
&\leq n - 2,
\end{aligned} \tag{B78}$$

where we note that we can prove that $(j+2)(j+4) \leq 2^{j+3}$ for all $j \in \mathbb{N}$ by the mathematical induction. By Eqs. (B77) and (B78), we get $c_{n,k} \leq \binom{n}{\lfloor n/2 \rfloor} - \binom{n}{\lfloor n/2 \rfloor - 1}$.

When n is odd, $n+1$ is even, and we have $n+1 \geq 2^{2(\lfloor k/2 \rfloor + 1)}$. Thus we can substitute $n \mapsto n+1$ in the result in the case when n is even, Then, we get

$$c_{n,k} \leq c_{n+1,k} \leq \binom{n+1}{\lfloor \frac{n+1}{2} \rfloor} - \binom{n+1}{\lfloor \frac{n+1}{2} \rfloor - 1}. \tag{B79}$$

We note that

$$\begin{aligned}
\binom{n+1}{\lfloor \frac{n+1}{2} \rfloor} - \binom{n+1}{\lfloor \frac{n+1}{2} \rfloor - 1} &= \binom{n+1}{\frac{n+1}{2}} - \binom{n+1}{\frac{n-1}{2}} \\
&= \left(\binom{n}{\frac{n-1}{2}} + \binom{n}{\frac{n+1}{2}} \right) - \left(\binom{n}{\frac{n-3}{2}} + \binom{n}{\frac{n-1}{2}} \right) \\
&= \binom{n}{\frac{n+1}{2}} - \binom{n}{\frac{n-3}{2}} \\
&= \binom{n}{\frac{n-1}{2}} - \binom{n}{\frac{n-3}{2}} \\
&= \binom{n}{\lfloor \frac{n}{2} \rfloor} - \binom{n}{\lfloor \frac{n}{2} \rfloor - 1}.
\end{aligned} \tag{B80}$$

By plugging Eq. (B80) into Eq. (B79), we get $c_{n,k} \leq \binom{n}{\lfloor n/2 \rfloor} - \binom{n}{\lfloor n/2 \rfloor - 1}$. $\square$

We are going to see two properties of the sequence $(a_{n,k,j})_{j=1}^{\infty}$ defined by Eq. (A16), i.e.,

$$a_{n,k,j} := \sum_{p=0}^j \binom{n}{j-p} \binom{n-k+p-1}{p}. \tag{B81}$$

First, we prepare the property that we used to get the explicit expression of the result of Theorem 5.

Lemma 24. *Let $n, k \in \mathbb{Z}$ satisfy $0 \leq k \leq n-1$ and the sequence $(a_{n,k,j})_{j=0}^{\infty}$ be defined by Eq. (A16). Then,*

$$a_{n,2k,k} = \frac{2^k}{k!} \prod_{\alpha=1}^k (n-2\alpha+1). \tag{B82}$$

Proof. We are going to prove that

$$\sum_{p=0}^k \left[\frac{1}{(k-p)!} \prod_{\beta=1}^{k-p} (z - \beta + 1) \right] \left[\frac{1}{p!} \prod_{\beta=1}^p (z - 2k + p - \beta) \right] = \frac{2^k}{k!} \prod_{\alpha=1}^k (z - 2\alpha + 1) \quad (\text{B83})$$

for all $z \in \mathbb{C}$, which gives Eq. (B82) as a special case of $z = n$. We define a polynomial $q(z)$ as the l.h.s. of Eq. (B83). Since the both sides of Eq. (B83) are polynomials of degree k , it is sufficient to show that Eq. (B83) holds for $z = 2k$ and $z = 2\alpha - 1$ with $\alpha \in \{1, 2, \dots, k\}$. First, when $z = 2k$, we have

