UNITARY OPERATORS AND SYMMETRY TRANSFORMATIONS FOR QUANTUM THEORY

HASSAN NARAGHI

Abstract. Unitary spaces, transformations, matrices and operators are of fundamental importance in quantum mechanics. In quantum mechanics symmetry transformations are induced by unitary. This is the content of the well known Wigner theorem. In this paper we determine those unitary operators U are either parallel with or orthogonal to . We give some examples of simple unitary transforms, or "quantum gates." A quantum operation which copied states would be very useful. For example, we considered the following problem in Homework 1: Given an unknown quantum state, either and , use a measurement to guess which one. If and are not orthogonal, then no measurement perfectly distinguishes them, and we always have some constant probability of error. However, if we could make many copies of the unknown state, then we could repeat the optimal measurement many times, and make the probability of error arbitrarily small. The no cloning theorem says that this isn't physically possible. Only sets of mutually orthogonal states can be copied by a single unitary operator.

1. Introduction

Unitary spaces, transformations, matrices and operators are of fundamental importance in quantum mechanics. In quantum mechanics symmetry transformations are induced by unitary. This is the content of the well known Wigner theorem. In this paper we determine those unitary operators U are either parallel with or orthogonal to φ. We give some examples of simple unitary transforms, or "quantum

2000 *Mathematics Subject Classification.* 46N50, 47A05, 81Q10.

Key words and phrases. Unitary Operators, Symmetry Transformations, quantum mechanic.

gates." A quantum operation which copied states would be very useful. For example, we considered the following problem in Homework 1: Given an unknown quantum state, either $|\alpha$ and $|\beta$, use a measurement to guess which one. If $|\alpha$ and $|\beta$ are not orthogonal, then no measurement perfectly distinguishes them, and we always have some constant probability of error. However, if we could make many copies of the unknown state, then we could repeat the optimal measurement many times, and make the probability of error arbitrarily small. The no cloning theorem says that this isn't physically possible. Only sets of mutually orthogonal states can be copied by a single unitary operator. Time evolution is the change of state brought about by the passage of time, applicable to systems with internal state (also called state full systems). In this formulation, time is not required to be a continuous parameter, but may be discrete or even finite. In classical physics, time evolution of a collection of rigid bodies is governed by the principles of classical mechanics. In their most rudimentary form, these principles express the relationship between forces acting on the bodies and their acceleration given by Newton's laws of motion. These principles can also be equivalently expressed more abstractly by Hamiltonian mechanics or Lagrangian mechanics. In quantum mechanics, the state of any physical system is represented by a vector. Suppose that $|\alpha$ is such a vector. Time evolution is the process $|\alpha \to e^{-iHt}|\alpha$ where H is the Hamiltonian operator. You can think of the state vector as a representation of all properties of the system, in the past, present, and future. The effect of the time evolution operator is then to transform our state vector to the state vector that another observer would use to describe the same system. This would be an observer whose clock shows zero t seconds after ours does.

2. Unitary Operators and Quantum Gates

2.1. **Unitary Operators.** A postulate of quantum physics is that quantum evolution is unitary. That is, if we have some arbitrary quantum system U that takes as input a state $|\phi>$ and outputs a different state $U|\phi>$, then we can describe U as a unitary linear transformation, defined as follows.

If U is any linear transformation, the adjoint of U, denoted $U^\dagger$, is defined by $(U\overrightarrow{v}, \overrightarrow{w}) = (\overrightarrow{v}, U^\dagger\overrightarrow{w})$. In a basis, $U^\dagger$ is the conjugate transpose of U; for example, for an operator on $\mathbb{C}^2$,

$$U = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Rightarrow U^\dagger = \begin{pmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{pmatrix}.$$

We say that U is unitary if $U^\dagger = U^{-1}$. For example, rotations and reflections are unitary. Also, the composition of two unitary transformations is also unitary (Proof: U, V unitary, then $(UV)^\dagger = V^\dagger U^\dagger = V^{-1}U^{-1} = (UV)^{-1}$.

