Preparing many copies of a quantum state in the black-box model

Yassine Hamoudi *

Simons Institute for the Theory of Computing, Berkeley, California 94720, USA

(Received 13 February 2022; accepted 3 June 2022; published 23 June 2022)

We describe a simple quantum algorithm for preparing K copies of an N-dimensional quantum state whose amplitudes are given by a quantum oracle. Our result extends a previous work of Grover, who showed how to prepare one copy in time $O(\sqrt{N})$. In comparison with the naive $O(K\sqrt{N})$ solution obtained by repeating this procedure K times, our algorithm achieves the optimal running time of $\Theta(\sqrt{KN})$. Our technique uses a refinement of the quantum rejection sampling method employed by Grover. As a direct application, we obtain a similar speedup for obtaining K independent samples from a distribution whose probability vector is given by a quantum oracle.

DOI: 10.1103/PhysRevA.105.062440

I. INTRODUCTION

The preparation of a specific quantum state is an important building block and a critical bottleneck in many quantum algorithms [1–4]. The objective of the state preparation problem is to find the minimum amount of resources needed to generate a quantum state given some description of it. In general, the complexity of this problem scales linearly with the dimension of the state to be prepared [5,6]. Yet, it is possible to achieve sublinear bounds for particular states or input models. One such example is the *black-box model* where, given oracle access to a nonzero non-negative vector $w = (w_1, \ldots, w_N)$, the objective is to load the associated normalized probability vector into the amplitudes of the $\log(N)$-qubit state $|w\rangle$ defined as

$$|w\rangle := \frac{1}{\sqrt{\mathcal{W}}} \sum_{i=1}^{N} \sqrt{w_i}|i\rangle, \tag{1}$$

where $\mathcal{W} = \sum_{i=1}^{N} w_i$ is the (unknown) normalization factor. Grover adapted his celebrated quantum search algorithm to this problem in Ref. [7], where he showed that $O(\sqrt{N})$ queries to w are sufficient to prepare $|w\rangle$. In practice, one can expect that *several* copies of the same quantum state are needed for further use. For instance, $|w\rangle$ may be fed in an algorithm that fails with some probability and that must be repeated several times. The no-cloning theorem prevents the state $|w\rangle$ from being easily duplicated. In fact, it is easy to show that additional queries to the input are required to prepare several copies of $|w\rangle$. The problem of adapting the state preparation procedure to the desired number K of copies has received little attention. Usually, it is possible to simply repeat K times the procedure used to prepare one copy, but the complexity grows linearly with K. For instance, the algorithm of Grover leads to a query complexity of $O(K\sqrt{N})$ for preparing the K-fold state $|w\rangle^{\otimes K}$. In this paper, we investigate the question of whether a more efficient approach exists. We describe a two-phase algorithm consisting of a preprocessing step that uses $O(\sqrt{KN})$ queries, after which each copy of $|w\rangle$ requires only $O(\sqrt{N/K})$ queries to be prepared. Our result improves upon the previous approach by a factor of $\sqrt{K}$, and it is shown to be optimal.

A. Related work

Our work is based on the *quantum rejection sampling* method, where a state that is easy to prepare (e.g., a uniform superposition) is mapped to a target state by amplitude amplification. This method was pioneered by Grover in Ref. [7] and subsequently studied in Refs. [8–11]. All of these works (except for Ref. [10]) take place in the quantum oracle model and they often require a number of queries that is polynomial in the dimension N of the state. In the nonoracular setting, the problem of loading an arbitrary vector $(w_1, \ldots, w_N)$ into the amplitudes of a quantum state can be done with a circuit of depth $O(N)$ and width $O(\log N)$ [5,6]. It is possible to use only polylog(N) resources for specific cases such as efficiently integrable probability distributions [12–14] (Proposition 4), uniformly bounded amplitudes [15], Gaussian states [16], or probability distributions resulting from a Bayesian network [10]. A different line of work [17–22] studied the preparation of a quantum state that corresponds to the stationary distribution of a Markov chain. These algorithms use Markov chain Monte Carlo methods and quantum walk techniques to obtain a preparation time scaling with the spectral gap. Aharonov and Ta-Shma [17] also showed that the existence of an efficient procedure to convert any circuit into a coherent state encoding the output distribution of that circuit would imply that $\mathsf{SZK} \subseteq \mathsf{BQP}$.

