

PHY662, Spring 2004
Outline for Thurs. Jan. 22, 2004
More Spin- $\frac{1}{2}$, Cryptography

22nd January 2004

1 Administration

- e-mail addresses?
- Acknowledgements on HWK. If none, please write “I did these problems independently.”
- Homework due Jan. 27 but will be handed out: see HWK for reading and problems.
- Next week is magnetic resonance and possibly two-level systems. We will not use Shankar for those topics next week.

Today

1. A couple of results for Pauli matrices.
2. Symmetry and conservation laws.
3. Quantum cryptography.
4. Spins and their magnetic moment: magnetic fields.

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

**** Establish the expression [exercise]

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

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

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

Note “interesting” that one can go back and forth between $\langle \vec{S} \rangle$ and \hat{n} . [Not true for other spins. Why not?]

3 Introduction to quantum cryptography

3.1 Classical cryptography

1. Not everyone wants their mail easily readable.
2. Encryption of a *plaintext* to *cyphertext* 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. Interesting consequences of that.
5. *Public-key cryptography* has revolutionized classical cryptography, but assumes that some problems, like factoring very large integers, are difficult to solve. They are based on trap door functions: you hand out padlocks, publicly, then someone who wants to write a message “locks” their message. Even the sender can’t “unlock” the message. But with your private key, you can.
6. One code that is theoretically unbreakable (code “X” if you will): one-time pads. This code is used only for very secure communications that are infrequent, as key distribution can be cumbersome and insecure.

3.2 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. Other schemes also depend on quantum “entanglement”.

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

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

The particles are sent to Bob.

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

At this point Alice *publicly announces* “ z, x, x, z, x, z ” and Bob *publicly 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 $\text{plaintext} \oplus \text{key} = 001 \oplus 101 = 100$. 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.]

4 Conservation and Symmetry

Symmetries and Conservation Laws - a reminder

NOTE: the rotation operators in Feynman are for a change of the frame (passive transformation). *So all angles are inverted to get the rotation operators in Shankar!*

1. For spin, what is the conservation law and what is the symmetry?
2. How are rotations and spin related by logarithms?
3. How unitary symmetry operators are related to conserved Hermitian operators. [See Ch. 11 in Shankar for translation/momentum.]

5 Spins in a constant magnetic field

This is very simple, really, in quantum mechanics. To explain magnetic moments in a constant magnetic field, one needs all these ideas of torque, etc.

The result is *precession*, similar to precession in classical mechanics, but easier.

The Hamiltonian for a magnetic moment in a magnetic field is

$$H = -\vec{\mu} \cdot \vec{B},$$

where the magnetic moment operator is related to the spin operator by

$$\vec{\mu} = \gamma \vec{S} = \frac{gq}{2mc} \vec{S}.$$

Where the proportionality constant γ has been redefined in terms of a unitless “ g -factor”. For orbital angular momentum, $g = 1$. For spin, it depends: $g_{\text{electron}} \approx 2$, $g_{\text{proton}} \approx 5.6$, and $\gamma_{\text{neutron}} = -3.8 \left(\frac{e}{2M_{\text{neutron}}c} \right)$.

The time evolution operator $U(t)$ is now given by $U(t) = \exp(-iHt/\hbar) = \exp[i\gamma t(\vec{S} \cdot \vec{B})/\hbar]$. *What other operator is this equal to?*

Example: consider a spin-1/2 particle in the state $|+, \hat{x}\rangle$ in a field oriented in the \hat{z} -direction. What is its state as a function of time? What are $\langle S_x(t) \rangle$, $\langle S_y(t) \rangle$, and $\langle S_z(t) \rangle$?

Note the μ -decay experiment and possible indications of new particles (supersymmetry).