$$\begin{aligned} q(2k) &= \sum_{p=0}^k \left[\frac{1}{(k-p)!} \prod_{\beta=1}^{k-p} (2k - \beta + 1) \right] \left[\frac{1}{p!} \prod_{\beta=1}^p (p - \beta) \right] \\ &= \frac{1}{k!} \prod_{\beta=1}^k (2k - \beta + 1) \\ &= \frac{1}{k!} \cdot \frac{\prod_{\beta=1}^{2k} (2k - \beta + 1)}{\prod_{\beta=k+1}^{2k} (2k - \beta + 1)} \\ &= \frac{1}{k!} \cdot \frac{\left[\prod_{\beta=1}^k (2k - 2\beta + 1) \right] \left[\prod_{\beta=1}^k (2k - 2\beta + 2) \right]}{\prod_{\beta=1}^k (k - \beta + 1)} \\ &= \frac{2^k}{k!} \prod_{\beta=1}^k (2k - 2\beta + 1), \end{aligned} \quad (\text{B84})$$

where we used $\prod_{\beta=1}^p (p - \beta) = \delta_{p,0}$ in the second equality. Next, we consider the case when $z = 2\alpha - 1$ with $\alpha \in \{1, 2, \dots, k\}$. By substitution, we have

$$q(2\alpha - 1) = \sum_{p=0}^k \left[\frac{1}{(k-p)!} \prod_{\beta=1}^{k-p} (2\alpha - \beta) \right] \left[\frac{1}{p!} \prod_{\beta=1}^p (2\alpha - 2k + p - \beta - 1) \right]. \quad (\text{B85})$$

We note that

$$\begin{aligned} \prod_{\beta=1}^p (2\alpha - 2k + p - \beta - 1) &= \prod_{\beta=1}^p [2\alpha - 2k + p - (p + 1 - \beta) - 1] \\ &= \prod_{\beta=1}^p (2\alpha - 2k + \beta - 2) \\ &= (-1)^p \prod_{\beta=1}^p (2k - 2\alpha - \beta + 2). \end{aligned} \quad (\text{B86})$$

By plugging Eq. (B86) into Eq. (B85), we get

$$\begin{aligned} q(2\alpha - 1) &= \sum_{p=0}^k (-1)^p \left[\frac{1}{(k-p)!} \prod_{\beta=1}^{k-p} (2\alpha - \beta) \right] \left[\frac{1}{p!} \prod_{\beta=1}^p (2k - 2\alpha - \beta + 2) \right] \\ &= \sum_{p \in [0, k] \cap [k - 2\alpha + 1, 2k - 2\alpha + 1] \cap \mathbb{Z}} (-1)^p \left[\frac{1}{(k-p)!} \prod_{\beta=1}^{k-p} (2\alpha - \beta) \right] \left[\frac{1}{p!} \prod_{\beta=1}^p (2k - 2\alpha - \beta + 2) \right] \end{aligned}$$

$$= \sum_{p \in [0, k] \cap [k-2\alpha+1, 2k-2\alpha+1] \cap \mathbb{Z}} (-1)^p \binom{2\alpha-1}{k-p} \binom{2k-2\alpha+1}{p}, \quad (\text{B87})$$

where we used $\prod_{\beta=1}^{k-p} (2\alpha - \beta) = 0$ if $p \leq k - 2\alpha$, and $\prod_{\beta=1}^p (2k - 2\alpha - \beta + 2) = 0$ if $p \geq 2k - 2\alpha + 2$ in the second equality. By noting that the condition $p \in [0, k] \cap [k - 2\alpha + 1, 2k - 2\alpha + 1] \cap \mathbb{Z}$ is invariant under the transformation $p \mapsto 2k - 2\alpha + 1 - p$, we have

$$\begin{aligned} q(2\alpha - 1) &= \sum_{p \in [0, k] \cap [k-2\alpha+1, 2k-2\alpha+1] \cap \mathbb{Z}} (-1)^{2k-2\alpha+1-p} \binom{2\alpha-1}{k-(2k-2\alpha+1-p)} \binom{2k-2\alpha+1}{2k-2\alpha+1-p} \\ &= - \sum_{p \in [0, k] \cap [k-2\alpha+1, 2k-2\alpha+1] \cap \mathbb{Z}} (-1)^p \binom{2\alpha-1}{2\alpha-k+p-1} \binom{2k-2\alpha+1}{2k-2\alpha+1-p} \\ &= - \sum_{p \in [0, k] \cap [k-2\alpha+1, 2k-2\alpha+1] \cap \mathbb{Z}} (-1)^p \binom{2\alpha-1}{k-p} \binom{2k-2\alpha+1}{p}. \end{aligned} \quad (\text{B88})$$

By Eqs. (B87) and (B88), we get $q(2\alpha - 1) = 0$. $\square$

Next, by using the lemma above, we derive another property of the sequence $(a_{n,k,j})_{j=0}^{\infty}$ for the explicit expression of the result of Theorem 3.

