

PHY662, Spring 2004
Outline for Tues. Jan. 20, 2004
More Spin- $\frac{1}{2}$, Cryptography (if time allows)

20th January 2004

1 Administration

- e-mail addresses?
- Sections 2 and 3 in this outline are supplementary material that we won't dwell on in lecture, unless there are questions.
- Homework due Jan. 27 but will be handed out: see HWK for reading and problems.
- For Thursday, read Shankar through p. 392, then pp. 397 through 401. Plan for Thursday is electron in constant magnetic field and coupling to spatial degrees of freedom. Next week is magnetic resonance and two-level systems. We will not use Shankar for those topics next week.

Today

1. We will review the homework
2. This will be a base for a review of operators, the presentation in Ch. 6 of Feynman, and Pauli matrices.
3. We will then start on quantum cryptography.

2 Operators - a reminder

We will be dealing with a variety of operators and their representation by matrices. So it is useful to remember the distinctions among them.

Real matrices correspond to linear transformations on vector spaces with real coefficients.

Real orthogonal matrices rotate vectors, preserving length (HWK #1, problem #1).

Hermitian operators have the property they are self-adjoint $H^\dagger = H$, so that their representation by matrices H_{ij} satisfy $H_{ij} = H_{ji}^*$. The eigenvalues of Hermitian operators are real. All observables are Hermitian.

Unitary operators leave inner products invariant: if U is unitary, with $|\psi'\rangle = U|\psi\rangle$, $|\chi'\rangle = U|\chi\rangle$, then $\langle\psi'|\chi'\rangle = \langle\psi|U^\dagger U|\chi\rangle = \langle\psi|I|\chi\rangle = \langle\psi|\chi\rangle$. In a given basis, the inner product $\langle\chi|\psi\rangle$ for two vectors ψ_i and χ_i is $\chi_i^* \psi_i$ (note the implicit sum over i here). This gives $U_{ji}^* U_{jk} = \delta_{ik}$. The eigenvalues of unitary operators are of the form $e^{i\lambda}$, for real λ . Unitary operators correspond to symmetry operations: translations in space, rotations, and translation in time.

In general, the exponential of iA , where A is Hermitian, is a unitary operator: if $U = e^{iA}$, $U^\dagger = e^{-iA^\dagger} = e^{-iA}$, so that $U^\dagger U = I$. The most important unitary operator is the time translation operator $e^{i\mathcal{H}}$, where \mathcal{H} is the Hamiltonian.

It is very useful to remember what type of operators we are working with :

- **Rotation of coordinate frames** are elements of $SO(3)$. The rotation of coordinate frames can be represented by real orthogonal matrices with unit determinant: in this case, the matrices for the representation operate on real 3-dimensional vectors. These elements can be parametrized by rotations $\vec{\theta} = \theta\hat{\theta}$, since $SO(3)$ is three-dimensional.
- The three **spin operators** $\vec{S} = (S_x, S_y, S_z)$ in any frame are Hermitian operators. For spin-1/2, they operate on *spinors* which have two components. Given a choice of \hat{z} , these 3 operators do not commute: a particle cannot have a definite spin along more than one direction at the same time. They each commute with \vec{S}^2 .
- The **rotation operators** must be unitary to conserve probability and in fact are *generated* by the Hermitian \vec{S} . A rotation $\vec{\theta}$ can be written as $e^{i\vec{\theta}\cdot\vec{S}}$. The rotation operators are elements of $SU(2)$: they conserve probability (unitary), transform 2-component “spinors” (2), and have determinant 1 (by convention - they need to have some phase, after all).

3 Showing linearity - an aside

This section is supplementary for people who want to review why natural behavior for the composition of operations gives linear functions.

Linearity is natural in many situations, but to be sure, one should prove it. In class last time, it was argued that rotations about the \hat{z} -direction generated a phase change in $|+\rangle$ states. The principle used here is used many times in physics: it relies on composition of operations and continuity. For example, a similar argument leads to power-law scaling in “scale-invariant” systems, such as a physical system at a second-order phase transition point (like magnets).

