PAPER • OPEN ACCESS

Quantum-driven sampling of the almost-uniform distribution via quantum walks

To cite this article: Marco Radaelli *et al* 2026 *New J. Phys.* **28** 034510

IOP Publishing New J. Phys. 28 (2026) 034510 https://doi.org/10.1088/1367-2630/ae4820

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

PAPER

Quantum-driven sampling of the almost-uniform distribution via quantum walks

Marco Radaelli[1,2,3], **Claudia Benedetti**[1,4,*] and **Stefano Olivares**[1,4,*]

[1] Dipartimento di Fisica 'Aldo Pontremoli', Università degli Studi di Milano, via Celoria 16, I-20133 Milan, Italy
[2] School of Physics, Trinity College Dublin, Dublin 2, Ireland
[3] Trinity Quantum Alliance, Unit 16, Trinity Technology and Enterprise Centre, Pearse Street, Dublin 2 D02 YN67, Ireland
[4] Istituto Nazionale di Fisica Nucleare, Sezione di Milano, I-20133 Milan, Italy
[*] Authors to whom any correspondence should be addressed.

E-mail: claudia.benedetti@unimi.it and stefano.olivares@fisica.unimi.it

Keywords: quantum walks, uniform distribution, uniform sampling

OPEN ACCESS

RECEIVED
3 December 2025

REVISED
10 February 2026

ACCEPTED FOR PUBLICATION
19 February 2026

PUBLISHED
13 March 2026

Abstract

We investigate the use of discrete-time quantum walks to sample from an almost-uniform distribution, in the absence of any external source of randomness. Integers are encoded on the vertices of a cycle graph, and a quantum walker evolves for a fixed number of steps before its position is measured and recorded. The walker is then reset to the measured site, and the procedure is iterated to generate the sequence of outcomes. We show that when the number of nodes of the graph is odd, i.e. the condition of the ergodic theorem for classical random walks on finite groups are satisfied, the marginal distributions converges to the uniform distribution. Although correlations between successive outcomes are unavoidable, they can be significantly reduced by a suitable choice of the evolution time.

Introduction

Uniform distributions are central to many applications in science and technology, since they are the fundamental model for processes with equally likely outcomes. In random number generation, they are essential for producing unbiased random sequences and they are the basis to derive more complex distributions. Indeed, many technological applications require random numbers, such as Monte Carlo simulations, cryptography, numerical integration and testing of computer programs [1]. In general, we can identify two main families of methods to generate random numbers. On the one hand, *pseudo-random* number generators exploit deterministic algorithms, able to provide sequences of values having similar statistical properties to a truly random sequence [2]. On the other hand, *true-random* number generators are based on either chaotic classical physical systems [3, 4] or quantum mechanical devices [5–7]. Among the most used methods to produce a string of random numbers there are radioactive decay [8, 9] and quantum optical systems [10–13]. In most random number generation tasks, it is essential to produce values sampled from a uniform distribution, which can then be used either directly or as a building block for generating other distributions.

Recently, discrete-time quantum walks (DTQWs) have been used to develop random number generator protocols [14–16]. DTQWs were first introduced as one of the possible ways to naturally generalize classical random walks into a quantum mechanical framework [17], together with their continuous-time counterparts [18, 19]. Although the relation between the two models has not been completely clarified, it has been subject of intense recent research [20–23]. A DTQW describes the coherent motion of a quantum particle that can jump among connected discrete positions in discrete time steps and is equipped with an internal degree of freedom, called the quantum coin [24, 25].

DTQWs find applications in different contexts. They provide a universal model for quantum computation [26] and they are employed to solve a variety of problems, such as quantum spatial search [27–29], quantum teleportation [30, 31] graph isomorphism [32, 33] and quantum metrology [34–36].

DTQWs are also used to achieve quantum state transfer [37–39]. Moreover, they are suitable candidates to build cryptographic protocols [40, 41], security schemes [42, 43] and image encryption [44]. Wavefunction interference in the unitary DTQW dynamics leads to spatial probability distributions that depend sensitively on the initial state, the coin operator, and the evolution time. When measurements are performed, the Born rule maps the quantum state to intrinsically random classical outcomes, which can be exploited for randomness generation [45, 46].

Even though techniques for randomness generation are well established, we consider a scenario in which the only available physical resource is a quantum walk and we investigate whether randomness can be generated from its dynamics, analyzing the strengths and limitations of the resulting approach. In particular, we analyze whether it is possible to exploit a DTQW to generate outcomes whose probability distribution is uniform over the sample space. This means that each outcome has a uniform marginal distribution. Accordingly, in this work we do not address the problem of random number generation, but we focus specifically on the task of uniform sampling in this sense.

We focus on DTQW on cycle graphs, which, compared to quantum walks on an infinite line, allow for a compact implementation and, thus, can be embedded in more complex networks. Suitable platforms to implement these systems include optical [47–49], photonic [50–52] and solid-state physics settings [53–55]; moreover, they can also be efficiently simulated on quantum computers and processors [56, 57].

Here, we first briefly review previously proposed algorithms [14, 58] and then we introduce a protocol to uniform sampling, based on the iterated convolution of the transition probability of a DTQW. Specifically, the resulting dynamics can be described in terms of classical Markov chains driven by transition probabilities derived from the DTQW dynamics. We also assess the presence of correlations in the sequence of drawn numbers which are typical of this kind of protocol, and we provide an operational strategy to reduce them.

The paper is organized as follows: in section 1 we introduce the basic tools to describe DTQWs together with the concept of randomness associated with its limiting distribution; in section 2 we briefly review existing DTQW-based protocols for almost uniform sampling and, then, in section 3 we present a novel scheme for sampling numbers from a uniform distribution on a cycle graph using DTQW, along with a proof of its convergence. We conclude the paper with some final remarks in section 4.

1. DTQWs

DTQWs, first introduced in Rqf. [17], describe the time-step evolution of a quantum particle with an internal degree of freedom, called quantum coin, on a set of N discrete positions. They are defined on the composite Hilbert space $\mathscr{H}_c \otimes \mathscr{H}_p$, where $\mathscr{H}_p$ represents a positional Hilbert space, while $\mathscr{H}_c$ is the coin space. The spatial basis vectors are localized states over the N discrete positions $\{|x\rangle\} \in \mathscr{H}_p$, with $x = 0, \ldots, N-1$. The coin is a two-level quantum system described by the orthonormal basis $\{|\uparrow\rangle, |\downarrow\rangle\}$ in $\mathscr{H}_c$. The unitary operator $\hat{\mathcal{U}}$, that is applied at each time-step, is composed by two contributions: a coin-flip operator $\hat{\mathcal{C}}$, acting on $\mathscr{H}_c$, and a conditional shift operator $\hat{\mathcal{S}}$ on the global system. The coin operator $\hat{\mathcal{C}}$ can be written as a general element of $U(2)$:

$$\hat{\mathcal{C}}(\theta, \alpha, \beta, \gamma) = \mathrm{e}^{\mathrm{i}\gamma} \begin{pmatrix} \cos\theta\, \mathrm{e}^{\mathrm{i}\alpha} & \sin\theta\, \mathrm{e}^{\mathrm{i}\beta} \\ -\sin\theta\, \mathrm{e}^{-\mathrm{i}\beta} & \cos\theta\, \mathrm{e}^{-\mathrm{i}\alpha} \end{pmatrix}, \tag{1}$$

which includes the Hadamard coin $\mathcal{C}_H = \hat{\mathcal{C}}\left(\frac{\pi}{4}, \frac{\pi}{2}, \frac{\pi}{2}, -\frac{\pi}{2}\right)$ and the x-axis rotation $\hat{\mathcal{C}}_X = \hat{\mathcal{C}}\left(\frac{\pi}{4}, 0, \frac{\pi}{2}, 0\right)$.