Lemma 25. *Let $n, k \in \mathbb{Z}$ satisfy $0 \leq k \leq n - 1$ and the sequence $(a_{n,k,j})_{j=0}^{\infty}$ be defined by Eq. (A16). Then,*

$$\frac{a_{n,k,\lceil k/2 \rceil} + a_{n,k,\lfloor k/2 \rfloor}}{2} = \frac{2^{\lfloor k/2 \rfloor}}{\lceil \frac{k}{2} \rceil!} \prod_{\alpha=1}^{\lceil k/2 \rceil} (n - k + 2\alpha - 1). \quad (\text{B89})$$

Proof. First, when k is even, by Lemma 24, we have

$$\begin{aligned} \frac{a_{n,k,\lceil k/2 \rceil} + a_{n,k,\lfloor k/2 \rfloor}}{2} &= a_{n,k,k/2} \\ &= \frac{2^{k/2}}{(\frac{k}{2})!} \prod_{\alpha=1}^{k/2} (n - 2\alpha + 1) \\ &= \frac{2^{k/2}}{(\frac{k}{2})!} \prod_{\alpha=1}^{k/2} \left[n - 2 \left(\frac{k}{2} + 1 - \alpha \right) + 1 \right] \\ &= \frac{2^{\lfloor k/2 \rfloor}}{\lceil \frac{k}{2} \rceil!} \prod_{\alpha=1}^{\lceil k/2 \rceil} (n - k + 2\alpha - 1). \end{aligned} \quad (\text{B90})$$

Next, we consider the case when k is odd. We note that

$$\begin{aligned} a_{n,k,j+1} + a_{n,k,j} &= \sum_{p=0}^{j+1} \binom{n}{j+1-p} \binom{n-k+p-1}{p} + \sum_{p=0}^j \binom{n}{j-p} \binom{n-k+p-1}{p} \\ &= \sum_{p=0}^{j+1} \left(\binom{n}{j+1-p} + \binom{n}{j-p} \right) \binom{n-k+p-1}{p} \\ &= \sum_{p=0}^{j+1} \binom{n+1}{j+1-p} \binom{n-k+p-1}{p} \\ &= a_{n,k+1,j+1}, \end{aligned} \quad (\text{B91})$$

which implies that

$$\frac{a_{n,k,\lceil k/2 \rceil} + a_{n,k,\lfloor k/2 \rfloor}}{2} = \frac{a_{n,k,(k+1)/2} + a_{n,k,(k-1)/2}}{2} = \frac{a_{n+1,k+1,(k+1)/2}}{2}. \quad (\text{B92})$$

By applying Lemma 24 to the r.h.s. of this equation, we get

$$\begin{aligned}
\frac{a_{n,k,\lceil k/2 \rceil} + a_{n,k,\lfloor k/2 \rfloor}}{2} &= \frac{1}{2} \frac{2^{(k+1)/2}}{\left(\frac{k+1}{2}\right)!} \prod_{\alpha=1}^{(k+1)/2} (n - 2\alpha + 2) \\
&= \frac{2^{(k-1)/2}}{\left(\frac{k+1}{2}\right)!} \prod_{\alpha=1}^{(k+1)/2} \left[n - 2 \left(\frac{k+1}{2} + 1 - \alpha \right) + 2 \right] \\
&= \frac{2^{(k-1)/2}}{\left(\frac{k+1}{2}\right)!} \prod_{\alpha=1}^{(k+1)/2} (n - k + 2\alpha - 1) \\
&= \frac{2^{\lfloor k/2 \rfloor}}{\left(\lceil \frac{k}{2} \rceil\right)!} \prod_{\alpha=1}^{(k+1)/2} (n - k + 2\alpha - 1). \tag{B93}
\end{aligned}$$

□

In the following, we prepare two properties about binomial coefficients for the proof of Lemma 9. First, we prove a property used for proving that the equations in Lemma 9 imply the ones in Theorem 1.