Suppose that rotation of the coordinate frame by an angle α about the \hat{z} -direction generates a phase change $\phi(\alpha)$, i.e., $|+\rangle \rightarrow e^{i\phi(\alpha)}|+\rangle$ (and $|-\rangle \rightarrow e^{-i\phi(\alpha)}|-\rangle$). One then can show that, since two rotations by angle α must give the same phase change as a rotation by the angle 2α ,

$$\phi(2\alpha) = 2\phi(\alpha),$$

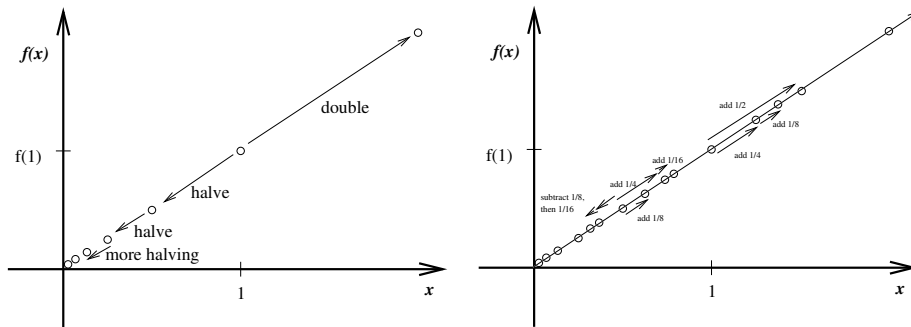
and more generally, by the same principle,

$$\phi(\alpha_1 + \alpha_2) = \phi(\alpha_1) + \phi(\alpha_2).$$

Assuming that $\phi(\alpha)$ is continuous, this can be used to show that $\phi(\alpha)$ is truly linear in α , that is $\phi(\alpha) = m\alpha$, for some m .

In general, let $f(x)$ be a continuous function with $f(2x) = 2f(x)$. Then $f(x) = 2f(x/2)$, $f(x/2) = f(x/4)$, etc. Suppose we want to compute $f(y)$ for some value y and all we know is $f(1)$. Expand y in binary notation to a given number of digits. For example, if $y = 1/3$, $y = 0.01010101\dots$ in binary (as $11 \times 0.1010101\dots = 0.1111111\dots = 1$), i.e., $y = \frac{1}{4} + \frac{1}{16} + \frac{1}{64} + \dots$. As $f(\frac{1}{4}) = f(1)/4$, $f(\frac{1}{16}) = f(1)/16$, $f(\frac{1}{64}) = f(1)/64$, etc., one can approximate $f(1/3)$ by taking the limit of the values $f(\frac{1}{4}) = \frac{f(1)}{4}$, $f(\frac{1}{4} + \frac{1}{16}) = \frac{f(1)}{4} + \frac{f(1)}{16}$, $f(\frac{1}{4} + \frac{1}{16} + \frac{1}{64}) = \frac{f(1)}{4} + \frac{f(1)}{16} + \frac{f(1)}{64}$, giving $f(1) \cdot (\frac{1}{4} + \frac{1}{16} + \frac{1}{64} + \dots) = f(1) \cdot \frac{1}{3}$. So choosing $m = f(1)$ works for this fraction. The argument can be made for a general binary expansion (and for arguments $x > 1$ including positive powers of 2), to give the result $f(x) = xf(1) = mx$, with $m = f(1)$.

A “proof by graph” might help one understand and visualize this. The following pair of graphs shows how you can first double and halve the arguments to f , then add them in combination to give the function definition on a dense. Repeating this for a while gives a countable subset of the x -axis, with $f(x)$ linear on the defined points. Continuity then gives that the function is linear on the full real interval.