We consider discrete spatial positions arranged as the vertices of a cycle graph, with the boundary condition $|N\rangle \equiv |0\rangle$. The conditional shift $\hat{\mathcal{S}}$ then moves the walker, according to the state of the coin, between adjacent sites:

$$\hat{\mathcal{S}} = |\uparrow\rangle\langle\uparrow| \otimes \sum_{x=0}^{N-1} |(x+1)_N\rangle\langle x| + |\downarrow\rangle\langle\downarrow| \otimes \sum_{x=0}^{N-1} |(x-1)_N\rangle\langle x|, \tag{2}$$

where the symbol $(x)_N$ stands for $x \mod N$. The single-step operator $\hat{\mathcal{U}}$ is therefore defined as:

$$\hat{\mathcal{U}} = \hat{\mathcal{S}}\left(\hat{\mathcal{C}} \otimes \hat{\mathbb{I}}_p\right), \tag{3}$$

where $\hat{\mathbb{I}}_p$ is the identity operator on the positional space. Given an initial state $|\Psi_0\rangle \in \mathscr{H}_c \otimes \mathscr{H}_p$, the final state of the DTQW after $t \in \mathbb{N}$ steps is given by

$$|\Psi_t\rangle = \hat{\mathcal{U}}^t |\Psi_0\rangle. \tag{4}$$

The probability for the walker to be found on site $|x\rangle$ after t steps is

$$p_x(t) = |\langle\uparrow| \otimes \langle x|\Psi_t\rangle|^2 + |\langle\downarrow| \otimes \langle x|\Psi_t\rangle|^2. \tag{5}$$

The outcomes of a position measurement for the walker are intrinsically random, distributed according to the probability distribution in equation (5). This randomness can be exploited to generate strings of random numbers that can be used also for quantum cryptographyc tasks. Therefore, it is important to have a tool to assess the unpredictability of the QW measurement outcomes.

Entropy is a reliable way to quantify the randomness of independent and identically distributed (i.i.d.) outcomes. Consider a random variable X with possible discrete values $(x_0, x_1, \ldots, x_{N-1})$ and probability distribution $\mathbb{P}(X) = (p_0, p_1, \ldots, p_{N-1})$, where p_k is the probability to obtain the outcome x_k, $k = 0, \ldots N-1$. The randomness associated with the random variable X can be computed with the Shannon entropy [59], defined as:

$$H(X) = -\sum_{x=0}^{N-1} p_x \log_2 p_x. \tag{6}$$

In this framework, the set $\{x_k\}$ corresponds to the possible QW positions over a cycle graph and the set $\{p_k\}$ to the QW spatial probability distribution at time t, as represented by equation (5).

When generating randomness, the goal is to produce outcomes whose probability distribution has maximal entropy. The maximum value of the Shannon entropy is obtained for a variable X_u distributed according to the uniform distribution $\mathbb{P}_\mathrm{u}(X_\mathrm{u}) = (1/N, 1/N, \ldots, 1/N)$ and it takes the value $H(X_\mathrm{u}) = \log_2 N$. The uniform distribution thus serves as the reference for randomness generation. It is therefore necessary to quantify how close a given probability distribution is to the uniform one. To this purpose, we employ the Kolmogorov distance, also known as the total variation distance, between two discrete probability distributions $\{p_x\}$ and $\{q_x\}$, [60]:

$$K(\{p_x\}, \{q_x\}) = \frac{1}{2}\sum_{x=0}^{N-1} |p_x - q_x|. \tag{7}$$

The quantity in equation (7) vanishes if and only if the two distributions are identical. Following [58], *almost-uniform sampling* refers to a procedure that outputs elements whose distributions are within ϵ total variation distance of the uniform distribution over a finite set, for an arbitrary accuracy parameter $\epsilon > 0$.

2. Approaches to (almost) uniform randomness via QW

In this section, we briefly review two techniques that have been employed to achieve an approximate uniform sampling through quantum walk measurements on a cycle graph.

The simplest technique consists of sampling directly from the spatial distribution of the quantum walker after a fixed number of timesteps T. Due to the reversible nature of the quantum evolution, this distribution does not converge to the uniform one, regardless of the number of timesteps considered. Therefore, an approximation is necessary, and T must be chosen to minimize the deviation of the distribution from uniformity, corresponding to the maximization of its Shannon entropy. In figure 1, the behavior of the Shannon entropy H of the QW-distribution (direct sampling) is shown as a function of the number of timesteps T, compared with the uniform one. To achieve quasi-uniformity T must be chosen to correspond to the maximum value of H within the attainable timestep interval.

The random number generation performance of quantum walks on the bi-infinite line by using this direct protocol has been discussed in [14].

A different technique is based on the sampling of the so called Cesáro distribution [61]. This protocol introduces an element of irreversibility in the procedure, thus allowing the convergence of the spatial distribution to the almost uniform one.

Given the probability distribution of the position variable X, $\mathbb{P}_t(X)$ at the timestep t, the Cesáro distribution is defined as its time-average up to $T \gg 1$ timesteps, namely:

$$\overline{\mathbb{P}}_T(X) = \frac{1}{T}\sum_{t=1}^{T} \mathbb{P}_t(X). \tag{8}$$

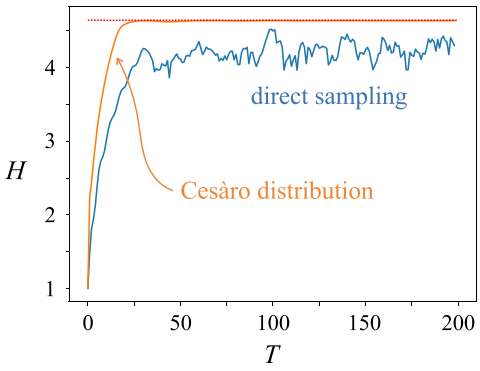

Figure 1. Shannon entropy of the spatial probability distribution on an $N = 25$ cycle as a function of timesteps T, both for the direct sampling and for the Cesáro distribution obtained with Hadamard coin (see the main text for details).

It is straightforward to prove that, $\forall T$, $\overline{\mathbb{P}}_T(X)$ is a normalized probability distribution if and only if $\mathbb{P}_t(X)$ is. If the number of positions on the cycle N is odd then the time-average distribution, obtained using the Hadamard coin, converges to the uniform one (see [61]), as shown in figure 1. However, if the evolution operator (3) admits degeneracy in the spectrum, the Cesáro distribution does not converge to the uniform one. Specifically, for the coin operator $\hat{C}_X$, the uniformity cannot be attained (see appendix A for details).