Some properties of a unitary transformation U:

- The rows of U form an orthonormal basis.
- The columns of U form an orthonormal basis.
- U preserves inner products, i.e. $(\overrightarrow{v}, \overrightarrow{w}) = (U\overrightarrow{v}, U\overrightarrow{w})$. Indeed, $(U\overrightarrow{v}, U\overrightarrow{w}) = (U| > v)^\dagger U|w> = < v|U^\dagger U|w> = < v, w >$. Therefore, U preserves norms and angles (up to sign).
- The eigenvalues of U are all of the form $e^{i\theta}$(since U is length-preserving, i.e., $(\overrightarrow{v}, \overrightarrow{v}) = (U\overrightarrow{v}, U\overrightarrow{v})$).
- U can be diagonalized into the form

$$\begin{pmatrix} e^{i\theta_1} & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & e^{i\theta_d} \end{pmatrix}$$

2.2. **Quantum Gates.** We give some examples of simple unitary transforms, or quantum gates. Some quantum gates with one qubit:

- Hadamard Gate. Can be viewed as a reflection around $\pi/8$, or a rotation around $\pi/4$ followed by a reflection.

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

The Hadamard Gate is one of the most important gates. Note that $H\dagger = H($ since H is real and symmetric) and $H^2 = I$.

- Rotation Gate. This rotates the plane by θ.

$$U = \begin{pmatrix} cos\theta & -sin\theta \\ sin\theta & cos\theta \end{pmatrix}$$

- NOT Gate. This flips a bit from 0 to 1 and vice versa.

$$NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

- Phase Flip.

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

The phase flip is a NOT gate acting in the $|+>=\frac{1}{\sqrt{2}}(|0>+|1>), |->=\frac{1}{\sqrt{2}}(|0>-|1>)$ basis. Indeed,$Z|+>=|_{>}$ and $Z|_{>}=|+>$.

And a two-qubit quantum gate:

- Controlled Not (CNOT).

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

The first bit of a CNOT gate is the control bit; the second is the target bit. The control bit never changes, while the target bit flips if and only if the

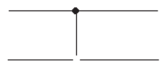

FIGURE 1.

control bit is 1. The CNOT gate is usually drawn as follows, with the control bit on top and the target bit on the bottom:

2.3. **Tensor product of operators.** Suppose $|v>$ and $|w>$ are unentangled states on $\mathbb{C}^m$ m and $\mathbb{C}^n$, respectively. The state of the combined system is $|v> \otimes |w>$ on $\mathbb{C}^{mn}$. If the unitary operator A is applied to the first subsystem, and B to the second subsystem, the combined state becomes $A|v> \otimes B|w>$.

In general, the two subsystems will be entangled with each other, so the combined state is not a tensor product state. We can still apply A to the first subsystem and B to the second subsystem. This gives the operator $A \otimes B$ on the combined system, defined on entangled states by linearly extending its action on unentangled states. Let $|e_1>, ..., |e_m>$ be a basis for the second subsystem, and write $B = \sum_{k,l=1}^{n} b_{kl}|f_k><f_l|$. Then a basis for the combined system is $|e_i> \otimes |f_j>$, for $i = 1, ..., m$ and $j = 1, ..., n$. The operator $A \otimes B$ is

$$\begin{aligned} A \otimes B &= (\sum_{ij} a_{ij}|e_i><e_j|) \otimes (\sum_{kl} b_{kl}|f_k><f_l|) \\ &= \sum_{ijkl} a_{ij}b_{kl}|e_i><e_j| \otimes |f_k><f_l| \\ &= \sum_{ijkl} a_{ij}b_{kl}(|e_i> \otimes |f_k>)(<e_j| \otimes <f_l|). \end{aligned}$$

Therefore the $(i, k), (j, l)$th element of $A \otimes B$ is $a_{ij}b_{kl}$. If we order the basis $|e_i> \otimes |f_j>$ lexicographically, then the matrix for $A \otimes B$ is

$$\begin{pmatrix} a_{11}B & a_{12}B & \cdots \\ a_{21}B & a_{22}B & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix};$$

in the i, jth subblock, we multiply a_{ij} by the matrix for B.

3. No cloning theorem

A quantum operation which copied states would be very useful. For example, we considered the following problem in Homework 1: Given an unknown quantum state, either $|\phi>$ or $|\psi>$, use a measurement to guess which one. If $|\phi>$ and $|\psi>$ are not orthogonal, then no measurement perfectly distinguishes them, and we always have some constant probability of error. However, if we could make many copies of the unknown state, then we could repeat the optimal measurement many times, and make the probability of error arbitrarily small. The no cloning theorem says that this is not physically possible. Only sets of mutually orthogonal states can be copied by a single unitary operator.