4 Today - Continued Discussion of Feynman's Derivation

4.1 Clarifying last times' discussion of rotations by π

- Feynman et al. write “We must have the situation that a rotation by 360° and *no smaller angle* reproduces the same physical state.” (Same physical state does not mean the same amplitude, though).
- We got to the point of showing that a rotation of angle α about the \hat{z} -axis gives a phase change of $m\alpha$ for the $|+\rangle$ state and a phase change of $-m\alpha$ for the $|-\rangle$ state. But we need to figure out what m is.
- What if $m = 1$? Then a rotation by 2π would give the same physical state, as $e^{i \cdot 1 \cdot 2\pi} = e^{-i \cdot 1 \cdot 2\pi} = 1$. But this gives a problem, as a rotation by π would give the same physical state: $e^{im\pi} = -1 = e^{-im\pi}$, if $m = 1$, so that the two states $|\pm\rangle$ each would be multiplied by -1, so that *all observables would be unchanged*. A rotation by π , however, must change the expectation value for S_x . [Draw diagram to see this: note that the open apparatuses in the diagram are there to indicate that we could measure the amplitudes in the relatively rotated frames if we wished.]
- What if there were more spin states?? Does m need to be $\frac{1}{2}$?

4.2 y-rotations

- Rotation by π about \hat{y} must give

$$C'_+ = e^{i\beta}C_-, \quad C'_- = e^{i\gamma}C_+ .$$

- 2π rotation about \hat{y} must give the same phase change as a 2π rotation about \hat{z} . This gives a constraint on γ and β . Then set γ by convention to get Eq. (6.22).

4.3 Rotations in general

I will not take the time to reproduce the arguments from FES's Ch. 6 in detail. If you read it and understand it, that would be great. The main sticking point is the notation and diagrams, which could be more clear. The main point is that since combinations of rotations about \hat{z} and \hat{y} can be used to generate rotations about \hat{x} , we can next deduce the effects of rotations about the \hat{x} -axis. You should be familiar with the results at the end of this chapter, however. We will also arrive at the same results in a more abstract fashion, using the commutation relations for spin.

Following Shankar, by using $[S_i, S_j] = i\hbar\epsilon_{ijk}S_k$ and assuming 2 states

Notation:

\hat{n} is a unit vector in 3D.

$\vec{\theta}$ defines a rotation by angle θ about the direction $\hat{\theta}$. [Only in 3D can one represent rotations by vectors.]

ϕ is the angle of a rotation about the \hat{z} axis, while θ is the angle away from the \hat{z} -axis (polar coordinates).

We will use implicit summations: $a_i b_i = \sum_i a_i b_i$.

Note: Shankar writes vectors as \mathbf{A} . I will use \vec{A} .

$S_+ = S_x + iS_y$; $S_- = S_x - iS_y$.

$\vec{\sigma}$ are the three Pauli matrices, arranged as a vector σ_i , with $\vec{A} \cdot \vec{\sigma} = A_i \sigma_i$ being an operator on spinors.

In this section, we will review commutation relations, representations for spin.

In earlier chapters, when studying orbital angular momentum, the commutation relations $[J_i, J_j] = i\hbar\epsilon_{ijk}J_k$ are used to determine the finite-dimensional representations for the angular momentum operators \vec{J} . This is done especially through the use of the raising and lowering operators $J_+ = J_x + iJ_y$ and $J_- = J_x - iJ_y$ and commutation relations between them and J_z and $J^2 = J_x^2 + J_y^2 + J_z^2$, with $J^2 = J_- J_+ + J_z^2 - \hbar J_z$ (see p. 327, for derivation of Eq. (12.5.20) in Shankar, especially).

Uniqueness of the wave function in real space (x, y, z points) implies *orbital* angular momenta are quantized in units of \hbar .

Discussion of important expressions:

This is the most basic one: it is derived from the symmetries of rotation and is used to derive the rest:

$$[S_i, S_j] = i\hbar\epsilon_{ijk}S_k$$

If there are only two states, as is seen for Ag atoms, e.g., these operators have as one representation

$$\vec{S} = \frac{\hbar}{2}\vec{\sigma}$$

where the Pauli matrices are defined as

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

This is the representation of spin- $\frac{1}{2}$ and these operators operate on two-component "spinors". These two-component objects contain the amplitudes for up and down spins.

The σ_i anticommute with each other, with

$$\sigma_i \sigma_j = -\sigma_j \sigma_i \quad (i \neq j)$$

are square roots of the identity:

$$\sigma_i^2 = I$$

and are traceless.