An efficient protocol for sampling from the Cesáro distribution was proposed in [58] and consists of the following steps: first, a random integer time $t \in [0, T]$ is generated; the quantum walk is then evolved up to time t, after which a position measurement is performed; these steps are repeated as many times as needed to obtain a sample of the desired length. This protocol allows for the sampling of an asymptotically uniform distribution. However, a significant limitation is that it requires as input a source of uniform randomness, to be used to extract the times t (for details about this protocol and its performance see [58]).

3. Almost-uniform sampling via DTQW

In this section, we propose an alternative method for almost-uniform sampling based on the evolution of a DTQW on a cycle graph. Unlike the approach of [58], here we assume that we have no access to an external source of randomness. It relies on the spatial measurements of a DTQW and the concept of convolution of probability distributions.

Due to the translational symmetry of the cycle graph, the protocol is independent of the choice of the initial position x_0. The steps of the protocol are the following:

(I) fix an integer number m and prepare the initial state $|\Psi_0\rangle$ for the DTQW by choosing an arbitrary initial position x_0 and setting the coin state to an arbitrary fixed initial state $|c_0\rangle$, such that $|\Psi_0\rangle = |c_0\rangle \otimes |x_0\rangle$;
(II) evolve the quantum walk for m steps, according to equation (4); then perform a position measurement and record the outcome x;
(III) reset the coin to its initial state and initialize the walker at the measured position x, i.e. $|\Psi_0\rangle = |c_0\rangle \otimes |x\rangle$.
(IV) repeat steps II–III as many times as needed to generate a sequence of integers.

The protocol generates a sequence of outcomes whose extracted values are marginally uniformly distributed in the asymptotic regime. This marginal uniformity, however, does not imply that the outcomes are i.i.d., since the underlying process is Markovian rather than i.i.d. Notably, re-initializing the walker at the previously measured position (see the step III) introduces correlations among successive outputs, as each new initial state depends on the outcome of the previous measurement. This distinguishes the protocol from the one in section 2, which sampled i.i.d. random variables. Below, we discuss the implications of these correlations for random number generation. Here we just note that, if access to

an external source of randomness is allowed, such that it is possible to extract a random number q uniformly in $[0, N-1]$, then one could replace the initial state in step III above with $|c_0\rangle \otimes |q\rangle$. In this way, one can still get the smoothening effect of the change in the initial position, but without introducing correlations. However, using an external source of randomness is not always feasible, and it is precisely this scenario that we are addressing in the present work.

With the introduction of the correlations mentioned above, it is very important to clarify the terminology that we are going to employ. In particular, the protocol generates a realization of a string of correlated random variables $X_{1:S} = \{X_1 \dots X_S\}$, associated with a *joint* probability distribution $\mathbb{P}(X_{1:S})$. The marginal probability distribution $\mathbb{P}(X_n)$ refers to the nth outcome alone, and it is obtained by marginalizing over all the other random variables in the string.

In the present protocol, the probability distribution of the variable X_n only depends on the previously extracted value X_{n-1}, the dependence being given by the spatial re-initialization of the walker. The joint probability distribution $\mathbb{P}(X_{1:S})$ then corresponds to a classical Markov chain, where the transition probabilities are generated by the very quantum dynamics of the walk after m steps:

$$\mathbb{P}\left(X_n = x_n | X_{n-1} = x_{n-1}\right) = \sum_c |\langle c \otimes x_n | \hat{\mathcal{U}}^m | c_0 \otimes x_{n-1} \rangle|^2 \tag{9}$$

in accordance with equation (5).

In the following, we prove that the marginal distribution $\mathbb{P}(X_n)$, namely that of the n^{th} outcome, converges to the uniform distribution in the asymptotic regime $n \gg 1$.

3.1. Convergence of the marginal $\mathbb{P}(X_n)$ to the uniform distribution

The discrete rotational symmetry of the cycle implies invariance under translations of the initial node of the walk and therefore we can choose site $x_0 = 0$ as the starting point, without loss of generality. The transition probability for the first step of the protocol, which we call $\mu(x_1)$, is the conditional probability of reaching node x_1 starting from the initial node 0:

$$\mu\left(x_1\right) = \mathbb{P}\left(X_1 = x_1 | X_0 = 0\right). \tag{10}$$

$\mu(x)$ is also referred to as the propagator and, for a fixed graph size N, it depends on the coin operator, the number of steps m and the initial state of the system $|\Psi_0\rangle$, in accordance with equation (9). Hereafter, we use the shorthand notations:

$$\mathbb{P}\left(X_j | X_k\right) \equiv \mathbb{P}\left(X_j = x_j | X_k = x_k\right) \tag{11}$$

$$\mathbb{P}\left(X_j\right) \equiv \mathbb{P}\left(X_j = x_j\right). \tag{12}$$

The rotational symmetry of the cycle graph implies that

$$\mathbb{P}\left(X_2 | X_1\right) = \mathbb{P}\left(X_2 \ominus X_1 | X_0 = 0\right) = \mu\left(x_2 \ominus x_1\right), \tag{13}$$

where the symbol $\ominus$ represents the difference modulo N. In other words, the probability of finding the quantum walker at position x_2 starting from x_1 on the cycle is equal to the probability of finding the walker at position $x_2 \ominus x_1$ starting from the position $x_0 = 0$. It follows that $\mu(x)$ represents the transition probability between two sites separated by a displacement x (modulo N).

The marginal probability of X_1 is thus given by $\mathbb{P}(X_1) = \mu(x_1)$. For the second step, the chain rule for joint probabilities gives:

$$\mathbb{P}\left(X_{1:2}\right) = \mu\left(x_2 \ominus x_1\right) \mu\left(x_1\right), \tag{14}$$

and, marginalizing over X_1, we obtain

$$\mathbb{P}\left(X_2\right) = \sum_{x_j=0}^{N-1} \mu\left(x_2 \ominus x_j\right) \mu\left(x_j\right) = \mu^{\star 2}\left(x_2\right), \tag{15}$$

where '$\star$' denotes the convolution operator, defined recursively as

$$\mu^{\star n}\left(x\right) = \left[\mu \star \mu^{\star (n-1)}\right](x) \qquad \text{for } n \geqslant 2, \tag{16}$$

