

Quantum Simulation of Random Unitaries from Clebsch–Gordan Transforms

Dmitry Grinko^{1,2,3,*} and Satoshi Yoshida^{4,*}

¹*QuSoft, Amsterdam, The Netherlands*

²*Institute for Logic, Language and Computation, University of Amsterdam, The Netherlands*

³*Korteweg-de Vries Institute for Mathematics, University of Amsterdam, The Netherlands*

⁴*Department of Physics, Graduate School of Science, The University of Tokyo, Japan*

(Dated: September 2025)

We present a general method for simulating an action of t copies of a Haar random unitary for arbitrary compact groups. This construction can be viewed as a representation-theoretic generalization of Zhandry’s compressed function oracle technique. It is conceptually simple, exact and utilizes Clebsch–Gordan transforms as main building blocks. In particular, for the unitary group, our method is efficient in space and time. Finally, our general oracle for forward queries can be easily modified into oracles for conjugate, transpose, and inverse queries, thus unifying all four query types.

Random unitary operation offers a universal primitive for various quantum information processing including shadow tomography [1–8], random sampling [9–14], randomized benchmarking [15–19] and quantum random oracle model in cryptography [20–26]. It also offers a fundamental understanding of physical systems, including black holes and chaotic systems [27–37]. Random distribution of d -dimensional unitary operation is modeled by the Haar measure. There are three common ways to simulate the Haar-random unitary in the quantum circuit model: *unitary t -design*, *pseudorandom unitary (PRU)*, and *compressed oracle*.

Unitary t -design is given by a probability distribution $\{p_i\}_i$ on a finite set of unitary operators $\{U_i\}_i$ (we shortly write it as $\{p_i, U_i\}_i$) and it can simulate a quantum circuit having t queries to a Haar-random unitary operation U , its complex conjugate $\bar{U}$, its transpose $U^\top$, and its inverse $U^\dagger$ [17, 38, 39] [see Fig. 1 (a) and (b)]. *Pseudorandom unitary (PRU)* is a probability distribution $\{p_i, U_i\}_i$ on n -qubit unitaries such that any polynomial-time quantum circuit cannot distinguish it from the Haar measure [40], where the distinguisher is allowed to query only U_i , or U_i and $U_i^\dagger$, or $U_i, U_i^\dagger, \bar{U}_i$, and $U_i^\top$ depending on the setting. *Compressed oracle* is another way to simulate an action of random unitaries by using quantum memory to purify the classical randomness associated with the underlying measure. It is defined as unitary operations fO, cO, tO, iO called the forward, conjugate, transposed, and inverse oracles, respectively, acting on a system and auxiliary memory system. By tracing out the memory system in the end, it simulates the forward query U , the conjugate query U^* , the transposed query $U^\top$, and the inverse query $U^\dagger$ of the Haar-random unitary U , respectively [see Fig. 1 (c)]. This is a natural generalization of the same problem for random functions [22], and it

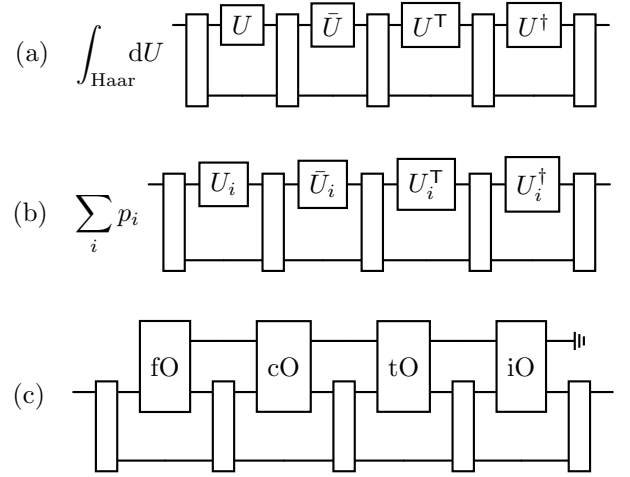


FIG. 1. (a) A quantum circuit involving t queries to a unitary operations $U, \bar{U}, U^\top$ and $U^\dagger$, where U is drawn from the Haar measure. The boxes other than U represent arbitrary quantum channels. (b) Unitary t -design $\{p_i, U_i\}_i$ can simulate the quantum circuit (a) by using U_i with probability p_i . (c) Our construction simulates the quantum circuit (a) exactly by using the compressed oracles fO, cO, tO, iO and tracing out the auxiliary register.

was recently used in the adaptive security proof of a certain PRU construction [41], and can be used to construct cryptographic protocols such as quantum money [42, 43]. These notions are extended to several subgroups of the unitary groups, e.g., orthogonal t -design is defined for the orthogonal group [44], and pseudorandom permutation [45] and the compressed permutation oracle [46, 47] are defined for the permutation group.

Approximate unitary t -design can be implemented efficiently [48–68] with the state-of-the-art circuit complexity $\tilde{O}(nt)$ given in Refs. [67, 68] matching with the lower bound $\Omega(nt)$ shown in Ref. [34]. Known implementation of exact t -design is highly inefficient [69] except for $t \leq 3$ [17, 70, 71]. The recent breakthrough in the con-

* All authors contributed equally to this work.

Dmitry Grinko: grinko.dimitry@gmail.com

Satoshi Yoshida: satoshiyoshida.phys@gmail.com

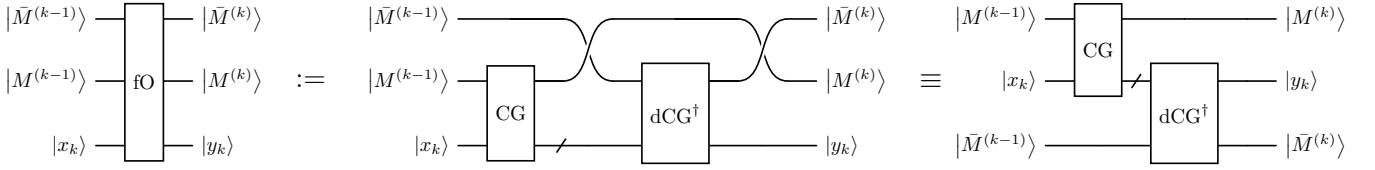


FIG. 2. Compressed oracle fO for an arbitrary group G written in standard quantum circuit notation (time goes from left to right). x_k denotes the input, y_k —the output, while M and $\bar{M}$ label basis states of the ancilla registers, which store irreducible representations of G . Clebsch–Gordan transform decomposes tensor product of representations $\lambda \otimes R$, where λ is some irrep and R is a given unitary representation of G . Such decomposition is in general not multiplicity-free, and the register carrying the multiplicity is highlighted with a slash wire.

struction of secure PRU [41], based on the PFC construction of Ref. [63], shows the adaptive security proof based on the compressed oracle called the path-recording oracle simulating the Haar-random unitary approximately with the forward and inverse queries. However, the path-recording oracle cannot choose the precision arbitrarily. Reference [43] proposes an exact simulation of the forward query of a random unitary with efficient memory size, but it is not constructive, and its efficiency in circuit complexity is not known. The extension to subgroups of the unitary group is less clarified; e.g., an efficient construction of the compressed permutation oracle is a long-standing open problem [46, 47]. In another line of research, the work [72] introduced a duality between so-called Fourier subspace extraction and implementation of group representation, which was then used in the construction of quantum money.

In this work, we present an exact construction of the compressed oracle for the Haar random ensemble corresponding to any unitary representation $R : G \rightarrow \text{End}(V)$ of a compact group G . We provide an efficient construction for the unitary group ($G = \text{U}(d)$, $R(U) = U$) with the circuit complexity given by $\text{poly}(n, t, \log \epsilon^{-1})$ with the compilation error ϵ and $n = \log(d)$. Our construction is based on basic facts from the representation theory of compact groups and efficient implementation of the (dual) Clebsch-Gordan (CG) transforms for the unitary group [73–78]. Moreover, we can simulate not only forward queries, but also conjugate, transpose and inverse queries. This versatility is quite interesting, and in the light of recent attention to conjugate and transpose queries [79] our work unifies simulation of all four query types. We conjecture that this generalization could be efficiently implemented for a wide variety of groups. In particular, our construction applied to the permutation group provides a compressed oracle for the random permutations [46, 47]. Our simulator can also be used to twirl a given quantum supermap, which can convert algorithmic errors in certain tasks to a white-noise error in higher-order quantum transformations of unitary channels [80].

Main results.— Now we state informally our two main results. First, for an arbitrary given compact group G

together with some unitary representation $R : G \rightarrow \text{End}(V)$, where $\text{End}(V)$ is the space of linear operators on a finite-dimensional linear space V . Second, specifically for the unitary group $\text{U}(d)$ and R being the defining representation (labelled by Young diagram $\square$), we explain how to efficiently implement forward queries. We briefly explain the main ideas behind the proofs, while the full proofs could be found in Appendix A.