Theorem 3.1. *No Cloning Theorem. Assume we have a unitary operator U and two quantum states $|\phi>$ and $|\psi>$ which U copies, i.e.,*

$$|\phi> \otimes |0> \longrightarrow^U |\phi> \otimes |\phi>$$

$$|\psi> \otimes |0> \longrightarrow^U |\psi> \otimes |\psi> .$$

Then $<\phi|\psi>$ is o or 1.

Proof. $<\phi|\psi> = (<\phi| \otimes <0|)(|\psi> \otimes |0>) = (<\phi| \otimes <\phi|)(|\psi> \otimes |\psi>) = <\phi|\psi>^2$. In the second equality we used the fact that U, being unitary, preserves inner products. □

4. Superdense Coding

Suppose Alice and Bob have a quantum communications channel, over which Alice can send qubits to Bob. However, Alice just wants to send a regular classical letter (sequence of bits). One way to send her message is to encode a 0 as $|0>$ and a 1 as $|1>$. But can she do better than sending as many qubits as bits in her message? Intuitively, since quantum systems are more complex than classical systems, they can hold informationso maybe Alice can do better. But quantum information is hard to access; when you measure a quantum state, it looks classicalso maybe she cant. In fact, if Alice and Bob share a Bell state, then she can send two classical bits of information using only one qubit. Say Alice and Bob share $|\Phi^+ >= \frac{1}{\sqrt{2}}(|00> +|11>)$. Depending on the message Alice wants to send, she applies a gate to her qubit, then sends it to Bob. If Alice wants to send 00, then she does nothing to her qubit, just sends it to Bob. If Alice wants to send 01, she applies the phase flip Z to her qubit, changing the quantum state to $\frac{1}{\sqrt{2}}(|00> -|11>) = \Phi^- >$. To send 10, she applies the NOT gate, giving $\frac{1}{\sqrt{2}}(|10> +|01>) = \Psi^+ >$. To send 11, she applies both NOT and Z, giving $\frac{1}{\sqrt{2}}(|01> -|10>) = \Phi^- >$. After receiving the qubit from Alice, Bob has one of the four mutually orthogonal Bell states. He can therefore apply a measurement to distinguish between them with certainty, and determine Alices message. Note that Alice really did use two qubits total to send the two classical bits. After all, Alice and Bob somehow had to start with a shared Bell state. However, the first qubitBobs half of the Bell statecould have been sent well before Alice had decided what message she wanted to send. Perhaps only much later did she decide on her message and send over the second qubit. One can show that it is not possible to do any better. Two qubits are necessary to send two classical bits. Superdense coding allows half the qubits to be sent before the message has been chosen.

5. Symmetries in quantum mechanics

Whenever possible we follow the notation and terminology of [4].

5.1. **Repetition and Notation.** A quantum mechanical system is a pair $(\mathbb{H}, H)$ whose most important properties are as follows.

- $\mathbb{H}$ is a separable Hilbert space over $\mathbb{C}$.
- Elements $f \in \mathbb{H}$ are considered as states of the system. Two elements $f, g \in \mathbb{H}$ are physically equivalent if there is $C \in \mathbb{C} \setminus \{0\}$ such that $f = C \cdot g$. In other words, the states may be considered as elements of the projective space $\mathbb{P} := \mathbb{P}(\mathbb{H})$. Let $[\cdot] : \mathbb{H} \to \mathbb{P}, f \mapsto [f]$ be the canonical projection map (which is surjective).
- For two states $[f], [g] \in \mathbb{P}$, the (well-defined) quantity $\delta([f],[g]) := \frac{|<f,g>|^2}{||f||^2||g||^2}$ is considered as the transition probability from one state to the other.
- Observables are selfadjoint (unbounded) operators in $\mathbb{H}$.
- H(the Hamiltonian) is an observable which governs the time evolution of a state $\phi = [f] = [f_t] \in \mathbb{P}$ via the differential equation(Schrödinger equation):

$$i\hbar\frac{\partial f}{\partial t} = H(f) \tag{1}$$

  We say that ϕ satisfies the Schrödinger equation if $f \in \mathbb{H}$ such that $[f] = \phi \in \mathbb{P}$ does. By linearity, this is independent of the choice of a representative $f \in [\cdot]^{-1}(\phi)$.