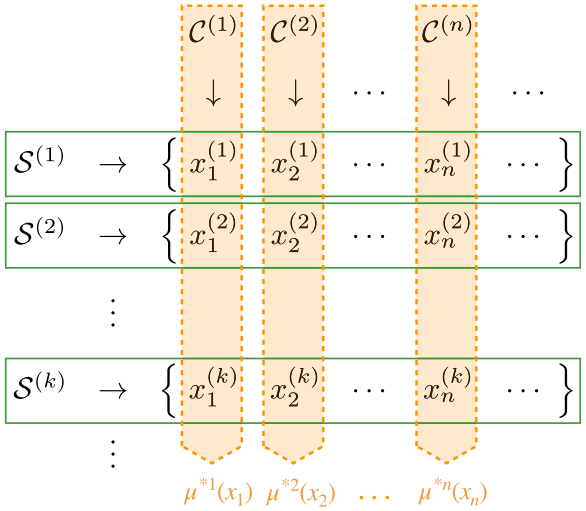

Figure 2. A single application of the protocol of section 3 yields a string $\mathcal{S}^{(k)}$ of correlated outcomes, although each element is marginally distributed according to μ^{*n}, which converges to the uniform distribution for $n \gg 1$. By resetting and repeating the protocol to generate independent strings $\{\mathcal{S}^{(k)}\}$, the set $\mathcal{C}^{(n)} = \{x_n^{(1)}, x_n^{(2)}, \dots\}$ forms a sample of iid uniformly distributed variables.

with $\mu^{\star 1}(x) = \mu(x)$. Generalizing, we obtain the marginal probability for the nth extraction:

$$\mathbb{P}(X_n) = \mu^{\star n}(x_n). \tag{17}$$

Proving that the marginal probability $\mathbb{P}(X_n)$ converges to the uniform is, hence, equivalent to proving that

$$\lim_{n\to\infty} \mu^{\star n}(x) = \frac{1}{N} \qquad \forall x \in [0, N-1]. \tag{18}$$

A classical random walk that satisfies this property is called *ergodic*. We now resort to the following theorem for random walks on finite groups [62, 63]:

Theorem 3.1 (Ergodic theorem). *A random walk with transition probability μ on the N-cycle is ergodic if and only if the support of μ is not contained in any coset of a proper subgroup of the N-cycle.*

As long as the number of nodes of graph are properly chosen, the hypotheses of the ergodic theorem are easily satisfied. In fact, every proper subgroup of the N-cycle is generated by each of the non-trivial divisors of N. As an example, consider the group $C_6 = \{0,1,2,3,4,5\}$, which is isomorphic to the additive group of $\mathbb{Z}_6$. It has two proper subgroups, namely $\{0,2,4\}$, generated by 2, and $\{0,3\}$, generated by 3. The cosets of a subgroup are all the possible translations of such a subgroup on the cycle. To ensure an ergodic random walk, it is therefore sufficient that the support of $\mu(x)$ does not follow the structure of any subgroup (or its cosets). This implies, for instance, that when the number of nodes N is even, the conditions of the ergodic theorem are not satisfied since the support of μ is always contained in a coset of a proper subgroup of the N-cycle, thus preventing convergence to the uniform distribution.

Thanks to the ergodic theorem, the n^{th} extracted value x_n is distributed according to μ^{*n} which converges to the uniform distribution for sufficiently large n. However, successive outcomes within a single realization of the protocol i.e. steps I–IV, are correlated and therefore cannot be regarded as independent random samples. To generate an ensemble of independent and uniformly distributed outcomes, the protocol described in section 3 must be repeated multiple times. Specifically, one generates independent strings $\{\mathcal{S}^{(k)} = X_{1:n}^{(k)}\}$, by restarting the protocol from step I after each string realization. Then, from each string only the final outcome $x_n^{(k)}$ is retained. The resulting set $\mathcal{C}^{(n)} = \{x_n^{(1)}, x_n^{(2)}, \dots\}$ then constitutes an independent sample drawn from the uniform distribution. A schematic representation of this procedure is shown in figure 2.

Different choices of m, $\hat{\mathcal{C}}$ and initial state, for fixed N, affect the convergence speed of the marginal distribution toward uniformity. The convergence can be quantified through the Kolmogorov distance between the marginal μ^{*n} and the uniform distribution $\mathbb{P}_{\text{u}}$, namely:

$$K(\mu^{*n}, \mathbb{P}_{\text{u}}) = \frac{1}{2} \sum_{x=0}^{N-1} \left| \mu^{*n}(x) - \frac{1}{N} \right|. \tag{19}$$

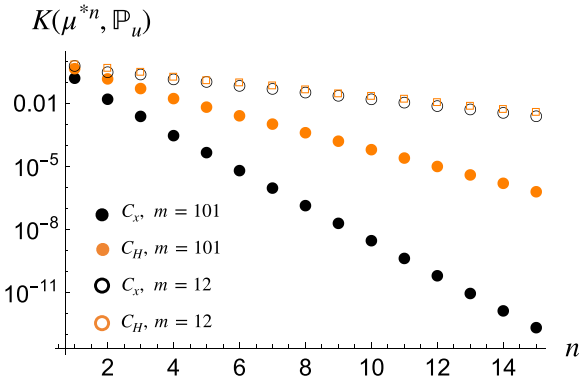

Figure 3. Cycle graph size: $N = 25$. Kolmogorov distance between the convoluted probability $\mu^{*n}(x)$ and the uniform distribution as a function of the number of iterations n, for two different coin operators, $\hat{C}_{\mathrm{H}}$ and $\hat{C}_X$ and two different numbers of timestep m. The initial coin state is fixed: $|c_0\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\downarrow\rangle)$.

As an illustrative example, in figure 3, we report $K(\mu^{*n}, \mathbb{P}_{\mathrm{u}})$ as a function of n, for two different coin operators and number of the DTQW steps m, for a fixed initial state and graph size N. Faster convergence toward uniformity is observed when the transition probability is more evenly distributed over the nodes of the graph. The probability distributions corresponding to $m = 12$ and $m = 101$ for the coin operators used in figure 3 are shown in the the bottom panels of figure 4. It is worth noting that, for a cycle graph, which has a finite a periodic structure, the spatial distribution μ spreads monotonically only for small values of m while, as m increases further, the spreading exhibits a non-monotonic behavior. These considerations shows that the choice of different coin operators and the parameter m can significantly influence the convergence rate, indicating that appropriate operating conditions are required to achieve almost-uniform sampling.

We remark that the same analysis can also be applied to other choices of the coin operator and initial coin states, provided that the conditions of the ergodic theorem are satisfied.

Assuming that the hypotheses of the ergodic theorem are satisfied, it is also possible to derive a lower bound for the convergence of the Shannon entropy of the marginal distribution to its maximum value, which corresponds to the uniform distribution. Given the Fourier coefficients of μ as

$$\hat{\mu}(k) = \sum_{s=0}^{N-1} \mu(s)\, \mathrm{e}^{-\mathrm{i}2\pi ks/N}, \tag{20}$$

the Diaconis–Shashahani bound [62] yields for the Shannon entropy of the marginal distributions:

$$H(\mu^{\star n}) \geqslant \log_2 N - (\log_2 N + 1)\sqrt{\sum_{k=1}^{N-1} |\hat{\mu}(k)|^{2n}}. \tag{21}$$

If the support of μ is not contained in any coset of a proper subgroup of $\mathbb{Z}_N$, then every nonzero Fourier coefficient satisfies $|\hat{\mu}(k)| < 1$. Under this hypothesis, the Diaconis–Shahshahani bound ensures that $H(\mu^{\star n}) \to \log_2 N$ as $n \to \infty$, since the sum under the square root tends to zero exponentially fast.