Theorem 1 (Informal). *For any compact group, there exists exact compressed oracles fO, cO, iO and tO, which can simulate respectively forward, conjugate, inverse and transpose of an action of Haar random group elements in a given unitary representation. These oracles can be easily constructed from two Clebsch–Gordan transforms.*

Proof idea. We use the notation introduced in the End Matter for the representation theory. The main idea behind the proof technique is schematically described in Fig. 4 for the case of forward queries fO: the quantum circuit consisting of our compressed oracles from Fig. 2 can be easily seen to be equivalent to the tensor network contraction involving Clebsch–Gordan tensors, which is the tensor network representation of the Clebsch–Gordan transform. Namely, top and bottom tensor networks in the middle of the equation in Fig. 4 correspond to matrix units $E_{T,S}^\lambda$ of the commutant of the tensor action $R^{\otimes t}$. The summation is done over all possible matrix units $E_{T,S}^\lambda$ of the commutant for $\lambda \in \hat{G}^{(t)}$, $S = (S_0, s_1, S_1, \dots, s_t, S_t)$, $T = (T_0, t_1, T_1, \dots, t_t, T_t) \in B(\lambda)$. As a final technical step, Lem. 3 in Thm. 4 shows how to connect such a sum of matrix units with the required Haar integral. A slight modification of the above argument also works for other query types cO, tO, iO (conjugate, transpose and inverse): one needs to swap the positions of CG and dCG in all possible ways (horizontally and vertically) to realize them, see Fig. 3. The full proof can be found in Appendix A. $\square$

Theorem 2. *Successive application of forward oracles fO can simulate t queries of the Haar random unitary group $\text{U}(d)$ elements with total gate and depth complexity $t^5 \text{polylog}(d, \epsilon^{-1})$. The memory cost is $t^2 \text{polylog}(d, \epsilon^{-1})$.*

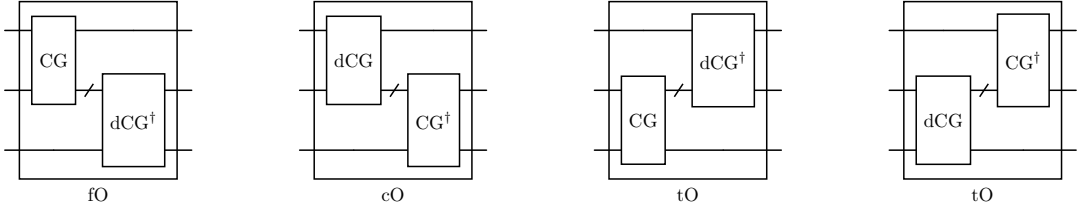


FIG. 3. Four types of oracles based on the corresponding query types: forward fO, conjugate cO, transpose tO, inverse iO.

$$\begin{aligned}
 & \sum_{\lambda \in \widehat{G}^{(t)}} \sum_{T, S \in B(\lambda)} \\
 & \int_{\text{Haar}} dg \langle y_t | R(g) | x_t \rangle \cdots \langle y_1 | R(g) | x_1 \rangle \cdot \langle \hat{x}_1 | R(g^{-1}) | \hat{y}_1 \rangle \cdots \langle \hat{x}_t | R(g^{-1}) | \hat{y}_t \rangle
 \end{aligned}$$

FIG. 4. Proof idea behind the construction of our compressed oracle fO. The top figure is drawn in the Heisenberg picture and represents t queries to the oracle fO. The middle figure is the rewriting of the top one in terms of (dual) Clebsch–Gordan tensors, which comprise matrix units of the commutant of $R^{\otimes t}$ action. The bottom is an equivalent Haar integral expression. The equalities are proven in detail in Appendix A of the SM [81].

Proof idea. The main idea behind this theorem is that for the case of the unitary group $U(d)$, the construction of the t -th CG transform is efficient in t and d , having $\tilde{O}(t^4)$ gate and depth complexity and $\tilde{O}(t^2)$ memory complexity, where $\tilde{O}(\cdot)$ hides polylogarithmic factors in d and ϵ^{-1} . See Appendix B of the Supplementary Material (SM) [81] for details. If we have in total t calls to simulate, then the total time and depth complexity is given by $\sum_{k=1}^t \tilde{O}(k^4) = \tilde{O}(t^5)$, while the memory complexity is $\tilde{O}(t^2)$ since we are reusing and adding new memory “on the fly”. This construction relies on the fact that we can efficiently and reversibly compress Gelfand–Tsetlin patterns, which label basis vectors of irreducible representations (irreps) of the unitary group $U(d)$. $\square$

Comparison with the previous works.— We compare the construction of the compressed oracles for t queries of the Haar-random n -qubit unitary with the previous works [41, 43] (see Tab. I). The exact simulation of the Haar-random unitary shown in Ref. [43] uses $O(nt)$ qubits, but it is not constructive, and the depth is not bounded. The path-recording oracle shown in Ref. [41] is

efficient in memory and depth, but its precision is fixed to be $O(t^2/2^n)$, where the precision is given by the worst-case diamond-norm error between the quantum channels given in Figs. 1 (a) and (c), where we take the worst case with respect to the quantum channels inserted in between the random unitaries. Our construction provides efficiency in memory and depth, and its precision can be chosen arbitrarily since the error only comes from the compilation error of implementing the CG transforms.

Application for the quantum cryptography.— Our random unitary simulator can be applied for the permuta-

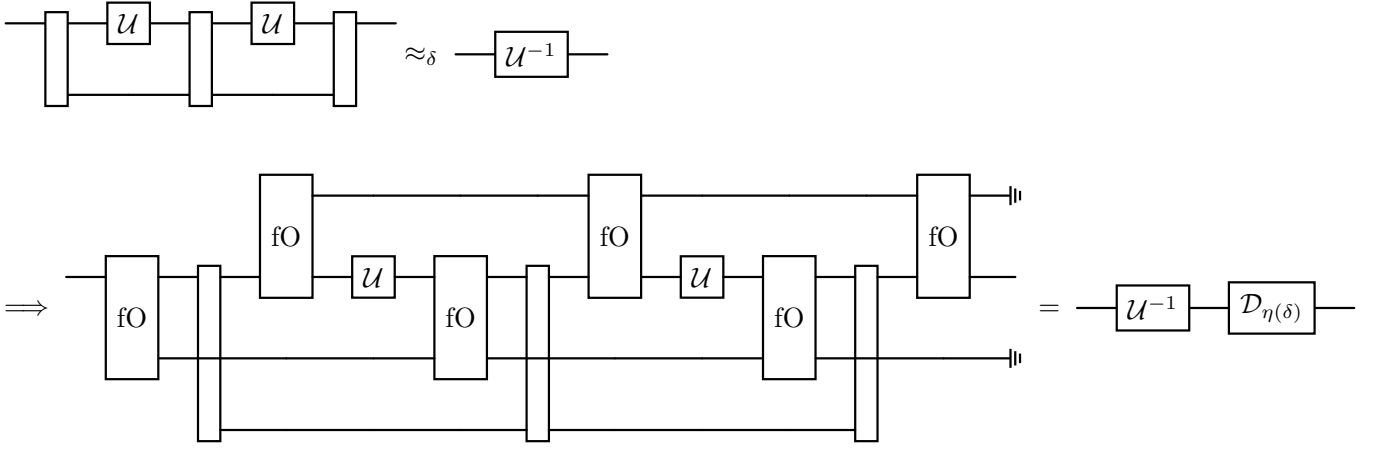


FIG. 5. Twirling of the approximate unitary inversion protocol using the forward compressed oracle fO. The top figure corresponds to a quantum comb that approximately implements unitary inversion with n queries to the input unitary channel U with the average-case channel fidelity $F = 1 - \delta$ defined in Eq. (3). The bottom figure corresponds to the twirled quantum comb that transforms n queries of U into the channel given by $\mathcal{D}_{\eta(\delta)} \circ \mathcal{U}^{-1}$, where $\mathcal{D}_{\eta(\delta)}$ is a depolarizing channel with the noise parameter given by $\eta(\delta) = \frac{d^2}{d^2-1}\delta$.

tion group $G = \mathfrak{S}_d$ with the representation¹

$$g \in \mathfrak{S}_d \mapsto V_g := \sum_{x=1}^d |g(x)\rangle\langle x| \in \text{End}(\mathbb{C}^d). \quad (2)$$

This construction provides a compressed oracle for random permutation (compressed permutation oracle), whose construction was a long-standing open problem [46]. Reference [47] proposes a construction of a compressed permutation oracle, but it is inefficient. We conjecture that our random unitary simulator applied to the permutation group presents an efficient implementation of a compressed permutation oracle, which can potentially be shown by constructing the (dual) CG transforms for the permutation group efficiently.

Application for the quantum supermaps.— Reference [80] shows that any approximate unitary inversion protocol can be converted to a unitary inversion protocol with the white-noise error. This conversion is done by twirling the corresponding Choi matrix, but it is unknown how the conversion is done on the level of a quantum circuit. Our simulator makes this conversion possible as shown in Fig. 5, which uses the forward compressed oracle fO to implement the twirling of the quantum comb.

¹ Oracle accesses to V_g and $V_{g^{-1}}$ are equivalent to oracle accesses to U_g and $U_{g^{-1}}$ for the following more standard oracle:

$$U_g := \sum_{x,y=1}^d |x, y \oplus_d g(x)\rangle\langle x, y|, \quad (1)$$

where $\oplus_d$ represents the summation modulo d , since either can be simulated using two queries to the other [see Appendix C of the SM [81] for the details].