Lemma 26. *Let $n, k \in \mathbb{Z}_{\geq 0}$ satisfy $n \geq k$. Then, for any $j \in \{0, 1, \dots, \lfloor k/2 \rfloor\}$, there exists $(v_{j,l})_{j,l \in \{0,1,\dots,\lfloor k/2 \rfloor\}} \in \mathbb{R}^{(\lfloor k/2 \rfloor + 1)^2}$ such that for any $\alpha \in \mathbb{Z}$,*

$$\binom{n-k}{\alpha-j} + \binom{n-k}{\alpha-k+j} = \sum_{l=0}^{\lfloor k/2 \rfloor} v_{j,l} \binom{n-2l}{\alpha-l}. \tag{B94}$$

Proof. We prove this lemma by the mathematical induction about k . The statement trivially holds for $k = 0$, because when $j = 0$ and $v_{0,0} = 2$, Eq. (B94) holds for all $\alpha \in \mathbb{Z}$. We take arbitrary $K \in \mathbb{Z}_{\geq 0}$ and suppose that this statement holds for $k = K$, i.e., for any $j \in \{0, 1, \dots, \lfloor K/2 \rfloor\}$, we can take $v'_{j,l \in \{0,1,\dots,\lfloor K/2 \rfloor\}} \in \mathbb{R}^{(\lfloor K/2 \rfloor + 1)^2}$ such that for any $\alpha \in \mathbb{Z}$,

$$\binom{n-K}{\alpha-j} + \binom{n-K}{\alpha-K+j} = \sum_{l=0}^{\lfloor K/2 \rfloor} v'_{j,l} \binom{n-2l}{\alpha-l}. \tag{B95}$$

In the following, we are going to prove that the statement holds for $k = K + 1$. When K is even, for any $j, l \in \{0, 1, \dots, K/2\}$, we set

$$v_{j,l} = (-1)^{K/2-j} \delta_{K/2,l} + \sum_{p=j}^{K/2-1} (-1)^{p-j} v'_{p,l}, \tag{B96}$$

where we note that this means that $v_{K/2,l} = \delta_{K/2,l}$. Then, for any $\alpha \in \mathbb{Z}$, we have

$$\begin{aligned}
\sum_{l=0}^{K/2} v_{j,l} \binom{n-2l}{\alpha-l} &= (-1)^{K/2-j} \binom{n-K}{\alpha-K/2} + \sum_{p=j}^{K/2-1} \left[(-1)^{p-j} \sum_{l=0}^{K/2} v'_{p,l} \binom{n-2l}{\alpha-l} \right] \\
&= (-1)^{K/2-j} \binom{n-K}{\alpha-K/2} + \sum_{p=j}^{K/2-1} (-1)^{p-j} \left(\binom{n-K}{\alpha-p} + \binom{n-K}{\alpha-K+p} \right) \\
&= \sum_{p=j}^{K-j} (-1)^{p-j} \binom{n-K}{\alpha-p} \\
&= \sum_{p=j}^{K-j} \left[(-1)^{p-j} \binom{n-(K+1)}{\alpha-p} - (-1)^{(p+1)-j} \binom{n-(K+1)}{\alpha-(p+1)} \right] \\
&= \binom{n-(K+1)}{\alpha-j} + \binom{n-(K+1)}{\alpha-K+j}. \tag{B97}
\end{aligned}$$