The state preparation problem is also related to the task of preparing samples from a discrete distribution. We refer the reader to Refs. [23–25] for a general introduction on the latter topic. In particular, the importance sampling problem (also called weighted sampling or L_1 sampling) asks to generate K independent samples from the probability vector $(\frac{w_1}{\mathcal{W}}, \ldots, \frac{w_N}{\mathcal{W}})$ associated with a non-negative weight vector w. The *alias method* [26–29] solves this problem with a

*hamoudi@berkeley.edu

preprocessing cost of $O(N)$ operations, and a generating cost of $O(1)$ operations per sample. Grover [7,30] suggested a quadratically faster algorithm for obtaining one sample, based on preparing the state $|w\rangle$ and measuring it in the computational basis. Our state preparation algorithm extends the work of Grover to the case of generating K independent samples with a total cost of $O(\sqrt{KN})$ operations. An alternative quantum algorithm for (approximately) generating K such samples was proposed before in Ref. [31], where it was combined with the stochastic gradient descent method to address the submodular function minimization problem.

B. Overview

The two parts of our state preparation algorithm are described in Theorems 2 and 3. Combined together, these results lead to the following main theorem.

Theorem 1. There is a quantum algorithm with the following properties. Consider two integers $1 \leqslant K \leqslant N$, a real $\delta \in (0, 1)$ and a nonzero vector $w \in \mathbb{R}^N_{\geqslant 0}$. Then, with probability at least $1 - \delta$, the algorithm outputs K copies of the state $|w\rangle$ and it uses $O(\sqrt{KN}\log(1/\delta))$ queries to w in expectation.

We now provide a high-level description of how the algorithm works. Our starting point is the result from Grover [7] for preparing one copy of the state $|w\rangle$ in the black-box model. Given an upper bound h on the largest value $\max_i w_i$, this algorithm uses two queries and one controlled rotation to implement a unitary U such that

$$U|\vec{0}\rangle = \frac{1}{\sqrt{N}}\sum_{i=1}^{N}|i\rangle\left(\sqrt{\frac{w_i}{h}}|0\rangle + \sqrt{1-\frac{w_i}{h}}|1\rangle\right). \tag{2}$$

The state $|w\rangle|0\rangle$ has amplitude $\sqrt{\frac{\mathcal{W}}{Nh}}$ in $U|\vec{0}\rangle$, thus it can be extracted by using the amplitude amplification algorithm with $O(\sqrt{\frac{Nh}{\mathcal{W}}})$ applications of U and U^{-1}. In particular, if the largest coordinate of w is smaller than $h = \mathcal{W}/K$, then we can prepare one copy of $|w\rangle$ in time $O(\sqrt{N/K})$, and K copies in time $O(\sqrt{KN})$. We use this observation to construct a new circuit $\mathcal{C}$ (Fig. 2) such that $|w\rangle|0\rangle$ has amplitude at least $\sqrt{K/N}$ in $\mathcal{C}|\vec{0}\rangle$, *even* if w contains large coordinates. This circuit uses only two queries to w, but it requires $O(\sqrt{KN})$ queries to be constructed during a preprocessing phase that is executed only once (Theorem 2). The preprocessing phase consists first of computing the set H that contains the positions of the K largest coordinates in w, by using a variant of the quantum maximum finding algorithm (Proposition 2). The circuit $\mathcal{C}$ is then defined to proceed in two stages. First, it prepares a state whose amplitudes depend only on the values in $\{w_i : i \in H\}$ [Eq. (4)]. Next, it modifies this state by querying the set $\{w_i : i \notin H\}$ in a way that is similar to that of U. The crucial observation is that the values in $\{w_i : i \notin H\}$ must be smaller than $\mathcal{W}/K$ by definition of H, thus they can be amplified at a smaller cost. Finally, each copy of $|w\rangle$ can be obtained by one application of the amplitude amplification algorithm on $\mathcal{C}$ (Theorem 3).