3.2. Single application of the protocol

It is important to remark that a single run of the protocol does not provide a sample of independent random variables. Indeed, the values within a single string are generated by a classical Markov chain with the same transition probability μ and are therefore correlated. As a consequence, despite each outcome being marginally uniformly distributed in the asymptotic regime, a single string cannot be regarded as a sample of true randomness in the sense of i.i.d. variables.

In general, uniform marginal distributions do not necessarily imply a uniform joint distribution. The dependence between the two random variables X_n and X_{n-1} is strongest when the conditional distribution $\mathbb{P}(X_n|X_{n-1})$ deviates most from the uniform distribution $\mathbb{P}_{\mathrm{u}}(X_n)$. Therefore, to minimize correlations between consecutive outcomes, the protocol parameters $(m, \hat{C}, |c_0\rangle)$, for a fixed graph size, should be chosen so that the transition probability, $\mu(x_n \ominus x_{n-1})$ is as close as possible to uniform. This can be quantified by minimizing the Kolmogorov distance between the transition probability and the uniform distribution, $K(\mu, \mathbb{P}_{\mathrm{u}})$.

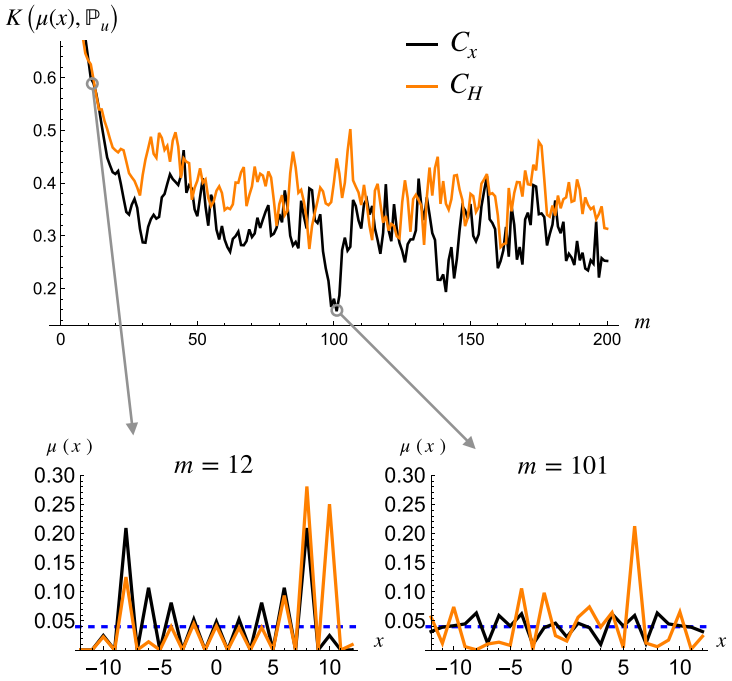

Figure 4. Cycle graph size: $N = 25$. Upper plot: Kolmogorov distance between the transition probability $\mu(x)$ and the uniform distributions as a function of the number of timesteps m, for two different coin operators, $\hat{C}_{\mathrm{H}}$ and $\hat{C}_X$. The initial coin state for both evolutions is $|c_0\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\downarrow\rangle)$. Bottom plots: Transition probability $\mu(x)$ for two selected values of m, obtained for the same coin operators and initial state as above. The blue dashed line is a guide for the eye, corresponding to the uniform distribution.

As an example, figure 4 shows the Kolmogorov distance as a function of the number of timesteps m, for a fixed graph size N and initial coin state, for two representative coin operators. We consider C_X which leads to a symmetric transition probability, and C_{H} which results in an asymmetric dynamics for the chosen initial state (see bottom plots). Small values of the Kolmogorov distance indicate a transition probability closer to uniformity and therefore weaker correlations between following outputs. For small m, K decreases as the transition probability spreads over the nodes. For larger m, however, the dependence on m becomes non-monotonic, showing that increasing the number of steps does not necessary improve uniformity. Consequently, the choice of m must be made carefully to mitigate correlations between successive outcomes. Similar considerations apply to other choices of coin operators and initial conditions.

The correlation length in a single string can be quantified through the correlation function:

$$C(r) = \langle x_j x_{j+r}\rangle - \langle x_j\rangle\langle x_{j+r}\rangle. \tag{22}$$

Correlations decay for outcome separations $r \gtrsim \overline{n}$, where $\overline{n}$ is the minimum number of iterations required for the the random walk to become ergodic, i.e. such that $\mu^{*\overline{n}}(x) \approx 1/N$, (see appendix B for details).

4. Conclusions

Being able to sample uniformly distributed numbers is a crucial task for many applications, from quantum cryptography to quantum information processing. In this work, we have proposed and analyzed a quantum-inspired protocol for sampling from an almost-uniform distribution by exploiting the dynamics of a DTQW on the cycle graph, under the assumption that no external source of randomness is available. To achieve randomness in this setting, it is necessary to introduce irreversibility into the procedure. We do so by means of a measure-and-reset scheme: the quantum walk is initialized in a state that gives rise to the transition probability $\mu(x)$ with a significant support across the nodes of the graph; the walker evolves for m steps, after which its position is measured; the corresponding vertex label is recorded; the walker is reset to the measured site with its coin prepared in the fixed initial state. The

previous steps are repeated n times. In the limit of large n, this protocol returns a string of n integers with almost-uniform randomness.

Although correlations between successive outcomes cannot be completely removed, they can be significantly reduced by a suitable choice of the timestep parameter m, for fixed initial state and coin operator. Using the ergodic theorem for Markov chains on the N-cycle and the properties of iterated self-convolution of transition distributions, we have proved that, for sufficiently long strings, the marginal distribution $\mathbb{P}(X_n)$ converges to the uniform distribution in the limit of large n. Moreover, by analyzing the Fourier spectrum of the transition probability $\mu(x)$, we have shown that the convergence of the Shannon entropy towards its maximal (uniform) value can be quantitatively bounded using the Diaconis–Shahshahani inequality.

The results of our research can stimulate further investigations on randomness generation based on quantum walk evolutions. This simple model may serve as a building block for more complex architectures and for the design of realistic and reliable platforms for the quantum random number generation. Such platforms could to be embedded into larger and more sophisticated quantum devices, such as quantum computers or quantum networks.

Acknowledgments

The authors thank Andrea Smirne for useful discussions. CB and SO acknowledges support from MUR and EU via the PRIN 2022 scorrimento Project EQWALITY (Contract No. 202224BTFZ), QSTI-Spoke1-BaC QSynKrono (contract No. PE00000002-QuSynKrono), and Piano di Sviluppo UniMi 2023. MR acknowledges funding by the Irish Research Council under Government of Ireland Postgraduate Scheme Grant No. GOIPG/2022/2321. This work was supported by RIT (Research IT, Trinity College Dublin), some of the calculations were performed on the Lonsdale cluster maintained by the Trinity Centre for High Performance Computing. This cluster was funded through grants from Science Foundation Ireland.

Data availability statement

All data that support the findings of this study are included within the article (and any supplementary files).

