1

Grover Search

1.1 States

Any quantum system has a state space, which is a complex inner product space. For us, this will usually be finite dimensional, just $\mathbb{C}^d$ for some d. The actual states are the 1-dimensional subspaces of this vector space. We could specify a subspace U of the complex inner product space V by giving an orthonormal basis $u_1, \ldots, u_k$, but it is often more convenient to define U in terms of the orthogonal projection P onto U – this is the idempotent Hermitian matrix with image equal to U. In fact, if v^* denotes the conjugate transpose of the vector (or matrix) v, then

$$P = \sum_i u_i u_i^*,$$

but, despite appearances, P is independent of the choice of orthonormal basis for U.

Operations on the state space correspond to unitary matrices. If U is unitary and the state of our system is given by a unit vector z, then the vector Uz defines the new state. If we choose to work with projections, our initial state is given by zz^*, and the state after we apply U is Uzz^*U^*.

The outcome of a measurement of a quantum system modelled by $\mathbb{C}^d$ can be taken to be an element of $\{1, \ldots, d\}$. However, the result is actually a random variable: there are probabilities $p_1, \ldots, p_d$ summing to 1, such that we observe outcome i with probability p_i. Thus, we have a probability density defined on the set $\{1, \ldots, d\}$. This means we can view the outcome of a measurement as a probability density. This probability density will depend on the initial state of our system, the operations we apply to the system, and the choice of measurement.

Mathematically, a measurement is represented by a sequence $M_1, \ldots, M_e$ of positive semidefinite matrices such that $\sum_i M_i = I$. The simplest case is

https://doi.org/10.1017/9781009261692.002 Published online by Cambridge University Press

when $e = d$ and $M_i = e_i e_i^T$ (here e_i denotes the characteristic vector of i, and ^{T} denotes the transpose). We describe this as 'measurement relative to the standard basis.' If the state of the system is zz^*, then the probability that we observe the ith outcome is

$$\mathrm{tr}(M_i zz^*) = z^* M_i z,$$

which is equal to the inner product $\langle M_i, zz^* \rangle$; if we are measuring relative to the standard basis, the probability is

$$z^* e_i e_i^T z = |\langle z, e_i \rangle|^2.$$

Thus, it is the square of the absolute value of the ith entry of z.

1.2 Discrete Walks

For our purposes, a *discrete quantum walk* is specified by a unitary matrix U. We call it the *transition matrix* of the walk. If U is $d \times d$, we view it as acting on a quantum system with state space $\mathbb{C}^d$. The system evolves under repeated applications of U; thus, if the initial state of the system is represented by the unit vector z, then after m steps, the state of the system would be $U^m z$. If we measure the system after k steps relative to the standard basis, the outcome will be e_j with probability

$$|\langle e_j, U^m z \rangle|^2.$$

Our view of a discrete quantum walk is more general than taken by physicists. We find the generality useful, but there are two problems. The first is mathematical: at this level of generality, we may lack the mathematical tools needed to determine interesting properties of parameters of the walk. The second is physical: some unitary matrices decribe operations that are not easily implemented in practice; thus, we will see that U is usually defined as a product of simple unitary matrices, often sparse.

One common feature of nearly all discrete walks in this book will be that the state space is the set of complex functions on the arcs of a graph. Here an *arc* of a graph is an ordered pair of adjacent vertices. Thus, if X is an undirected graph with m edges, then it has $2m$ arcs, and the associated state space will have dimension $2m$.

1.3 Grover Search

We present one of the most important applications of quantum walks, Grover's search algorithm. Basically we have a system with state space $\mathbb{C}^d$ and two unitary operators R and S. The operators have a special form; they are *reflections*. We explain what this means.

https://doi.org/10.1017/9781009261692.002 Published online by Cambridge University Press

If P is a projection, then

$$(2P - I)^2 = 4P^2 - 4P + I = I,$$

and it follows that $2P-I$ is unitary with order two. It fixes each vector in $\mathrm{im}(P)$ and maps a vector v in $\ker(P) = U^\perp$ to $-v$. Thus, $2P - I$ represents reflection in $\mathrm{im}(P)$.

The simplest case is when $\mathrm{im}(P)$ is 1-dimensional, namely $\mathrm{rk}(P) = 1$. If $\mathrm{im}(P)$ is spanned by a, then

$$P = \frac{1}{\langle a, a\rangle} aa^*$$

and $\ker(P) = a^\perp$. We say that $2P - I$ represents reflection in the hyperplane $a^\perp$.