Suppose we have a quantum comb $\mathcal{C}$ approximately implementing unitary inversion with n queries to the input unitary channel $U \in U(d)$ with the average-case channel fidelity $F = 1 - \delta$, where F is defined by

$$F := \int dU F_{\text{ch}}(\mathcal{C}[\mathcal{U}^{\otimes n}], \mathcal{U}^{-1}), \quad (3)$$

where dU is the Haar measure of $U(d)$, $\mathcal{U}(\cdot) = U \cdot U^{-1}$ and $\mathcal{U}^{-1}(\cdot) = U^{-1} \cdot U$ are the unitary channel corresponding to U and U^{-1} , and $F_{\text{ch}}(\mathcal{C}[\mathcal{U}^{\otimes n}], \mathcal{U}^{-1})$ is the channel fidelity given by $F_{\text{ch}}(\mathcal{C}[\mathcal{U}^{\otimes n}], \mathcal{U}^{-1}) := \frac{1}{d^2} \sum_i |\text{Tr}(K_i U)|^2$ using the Kraus operators $\{K_i\}$ satisfying $\mathcal{C}[\mathcal{U}^{\otimes n}](\cdot) = \sum_i K_i \cdot K_i^\dagger$. Then, we can construct a quantum comb that transforms n queries of U into the channel given by

$$\mathcal{D}_{\eta(\delta)} \circ \mathcal{U}^{-1}, \quad (4)$$

where $\mathcal{D}_{\eta(\delta)}$ is a depolarizing channel defined by

$$\mathcal{D}_{\eta(\delta)}(\cdot) = [1 - \eta(\delta)] \cdot + \eta(\delta) \frac{\mathbb{1}_d}{d} \text{Tr}[\cdot] \quad (5)$$

with the noise parameter given by $\eta(\delta) = \frac{d^2}{d^2-1}\delta$. This conversion can be extended to other tasks, such as unitary transposition [80] and unitary complex conjugation [82, 83] using the corresponding compressed oracles. The conversion to the white-noise error is beneficial in two ways. First, this conversion makes the algorithmic error independent of the input unitary channel U , and the worst-case error of the converted protocol is the same as the average-case error of the original protocol [80]. Secondly, the white-noise error can be treated more easily than the general error, e.g., the white-noise error can be mitigated in a cost-optimal way using the rescaling method [84], and the white-noise error on the quantum

TABLE I. Comparison of spacetime cost for simulation of t queries of n -qubit Haar random unitary with Ref. [43] and the path-recording oracle in Ref. [41]. Since the results of Ref. [43] are not constructive, the depth and precision are not studied. Error ϵ is an artifact of the compilation process: in particular, our construction can be made exact in theory (i.e. $\epsilon = 0$), while Ref. [41] always has an inherent error of order $O(t^2/2^n)$.

	Memory	Depth	Precision
Ref. [43]	$O(nt)$	—	—
Ref. [41]	$nt \cdot \text{polylog}(\epsilon^{-1})$	$\text{poly}(t, n, \log \epsilon^{-1})$	$\epsilon + O(t^2/2^n)$
This work	$t^2 \text{poly}(n, \log \epsilon^{-1})$	$t^5 \text{poly}(n, \log \epsilon^{-1})$	ϵ

state can be efficiently purified by using multiple rounds of the swap test [85] or using the Schur sampling [86].

Conclusion.— This Letter presents an exact implementation of the Haar-random ensemble of any unitary representation of a compact group using the (dual) CG transforms. This construction provides an efficient simulation of the Haar-random unitary with arbitrary precision. Our construction applied to the permutation group implements the compressed permutation oracle, which will be helpful in the construction and the security proof of the pseudorandom permutation. Our construction can also be used to implement the twirling of the quantum supermap at the circuit level, which can be used to transform the algorithmic error into the white-noise error.

Our work shows that an efficient simulation of the Haar-random ensemble is possible once the corresponding (dual) CG transforms are implemented efficiently. Moreover, our results highlight the quantum information theoretic importance of the CG transforms and motivates studying the CG transforms beyond the unitary group. We leave it as an open problem to provide efficient implementations of the CG transforms for several groups, such as the permutation group.

Note added.— During the preparation of this work, an independent work [87] shows a different construction of a compressed permutation oracle than ours, which is applied for the security proofs of pseudorandom permutation and quantum query lower bounds in the random permutation model.

Acknowledgments.— We acknowledge Mio Murao, Shogo Yamada, Adam Burchardt, Maris Ozols, Yu-Hsuan Huang, Gina Muuss, Silvia Ritsch, Christian Schaffner, Michael Walter and Christian Majenz for fruitful discussions. S. Y. acknowledges support by Japan Society for the Promotion of Science (JSPS) KAKENHI Grant Number 23KJ0734, FoPM, WINGS Program, the University of Tokyo, and DAIKIN Fellowship Program, the University of Tokyo. D. G. acknowledges support by NWO grant NGF.1623.23.025 (“Qudits in theory and experiment”) and NWO Vidi grant (Project No. VI.Vidi.192.109).

- [1] H.-Y. Huang, R. Kueng, and J. Preskill, Predicting many properties of a quantum system from very few measurements, *Nature Physics* **16**, 1050 (2020), [arXiv:2002.08953](#).
- [2] A. Zhao, N. C. Rubin, and A. Miyake, Fermionic Partial Tomography via Classical Shadows, *Phys. Rev. Lett.* **127**, 110504 (2021), [arXiv:2010.16094](#).
- [3] A. Elben, S. T. Flammia, H.-Y. Huang, R. Kueng, J. Preskill, B. Vermersch, and P. Zoller, The randomized measurement toolbox, *Nature Reviews Physics* **5**, 9 (2023), [arXiv:2203.11374](#).
- [4] C. Bertoni, J. Haferkamp, M. Hinsche, M. Ioannou, J. Eisert, and H. Pashayan, Shallow Shadows: Expectation Estimation Using Low-Depth Random Clifford Circuits, *Phys. Rev. Lett.* **133**, 020602 (2024), [arXiv:2209.12924](#).
- [5] K. Wan, W. J. Huggins, J. Lee, and R. Babbush, Matchgate shadows for fermionic quantum simulation, *Communications in Mathematical Physics* **404**, 629 (2023), [arXiv:2207.13723](#).
- [6] J. Kunjummen, M. C. Tran, D. Carney, and J. M. Taylor, Shadow process tomography of quantum channels, *Phys. Rev. A* **107**, 042403 (2023), [arXiv:2110.03629](#).
- [7] R. Levy, D. Luo, and B. K. Clark, Classical shadows for quantum process tomography on near-term quantum computers, *Phys. Rev. Res.* **6**, 013029 (2024), [arXiv:2110.02965](#).
- [8] J. Helsen, M. Ioannou, J. Kitzinger, E. Onorati, A. Werner, J. Eisert, and I. Roth, Shadow estimation of gate-set properties from random sequences, *Nature Communications* **14**, 5039 (2023), [arXiv:2110.13178](#).
- [9] 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 Physics* **14**, 595 (2018), [arXiv:1608.00263](#).
- [10] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. Brandao, D. A. Buell, *et al.*, Quantum supremacy using a programmable superconducting processor, *Nature* **574**, 505 (2019).
- [11] B. Ware, A. Deshpande, D. Hangleiter, P. Niroula, B. Fefferman, A. V. Gorshkov, and M. J. Gullans, A sharp phase transition in linear cross-entropy benchmarking, [arXiv:2305.04954](#) (2023).
- [12] D. Hangleiter and J. Eisert, Computational advantage of quantum random sampling, *Rev. Mod. Phys.* **95**, 035001 (2023), [arXiv:2206.04079](#).
- [13] A. Morvan, B. Villalonga, X. Mi, S. Mandra, A. Bengtsson, P. Klimov, Z. Chen, S. Hong, C. Erickson, I. Drozdov, *et al.*, Phase transitions in random circuit sampling, *Nature* **634**, 328 (2024), [arXiv:2304.11119](#).
- [14] B. Fefferman, S. Ghosh, and W. Zhan, Anti-concentration for the unitary Haar measure and applications to random quantum circuits, [arXiv:2407.19561](#) (2024).
- [15] J. Emerson, R. Alicki, and K. Życzkowski, Scalable noise estimation with random unitary operators, *Journal of Optics B: Quantum and Semiclassical Optics* **7**, S347 (2005), [arXiv:quant-ph/0503243](#).
- [16] E. Knill, D. Leibfried, R. Reichle, J. Britton, R. B. Blakestad, J. D. Jost, C. Langer, R. Ozeri, S. Sei-