We show in the next proposition that our algorithm is optimal by a simple reduction from the K-search problem.

Proposition 1. Any bounded-error quantum algorithm that can output K copies of the quantum state $|w\rangle$ given oracle access to any nonzero vector $w \in \mathbb{R}^N_{\geqslant 0}$ must perform at least $\Omega(\sqrt{KN})$ quantum queries to w.

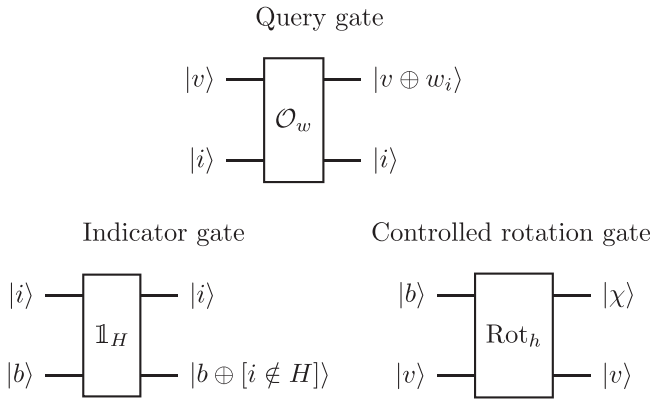

FIG. 1. Three gates used in our circuits. The state $|\chi\rangle$ is defined as $\sqrt{\frac{v}{h}}|b\rangle + \sqrt{1-\frac{v}{h}}|1-b\rangle$ if $0 < v \leqslant h$, and $|b\rangle$ otherwise.

Proof. We consider a variant of the K-search problem where the objective is to find K preimages of 1 in an oracle $\mathcal{O} : [N] \to \{0, 1\}$ containing at least $2K$ such preimages. The bounded-error quantum query complexity of this problem is $\Theta(\sqrt{KN})$ (the proof can easily be derived from Appendix A in Ref. [32], for instance). On the other hand, by a coupon collector argument [33], if we prepare and measure in the computational basis $\Theta(K)$ copies of $|w\rangle$ where $w = (\mathcal{O}(1), \ldots, \mathcal{O}(N)) \in \{0, 1\}^N$, then we obtain the positions of at least K different preimages of 1 with constant success probability. It implies that generating $\Omega(K)$ such copies requires using at least $\Omega(\sqrt{KN})$ quantum queries to w. ■

II. PRELIMINARIES

A. Computational model

We use the quantum circuit model over a universal gate set made of the controlled-NOT (CNOT) gate and of all one-qubit gates. We suppose that the real numbers manipulated by our algorithms (such as the coordinates of w) can be encoded over c bits, for a fixed value of c. In particular, these numbers can be stored in quantum registers of size c. We also add the three gates described in Fig. 1. The indicator gate $\mathbb{1}_H$ is specified by a subset $H \subseteq [N]$. It operates on a Boolean value b and an index $i \in [N]$. The Boolean value $[i \notin H]$ is equal to 1 if and only if $i \notin H$. The query gate $\mathcal{O}_w$ is specified by the input vector w to the problem. It operates on an index $i \in [N]$ and a real v (encoded over c bits). Finally, the controlled rotation gate Rot_h is specified by a real $h > 0$ and it operates on a Boolean value b and a real v. We refer the reader to Refs. [9,34] and references therein for efficient implementations of the arithmetic gates and controlled rotation gates with a given precision. We will also use $|\vec{0}\rangle$ in our notations to represent a multiqubit basis state $|0\rangle^{\otimes \ell}$ for some $\ell > 1$.

The *query complexity* of an algorithm is the number of times it uses the oracle gate $\mathcal{O}_w$ to access the input w. If not specified, the total number of elementary gates used by our algorithms will be larger than their respective query complexity by at most a polylog(N) factor.

Algorithm 1 Preprocessing phase.