Appendix A. On the Cesáro convergence for a DTQW distribution with a degenerate spectrum

Here we derive the long-time averaged (Cesáro) spatial probability distribution for a DTQW with a degenerate spectrum and show that, in general, it does not converge to the uniform one.

Following [61], we consider a walk with initial state $|\Psi_0\rangle = |c_0\rangle \otimes |0\rangle$. The state after t steps is given by $|\Psi_t\rangle = \hat{\mathcal{U}}^t|\Psi_0\rangle$, where $\hat{\mathcal{U}}$ is the unitary step operator of equation (3). The time-averaged probability distribution of a walker over the node set $\{|v\rangle\}$ is

$$\overline{p}_T(v) = \frac{1}{T}\sum_{t=0}^{T-1} p_t(v)\,. \tag{23}$$

The long-time limit averaged distribution is

$$\pi(v) = \lim_{T\to\infty} \overline{p}_T(v)\,. \tag{24}$$

To compute $\pi(v)$, we consider the following theorem.

Theorem A.1. *Let $\{\lambda_j, |\phi_j\rangle\}$ be the eigenvalues and eigenvectors of the step operator $\hat{\mathcal{U}}$. If $a_n = \langle\phi_n|\Psi_0$, then the limiting time-averaged distribution is*

$$\pi(v) = \sum_c \sum_{n,m} a_n a_m^* \langle c, v|\phi_n\rangle\langle\phi_m|c, v\rangle \delta_{\lambda_n\lambda_m}, \tag{25}$$

where $|c, v\rangle$ denotes the DTQW basis state in $\mathscr{H}_c \otimes \mathscr{H}_p$. Notice that the sum has contributions only from the pairs (n, m) such that $\lambda_n = \lambda_m$.

Proof. Upon expanding the generic state $|\Psi_t\rangle$ of the DTQW after t time steps in the basis state $|c,v\rangle$, we have:

$$|\langle c,v\rangle\Psi_t|^2 = \left|\sum_n \lambda_n^t a_n \langle c,v\rangle\phi_n\right|^2 = \sum_{n,m} a_n a_m^* \left(\lambda_n\lambda_m^*\right)^t \langle c,v\rangle\phi_n\langle\phi_m\rangle c,v. \tag{26}$$

Now, as proved in [61], for $T \gg 1$ the quantity $T^{-1}\sum_{t=0}^{T-1}(\lambda_n\lambda_m^*)^t$ converges to 1 if $\lambda_n = \lambda_m$ and to 0 otherwise. Thereafter, taking the time average

$$\frac{1}{T}\sum_{t=0}^{T-1}|\langle c,v\rangle\Psi_t|^2 \tag{27}$$

and summing over all the coin states $|c\rangle$, one straightforwardly obtains equation (25). □

We can now prove the following Corollary.

Corollary A.1.1. *Let $\hat{\mathcal{U}}$ be the step operator of a DTQW on an N-cycle, with coin operator $\hat{\mathcal{C}}_X$ defined in section 1. If N is odd, then the limiting time-averaged distribution equation (25) does not converge to the uniform one.*

Proof. For a walk on a cycle, $\hat{\mathcal{U}}$ has the form given in equation (3), with operators $\hat{\mathcal{C}}$ and $\hat{\mathcal{S}}$ defined in the main text. In order to build the eigenvectors of such operator, we introduce the Fourier (momentum) states

$$|\chi_k\rangle = \frac{1}{\sqrt{N}}\sum_{v=0}^{N-1} e^{i\frac{2\pi}{N}kv}|v\rangle, \tag{28}$$

with $k = 0,\ldots,N-1$. A reasonable guess for the form of the $2N$ eigenvectors of $\hat{\mathcal{U}}$ is then:

$$\hat{\mathcal{U}}|\phi_k^{\pm}\rangle = \lambda_k^{\pm}|\phi_k^{\pm}\rangle \tag{29}$$

with

$$|\phi_k^{\pm}\rangle = |\gamma_k^{\pm}\rangle \otimes |\chi_k\rangle, \tag{30}$$

where $\lambda_k^{\pm} = e^{\pm i\theta_k}$ and $|\gamma_k^{\pm}\rangle$ are eigenvectors of the 2×2 matrix

$$H_k = \Lambda_k\hat{\mathcal{C}}, \qquad \Lambda_k = \begin{pmatrix} e^{2\pi ik/N} & 0 \\ 0 & e^{-2\pi ik/N}\end{pmatrix}$$

with eigenvalues $\lambda_k^{\pm}$. We remark that $\langle\gamma_k^s|\gamma_k^{s'}\rangle = \delta_{ss'}$ and, in general, for $k \neq j$, $\langle\gamma_k^s|\gamma_j^s\rangle \neq 0$, with $s,s' \in \{\pm\}$. Using the expression for the $\hat{\mathcal{C}}_X$ coin operator, we obtain the eigenvalue equation for H_k:

$$\left(\lambda_k^{\pm}\right)^2 - \sqrt{2}\,\lambda_k^{\pm}\cos\left(\frac{2\pi k}{N}\right) + 1 = 0. \tag{31}$$

which gives the relation:

$$\cos(\theta_k) = \frac{1}{\sqrt{2}}\cos\left(\frac{2\pi k}{N}\right). \tag{32}$$

For a fixed value of k, there are two distinct solutions associated with θ_k e $2\pi - \theta_k$ belonging to the intervals $[\pi/4, 3\pi/4]$ and $[5\pi/4, 7\pi/4]$. However, for different momenta k and k' the degeneracy occurs when $k' = N - k$. Referring to equation (25), the only terms that survive in the sum are those corresponding to degenerate eigenvalues and those with $n = m$.

If we consider N odd, all eigenvectors are pairwise degenerate except for $k = 0$ which corresponds to the only non-degenerate eigenvectors $|\phi_{k=0}^{\pm}\rangle$. Substituting equation (30) into the long-time averaged distribution $\pi(v)$ and summing over the coin states, one obtains:

$$\pi(v) = \frac{1}{N} + \frac{1}{N^2}\sum_{n=1}^{N-1}\exp\left(-i\frac{4\pi nv}{N}\right) \times \sum_{s=\pm}\langle\gamma_n^s|\gamma_{N-n}^s\rangle\langle\gamma_{N-n}^s|\Pi_0|\gamma_n^s\rangle \tag{33}$$

where $\Pi_0 = |c_0\rangle\langle c_0|$ is the projector onto the initial coin state. The first term, N^{-1}, is the contribution from same index eigenvectors, i.e. $n = m$ in equation (33) and yields a uniform distribution: this is the only term

that survives in the presence of non-degenerate spectra. The second term in equation (33) does not vanishes and induces deviation from uniformity, hence the thesis follows. □

Similar arguments can be applied to the case with an even number of nodes N. We eventually note that, in the presence of the Hadamard coin, the last term in equation (33) vanishes leading to the convergence of the Cesáro distribution to the uniform one [61].