- delin, and D. J. Wineland, Randomized benchmarking of quantum gates, *Phys. Rev. A* **77**, 012307 (2008), [arXiv:0707.0963](#).
- [17] 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), [arXiv:quant-ph/0606161](#).
- [18] E. Magesan, J. M. Gambetta, and J. Emerson, Scalable and Robust Randomized Benchmarking of Quantum Processes, *Phys. Rev. Lett.* **106**, 180504 (2011), [arXiv:1009.3639](#).
- [19] J. Eisert, D. Hangleiter, N. Walk, I. Roth, D. Markham, R. Parekh, U. Chabaud, and E. Kashefi, Quantum certification and benchmarking, *Nature Reviews Physics* **2**, 382 (2020), [arXiv:1910.06343](#).
- [20] M. Bellare and P. Rogaway, Random oracles are practical: A paradigm for designing efficient protocols, in *Proceedings of the 1st ACM Conference on Computer and Communications Security* (1993) pp. 62–73.
- [21] D. Boneh, Ö. Dagdelen, M. Fischlin, A. Lehmann, C. Schaffner, and M. Zhandry, Random Oracles in a Quantum World, in *Advances in Cryptology—ASIACRYPT 2011: 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4–8, 2011. Proceedings 17* (Springer, 2011) pp. 41–69, [arXiv:1008.0931](#).
- [22] M. Zhandry, How to Record Quantum Queries, and Applications to Quantum Indifferentiability, in *Advances in Cryptology—CRYPTO 2019: 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18–22, 2019, Proceedings, Part II 39* (Springer, 2019) pp. 239–268.
- [23] L. Chen and R. Movassagh, Quantum Merkle Trees, *Quantum* **8**, 1380 (2024), [arXiv:2112.14317](#).
- [24] A. Bouland, B. Fefferman, and U. Vazirani, Computational pseudorandomness, the wormhole growth paradox, and constraints on the AdS/CFT duality, [arXiv:1910.14646](#) (2019).
- [25] P. Ananth, J. Bostanci, A. Gulati, and Y.-T. Lin, Pseudorandomness in the (Inverseless) Haar Random Oracle Model, in *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (Springer, 2025) pp. 138–166, [arXiv:2410.19320](#).
- [26] M. Hhan and S. Yamada, Pseudorandom Function-like States from Common Haar Unitary, [arXiv:2411.03201](#) (2024).
- [27] D. N. Page, Information in black hole radiation, *Phys. Rev. Lett.* **71**, 3743 (1993), [arXiv:hep-th/9306083](#).
- [28] P. Hayden and J. Preskill, Black holes as mirrors: quantum information in random subsystems, *Journal of High Energy Physics* **2007**, 120 (2007), [arXiv:0708.4025](#).
- [29] P. Hosur, X.-L. Qi, D. A. Roberts, and B. Yoshida, Chaos in quantum channels, *Journal of High Energy Physics* **2016**, 1 (2016), [arXiv:1511.04021](#).
- [30] D. A. Roberts and B. Yoshida, Chaos and complexity by design, *Journal of High Energy Physics* **2017**, 1 (2017), [arXiv:1610.04903](#).
- [31] A. Nahum, J. Ruhman, S. Vijay, and J. Haah, Quantum Entanglement Growth under Random Unitary Dynamics, *Phys. Rev. X* **7**, 031016 (2017), [arXiv:1608.06950](#).
- [32] A. Nahum, S. Vijay, and J. Haah, Operator Spreading in Random Unitary Circuits, *Phys. Rev. X* **8**, 021014 (2018), [arXiv:1705.08975](#).
- [33] J. Kudler-Flam, V. Narovlansky, and S. Ryu, Distinguishing Random and Black Hole Microstates, *PRX Quantum* **2**, 040340 (2021), [arXiv:2108.00011](#).
- [34] F. G. Brandão, W. Chemissany, N. Hunter-Jones, R. Kueng, and J. Preskill, Models of quantum complexity growth, *PRX Quantum* **2**, 030316 (2021), [arXiv:1912.04297](#).
- [35] J. Haferkamp, P. Faist, N. B. Kothakonda, J. Eisert, and N. Yunger Halpern, Linear growth of quantum circuit complexity, *Nature Physics* **18**, 528 (2022), [arXiv:2106.05305](#).
- [36] M. P. Fisher, V. Khemani, A. Nahum, and S. Vijay, Random quantum circuits, *Annual Review of Condensed Matter Physics* **14**, 335 (2023), [arXiv:2207.14280](#).
- [37] R. Suzuki, J. Haferkamp, J. Eisert, and P. Faist, Quantum complexity phase transitions in monitored random circuits, *Quantum* **9**, 1627 (2025), [arXiv:2305.15475](#).
- [38] A. Ambainis and J. Emerson, Quantum t-designs: t-wise independence in the quantum world, in *Twenty-Second Annual IEEE Conference on Computational Complexity (CCC’07)* (IEEE, 2007) pp. 129–140, [arXiv:quant-ph/0701126](#).
- [39] A. A. Mele, Introduction to Haar measure tools in quantum information: A beginner’s tutorial, *Quantum* **8**, 1340 (2024), [arXiv:2307.08956](#).
- [40] Z. Ji, Y.-K. Liu, and F. Song, Pseudorandom quantum states, in *Advances in Cryptology—CRYPTO 2018: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part III 38* (Springer, 2018) pp. 126–152.
- [41] F. Ma and H.-Y. Huang, How to construct random unitaries, [arXiv:2410.10116](#) (2024).
- [42] S. Wiesner, Conjugate coding, *ACM Sigact News* **15**, 78 (1983).
- [43] G. Alagic, C. Majenz, and A. Russell, Efficient simulation of random states and random unitaries, in *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (Springer, 2020) pp. 759–787, [arXiv:1910.05729](#).
- [44] R. O’Donnell, R. A. Servedio, and P. Paredes, Explicit orthogonal and unitary designs, in *2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS)* (2023) pp. 1240–1260, [arXiv:2310.13597](#).
- [45] M. Zhandry, A note on quantum-secure PRPs, *Quantum* **9**, 1696 (2025), [arXiv:1611.05564](#).
- [46] D. Unruh, Towards compressed permutation oracles, in *International Conference on the Theory and Application of Cryptology and Information Security* (Springer, 2023) pp. 369–400.
- [47] C. Majenz, G. Malavolta, and M. Walter, Permutation superposition oracles for quantum query lower bounds, in *Proceedings of the 57th Annual ACM Symposium on Theory of Computing* (2025) pp. 1508–1519, [arXiv:2407.09655](#).
- [48] J. Emerson, E. Livine, and S. Lloyd, Convergence conditions for random quantum circuits, *Phys. Rev. A* **72**, 060302 (2005), [arXiv:quant-ph/0503210](#).
- [49] A. W. Harrow and R. A. Low, Random quantum circuits are approximate 2-designs, *Communications in Mathematical Physics* **291**, 257 (2009), [arXiv:0802.1919](#).
- [50] W. G. Brown and L. Viola, Convergence Rates for Arbitrary Statistical Moments of Random Quantum Circuits, *Phys. Rev. Lett.* **104**, 250501 (2010), [arXiv:0910.0913](#).
- [51] F. G. S. L. Brandão, A. W. Harrow, and M. Horodecki,