When K is odd, for any $j \in \{0, 1, \dots, (K+1)/2\}$, we set

$$v_{j,l} = \sum_{p=j}^{(K-1)/2} (-1)^{p-j} v'_{p,l} \quad \forall l \in \{0, 1, \dots, (K-1)/2\}, \quad (\text{B98})$$

$$v_{j,(K+1)/2} = 2(-1)^{(K+1)/2-j}. \quad (\text{B99})$$

Then, for any $\alpha \in \mathbb{Z}$, we have

$$\begin{aligned} \sum_{l=0}^{(K+1)/2} v_{j,l} \binom{n-2l}{\alpha-l} &= 2(-1)^{(K+1)/2-j} \binom{n-(K+1)}{\alpha - \frac{K+1}{2}} + \sum_{p=j}^{(K-1)/2} \left[(-1)^{p-j} \sum_{l=0}^{(K-1)/2} v'_{p,l} \binom{n-2l}{\alpha-l} \right] \\ &= 2(-1)^{(K+1)/2-j} \binom{n-(K+1)}{\alpha - \frac{K+1}{2}} + \sum_{p=j}^{(K-1)/2} (-1)^{p-j} \left(\binom{n-K}{\alpha-p} + \binom{n-K}{\alpha-K+p} \right). \end{aligned} \quad (\text{B100})$$

We note that

$$\begin{aligned} &\sum_{p=j}^{(K-1)/2} (-1)^{p-j} \left(\binom{n-K}{\alpha-p} + \binom{n-K}{\alpha-K+p} \right) \\ &= \sum_{p=j}^{(K-1)/2} (-1)^{p-j} \binom{n-K}{\alpha-p} - \sum_{p=(K+1)/2}^{K-j} (-1)^{p-j} \binom{n-K}{\alpha-p} \\ &= \sum_{p=j}^{(K-1)/2} \left[(-1)^{p-j} \binom{n-(K+1)}{\alpha-p} - (-1)^{(p+1)-j} \binom{n-(K+1)}{\alpha-(p+1)} \right] \\ &\quad - \sum_{p=(K+1)/2}^{K-j} \left[(-1)^{p-j} \binom{n-(K+1)}{\alpha-p} - (-1)^{(p+1)-j} \binom{n-(K+1)}{\alpha-(p+1)} \right] \\ &= \left[\binom{n-(K+1)}{\alpha-j} - (-1)^{(K+1)/2-j} \binom{n-(K+1)}{\alpha - \frac{K+1}{2}} \right] - \left[(-1)^{(K+1)/2-j} \binom{n-(K+1)}{\alpha - \frac{K+1}{2}} - \binom{n-(K+1)}{\alpha-(K+1)+j} \right] \\ &= \left(\binom{n-(K+1)}{\alpha-j} + \binom{n-(K+1)}{\alpha-(K+1)+j} \right) - 2(-1)^{(K+1)/2-j} \binom{n-(K+1)}{\alpha - \frac{K+1}{2}}. \end{aligned} \quad (\text{B101})$$

By plugging Eq. (B101) into Eq. (B100), we get

$$\sum_{l=0}^{(K+1)/2} v_{j,l} \binom{n-2l}{\alpha-l} = \binom{n-(K+1)}{\alpha-j} + \binom{n-(K+1)}{\alpha-(K+1)+j}. \quad (\text{B102})$$

We have thus proven that the statement holds for $k = K+1$. $\square$

Next, we prove a property used for proving that the equations in Theorem 1 imply the ones in Lemma 9.

Lemma 27. *Let $n, k \in \mathbb{Z}_{\geq 0}$ satisfy $n \geq k$. Then, for any $j \in \{0, 1, \dots, \lfloor k/2 \rfloor\}$, there exists $(w_{j,l})_{j,l \in \{0,1,\dots,\lfloor k/2 \rfloor\}} \in \mathbb{R}^{(\lfloor k/2 \rfloor + 1)^2}$ such that for any $\alpha \in \mathbb{Z}$,*

$$\binom{n-2j}{\alpha-j} = \sum_{l=0}^{\lfloor k/2 \rfloor} w_{j,l} \left(\binom{n-2l}{\alpha} + \binom{n-2l}{\alpha-2l} \right). \quad (\text{B103})$$

Proof. We prove this lemma by the mathematical induction about k . We take arbitrary $K \in \mathbb{Z}_{\geq 0}$ and suppose that this lemma holds for $k = K$, i.e., for any $j \in \{0, 1, \dots, \lfloor K/2 \rfloor\}$, we can take $(w'_{j,l})_{j,l \in \{0,1,\dots,\lfloor K/2 \rfloor\}} \in \mathbb{R}^{(\lfloor K/2 \rfloor + 1)^2}$ such that for any $\alpha \in \mathbb{Z}$,

$$\binom{n-2j}{\alpha-j} = \sum_{l=0}^{\lfloor K/2 \rfloor} w'_{j,l} \left(\binom{n-2l}{\alpha} + \binom{n-2l}{\alpha-2l} \right). \quad (\text{B104})$$