**** Show that $(\hat{n} \cdot \sigma)^2 = I$.

**** Establish the expression

$$(\vec{A} \cdot \vec{\sigma})(\vec{B} \cdot \vec{\sigma}) = \vec{A} \cdot \vec{B} + i(\vec{A} \times \vec{B}) \cdot \vec{\sigma},$$

for vector operators \vec{A}, \vec{B} that commute with $\vec{\sigma}$.

**** Reproduce effect of S_+ and S_- on spinors - check with Pauli matrices.

**** Show how S_x both measures and generates spins about \hat{x} .

In the \hat{n} basis, the base states are $|\hat{n}, +\rangle$ and $|\hat{n}, -\rangle$, are eigenvectors of the operator $\hat{n} \cdot \vec{S}$, with the same eigenvalues for \vec{S} of $\pm\hbar/2$, as shown in HWK #1, problem #3.

HWK#1, problem #3 shows that 2×2 matrices can be represented as linear combinations of Pauli matrices and the identity matrix.

Carry out derivation of 14.3.39, after introducing commutation and anti-commutation relations for the σ_i .

Note “interesting” that one can go from $\langle \vec{S} \rangle$ to an \hat{n} .

5 Introduction to quantum cryptography

5.1 Classical cryptography

1. Not everyone wants their mail easily readable.
2. Encryption of a *plaintext* is the conversion of the message to a form that is presumed to be readable only by the intended recipient.
3. Historically, there is a sequence of encryption schemes (simple substitution for letters, transpositions, polyalphabetic substitution (Vignere cipher), etc.) that are based on a shared *key* that is not too long.
4. Patterns lead to ability to read the message.
5. *Public-key cryptography* has revolutionized classical cryptography, but assumes some problems, like factoring very large integers, are difficult to solve.
6. One code that is theoretically unbreakable (code “X” if you will): one-time pads. This code is used for very secure communications that are infrequent, as key distribution can be cumbersome and insecure.

5.2 Quantum cryptography - key distribution

One use for quantum cryptography: securely distributing a one-time key (with no fear of eavesdropping). Relies on non-commutativity of the spin operators and the collapse of the wave function upon observation.

Here is the classic example, Bennett and Brassard, 1984 (adapted to spin-1/2 - usually is described with photons):

1. “Alice” sends a sequence of states randomly chosen from $|+, \hat{z}\rangle$, $|-, \hat{z}\rangle$, $|+, \hat{x}\rangle$, $|-, \hat{x}\rangle$.
2. “Bob” randomly chooses to measure in the \hat{z} or \hat{x} direction for each electron.
3. Afterwards, Alice and Bob *publicly announce* which axes they sent or measured the electron along.
4. *Where they used the same basis*, they have a sequence of up and down (translated into a sequence of 1’s and 0’s) that they agree on. This can be used as a one-time pad for a subsequent message sent classically.
5. *No one else* can know these states. For if “Claire” measured the electrons en route from Alice to Bob, Claire would have disturbed the wave function.

Example:

Alice chooses the random sequence

$|+, \hat{z}\rangle$, $|+, \hat{x}\rangle$, $|+, \hat{x}\rangle$, $|-, \hat{z}\rangle$, $|+, \hat{x}\rangle$, $|-, \hat{z}\rangle$

Bob makes measurements, randomly chosen, along the axes x, x, z, z, x, x .

At this point Alice announces “ z, x, x, z, x, z ” and Bob announces “ x, x, z, z, x, x ”.

They agree on the 2nd, 4th, and 5th spins. So they now jointly know the sequence “+,-,+” which they can use as a bit sequence “101”= key. Alice decides to send the message plaintext=001, which gets converted to plaintext \oplus key = $001 \oplus 101 = 100$. Only Bob, who knows that “101” is the key, can properly convert the ciphertext to plaintext: $100 \oplus 101 = 001$.

Now, Alice and Bob can also check for snoops who might be peeking at their bits. If Claire had been using an apparatus in between that was making measurements, it would change the amplitudes.

[This all gets more complicated with errors in the signal, etc. Errors in alignment of apparatus or patterns in random number generators might provide an attacker with clues. Photons work better than electrons or spin-1/2 atoms; here one sets polarizers in 4 directions left-right, up-down, and $2 \pi/4$ rotations to prepare photons polarized in 4 different directions, but the scheme is the same.]