The operator R is supplied to us and represents reflection in the subspace $e_j^\perp$. We do not know what the value of j is, and we want to determine it. (This is our search problem.) Let $\mathbf{1}$ denote the all-ones vector. The second operator S represents reflection in the orthogonal complement of the vector

$$y = \frac{1}{\sqrt{d}}\mathbf{1}.$$

Grover's strategy is very easy to describe. We initialize our system so that its state is y, we apply the operator $U = RS$ exactly m times, and then we measure relative to the standard basis. If we choose m correctly, the result of the measurement is j, with probability very close to 1. In fact, choosing m to be $O(\sqrt{d})$ will work, beating the classical bound, and this is Grover's algorithm.

In quantum computing there is a standard procedure for encoding 01-valued functions as unitary operators. The operator R is the encoding of a function f that takes the value 1 on j, and is zero on i if $i \neq j$. Clearly, given f we can determine j by trying each input in turn, and on average this will take $\frac{1}{2}d$ tries.

1.4 Justifying Grover's Algorithm

We use a geometric argument to show that Grover's algorithm will work. A real matrix Q represents an orthogonal mapping if $Q^TQ = I$. As

$$1 = \det(QQ^T) = \det(Q)^2,$$

the determinant of an orthogonal mapping is ± 1. A *rotation* is an orthogonal mapping with determinant 1.

Reflections form an important class of orthogonal mappings (which we will be making much use of). If W is a subspace of V, a *reflection in* W is the linear mapping that fixes each element in W and acts as $-I$ on $U^\perp$. Thus, the square

https://doi.org/10.1017/9781009261692.002 Published online by Cambridge University Press

of a reflection is the identity, as expected. For our use, the most important case will be reflection in a hyperplane, which can be described as follows. If $a \neq 0$, then the map τ_a defined by

$$\tau_a(x) := x - 2\frac{\langle a, x\rangle}{\langle a, a\rangle}a$$

is reflection in the hyperplane $a^\perp$. It is easy to see that $\tau_a^2 = I$ and $\tau_a(a) = -a$, hence τ_a is a reflection by definition. (You may find it worthwhile to verify that it is an orthogonal mapping.) Since the eigenvalues of τ_a are -1 (with multiplicity of one) and 1 with multiplicity $\dim(V) - 1$, we see that $\det(\tau_a) = -1$.

Now assume that a and b are linearly independent unit vectors with $\cos(\theta) = \langle a, b\rangle$. The product $U = \tau_a\tau_b$ has a determinant of one. Assume that $\dim(V) = n$ and let W be the subspace $a^\perp \cap b^\perp$ of V. Then $\dim(W) = d - 2$ and $W^\perp$ is the 2-dimensional subspace of V spanned by a and b. The restriction of U to W is an orthogonal mapping with determinant 1, and hence it is a rotation.

We claim the restriction of U to $W^\perp$ represents rotation by an angle of 2θ. Since the restriction is a rotation, it suffices to compute the angle between x and Ux for one vector x, and we may take x to be b. Then

$$\tau_a\tau_b(b) = \tau_a(-b) = -b + 2\langle a, b\rangle$$

and so

$$\langle b, Ub\rangle = -1 + 2\langle a, b\rangle^2 = 2\cos(\theta)^2 - 1 = \cos(2\theta).$$

Now we specialize to the case of interest. Assume

$$a := \frac{1}{\sqrt{d}}\mathbf{1}$$

and that b is a standard basis vector. Then

$$\langle a, b\rangle = \frac{1}{\sqrt{d}}$$

and therefore

$$\cos(2\theta) = \frac{2}{d} - 1.$$

Hence, when d is large, U is rotation through an angle a bit less than π, and $-U$ represents a rotation through a small positive angle, ϕ say. As

$$\cos(\phi) \approx 1 - \frac{1}{2}\phi^2,$$

we have

$$\phi \approx \frac{2}{\sqrt{d}}.$$

https://doi.org/10.1017/9781009261692.002 Published online by Cambridge University Press

Accordingly, if

$$N := \left\lfloor \frac{\pi\sqrt{d}}{4} \right\rfloor,$$

then $U^N a$ is very close to b or $-b$. Consequently, the result of a measurement in the standard basis after N applications of U will identify which standard basis vector is equal to b.