1: Compute a set $H \subseteq [N]$ of the positions of K largest entries in w by using the top-K maximum finding algorithm (Proposition 2) with failure probability δ.
2: Compute $h = \min_{i\in H} w_i$ and

$$\mathcal{Z} = (N-K)h + \sum_{i\in H} w_i. \tag{3}$$

3: Use the state preparation algorithm of Proposition 4 to construct a circuit $\mathcal{D}$ such that, on input $|\vec{0}\rangle_{\mathsf{out}}$, it prepares the state

$$\mathcal{D}|\vec{0}\rangle_{\mathsf{out}} = \sum_{i\in H}\sqrt{\frac{w_i}{\mathcal{Z}}}|i\rangle_{\mathsf{out}} + \sum_{i\notin H}\sqrt{\frac{h}{\mathcal{Z}}}|i\rangle_{\mathsf{out}}. \tag{4}$$

4: Output the circuit $\mathcal{C}$ represented in Fig. 2.

B. Quantum subroutines

The next algorithm generalizes the quantum minimum finding of Dürr and Høyer [35] to finding K largest entries in a vector w. The algorithm succeeds if it outputs a set $H \subset [N]$ of K coordinates that dominate all other entries. There is not necessarily a unique choice for H since different coordinates of w may be equal.

Proposition 2 (top-K maximum finding: Theorem 4.2 in Ref. [36]). There exists a quantum algorithm with the following properties. Consider two integers $1 \leqslant K \leqslant N$, a real $\delta \in (0, 1)$ and a vector $w \in \mathbb{R}^N_{\geqslant 0}$. Then, the algorithm outputs the positions of K largest entries in w with success probability at least $1-\delta$, and it performs $O(\sqrt{KN}\log(1/\delta))$ queries to w.

We also need the well-known amplitude amplification algorithm.

Proposition 3 (amplitude amplification: Theorem 3 in Ref. [37]). Let $\mathcal{C}$ be a quantum circuit that prepares the state $\mathcal{C}|\vec{0}\rangle = \sqrt{p}|\varphi\rangle|0\rangle + \sqrt{1-p}|\varphi^\perp\rangle|1\rangle$ for some $p \in [0, 1]$ and two unit states $|\varphi\rangle, |\varphi^\perp\rangle$. Then, the *amplitude amplification* algorithm outputs the state $|\varphi\rangle$ by using $O(1/\sqrt{p})$ applications of $\mathcal{C}$ and $\mathcal{C}^\dagger$ in expectation.

Finally, we will use the next quantum state preparation algorithm that requires having an efficient procedure to compute the partial sum $\sum_{\ell=i}^{j} w_\ell$ for any $1 \leqslant i \leqslant j \leqslant N$.

Proposition 4 (state preparation by integration [12–14]). There is a quantum algorithm with the following properties. Consider an integer N and a nonzero vector $w \in \mathbb{R}^N_{\geqslant 0}$ such that there is a (classical) reversible circuit with T gates that computes $\sum_{\ell=i}^{j} w_\ell$ given $i \leqslant j$. Then, the algorithm outputs $|w\rangle$ and it uses $O(T\log N)$ elementary gates.

III. MAIN ALGORITHM

We describe in details our state preparation algorithm for preparing K copies of $|w\rangle$ given oracle access to $w = (w_1, \ldots, w_N)$. The first step of the algorithm is a preprocessing phase (Algorithm 1) that constructs a particular circuit $\mathcal{C}$ described in Fig. 2.

Theorem 2 (preprocessing phase). Consider two integers $1 \leqslant K \leqslant N$, a real $\delta \in (0, 1)$ and a nonzero vector $w \in \mathbb{R}^N_{\geqslant 0}$. Then, Algorithm 1 outputs with probability at least $1-\delta$ the description of a quantum circuit $\mathcal{C}$ such that, on input $|\vec{0}\rangle$, it prepares the state

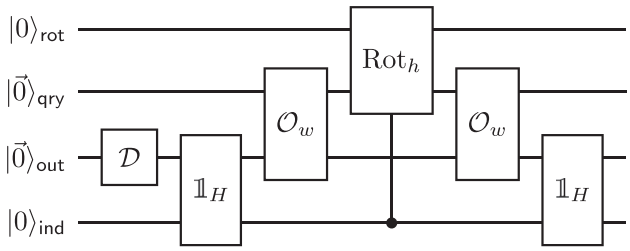

FIG. 2. Circuit $\mathcal{C}$ output at the end of the preprocessing phase (Algorithm 1).