- Local Random Quantum Circuits Are Approximate Polynomial-Designs, *Communications in Mathematical Physics* **346**, 397 (2016), [arXiv:1208.0692 \[quant-ph\]](#).
- [52] Y. Nakata, C. Hirche, C. Morgan, and A. Winter, Unitary 2-designs from random X - and Z -diagonal unitaries, *J. Math. Phys.* **58**, 052203 (2017), [arXiv:1502.07514 \[quant-ph\]](#).
- [53] Y. Nakata, C. Hirche, M. Mlinar, and J. Eisert, Efficient unitary designs with nearly time-independent hamiltonian dynamics, *Phys. Rev. X* **7**, 021006 (2017), [arXiv:1609.07021 \[quant-ph\]](#).
- [54] N. Hunter-Jones, Unitary designs from statistical mechanics in random quantum circuits, [arXiv:1905.12053](#) (2019).
- [55] J. Haferkamp and N. Hunter-Jones, Improved spectral gaps for random quantum circuits: Large local dimensions and all-to-all interactions, *Phys. Rev. A* **104**, 022417 (2021), [arXiv:2012.05259](#).
- [56] W. W. Ho and S. Choi, Exact Emergent Quantum State Designs from Quantum Chaotic Dynamics, *Phys. Rev. Lett.* **128**, 060601 (2022), [arXiv:2109.07491](#).
- [57] M. Liu, J. Liu, Y. Alexeev, and L. Jiang, Estimating the randomness of quantum circuit ensembles up to 50 qubits, *npj Quantum Information* **8**, 137 (2022), [arXiv:2205.09900](#).
- [58] J. Haferkamp, Random quantum circuits are approximate unitary t -designs in depth $O(nt^{5+o(1)})$, *Quantum* **6**, 795 (2022), [arXiv:2203.16571 \[quant-ph\]](#).
- [59] S.-K. Jian, G. Bentsen, and B. Swingle, Linear growth of circuit complexity from Brownian dynamics, *Journal of High Energy Physics* **2023**, 1 (2023), [arXiv:2206.14205](#).
- [60] J. Haferkamp, F. Montealegre-Mora, M. Heinrich, J. Eisert, D. Gross, and I. Roth, Efficient unitary designs with a system-size independent number of non-clifford gates, *Communications in Mathematical Physics* **397**, 995 (2023), [arXiv:2002.09524](#).
- [61] A. W. Harrow and S. Mehraban, Approximate Unitary t -Designs by Short Random Quantum Circuits Using Nearest-Neighbor and Long-Range Gates, *Communications in Mathematical Physics* **401**, 1529 (2023), [arXiv:1804.06957 \[quant-ph\]](#).
- [62] C.-F. Chen, J. Docter, M. Xu, A. Bouland, F. G. Brandão, and P. Hayden, Efficient Unitary Designs from Random Sums and Permutations, in *2024 IEEE 65th Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE, 2024) pp. 476–484, [arXiv:2402.09335](#).
- [63] T. Metger, A. Poremba, M. Sinha, and H. Yuen, Simple constructions of linear-depth t -designs and pseudorandom unitaries, in *2024 IEEE 65th Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE, 2024) pp. 485–492, [arXiv:2404.12647](#).
- [64] J. Haah, Y. Liu, and X. Tan, Efficient approximate unitary designs from random Pauli rotations, in *2024 IEEE 65th Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE, 2024) pp. 463–475, [arXiv:2402.05239](#).
- [65] C.-F. Chen, J. Haah, J. Haferkamp, Y. Liu, T. Metger, and X. Tan, Incompressibility and spectral gaps of random circuits, [arXiv:2406.07478](#) (2024).
- [66] 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, *PRX Quantum* **5**, 040344 (2024), [arXiv:2310.19783 \[quant-ph\]](#).
- [67] T. Schuster, J. Haferkamp, and H.-Y. Huang, Random unitaries in extremely low depth, [arXiv:2407.07754](#) (2024).
- [68] L. Cui, T. Schuster, F. Brandao, and H.-Y. Huang, Unitary designs in nearly optimal depth, [arXiv:2507.06216](#) (2025).
- [69] Y. Nakata, D. Zhao, T. Okuda, E. Bannai, Y. Suzuki, S. Tamiya, K. Heya, Z. Yan, K. Zuo, S. Tamate, *et al.*, Quantum circuits for exact unitary t -designs and applications to higher-order randomized benchmarking, *PRX Quantum* **2**, 030339 (2021), [arXiv:2102.12617](#).
- [70] Z. Webb, The clifford group forms a unitary 3-design, *Quantum Info. Comput.* **16**, 1379 (2016), [arXiv:1510.02769](#).
- [71] H. Zhu, Multiqubit clifford groups are unitary 3-designs, *Phys. Rev. A* **96**, 062336 (2017), [arXiv:1510.02619](#).
- [72] J. Bostanci, B. Nehoran, and M. Zhandry, A General Quantum Duality for Representations of Groups with Applications to Quantum Money, Lightning, and Fire, in *Proceedings of the 57th Annual ACM Symposium on Theory of Computing* (2025) pp. 201–212, [arXiv:2411.00529 \[quant-ph\]](#).
- [73] D. Bacon, I. L. Chuang, and A. W. Harrow, Efficient quantum circuits for Schur and Clebsch-Gordan transforms, *Phys. Rev. Lett.* **97**, 170502 (2006), [arXiv:quant-ph/0407082](#).
- [74] D. Bacon, I. L. Chuang, and A. W. Harrow, The Quantum Schur and Clebsch-Gordan Transforms: I. Efficient Qudit Circuits, in *Proceedings of the Eighteenth Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '07 (Society for Industrial and Applied Mathematics, USA, 2007) pp. 1235–1244, [arXiv:quant-ph/0601001](#).
- [75] Q. T. Nguyen, The mixed Schur transform: efficient quantum circuit and applications, [arXiv:2310.01613](#) (2023).
- [76] D. Grinko, A. Burchardt, and M. Ozols, Gelfand-Tsetlin basis for partially transposed permutations, with applications to quantum information, [arXiv:2310.02252](#) (2023).
- [77] J. Fei, S. Timmerman, and P. Hayden, Efficient quantum algorithm for port-based teleportation, [arXiv:2310.01637](#) (2023).
- [78] A. Burchardt, J. Fei, D. Grinko, M. Larocca, M. Ozols, S. Timmerman, and V. Visnevskyi, High-dimensional quantum Schur transforms (2025), [arXiv:2509.22640 \[quant-ph\]](#).
- [79] M. Zhandry, How to model unitary oracles, in *Annual International Cryptology Conference* (Springer, 2025) pp. 237–268.
- [80] M. T. Quintino and D. Ebler, Deterministic transformations between unitary operations: Exponential advantage with adaptive quantum circuits and the power of indefinite causality, *Quantum* **6**, 679 (2022), [arXiv:2109.08202](#).
- [81] See the Supplementary Material for the details.
- [82] J. Miyazaki, A. Soeda, and M. Murao, Complex conjugation supermap of unitary quantum maps and its universal implementation protocol, *Phys. Rev. Res.* **1**, 013007 (2019), [arXiv:1706.03481](#).
- [83] D. Ebler, M. Horodecki, M. Marciniak, T. Młynik, M. T. Quintino, and M. Studziński, Optimal universal quantum circuits for unitary complex conjugation, *IEEE Transactions on Information Theory* **69**, 5069 (2023), [arXiv:2206.00107](#).
- [84] K. Tsubouchi, T. Sagawa, and N. Yoshioka, Universal Cost Bound of Quantum Error Mitigation Based

- on Quantum Estimation Theory, *Phys. Rev. Lett.* **131**, 210601 (2023), [arXiv:2405.07720](#).
- [85] A. M. Childs, H. Fu, D. Leung, Z. Li, M. Ozols, and V. Vyas, Streaming quantum state purification, *Quantum* **9**, 1603 (2025), [arXiv:2309.16387](#).
- [86] Z. Li, H. Fu, T. Isogawa, and I. Chuang, Optimal quantum purity amplification, [arXiv:2409.18167](#) (2024).
- [87] J. Carolan, Compressed Permutation Oracles, [arXiv:2509.18586](#).
- [88] T. Cioppa and B. Collins, Matrix units in the symmetric group algebra, and unitary integration, [arXiv:1307.4766](#) (2013).
- [89] N. Y. Vilenkin and A. U. Klimyk, Representations in the Gel'fand-Tsetlin Basis and Special Functions, in *Representation of Lie Groups and Special Functions: Volume 3: Classical and Quantum Groups and Special Functions* (Springer Netherlands, Dordrecht, 1992) pp. 361–446.
- [90] A. W. Harrow, *Applications of coherent classical communication and the Schur transform to quantum information theory*, Ph.D. thesis, Massachusetts Institute of Technology, Cambridge, MA, USA (2005), [arXiv:quant-ph/0512255](#).
- [91] H. Krovi, An efficient high dimensional quantum Schur transform, *Quantum* **3**, 122 (2019), [arXiv:1804.00055](#).

End Matter

We summarize the basics and notations of the representation theory, which is used in the proof sketch of Thm 1 and Fig. 4, but we leave more details in the SM [81]. The tensor product $R^{\otimes t}(g)$ of the given representation $R : G \rightarrow \text{End}(V)$ is decomposed as

$$V^{\otimes t} \simeq \bigoplus_{\lambda \in \hat{G}^{(t)}} V_{\lambda} \otimes M_{\lambda}, \quad (6)$$

$$R(g)^{\otimes t} \simeq \bigoplus_{\lambda \in \hat{G}^{(t)}} R_{\lambda}(g) \otimes I_{M_{\lambda}} \quad \forall g \in G, \quad (7)$$

where V_{λ} is the representation space of an irrep R_{λ} , M_{λ} is the corresponding multiplicity space, and $\hat{G}^{(t)}$ is the set of irrep labels appearing in the decomposition. The decomposition is obtained by recursively applying the Clebsch–Gordan transform, which corresponds to the irreducible decomposition of $R_{\mu}(g) \otimes R(g)$ for $\mu \in \hat{G}^{(t-1)}$ by

$$R_{\mu}(g) \otimes R(g) \simeq \bigoplus_{\lambda \in \hat{G}^{(t)}} R_{\lambda}(g) \otimes I_{m_{\lambda,\mu}} \quad \forall g \in G, \quad (8)$$

where $m_{\lambda,\mu}$ is the multiplicity of the irrep R_{μ} in the decomposition. By concatenating this irreducible decomposition, we obtain the multiplicity space M_{λ} whose basis vector is labeled by

$$T \in B(\lambda) := \{(T_0, t_1, T_1, \dots, t_t, T_t) \mid T_i \in \hat{G}^{(i)}, t_i \in [m_{T_{i-1}, T_i}]\}. \quad (9)$$

Due to Schur's lemma, the commutant of $R^{\otimes t}$ is given by a linear span of the matrix units $E_{T,S}^{\lambda} \simeq I_{V_{\lambda}} \otimes |T\rangle\langle S|_{M_{\lambda}}$ for $\lambda \in \hat{G}^{(t)}$ and $T, S \in B(\lambda)$:

$$\{X \in \text{End}(V^{\otimes t}) \mid [X, R(g)^{\otimes t}] = 0, \forall g \in G\} = \text{span}\{E_{T,S}^{\lambda} \mid \lambda \in \hat{G}^{(t)}, T, S \in B(\lambda)\}. \quad (10)$$

CONTENTS

Appendix A: Proof of the Thm. 1	9
Appendix B: Efficient Clebsch–Gordan transforms for $U(d)$	11
Appendix C: Equivalence of the oracle accesses to $U_g, U_{g^{-1}}$ and those to $V_g, V_{g^{-1}}$	13

Appendix A: Proof of the Thm. 1

In this section and the rest of the Appendix, we assume that the reader is familiar with standard representation theoretic notions. To state our main result, we need the following lemma, which is inspired by [88, Theorem 1]:

Lemma 3. *For a given compact group G and a unitary representation $R : G \rightarrow \text{End}(V)$, we have the following relation:*

$$\int_{\text{Haar}} dg R(g)_{y_n, x_n} \dots R(g)_{y_1, x_1} R(g^{-1})_{\hat{x}_1, \hat{y}_1} \dots R(g^{-1})_{\hat{x}_n, \hat{y}_n} = \sum_{\lambda \in \hat{G}^{(n)}} \frac{1}{d_\lambda} \sum_{T, S \in B(\lambda)} \langle \hat{x} | E_{T, S}^\lambda | x \rangle \langle \hat{y} | E_{T, S}^\lambda | y \rangle, \quad (11)$$

where $B(\lambda)$ is a set of labels of some orthonormal basis in M_λ , and $E_{T, S}^\lambda$ is a set of orthogonal matrix units for the commutant of $R^{\otimes n}$ action.