1.5 Composite Quantum Systems

A *composite* quantum system is a system whose state space is the tensor product $U \otimes V$, where U and V are the state spaces of two "smaller" quantum systems. A system with state space of this form is said to be *bipartite*. The state space of a system of d qubits is the tensor product of d copies of $\mathbb{C}^2$. We could view this state space as the tensor product of $\mathbb{C}^2$ with $(\mathbb{C}^2)^{\otimes(d-1)}$. A bipartite system models the situation where we have two physicists, traditionally Alice and Bob, each with their own quantum systems. The complete system is described by a tensor product, but Alice and Bob work independently.

Given a bipartite system, we can operate on the individual parts separately; such operations are said to be *local*. More precisely, if R_1 and R_2 are unitary operations on state spaces U_1 and U_2 respectively, then $R_1 \otimes R_2$ is a local unitary operation on $U_1 \otimes U_2$.

Measurements become more complicated, or more interesting, because a measurement carried out on one part is not a measurement on the entire system. If Alice's measurement is specified by positive definite matrices M_r (with $\sum_r M_r = I$) and Bob's by positive semidefinite matrices N_s (with sum $\sum_s N_s = I$), then the Kronecker products

$$M_r \otimes N_s$$

define a measurement on the composite system.

We give an example. Consider the system with state space $\mathbb{C}^n \otimes \mathbb{C}^n$. We think of $\mathbb{C}^n$ as the space of complex functions on the vertices of the complete graph K_n; hence; we may view $\mathbb{C}^n \otimes \mathbb{C}^n$ as the space of complex functions on the arcs of the graph we get by adding a loop to each vertex of K_n. (So $e_u \otimes e_u$ represents a loop on vertex u.)

We introduce three operators on our state space. The first, denoted R, is the permutation operator given by

$$R(e_i \otimes e_j) = e_j \otimes e_i;$$

this is **not** a local operator.

https://doi.org/10.1017/9781009261692.002 Published online by Cambridge University Press

Let τ_j be the operator on $\mathbb{C}^n$ corresponding to reflection about e_j and let $\tau_{\mathbf{1}}$ be reflection in $\mathbf{1}^{\perp}$. Then $\tau_j \otimes I$ and $I \otimes \tau_{\mathbf{1}}$ are local operators.

We note that

$$R(\tau_j \otimes \tau_0)R = \tau_0 \otimes \tau_j$$

and it is not hard to see that, for any integer k,

$$\big(R(\tau_j \otimes \tau_0)\big)^{2k} = (\tau_0\tau_j)^k \otimes (\tau_j\tau_0)^k.$$

Thus, the action of

$$U := R(\tau_j \otimes \tau_0)$$

on $\mathbb{C}^n \otimes \mathbb{C}^n$ is completely determined by the actions of $\tau_0\tau_j$ and $\tau_j\tau_0$ on $\mathbb{C}^n$. (We note that $\tau_j\tau_0 = (\tau_0\tau_j)^{-1}$.)

Since $\tau_0\tau_j$ is the operator used in Grover's algorithm, it is possible to implement Grover's algorithm using the quantum walk (given by U) on the arcs and loops of K_n. This was first noted by Ambainis, Kempe, and Rivosh [4]. We present the details in the following section.

1.6 Grover via a Quantum Walk on Arcs

Assume $U := R(\tau_j \otimes \tau_0)$, as in the previous section. If we start with the uniform superposition

$$x_0 \otimes x_0 := \frac{1}{n}\mathbf{1} \otimes \mathbf{1},$$

then

$$U^k(x_0 \otimes x_0) \approx e_j \otimes \Big((\tau_j\tau_0)^k x_0\Big)$$

and measuring the first register at step k (relative to the standard basis) yields e_j with high probability.

If X is a graph, and u and v are two vertices, we write $u \sim v$ if u and v are adjacent, equivalently if $\{u, v\}$ is an edge of X. An *arc* is an ordered pair of adjacent vertices, denoted (u, v).