$$|\psi\rangle = \sqrt{p_w}|w\rangle|0\rangle + \sqrt{1-p_w}|w^\perp\rangle|1\rangle, \tag{5}$$

where $p_w \geqslant K/N$ and $|w^\perp\rangle$ is some unit state. The algorithm performs $O(\sqrt{KN}\log(1/\delta))$ queries to w. The circuit $\mathcal{C}$ performs two queries to w and it uses $O(K\log N)$ elementary gates.

Proof. We assume that the top-K maximum finding algorithm returns a correct set H at step 1 of Algorithm 1, which is the case with probability at least $1-\delta$. The circuit $\mathcal{C}$ represented in Fig. 2 operates on four registers: rot and ind that contain a Boolean value, qry that contains a real $v \geqslant 0$, and out that contains an integer $i \in [N]$. The indicator gate $\mathbb{1}_H$ flips the content of ind when the out register contains $i \notin H$, which allows the rotation gate Rot_h to be activated only when $i \notin H$. The gates $\mathcal{O}_w$ and $\mathbb{1}_H$ are applied a second time at the end of $\mathcal{C}$ to uncompute the registers qry and ind. A simple calculation shows that the final state is $\mathcal{C}|\vec{0}\rangle = |\vec{0}\rangle_{\mathsf{qry}}|0\rangle_{\mathsf{ind}}|\psi\rangle_{\mathsf{out,rot}}$ where

$$\begin{aligned}|\psi\rangle_{\mathsf{out,rot}} &= \sum_{i\in H}\sqrt{\frac{w_i}{\mathcal{Z}}}|i\rangle_{\mathsf{out}}|0\rangle_{\mathsf{rot}} \\ &\quad + \sum_{i\notin H}\sqrt{\frac{h}{\mathcal{Z}}}|i\rangle_{\mathsf{out}}\left(\sqrt{\frac{w_i}{h}}|0\rangle_{\mathsf{rot}} + \sqrt{1-\frac{w_i}{h}}|1\rangle_{\mathsf{rot}}\right) \\ &= \sqrt{\frac{\mathcal{W}}{\mathcal{Z}}}|w\rangle_{\mathsf{out}}|0\rangle_{\mathsf{rot}} + \sqrt{1-\frac{\mathcal{W}}{\mathcal{Z}}}|w^\perp\rangle_{\mathsf{out}}|1\rangle_{\mathsf{rot}}\end{aligned} \tag{6}$$

for some irrelevant unit state $|w^\perp\rangle_{\mathsf{out}}$. In order to lower bound the coefficient $p_w := \frac{\mathcal{W}}{\mathcal{Z}}$, we first observe that the smallest value $h = \min_{i\in H} w_i$ over H must satisfy $h \leqslant \frac{\mathcal{W}}{K}$ since otherwise $\sum_{i\in H} w_i$ would exceed $\mathcal{W}$. Thus, $p_w^{-1} = \frac{\mathcal{Z}}{\mathcal{W}} = \frac{(N-K)h+\sum_{i\in H} w_i}{\mathcal{W}} \leqslant \frac{N-K}{K} + 1 = \frac{N}{K}$.

The algorithm uses $O(\sqrt{KN}\log(1/\delta))$ queries at step 1 by Proposition 2. The set $\{w_i : i \in H\}$ can be computed with K queries, after which steps 2–4 do not need to perform any new query. For any $i \leqslant j$, the partial amplitude sum $\sum_{\ell=i}^{j}\langle\ell|\mathcal{D}|\vec{0}\rangle^2$ is equal to $\frac{1}{\mathcal{Z}}(\sum_{\ell\in H\cap\{i,\ldots,j\}} w_i + h\cdot|\{i,\ldots,j\}\setminus H|)$, which can be computed by a classical circuit with $O(K)$ gates since H is of size K. Thus, by Proposition 4, the circuit $\mathcal{D}$ constructed at step 3 requires $O(K\log N)$ elementary gates.