This list is not complete. For details, consult [7, Sec. 3.1] and other books on quantum mechanics.

5.2. **Symmetry Transformations.** A symmetry transformation of a quantum mechanical system is a map that leaves the physics invariant. Considering the properties listed above, this amounts to a map that

(1) transforms states into states and may be inverted.
(2) leaves the transition probability from one state to another invariant
(3) does not change the role of the Hamiltonian H: Any solution of the Schrödinger equations should map to another solution.

The first two items are made precise by the following definition, that we shall need later.

Definition 5.1. Denote by $Aut(\mathbb{P})$ the set of bijective functions $T : \mathbb{P} \to \mathbb{P}$ such that $\delta(\phi, \psi) = \delta(T\phi, T\psi)$.

It is easy to see that $Aut(\mathbb{P})$ is a group. The following definition includes the third item.

Definition 5.2. A symmetry transformation of a quantum mechanical system $(\mathbb{H}, H)$ is an element $T \in Aut(\mathbb{P})$ such that for every $\phi \in \mathbb{P}$ that satisfies the Schrödinger equation 1, the transformed state $T_\phi \in \mathbb{P}$ satisfies the Schrödinger equation, too.

Example 5.3. Consider the Hilbert space $H := L^2(\mathbb{R}^3, \mathbb{C})$ with scalar product
$\int_{\mathbb{R}^3} \overline{f(x)} \cdot g(x)dx$
and Hamiltonian $H := -\frac{\hbar^2}{2m} \triangle$. One can show that $T_R : \mathbb{P} \to \mathbb{P}$, which is defined by $T_R([f]) := [f(R^{-1}\cdot]$ for $f \in \mathbb{H}$ is indeed a symmetry transformation, where $R \in SO(3)$ is a (fixed) rotation.

5.3. **Unitary Symmetry Groups.** Although the projective space $\mathbb{P}$ and not $\mathbb{H}$ itself should be regarded as the space of states (see above), it is usually more convenient for calculations to deal with elements $f \in \mathbb{H}$ instead of $[f] \in \mathbb{P}$, often with the assumption that f be normed(i.e. $||f|| = 1$). The rest of this talk deals with how quantum symmetries may be phrased in terms of $\mathbb{H}$.

Definition 5.4. Denote by $U(\mathbb{H})$ the set of $\mathbb{C}$-linear bijective functions $R : \mathbb{H} \to \mathbb{H}$ such that the scalar product of $\mathbb{H}$ is left invariant: $< f, g >=< Rf, Rg >$.

It is easy to see that an $R \in U(\mathbb{H})$ leaves the transition probability invariant:
$([f], [g]) = \delta([Uf], [Ug])$
for all $f, g \in \mathbb{H}$. Hence to a unitary transformation $R \in U(\mathbb{H})$ is canonically associated

a well-defined map $[R] \in Aut(\mathbb{P})$ by prescribing $[R]([f]) := [Rf]$, which yields a projection map $[\cdot] : U(\mathbb{H} \to Aut(\mathbb{P}),\ R \mapsto [R] : \mathbb{P} \to \mathbb{P}$.

Lemma 5.5. *$U(\mathbb{H})$ is a topological group with respect to the strong topology, and $[\cdot] : U(\mathbb{H}) \to Aut(\mathbb{P})$ is a continuous homomorphism.*

Proof. Consult [8, Chp. 3], for details. □

Therefore, and since unitary transformations leave the transition probability invariant, one is lead to consider $U(\mathbb{H})$ to be corresponding to $Aut(\mathbb{P})$.

Definition 5.6. Let $(\mathbb{H}, H)$ be a quantum mechanical system and G be a topological group. Then G is called a symmetry group of the system if there is a projective representation $T : G \to Aut(\mathbb{P})$ such that T_g is a symmetry transformation for every $g \in G$.

Definition 5.7. A unitary symmetry transformation of a quantum mechanical system $(\mathbb{H}, H)$ is an element $R \in U(\mathbb{H})$ such that for every $f \in \mathbb{H}$ that satisfies the Schrödinger equation 1, the transformed state $Rf \in \mathbb{H}$ satisfies the Schrödinger equation, too.