Let X denote the complete graph on n vertices, with one loop on each vertex. (So its adjacency matrix is the all-ones matrix J.) The state space of the above walk is spanned by the characteristic vectors $e_u \otimes e_v$ of the arcs (u, v) of X. Thus, each state can be seen as a complex-valued function on the arcs of X. As an example, the initial state in Grover's search is

$$x_0 \otimes x_0 = \sum_{u \sim v} \frac{1}{n} e_u \otimes e_v,$$

https://doi.org/10.1017/9781009261692.002 Published online by Cambridge University Press

the constant function that maps each arc to $\frac{1}{n}$. Since U acts linearly on $\mathbb{C}^n \otimes \mathbb{C}^n$, it suffices to investigate its effect on the basis

$$\{e_u \otimes e_v : u \sim v\}.$$

The matrix

$$\tau_j \otimes \tau_0 = (2e_j e_j^T - I) \otimes \left(\frac{2}{n}J - I\right)$$

is usually referred to as the *coin operator*, for it acts as if one is flipping a quantum coin to determine which arc to move to, given the current position. Since

$$(\tau_j \otimes \tau_0)(e_u \otimes e_v) = \begin{cases} e_u \otimes \left(\frac{1}{\sqrt{n}} \sum_{w \sim u} e_w\right), & u \neq j, \\ e_u \otimes \left(-\frac{1}{\sqrt{n}} \sum_{w \sim u} e_w\right), & u = j, \end{cases}$$

the result of a coin flip is some superposition of outgoing arcs of current tail u. The matrix R is called the *arc-reversal operator*, as it maps the characteristic vector of (u, v) to the characteristic vector of (v, u). These describe how a quantum walker moves on X: in each step: she flips the coin to redistribute her amplitudes over the outgoing arcs, and then reverses all the arcs she is on.

1.7 Arc-Reversal Grover Walk

Rewrite the unitary matrix of Grover's search as

$$\begin{aligned} U &= R(\tau_j \otimes \tau_0) \\ &= R(I \otimes \tau_0)(\tau_j \otimes I), \end{aligned}$$

and define

$$U_0 := R(I \otimes \tau_0), \quad U_j := \tau_j \otimes I.$$

The first matrix U_0 defines a quantum walk on X, where the coin operator $I \otimes \tau_0$ treats all vertices equally. The second matrix U_j makes a difference between the marked and unmarked vertices: on outgoing arcs of j, it acts as $-I$, while on other arcs it acts as the identity.

The main focus of this book will be quantum walks on graphs with no marked vertices. In this section, we generalize the walk defined by U_0 to an *arc-reversal Grover walk* on any graph; this model was first studied by Watrous [71] and later formalized by Kendon [47].

Let X be a d-regular graph on n vertices. Consider the space $\mathbb{C}^n \otimes \mathbb{C}^d$ spanned by all complex functions on the arcs of X. To each vertex we assign the same *Grover coin*

https://doi.org/10.1017/9781009261692.002 Published online by Cambridge University Press

$$G := \frac{2}{d}J - I.$$

Thus, for vertex u, the amplitude transferred between two outgoing arcs of u is $2/d - 1$ if they are equal, and $2/d$ otherwise. The coin matrix, acting on $\mathbb{C}^n \otimes \mathbb{C}^d$, is then a direct sum of n Grover coins. Since G commutes with all permutations, we can write the coin matrix as $I \otimes G$ under any basis of $\mathbb{C}^n \otimes \mathbb{C}^d$. Let R be the matrix that reverses all arcs, and set

$$U := R(I \otimes G).$$

The quantum walk with U as the transition matrix is an *arc-reversal Grover walk* on X. It is not hard to extend this definition to an irregular graph: simply assign the Grover coin with $d = \deg(u)$ to vertex u.

1.8 Alternative Formulation of Arc-Reversal Walks

A state is a complex function on the arcs of a graph. Hence, it defines a special weighted adjacency matrix W, where the weight W_{uv} (possibly zero) is the amplitude on the arc (u, v), and

$$\sum_{u \sim v} |W_{uv}|^2 = 1.$$

Conversely, given a weighted adjacency matrix W, let $\mathrm{vec}(W)$ be the vector obtained from W by concatenating its columns. Clearly, $\mathrm{vec}(W)$ is indexed by all pairs of vertices; if we restrict it to the adjacent pairs only, then we have recovered our usual representation of the state.

This motivates an alternative description of arc-reversal walks with Grover coins. Let A be the 01-adjacency matrix of the graph, and D be the diagonal degree matrix. Let $\circ$ denote the Schur or entrywise product of two matrices. For any matrix state W, the arc-reversal operator simply transposes W, and the coin operator sends W to

$$2A((D^{-1}AM) \circ I) - W.$$

In other words, to update the entry W_{uv} after one iteration of the walk, we may first compute the column sum $\langle We_u, \mathbf{1} \rangle$, and then replace W_{uv} by

$$\frac{2}{\deg(u)} \langle We_u, \mathbf{1} \rangle - W_{vu}.$$

Below is a proof for the second statement. In this proof, we use the *vectorization operator* $\mathrm{vec}(\cdot)$, which sends a matrix M to a vector consisting of the columns of M.