Appendix B. Correlation length

Given the string:

$$\mathcal{S} = \{x_1, \ldots, x_j, \ldots, x_{j+r}, \ldots\} \tag{34}$$

of numbers $x_k \in \{0, 1, 2, \ldots, N-1\}$ generated by the protocol in section 3, we introduce the correlation function:

$$C(r) = \langle x_j x_{j+r} \rangle - \langle x_j \rangle \langle x_{j+r} \rangle, \tag{35}$$

where, following the formalism of subsection 3.1:

$$\langle x_j \rangle = \sum_{x_j} x_j \mu^{\star j}(x_j) \tag{36}$$

with:

$$\mu^{\star j}(x_j) = \sum_{x_1} \cdots \sum_{x_{j-1}} \prod_{k=1}^{j-1} \mu(x_{k+1} \ominus x_k)\, \mu(x_1 \ominus x_0), \tag{37}$$

$$\equiv \mu^{\star j}(x_j | x_0) \tag{38}$$

x_0 being a *fixed* starting number (see subsection 3.1). Thereafter, we have:

$$\langle x_j x_{j+r} \rangle = \sum_{x_j} \sum_{x_{j+r}} x_j x_{j+r} \mu^{\star(j+r)}(x_{j+r} | x_j)\, \mu^{\star j}(x_j | x_0), \tag{39}$$

with:

$$\mu^{\star(j+r)}(x_{j+r} | x_j) = \sum_{x_{j+1}} \cdots \sum_{x_{j+r-1}} \prod_{k=j+1}^{j+r-1} \mu(x_{k+1} \ominus x_k)\, \mu(x_{j+1} \ominus x_j). \tag{40}$$

We can now estimate the correlation length, that is the minimum value of r such that $C(r)$ vanishes. Assessing the Kolmogorov distance (19) between $\mu^{\star j}(x_j|x_0)$ and the uniform distribution $\mathbb{P}_u$, and invoking the ergodic theorem (see subsection 3.1), we can find the number of iterations $\overline{n}$ such that $\mu^{\star j}(x_j|x_0) \approx 1/N$. If $j \gtrsim \overline{n}$, the equation (39) reduces to:

$$\langle x_j x_{j+r} \rangle \approx \frac{1}{N} \sum_{x_j} \sum_{x_{j+r}} x_j x_{j+r} \mu^{\star(j+r)}(x_{j+r} | x_j), \tag{41}$$

while:

$$\langle x_j \rangle = \langle x_{j+r} \rangle \approx \frac{N-1}{2}. \tag{42}$$

We note that, due to the ergodic theorem, the x_j's appearing in $\mu^{\star(j+r)}(x_{j+r}|x_j)$ of equation (41) are uniformly distributed and, thus, given $j \gtrsim \overline{n}$ and for a fixed x_j, $\mu^{\star(j+r)}(x_{j+r}|x_j)$ plays the role of (38) with the replacement $x_0 \to x_j$ (the new starting number) and $x_j \to x_{j+r}$ (the drawn number after r steps). It is straightforward to see that if also $r \gtrsim \overline{n}$, then $\mu^{\star(j+r)}(x_{j+r}|x_j) \approx 1/N$, and equation (41) reduces to:

$$\langle x_j x_{j+r} \rangle \approx \left(\frac{1}{N} \sum_{x_j} x_j \right) \left(\frac{1}{N} \sum_{x_{j+r}} x_{j+r} \right) = \langle x_j \rangle \langle x_{j+r} \rangle, \tag{43}$$

leading to $C(r) \approx 0$. Clearly, the actual value of $\overline{n}$ depends on the transition probability and, thus, on the features of the quantum walk on the cycle. We can estimate it posing a suitable threshold on the Kolmogorov distance which is monotone with respect to the the number of iterations of our algorithm (see figure 3).

ORCID iD

Claudia Benedetti 0000-0002-8112-4907

References

[1] Knuth D E 2020 *The art of Computer Programming* vol 2 (Addison Wesley)
[2] James F and Moneta L 2020 Review of high-quality random number generators *Comput. Softw. Big Sci.* **4** 2
[3] L'Ecuyer P 2017 History of uniform random number generation *2017 Winter Simulation Conf. (WSC)* pp 202–30
[4] Torregrosa J R, Fei Y, Lixiang Li, Tang Q, Cai S, Song Y and Quan X 2019 A survey on true random number generators based on chaos *Discrete Dyn. Nat. Soc.* **2019** 2545123
[5] Xiongfeng M, Yuan X, Cao Z, Bing Q and Zhang Z 2016 Quantum random number generation *npj Quantum Inf.* **2** 16021
[6] Herrero-Collantes M and Garcia-Escartin J C 2017 Quantum random number generators *Rev. Mod. Phys.* **89** 015004
[7] Mannalath V, Mishra S and Pathak A 2022 A comprehensive review of quantum random number generators: Concepts, classification and the origin of randomness (arXiv:2203.00261)
[8] Manelis J B 1961 Generating random noise with radioactive sources *Electronics* **34** (available at: www.osti.gov/biblio/4837260)
[9] Vincent C H 1970 The generation of truly random binary numbers *J. Phys. E: Sci. Instrum.* **3** 594
[10] Jennewein T, Achleitner U, Weihs G, Weinfurter H and Zeilinger A 2000 A fast and compact quantum random number generator *Rev. Sci. Instrum.* **71** 1675–80
[11] Fürst H, Weier H, Nauerth S, Marangon D G, Kurtsiefer C and Weinfurter H 2010 High speed optical quantum random number generation *Opt. Express* **18** 13029–37
[12] Min Ren E W, Liang Y, Jian Y, Guang W and Zeng H 2011 Quantum random-number generator based on a photon-number-resolving detector *Phys. Rev. A* **83** 023820
[13] Collins M J, Clark A S, Xiong C, Mägi E, Steel M J and Eggleton B J 2015 Random number generation from spontaneous raman scattering *Appl. Phys. Lett.* **107** 141112
[14] Sarkar A and Chandrashekar C M 2019 Multi-bit quantum random number generation from a single qubit quantum walk *Sci. Rep.* **9** 12323
[15] Bae M and Krawec W O 2021 Semi-source independent quantum walk random number generation *2021 IEEE Information Theory Workshop (ITW)* pp 1–6
[16] Bae M J 2022 Quantum walk random number generation: Memory-based models *2022 IEEE Int. Conf. on Quantum Computing and Engineering (QCE) (Broomfield, CO, USA, 2022)* pp 372–83
[17] Aharonov Y, Davidovich L and Zagury N 1993 Quantum random walks *Phys. Rev. A* **48** 1687–90
[18] Farhi E and Gutmann S 1998 Quantum computation and decision trees *Phys. Rev. A* **58** 915–28
[19] Frigerio M, Benedetti C, Olivares S and Paris M G A 2021 Generalized quantum-classical correspondence for random walks on graphs *Phys. Rev. A* **104** L030201
[20] Strauch F W 2006 Connecting the discrete- and continuous-time quantum walks *Phys. Rev. A* **74** 030301
[21] Childs A M 2010 On the relationship between continuous- and discrete-time quantum walk *Comm. Math. Phys.* **294** 581–603
[22] D'Alessandro D 2010 Connection between continuous and discrete time quantum walks. From D-dimensional lattices to general graphs *Rep. Math. Phys.* **66** 85–102
[23] Schmitz A T and Schwalm W A 2016 Simulating continuous-time Hamiltonian dynamics by way of a discrete-time quantum walk *Phys. Lett. A* **380** 1125–34
[24] Kempe J 2003 Quantum random walks: an introductory overview *Contemp. Phys.* **44** 307–27
[25] Elías Venegas-Andraca S 2012 Quantum walks: a comprehensive review *Quantum Inf. Process.* **11** 1015–106
[26] Lovett N B, Cooper S, Everitt M, Trevers M and Kendon V 2010 universal quantum computation using the discrete-time quantum walk *Phys. Rev. A* **81** 042330
[27] Shenvi N, Kempe J and Whaley K B 2003 Quantum random-walk search algorithm *Phys. Rev. A* **67** 052307
[28] Potoček V, Gábris A, Kiss T and Jex I 2009 Optimized quantum random-walk search algorithms on the hypercube *Phys. Rev. A* **79** 012325
[29] Lovett N B, Everitt M, Heath R M and Kendon V 2019 The quantum walk search algorithm: factors affecting efficiency *Math. Struct. Comput. Sci.* **29** 389–429
[30] Wang Y, Shang Y and Xue P 2017 Generalized teleportation by quantum walks *Quantum Inf. Process.* **16** 221
[31] Yamagami T, Segawa E and Konno N 2021 General condition of quantum teleportation by one-dimensional quantum walks *Quantum Inf. Process.* **20** 224
[32] Douglas B L and Wang J B 2008 A classical approach to the graph isomorphism problem using quantum walks *J. Phys. A: Math. Theo.* **41** 075303
[33] Liu K, Zhang Y, Kai L, Wang X, Wang X and Tian G 2019 MapEff: an effective graph isomorphism agorithm based on the discrete-time quantum walk *Entropy* **21** 569
[34] Annabestani M, Hassani M, Tamascelli D and Paris M G A 2022 Multiparameter quantum metrology with discrete-time quantum walks *Phys. Rev. A* **105** 062411
[35] Cavazzoni S, Razzoli L, Ragazzi G, Bordone P and Paris M G A 2024 Coin dimensionality as a resource in quantum metrology involving discrete-time quantum walks *Phys. Rev. A* **109** 022432
[36] Cavazzoni S, Bordone P and Paris M G A 2024 Optimizing topology for quantum probing with discrete-time quantum walks *AVS Quantum Sci.* **6** 044401
[37] Kurzyński P and Wójcik A 2011 Discrete-time quantum walk approach to state transfer *Phys. Rev. A* **83** 062315
[38] Zhan X, Qin H, Bian Z-hao, Jian Li and Xue P 2014 Perfect state transfer and efficient quantum routing: a discrete-time quantum-walk approach *Phys. Rev. A* **90** 012331
[39] Štefaňák M and Skoupý S 2016 Perfect state transfer by means of discrete-time quantum walk search algorithms on highly symmetric graphs *Phys. Rev. A* **94** 022301
[40] Vlachou C, Rodrigues J, Mateus P, Paunković N and Souto A 2015 Quantum walk public-key cryptographic system *Int. J. Quantum Inf.* **13** 1550050
[41] Vlachou C, Krawec W, Mateus P, Paunković N and Souto A 2018 Quantum key distribution with quantum walks *Quantum Inf. Process.* **17** 1–37