Finally, the number of gates needed to implement the circuit $\mathcal{C}$ at step 4 is dominated by the number of gates needed in $\mathcal{D}$ since the other gates are included in the computational model (see Sec. II A). ■

We use the circuit $\mathcal{C}$ constructed during the above preprocessing phase, together with the amplitude amplification algorithm, to obtain the next state preparation phase that generates one copy of $|w\rangle$ in time $O(\sqrt{N/K})$.

Theorem 3 (state preparation phase). Consider two integers $1 \leqslant K \leqslant N$, a real $\delta \in (0, 1)$ and a nonzero vector $w \in \mathbb{R}^N_{\geqslant 0}$. Let $\mathcal{C}$ denote a quantum circuit obtained with Algorithm 1 on input K, δ, w that correctly prepares the state $|\psi\rangle$ described in Theorem 2. Then, given the description of $\mathcal{C}$, one can prepare the state $|w\rangle$ by using $O(\sqrt{N/K})$ queries to w in expectation.

Proof. This is a direct application of the amplitude amplification algorithm (Proposition 3) on $\mathcal{C}$, where the complexity is derived from the fact that $|w\rangle|0\rangle$ has amplitude at least $\sqrt{K/N}$ in $|\psi\rangle$ by Theorem 2. ■

IV. DISCUSSION

We did not address the precision errors in our analysis. In particular, it can be relevant to replace the controlled rotation gate (which requires to calculate the arcsine function) by the comparison-based circuit defined in Ref. [9] that avoids arithmetic. We also restricted ourselves to preparing states with non-negative real amplitudes. Arbitrary phase factors can be introduced by using the techniques discussed in Refs. [9,14].

[1] F. Magniez, A. Nayak, J. Roland, and M. Santha, Search via quantum walk, SIAM J. Comput. **40**, 142 (2011).

[2] A. W. Harrow, A. Hassidim, and S. Lloyd, Quantum Algorithm for Linear Systems of Equations, Phys. Rev. Lett. **103**, 150502 (2009).

[3] D. W. Berry, High-order quantum algorithm for solving linear differential equations, J. Phys. A: Math. Theor. **47**, 105301 (2014).

[4] S. Aaronson, Read the fine print, Nat. Phys. **11**, 291 (2015).

[5] M. Möttönen, J. J. Vartiainen, V. Bergholm, and M. M. Salomaa, Transformation of quantum states using uniformly controlled rotations, Quantum Inf. Comput. **5**, 467 (2005).

[6] M. Plesch and Č. Brukner, Quantum-state preparation with universal gate decompositions, Phys. Rev. A **83**, 032302 (2011).

[7] L. K. Grover, Synthesis of Quantum Superpositions by Quantum Computation, Phys. Rev. Lett. **85**, 1334 (2000).

[8] M. Ozols, M. Roetteler, and J. Roland, Quantum rejection sampling, ACM Trans. Comput. Theory **5**, 1 (2013).

[9] Y. R. Sanders, G. H. Low, A. Scherer, and D. W. Berry, Black-Box Quantum State Preparation without Arithmetic, Phys. Rev. Lett. **122**, 020502 (2019).

[10] G. H. Low, T. J. Yoder, and I. L. Chuang, Quantum inference on Bayesian networks, Phys. Rev. A **89**, 062315 (2014).

[11] N. Wiebe and C. Grandade, Can small quantum systems learn, Quantum Inf. Comput. **17**, 568 (2017).

[12] C. Zalka, Simulating quantum systems on a quantum computer, Proc. R. Soc. London, Ser. A **454**, 313 (1998).

[13] L. K. Grover and T. Rudolph, Creating superpositions that correspond to efficiently integrable probability distributions, arXiv:quant-ph/0208112.

[14] P. Kaye and M. Mosca, Quantum networks for generating arbitrary quantum states, in *Proceedings of the International Conference on Quantum Information (ICQI)*, 2001 OSA Technical Digest Series (Optica Publishing Group, Washington, DC, 2001), p. PB28.