Proof. Firstly, we rewrite the left-hand side of Eq. (11) by using the following identity:

$$R(g)_{y_n, x_n} \dots R(g)_{y_1, x_1} R(g^{-1})_{\hat{x}_1, \hat{y}_1} \dots R(g^{-1})_{\hat{x}_n, \hat{y}_n} = \text{Tr} \left[|x\rangle\langle y| \otimes |\hat{x}\rangle\langle \hat{y}| \cdot R(g)^{\otimes n} \otimes \bar{R}(g)^{\otimes n} \right], \quad (12)$$

where we used unitarity of the representation R : $R(g^{-1})^\top = \bar{R}(g)$, where $\bar{R}(g)$ denotes complex conjugate of $R(g)$. According to the Peter–Weyl theorem

$$V^{\otimes n} \simeq^{U_{\text{Sch}}} \bigoplus_{\lambda \in \hat{G}^{(n)}} V_\lambda \otimes M_\lambda, \quad (13)$$

where $\hat{G}^{(n)}$ is the set of irreps in the tensor product representation $V^{\otimes n}$, V_λ is the irrep of G with the label λ , and M_λ is the multiplicity space of $R^{\otimes n}$ action. The basis transformation is achieved via unitary matrix U_{Sch} called the Schur transform. Similar Peter–Weyl theorem holds for the dual representation $\bar{V}$ of R :

$$\bar{V}^{\otimes n} \simeq^{U_{\text{Sch}}} \bigoplus_{\lambda \in \hat{G}^{(n)}} V_{\bar{\lambda}} \otimes M_\lambda, \quad (14)$$

where $\bar{\lambda}$ is the label of the irrep corresponding to the dual representation of λ . Now we apply two Schur transforms U_{Sch} to block-diagonalise the whole operator according to the Peter–Weyl decomposition of both left and right parts of our space $V^{\otimes n} \otimes \bar{V}^{\otimes n}$:

$$\int_{\text{Haar}} dg (U_{\text{Sch}} R(g)^{\otimes n} U_{\text{Sch}}^\dagger) \otimes (U_{\text{Sch}} \bar{R}(g)^{\otimes n} U_{\text{Sch}}^\dagger) = \int_{\text{Haar}} dg \left(\bigoplus_{\lambda} R_\lambda(g) \otimes I_\lambda \right) \otimes \left(\bigoplus_{\lambda'} R_{\bar{\lambda}'}(g) \otimes I_{\lambda'} \right) \quad (15)$$

By using the grand orthogonality relations

$$\int_{\text{Haar}} dg R_\lambda(g)_{x, y} R_{\bar{\lambda}'}(g)_{x', y'} = \frac{1}{d_\lambda} \delta_{\lambda, \lambda'} \delta_{x, x'} \delta_{y, y'}, \quad (16)$$

we get

$$\int_{\text{Haar}} dg \left(\bigoplus_{\lambda} R_\lambda(g) \otimes I_\lambda \right) \otimes \left(\bigoplus_{\lambda'} R_{\bar{\lambda}'}(g) \otimes I_{\lambda'} \right) = \bigoplus_{\lambda \in \hat{G}^{(n)}} \frac{1}{d_\lambda} |\Phi_\lambda^+\rangle\langle \Phi_\lambda^+| \otimes I_\lambda \otimes I_\lambda \quad (17)$$

$$= \bigoplus_{\lambda \in \hat{G}^{(n)}} \frac{1}{d_\lambda} \sum_{T, S \in B(M_\lambda)} |\Phi_\lambda^+\rangle\langle \Phi_\lambda^+| \otimes |S, T\rangle\langle S, T| \quad (18)$$

where $|\Phi_\lambda^+\rangle := \text{vec}(R_\lambda(e))$ is the vectorisation of identity operator on the irrep λ , or, equivalently, unnormalized maximally entangled state.

Recall, that a matrix unit $E_{S,T}^\lambda$ is defined in the Schur basis as

$$U_{\text{Sch}} E_{S,T}^\lambda U_{\text{Sch}}^\dagger = \bigoplus_{\mu} \delta_{\lambda,\mu} I_{d_\mu} \otimes |S\rangle\langle T| \equiv I_{d_\lambda} \otimes |S\rangle\langle T|, \quad (19)$$

so this implies that we can write

$$\text{vec}(U_{\text{Sch}} E_{S,T}^\lambda U_{\text{Sch}}^\dagger) \text{vec}(U_{\text{Sch}} E_{S,T}^\lambda U_{\text{Sch}}^\dagger)^\dagger = |\Phi_\lambda^+\rangle\langle\Phi_\lambda^+| \otimes |S,T\rangle\langle S,T|. \quad (20)$$

Therefore, by combining everything we get:

$$\int_{\text{Haar}} dg \text{Tr} \left[|x\rangle\langle y| \otimes |\hat{x}\rangle\langle\hat{y}| \cdot R(g)^{\otimes n} \otimes \bar{R}(g)^{\otimes n} \right] = \quad (21)$$

$$= \text{Tr} \left[U_{\text{Sch}} |x\rangle\langle y| U_{\text{Sch}}^\dagger \otimes U_{\text{Sch}} |\hat{x}\rangle\langle\hat{y}| U_{\text{Sch}}^\dagger \int_{\text{Haar}} dg (U_{\text{Sch}} R(g)^{\otimes n} U_{\text{Sch}}^\dagger) \otimes (U_{\text{Sch}} \bar{R}(g)^{\otimes n} U_{\text{Sch}}^\dagger) \right] \quad (22)$$

$$= \sum_{\lambda \in \hat{G}^{(n)}} \frac{1}{d_\lambda} \sum_{T, S \in B(\lambda)} \text{Tr} \left[U_{\text{Sch}} |x\rangle\langle y| U_{\text{Sch}}^\dagger \otimes U_{\text{Sch}} |\hat{x}\rangle\langle\hat{y}| U_{\text{Sch}}^\dagger \text{vec}(U_{\text{Sch}} E_{S,T}^\lambda U_{\text{Sch}}^\dagger) \text{vec}(U_{\text{Sch}} E_{S,T}^\lambda U_{\text{Sch}}^\dagger)^\dagger \right] \quad (23)$$

$$= \sum_{\lambda \in \hat{G}^{(n)}} \frac{1}{d_\lambda} \sum_{T, S \in B(\lambda)} \langle \hat{x} | E_{T,S}^\lambda | x \rangle \langle \hat{y} | E_{T,S}^\lambda | y \rangle. \quad (24)$$

□

This lemma was proven for the unitary group in [88]. Similar statement trivially holds also for finite groups and their unitary representations. Now we are ready to present our main theorem, which is a formal version of Thm. 1:

Theorem 4. Consider the compressed oracle fO for arbitrary given compact group G together with its representation R , defined in Fig. 2. Then the following equality is true:

$$\sum_{\lambda \in \hat{G}^{(n)}} \frac{1}{d_\lambda} \sum_{T, S \in B(\lambda)} \langle \hat{x} | E_{T,S}^\lambda | x \rangle \langle \hat{y} | E_{T,S}^\lambda | y \rangle = \text{Tr}_\bullet \left[\text{fO}_{\bullet, (y_n, x_n)} \cdots \text{fO}_{\bullet, (y_1, x_1)} |\emptyset\rangle\langle\emptyset| \bullet \text{fO}_{\bullet, (\hat{x}_1, \hat{y}_1)}^\dagger \cdots \text{fO}_{\bullet, (\hat{x}_n, \hat{y}_n)}^\dagger \right] \quad (25)$$

where $B(\lambda)$ is a basis of irrep λ of the commutant of $R^{\otimes n}$ action, $E_{T,S}^\lambda$ are matrix units of the commutant, and $\text{fO}_{\bullet, (y_k, x_k)} := (I \otimes \langle y_k |) \text{fO}_{\text{aux, work}} (I \otimes |x_k\rangle)$, and compressed oracle fO acts on auxiliary and working registers.

Proof. As first step, we insert resolutions of identities on the multiplicity registers, and we redraw the RHS of Eq. (25) as in Fig. 4, where white circles correspond to Clebsch–Gordan tensor and grey circles correspond to dual Clebsch–Gordan tensors [76]. Secondly, note that the top tensor network in Fig. 4 is simply a matrix unit $E_{S,T}^\lambda$ of the commutant of $R^{\otimes n}$:

$E_{S,T}^\lambda :=$

$\langle x | E_{S,T}^\lambda | \hat{x} \rangle =$

(26)

where we are using notation $S = (S_0, s_1, S_1, s_2, S_2, \dots)$, $T = (T_0, t_1, T_1, t_2, T_2, \dots)$ to label basis vectors inside irreps of the commutant: s_i, t_i are multiplicity labels, and S_i, T_i are irrep labels. Note, that we avoid using multiplicity

indices in circles in most of the tensor network diagrams for brevity. Next, we use the following fact relating normal and dual Clebsch–Gordan tensors [89, Eq. (10), p. 289]:

$$\begin{array}{c} \nu \\ \nearrow \\ \bar{R} \end{array} \begin{array}{c} \circlearrowleft \\ i \end{array} \begin{array}{c} \searrow \\ \lambda \end{array} = \sqrt{\frac{d_\lambda}{d_\nu}} \begin{array}{c} \lambda \\ \nearrow \\ R \end{array} \begin{array}{c} \circlearrowleft \\ i \end{array} \begin{array}{c} \searrow \\ \nu \end{array}, \quad (27)$$

where i denotes multiplicity. Using this equality we can transform bottom tensor network of dual CG tensor into a tensor network with normal CG tensors:

$$\begin{array}{c} S_0 = \emptyset = T_0 \\ y_1 \rightarrow s_1 \xrightarrow{S_1} t_1 \leftarrow \hat{y}_1 \\ y_2 \rightarrow s_2 \xrightarrow{S_2} t_2 \leftarrow \hat{y}_2 \\ y_3 \rightarrow s_3 \xrightarrow{S_3} t_3 \leftarrow \hat{y}_3 \\ \vdots \\ y_{t-1} \rightarrow s_{t-1} \xrightarrow{S_{t-1}} t_{t-1} \leftarrow \hat{y}_{t-1} \\ y_t \rightarrow s_t \xrightarrow{S_t} t_t \leftarrow \hat{y}_t \\ S_t = \lambda = T_t \end{array} = \frac{1}{d_\lambda} \begin{array}{c} S_0 = \emptyset = T_0 \\ y_1 \rightarrow s_1 \xrightarrow{S_1} t_1 \leftarrow \hat{y}_1 \\ y_2 \rightarrow s_2 \xrightarrow{S_2} t_2 \leftarrow \hat{y}_2 \\ y_3 \rightarrow s_3 \xrightarrow{S_3} t_3 \leftarrow \hat{y}_3 \\ \vdots \\ y_{t-1} \rightarrow s_{t-1} \xrightarrow{S_{t-1}} t_{t-1} \leftarrow \hat{y}_{t-1} \\ y_t \rightarrow s_t \xrightarrow{S_t} t_t \leftarrow \hat{y}_t \\ S_t = \lambda = T_t \end{array} = \frac{1}{d_\lambda} \langle y | E_{S,T}^\lambda | \hat{y} \rangle, \quad (28)$$

so we see that the bottom tensor network in Fig. 4 can be identified with the LHS of Eq. (25). $\square$

Finally, we argue that the same proof with minor modifications also holds for oracles cO, tO, iO from Fig. 3. Consider, for example, oracle tO, which implements a transpose query. The reason this oracle works as intended can be seen from Eq. (12): if transpose is called at a given step i then

$$\cdots R(g)_{y_i, x_i}^\top \cdots R(g^{-1})_{y_i, x_i}^\top \cdots = \cdots R(g)_{x_i, y_i} \cdots R(g^{-1})_{x_i, y_i} \cdots \quad (29)$$

and the rest of the proofs of Lem. 3 and Thm. 4 proceeds in the same manner as for the case of forward oracle fO. For the conjugate query oracle cO the proof of Lem. 3 goes similarly, with the only difference that the relevant commutant comes from $R^{\otimes p} \otimes \bar{R}^{\otimes q}$ action, where $p + q = t$. Last, the proof for the inverse oracle iO uses the same trick based on cO oracle, as tO does it for fO.

Appendix B: Efficient Clebsch–Gordan transforms for $U(d)$

In this section, we provide a proof of Thm. 4 by describing an efficient construction of (dual) Clebsch–Gordan transforms for the unitary group with defining representation $\square$, which is needed to achieve $\text{poly}(n)$ complexity, where $n = \log_2(d)$. The main components of this construction were first described in detail explicitly in [78], based on the ideas from [90, 91]. We present them here with minor modifications and adaptations needed for our setting.

We start with the CG transform, which is presented in Fig. 6. It consists of two main components: preprocessing gate P and compressed CG transform.

The preprocessing gate P is needed to efficiently use the memory space by preparing the input $|x_k\rangle$ to be processed correctly within the compressed CG transform. The operation P consists of several steps, see Fig. 7.

The main intuition P comes from the following. Basis vectors of unitary group irreps are labelled by Gelfand–Tsetlin patterns or, equivalently, by Semistandard Young tableaux. Each pattern has an associated weight $w = (w_1, \dots, w_d)$, which counts number of 1, 2 and so on. It can be equivalently represented by a composition μ and an alphabet map p , that is, $w \cong (\mu, p)$, [78]. A given Gelfand–Tsetlin pattern $M \in \text{GT}(\lambda)$ can be equivalently represented by a smaller GT pattern $\tilde{M} \in \text{GT}(\lambda, \mu)$ of length $\ell(\mu)$, where $\ell(\mu)$ is the length of the composition μ , together with the alphabet map p , that is, $M \cong (\tilde{M}, p)$. For example, a Gelfand–Tsetlin pattern $M = ((0), (2, 0), (2, 0, 0), (2, 1, 0, 0), (3, 2, 0, 0, 0))$ corresponds to $\tilde{M} = ((2), (2, 1), (3, 2, 0))$ and $p = (2, 4, 5)$:

$$\begin{bmatrix} 3 & 2 & 2 & 0 & 0 & 0 & 0 \\ & 2 & 2 & 1 & 0 & 0 & 0 \\ & & 2 & 2 & 0 & 0 & 0 \\ & & & 2 & 0 & 0 & 0 \end{bmatrix} \equiv \left(\begin{bmatrix} 3 & 2 & 2 & 0 \\ & 2 & 2 & 1 \end{bmatrix}, (2, 4, 5) \right). \quad (30)$$

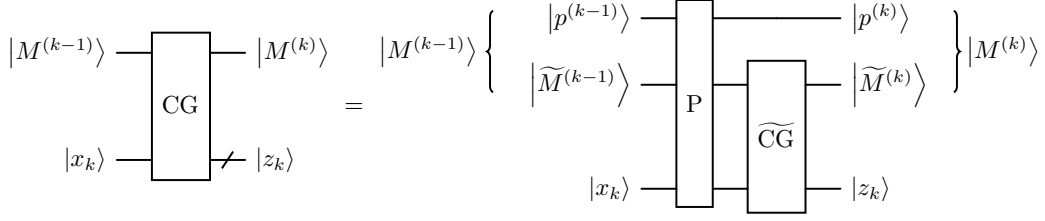


FIG. 6. Efficient CG transform consists of a preprocessing operation P , which is needed to modify compressed Gelfand–Tsetlin pattern $\widetilde{M}^{(k-1)}$ upon arrival of new symbol x_k .

Gate P effectively implements the above compression by handling newly arrived symbol $x_k \in [d]$ and updating old pair $(\widetilde{M}, p)$. It consists of four steps A , B , C , and D .

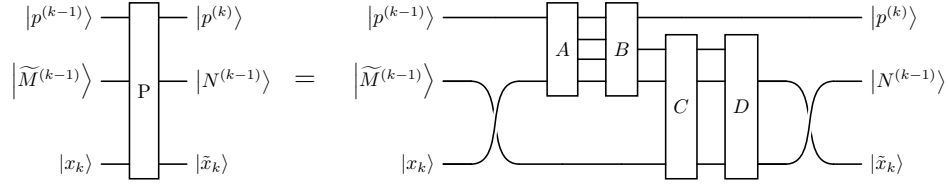


FIG. 7. Preprocessing operation P_k consists of four steps A , B , C and D . Steps A and B are needed to modify x_k and update weight information $p^{(k-1)}$ according the newly arrived symbol x_k . Step C modifies Gelfand–Tsetlin pattern $\widetilde{M}^{(k-1)}$ by adding one new row and shifting other rows according to the newly arrived symbol x_k . Finally, step D uncomputes one auxiliary register.

The transformation A records the value of $x_k \in [d]$ and transforms it into $\tilde{x}_k \in [k]$:

$$A : |p^{(k-1)}\rangle |x_k\rangle \rightarrow |p^{(k-1)}\rangle |x_k\rangle |c_k\rangle |\tilde{x}_k\rangle \quad (31)$$

$$c_k := \begin{cases} 1 & \text{if } x_k \in p^{(k-1)} \\ 0 & \text{if } x_k \notin p^{(k-1)} \end{cases} \quad (32)$$

$$\tilde{x}_k := \begin{cases} i \text{ s.t. } p_i^{(k-1)} = x_k & \text{if } x_k \in p^{(k-1)} \\ i \text{ s.t. } p_{i-1}^{(k-1)} < x_k < p_i^{(k-1)} & \text{if } x_k \notin p^{(k-1)} \end{cases} \quad (33)$$

where $c_k \in \{0, 1\}$ is a bit which indicated if the symbol x_k is new or not (if $x_k \in p^{(k-1)}$ then the symbol x_k have already appeared before), and i is a position of x_k within tuple $p^{(k-1)}$. Note that A is clearly reversible.

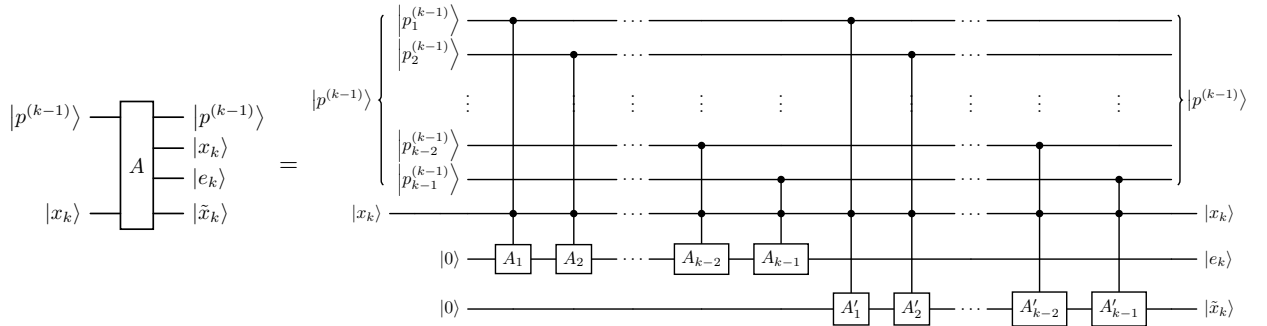


FIG. 8. Operation A . We refer to [78] for the details on the implementation of this gate.