[42] Rohde P P, Fitzsimons J F and Gilchrist A 2012 Quantum walks with encrypted data *Phys. Rev. Lett.* **109** 150501
[43] Chandrashekar C M and Busch T 2015 Localized quantum walks as secured quantum memory *Europhys. Lett.* **110** 10005
[44] Yang Y-G, Pan Q-X, Sun S-J and Xu P 2015 Novel image encryption based on quantum walks *Sci. Rep.* **5** 7784
[45] El-Latif A A A, Abd-El-Atty B and Venegas-Andraca S E 2019 A novel image steganography technique based on quantum substitution boxes *Opt. Laser Technol.* **116** 92–102
[46] El-Latif A A A, Abd-El-Atty B and Venegas-Andraca S E 2020 Controlled alternate quantum walk-based pseudo-random number generator and its application to quantum color image encryption *Physica A* **547** 123869
[47] Schreiber A, Gábris A, Rohde P P, Laiho K, Štefaňák M, Potoček V, Hamilton C, Jex I and Silberhorn C 2012 A 2D quantum walk simulation of two-particle dynamics *Science* **336** 55–58
[48] Smirne A, Nitsche T, Egloff D, Barkhofen S, De S, Dhand I, Silberhorn C, Huelga S F and Plenio M B 2020 Experimental control of the degree of non-classicality via quantum coherence *Quantum Sci. Technol.* **5** 04LT01
[49] Mizutani Y, Horikiri T, Matsuoka L, Higuchi Y and Segawa E 2022 Implementation of a discrete-time quantum walk with a circulant matrix on a graph by optical polarizing elements *Phys. Rev. A* **106** 022402
[50] Rohde P P, Schreiber A, Štefaňák M, Jex I and Silberhorn C 2011 Multi-walker discrete time quantum walks on arbitrary graphs, their properties and their photonic implementation *New J. Phys.* **13** 013001
[51] Qiang X, Shixin M and Song H 2024 Quantum walk computing: Theory, implementation and application *Intell. Comput.* **3** 0097
[52] Monika M *et al* 2025 Quantum state processing through controllable synthetic temporal photonic lattices *Nat. Photon.* **19** 95–100
[53] Ryan C A, Laforest M, Boileau J C and Laflamme R 2005 Experimental implementation of a discrete-time quantum random walk on an NMR quantum-information processor *Phys. Rev. A* **72** 062317
[54] Manouchehri K and Wang J B 2008 Quantum walks in an array of quantum dots *J. Phys. A: Math. Theor.* **41** 065304
[55] Ramasesh V V, Flurin E, Rudner M, Siddiqi I and Yao N Y 2017 Direct probe of topological invariants using Bloch oscillating quantum walks *Phys. Rev. Lett.* **118** 130501
[56] Razzoli L, Cenedese G, Bondani M and Benenti G 2024 Efficient implementation of discrete-time quantum walks on quantum computers *Entropy* **26** 4
[57] Gong M *et al* 2021 Quantum walks on a programmable two-dimensional 62-qubit superconducting processor *Science* **372** 948–52
[58] Richter P C 2007 Almost uniform sampling via quantum walks *New J. Phys.* **9** 72
[59] Shannon C E 1948 A mathematical theory of communication *Bell Syst. Tech. J.* **27** 379–423
[60] Nielsen M A and Chuang I L 2010 *Quantum Computation and Quantum Information* (Cambridge University Press)
[61] Aharonov D, Ambainis A, Kempe J and Vazirani U 2001 Quantum walks on graphs *Proc. Symp. on the Theory of Computing* pp 50–59
[62] Diaconis P 1988 Group representations in probability and statistics *Lecture Notes—Monograph Series* vol 11 (Institute of Mathematical Statistics)
[63] McCarthy J P 2021 The ergodic theorem for random walks on finite quantum groups *Commun. Algebra* **49** 3850–71