We are going to prove that this lemma holds for $k = K + 1$. When K is even, the statement trivially holds for $k = K + 1$, because Eq. (B103) is equivalent for $k = K$ and $k = K + 1$. In the following, we consider the case when K is odd. By Lemma 26, for any $p \in \{0, 1, \dots, (K - 1)/2\}$, we can take $(v_{p,q})_{p,q \in \{0, 1, \dots, (K-1)/2\}} \in \mathbb{R}^{[(K+1)/2]^2}$ such that for any $\alpha \in \mathbb{Z}$,

$$\binom{n-K}{\alpha-p} + \binom{n-K}{\alpha-K+p} = \sum_{q=0}^{(K-1)/2} v_{p,q} \binom{n-2q}{\alpha-q}. \quad (\text{B105})$$

For $j \in \{0, 1, \dots, (K-1)/2\}$, we set $w_{j,l} = w'_{j,l}$ and $w_{j,(K+1)/2} = 0$. Then, we have Eq. (B103) for all $\alpha \in \mathbb{Z}$. For $j = (K+1)/2$, we set

$$w_{(K+1)/2,l} = -\frac{1}{2} \sum_{p=0}^{(K-1)/2} \sum_{q=0}^{(K-1)/2} (-1)^{(K+1)/2+p} v_{p,q} w'_{q,l} \quad \forall l \in \left\{0, 1, \dots, \frac{K-1}{2}\right\}, \quad (\text{B106})$$

$$w_{(K+1)/2,(K+1)/2} = \frac{1}{2} (-1)^{(K+1)/2}. \quad (\text{B107})$$

For any $\alpha \in \mathbb{Z}$, by plugging $j = 0$ into Eq. (B101) in Lemma 26, we get

$$\begin{aligned} \binom{n-(K+1)}{\alpha - \frac{K+1}{2}} &= -\frac{1}{2} (-1)^{(K+1)/2} \sum_{p=0}^{(K-1)/2} (-1)^p \left(\binom{n-K}{\alpha-p} + \binom{n-K}{\alpha-K+p} \right) \\ &\quad + \frac{1}{2} (-1)^{(K+1)/2} \left(\binom{n-(K+1)}{\alpha} + \binom{n-(K+1)}{\alpha-(K+1)} \right). \end{aligned} \quad (\text{B108})$$

By plugging Eq. (B104) into Eq. (B105), we have

$$\binom{n-K}{\alpha-p} + \binom{n-K}{\alpha-K+p} = \sum_{q=0}^{(K-1)/2} \sum_{l=0}^{(K-1)/2} v_{p,q} w'_{q,l} \left(\binom{n-2l}{\alpha} + \binom{n-2l}{\alpha-2l} \right). \quad (\text{B109})$$

By plugging Eq. (B109) into Eq. (B108), we get

$$\begin{aligned} \binom{n-(K+1)}{\alpha - \frac{K+1}{2}} &= -\frac{1}{2} \sum_{p=0}^{(K-1)/2} \sum_{q=0}^{(K-1)/2} \sum_{l=0}^{(K-1)/2} (-1)^{(K+1)/2+p} v_{p,q} w'_{q,l} \left(\binom{n-2l}{\alpha} + \binom{n-2l}{\alpha-2l} \right) \\ &\quad + \frac{1}{2} (-1)^{(K+1)/2} \left(\binom{n-(K+1)}{\alpha} + \binom{n-(K+1)}{\alpha-(K+1)} \right) \\ &= \sum_{l=0}^{(K+1)/2} w_{(K+1)/2,l} \left(\binom{n-2l}{\alpha} + \binom{n-2l}{\alpha-2l} \right), \end{aligned} \quad (\text{B110})$$

where we used Eqs. (B106) and (B107). We have thus proven that the statement holds for $k = K + 1$. $\square$