[15] A. N. Soklakov and R. Schack, Efficient state preparation for a register of quantum bits, Phys. Rev. A **73**, 012307 (2006).

[16] A. Kitaev and W. A. Webb, Wavefunction preparation and resampling using a quantum computer, arXiv:0801.0342.

[17] D. Aharonov and A. Ta-Shma, Adiabatic quantum state generation, SIAM J. Comput. **37**, 47 (2007).

[18] R. D. Somma, S. Boixo, H. Barnum, and E. Knill, Quantum Simulations of Classical Annealing Processes, Phys. Rev. Lett. **101**, 130504 (2008).

[19] P. Wocjan and A. Abeyesinghe, Speedup via quantum sampling, Phys. Rev. A **78**, 042336 (2008).

[20] D. Orsucci, H. J. Briegel, and V. Dunjko, Faster quantum mixing for slowly evolving sequences of Markov chains, Quantum **2**, 105 (2018).

[21] S. Apers, Quantum walk sampling by growing seed sets, in *Proceedings of the 27th Annual European Symposium on Algorithms (ESA)*, edited by M. A. Bender, O. Svensson, and G. Herman, Leibniz International Proceedings in Informatics Vol. 144 (Schloss Dagstuhl - Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany, 2019), pp. 9:1–9:12.

[22] A. W. Harrow and A. Y. Wei, Adaptive quantum simulated annealing for Bayesian inference and estimating partition functions, in *Proceedings of the 2020 ACM-SIAM Symposium on Discrete Algorithms (SODA)* (ACM, New York, 2020), pp. 193–212.

[23] L. Devroye, *Non-Uniform Random Variate Generation* (Springer, Berlin, 1986).

[24] P. Bratley, B. L. Fox, and L. E. Schrage, *A Guide to Simulation*, 2nd ed. (Springer, Berlin, 1987).

[25] D. E. Knuth, *The Art of Computer Programming, Volume II: Seminumerical Algorithms*, 3rd ed. (Addison-Wesley, Boston, 1998).

[26] A. J. Walker, New fast method for generating discrete random numbers with arbitrary frequency distributions, Electron. Lett. **10**, 127 (1974).

[27] A. J. Walker, An efficient method for generating discrete random variables with general distributions, ACM Trans. Math. Software **3**, 253 (1977).

[28] R. A. Kronmal and A. V. Peterson, On the alias method for generating random variables from a discrete distribution, Am. Stat. **33**, 214 (1979).

[29] M. D. Vose, A linear algorithm for generating random numbers with a given distribution, IEEE Trans. Software Eng. **17**, 972 (1991).

[30] L. K. Grover, Rapid sampling through quantum computing, in *STOC '00: Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing* (ACM, New York, 2000), pp. 618–626.

[31] Y. Hamoudi, P. Rebentrost, A. Rosmanis, and M. Santha, Quantum and classical algorithms for approximate submodular function minimization, Quantum Inf. Comput. **19**, 1325 (2019).

[32] Y. Hamoudi and F. Magniez, Quantum time-space tradeoff for finding multiple collision pairs, in *Proceedings of the 16th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC)*, edited by M.-H. Hsieh, Leibniz International Proceedings in Informatics Vol. 197 (Schloss Dagstuhl - Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany, 2021), pp. 1:1–1:21.

[33] Coupon collector's problem to obtain at least half the coupons (2017), https://math.stackexchange.com/q/2117546/256631.

[34] T. Häner, M. Roetteler, and K. M. Svore, Optimizing quantum circuits for arithmetic, arXiv:1805.12445.

[35] C. Dürr and P. Høyer, A quantum algorithm for finding the minimum, arXiv:quant-ph.9607014.

[36] C. Dürr, M. Heiligman, P. Høyer, and M. Mhalla, Quantum query complexity of some graph problems, SIAM J. Comput. **35**, 1310 (2006).

[37] G. Brassard, P. Høyer, M. Mosca, and A. Tapp, Quantum amplitude amplification and estimation, Contemp. Math. **305**, 53 (2002).