The following lemma provides another (stronger) condition which is often called a symmetry condition in the literature (cf. e.g. [7, Sec. 3.3]).

Lemma 5.8. *Let $R \in U(\mathbb{H})$ be such that R commutes with the Hamiltonian: $R \circ H = H \circ R$, then R is a unitary symmetry transformation.*

Proof. Let $f \in \mathbb{H}$ a solution of the Schrödinger equation 1. Then $H(Rf) = RH(f) = Ri\hbar\frac{\partial f}{\partial t} = i\hbar\frac{\partial (Rf)}{\partial t}$ and $Rf$is a solution, too. □

Definition 5.9. Let G be a topological group and $\mathbb{H}$ as above. Then a unitary representation of G in $\mathbb{H}$ is a function $R : G \to U(\mathbb{H}), g \mapsto R_g : \mathbb{H} \to \mathbb{H}$

which is a continuous group homomorphism (wrt. the strong topology on U(H)), i.e.

- R preserves the group structure: $R_{g\cdot h} = R_g \circ R_h$.
- For all $f \in \mathbb{H}$, the induced function $G \to \mathbb{H}$, $g \mapsto R_g(f)$ is continuous.

Definition 5.10. Let $(\mathbb{H}, H)$ be a quantum mechanical system and G be a topological group. Then G is called a unitary symmetry group of the system if there is a unitary representation $R : G \to U(\mathbb{H})$ such that R_g is a unitary symmetry transformation for every $g \in G$.

Lemma 5.11. *Let G with $R : G \to U(\mathbb{H})$ be a unitary symmetry group. Then concatenation with the canonical projection $T := [\cdot] \circ R : G \to Aut(\mathbb{P})$, yields a symmetry group (G, T) in the sense of Definition 5.6.*

Proof. We have seen above (below Definition 5.4) that for every $g \in G$ indeed $T_g \in Aut(\mathbb{P})$. Now since for all $f \in H$, the map $G \to \mathbb{H}$, $g \mapsto R_g(f)$ is continuous and also the map $[\cdot]$ is continuous (cf. Lemma. 5.5), it follows that also $G \to \mathbb{P}$, $g \mapsto [\cdot] \circ R_g(f) = T_g([f])$ is continuous. T is a homomorphism since $R_{gh} = R_g R_h$ implies (for every $f \in \mathbb{H}$)

$$T_{gh}([f]) = [R_{gh}(f)] = [R_g(R_h(f))] = T_g([R_h(f)]) = Y_g T_h([f])$$

and therefore $T_{gh} = T_g T_h$. For all $g \in G$, R_g is a unitary symmetry transformation, that is any solution f of the Schrödinger equation 1 is mapped to a solution $R_g f$. Since $T_g([f]) = [R_g f]$, the analogous statement is true for T_g and thus T_g is a symmetry transformation. □

Groeger [4] studied the converse question:

Question 5.12. *Let G with $T : G \to Aut(\mathbb{P})$ be a symmetry group. Does there exist a unitary lift, i.e. a unitary symmetry group $(G, R : G \to U(\mathbb{H}))$ such that $T = [\cdot] \circ R$?*

References

[1] Bishop, E., Foundations of Constructive Analysis, *McGraw-Hill, N.Y*, (1967).

[2] Giles, R., Foundations for Quantum Mechanics. [Hoo], 277-322

[3] Greiner. W., Müller. B., Quantum mechanics: symmetries, *Springer-Verlag*, (1989).

[4] Groeger. J., Symmetries in Quantum Mechanics, *Lectuer*, (2010).

[5] Harter. W. G., Principles of symmetry, dynamics, and spectroscopy, *Wiley*, (1993).

[6] Fannes, M., Verbeure, A., On the Time Evolution Automorphisms of the CCR-Algebra for Quantum Mechanics, *Commun. Math. Phys*, **35**(1974)257–264.

[7] Schottenloher. M, Geometrie und Symmetrie in der Physik, *Vieweg*, (1995).

[8] Schottenloher. M, A Mathematical Introduction to Conformal Field Theory, *Springer-Verlag*, (2008).

Department of Mathematics, Ashtian Branch, Islamic Azad University, Iran.

E-mail address: naraghi@mail.aiau.ac.ir