The operation B updates the tuple $p^{(k-1)}$ to $p^{(k)}$ depending on the value of c_k :

$$B : |p^{(k-1)}\rangle |x_k\rangle |c_k\rangle |\tilde{x}_k\rangle \rightarrow |p^{(k)}\rangle |c_k\rangle |\tilde{x}_k\rangle \quad (34)$$

$$p^{(k)} := \begin{cases} (p^{(k-1)}, 0) & \text{if } c_k = 1 \\ (p_1^{(k-1)}, \dots, p_{\tilde{x}_k-1}^{(k-1)}, x_k, p_{\tilde{x}_k}^{(k-1)}, \dots, p_{k-1}^{(k-1)}) & \text{if } c_k = 0 \end{cases} \quad (35)$$

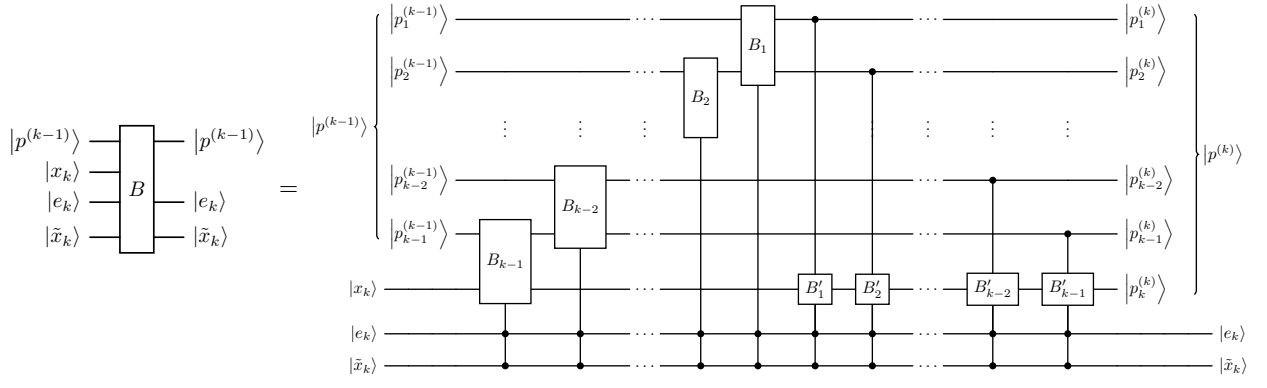


FIG. 9. Operation B . We refer to [78] for the details on the implementation of this gate.

Next, the operation C transforms the GT pattern $|\widetilde{M}^{(k-1)}\rangle$ differently according to the value of c_k :

$$C : |c_k\rangle|\tilde{x}_k\rangle|\widetilde{M}^{(k-1)}\rangle \rightarrow |c_k\rangle|\tilde{x}_k\rangle|N^{(k-1)}\rangle \quad (36)$$

$$\text{If } c_k = 1 : \quad (37)$$

$$N_l^{(k-1)} := \begin{cases} \widetilde{M}_l^{(k-1)}, & \text{if } 1 \leq l \leq k-1 \\ (\widetilde{M}_{k-1}^{(k-1)}, 0) & \text{if } l = k \end{cases} \quad (38)$$

$$\text{If } c_k = 0 : \quad (39)$$

$$N_l^{(k-1)} := \begin{cases} \widetilde{M}_l^{(k-1)} & \text{if } 1 \leq l < \tilde{x}_k \\ (\widetilde{M}_{l-1}^{(k-1)}, 0) & \text{if } \tilde{x}_k \leq l \leq k \end{cases} \quad (40)$$

The intuition behind transformation B_k is as follows. When x_k is a new symbol, i.e. when $c_k = 1$, then we need to simply copy the last row $\widetilde{M}_{k-1}^{(k-1)}$ of GT pattern $\widetilde{M}^{(k-1)}$ into a pattern $N^{(k-1)}$, which should have one more row. Otherwise, we need to copy a row somewhere inside the pattern $\widetilde{M}^{(k-1)}$.

Finally, the operation D uncomputes the additional bit c_k :

$$D : |c_k\rangle|\tilde{x}_k\rangle|N^{(k-1)}\rangle \rightarrow |0\rangle|\tilde{x}_k\rangle|N^{(k-1)}\rangle, \quad (41)$$

which is reversible since $c_k = 1$ is equivalent to $\sum_{i=1}^{\tilde{x}_k} N_{\tilde{x}_k, i}^{(k-1)} - \sum_{i=1}^{\tilde{x}_k-1} N_{\tilde{x}_k-1, i}^{(k-1)} = 0$, and $c_k = 0$ is equivalent to $\sum_{i=1}^{\tilde{x}_k} N_{\tilde{x}_k, i}^{(k-1)} - \sum_{i=1}^{\tilde{x}_k-1} N_{\tilde{x}_k-1, i}^{(k-1)} > 0$.

Remark 5. Note that implementing $\text{dCG}_k^\dagger$ is easy if we have a promise, that the output irrep of dCG_k is described by a Young diagram, i.e. there are no negative entries in the highest weight corresponding to the output. But this is indeed the case, since the input of the multiplicity space register from CG_k in Fig. 2 ensures that the output of $\text{dCG}_k^\dagger$ is a valid Young diagram: the “minus” gates in Fig. 10 when run in reverse never produce negative entries.

In total, operations A, B, C, D can be done in $O(k^3)$ gate and depth complexity [78]. Depth and gate complexity of $\widetilde{\text{CG}}$ and $\widetilde{\text{dCG}}$ transforms is $\widetilde{O}(k^4)$, while memory complexity is $\widetilde{O}(k^2)$ [75, 76, 78]. So, total complexity of CG_k and dCG_k is $\widetilde{O}(k^4)$, which implies $\widetilde{O}(k^4)$ gate and depth complexity for our compressed oracle cO .

Appendix C: Equivalence of the oracle accesses to U_g, U_{g-1} and those to V_g, V_{g-1}

The oracle accesses to U_g, U_{g-1} defined in Eq. (1) and those to V_g, V_{g-1} defined in Eq. (2) are equivalent since either can be simulated using two queries to the other. The simulation can be done as follows:

$$U_g|x, y\rangle = (V_{g-1} \otimes I_d)CX_d(V_g \otimes I_d)|x, y\rangle, \quad (42)$$

$$V_g|x\rangle = (I_d \otimes \langle 0|)U_{g-1} \cdot \text{SWAP} \cdot U_g|x, 0\rangle, \quad (43)$$

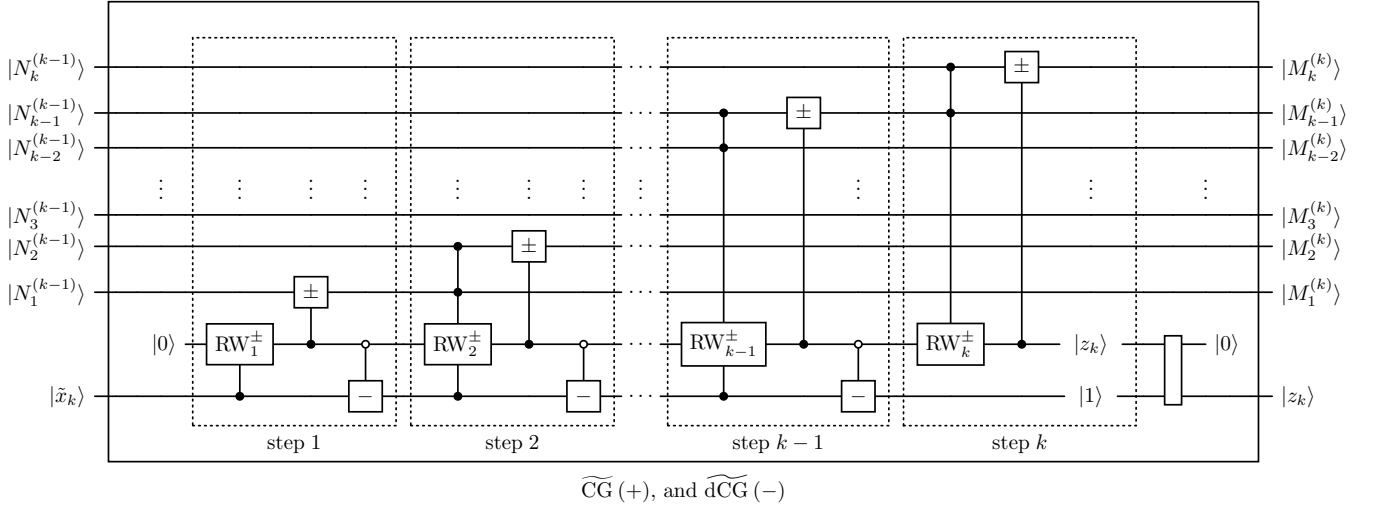


FIG. 10. Full circuit for (dual) Clebsch-Gordan transforms $\widetilde{CG}$ and $\widetilde{dCG}$ transforms (“+” corresponds to $\widetilde{CG}$ and “-” corresponds to $\widetilde{dCG}$). They consist of reduced Wigner transforms $RW^\pm$ and simple arithmetic gates. We refer to [76] for implementation details of the gates.

where I_d is the identity operator on $\mathbb{C}^d$ and CX_d and SWAP are two-qudit unitary operators defined by

$$CX_d := \sum_{x,y=1}^d |x, x \oplus_d y\rangle \langle x, y|, \quad (44)$$

$$SWAP := \sum_{x,y=1}^d |y, x\rangle \langle x, y|. \quad (45)$$