https://doi.org/10.1017/9781009261692.002 Published online by Cambridge University Press

1.8.1 Lemma. *Let C be the Grover coin operator, indexed by all pairs of vertices. Then*

$$C \operatorname{vec}(W) = \operatorname{vec} 2A((D^{-1}AM) \circ I) - W.$$

Proof We first write each coin as a weighted adjacency matrix:

$$\begin{aligned} C_u &= (AE_{uu}A) \circ \left(\frac{2}{\deg(u)} J - I \right) \\ &= \frac{2}{\deg(u)} AE_{uu}A - \sum_{v \sim u} E_{vv}. \end{aligned}$$

Since C is block-diagonal with C_u as the uu-block,

$$\begin{aligned} C \operatorname{vec} M &= \left(\sum_u E_{uu} \otimes C_u \right) \operatorname{vec} W \\ &= \sum_u (E_{uu}^T \otimes C_u) \operatorname{vec} W \\ &= \sum_u \operatorname{vec} C_u W E_{uu} \\ &= \operatorname{vec} \sum_u C_u W E_{uu}, \end{aligned}$$

where the second and third equalities follow from well-known identities of vectorization. Finally, notice that

$$\begin{aligned} \sum_u C_u W E_{uu} &= \sum_u \frac{2}{\deg(u)} AE_{uu}AWE_{uu} - \sum_u \sum_{v \sim u} E_{vv} M E_{uu} \\ &= 2A \sum_u \frac{1}{\deg(u)} (e_u^T AWe_u) E_{uu} - \sum_u \sum_{v \sim u} W_{vu} E_{vu} \\ &= 2A((D^{-1}AW) \circ I) - W \circ A \\ &= 2A((D^{-1}AW) \circ I) - W. \end{aligned}$$

□

The matrix $D^{-1}A$ is row stochastic and represents a simple random walk on the graph. This reveals a connection between certain classical walks and quantum walks.

Notes

In general, the coins of a quantum walk do not have to be identical. If we assign $-G$ to a special vertex and G elsewhere, then we have effectively introduced an oracle. This walk was proposed by Ambainis, Kempe, and Rivosh [4] as a quantum algorithm that generalizes Grover's search.

https://doi.org/10.1017/9781009261692.002 Published online by Cambridge University Press

More flexibly, we may assign any $\deg(u) \times \deg(u)$ unitary matrix C_u to a vertex u. However, unless it commutes with all permutations, we will need to specify a linear order on the neighbours of u,

$$f_u : \{1, 2, \cdots, \deg(u)\} \to \{v : u \sim v\},$$

in order to explain what C_u does. Let us refer to the vertex $f_u(j)$ as the jth neighbour of u, and the arc $(u, f_u(j))$ as the jth arc of u. Then, C_u sends the jth arc of u to a superposition of all outgoing arcs of u, in which the amplitudes come from the jth column of C_u:

$$C_u e_j = \sum_{k=1}^{\deg(u)} (e_k^T C_u e_j) e_k.$$

Thus, under the ordering of arcs:

$$\{\{(u, f_u(j)) : j = 1, \cdots, \deg(u)\} : u \in V(X)\},$$

and the transition matrix of our quantum walk is

$$U = R \begin{pmatrix} C_1 & & & \\ & C_2 & & \\ & & \ddots & \\ & & & C_n \end{pmatrix}.$$

The *Fourier coin*

$$F := \frac{1}{\sqrt{d}} (e^{2jk\pi i/d})_{jk}$$

has been frequently studied in the literature. It induces many non-classical behaviors of quantum walks; for example, on the infinite path, the probability distribution is asymmetric about the center [3]. We will visit this model in Chapter 8.

Some coins can be associated with combinatorial structures. If we convert the linear order f_u into a cyclic permutation, then we obtain a *rotation system*, which determines an orientable embedding of a graph (this will be explained in Chapter 6). The readers are invited to show that a unitary circulant matrix commutes with all cyclic permutations if and only if it has simple eigenvalues; this allows us to define, given a fixed $d \times d$ coin, a unique arc-reversal quantum walk for each rotation system of a d-regular graph. In [37], we studied arc-reversal walks on cubic graphs with different rotation systems and found some interesting connections between properties of the walk and properties of the embedding.

https://doi.org/10.1017/9781009261692.002 Published online by Cambridge University Press