

THE BASIC RULES of QMstate vector $|\psi\rangle$

N dimensional, where N is the number of observable states

eg. SCHRÖDINGER'S CAT

$$|\star\rangle = c_1 |\text{alive}\rangle + c_2 |\text{dead}\rangle$$

COEFFICIENTS
ARE AMPLITUDES
for those states

2 POSSIBLE
OBSERVABLE
STATES

(basis)

AMPLITUDE for state i is a \mathbb{C} # c_i

s.t. $|c_i|^2 = \text{PROBABILITY to OBSERVE state } i$
if we observed $|\psi\rangle$

eg. imagine an ensemble of 100 cats in a quantum superposition (quantum state) $|\psi\rangle$

and suppose $c_1 = 1/\sqrt{2}$, $c_2 = 1/\sqrt{2}$

$$\Rightarrow P(\text{alive}) = P(\text{DEAD}) = 1/2$$

if 100 scientists each observed one of those 100 cats, about 50 will be alive, 50 will be dead

if, on the other HAND, $c_1 = \sqrt{\frac{3}{4}}$, $c_2 = \sqrt{\frac{1}{4}}$

$$\Rightarrow P(\text{alive}) = 3/4 \quad P(\text{dead}) = 1/4$$

note: overall phase doesn't matter:

$$c_1 |1\rangle + c_2 |2\rangle \cong e^{i\theta} (c_1 |1\rangle + c_2 |2\rangle)$$

↓ \approx 8 qubit

FOR NOW, focus on 2 state systems (2 DIM)
in fact, we can restrict to \mathbb{R} vector space (\mathbb{R}^2).

BECAUSE the QUANTUM state will always be observed to be in one of the two observable states, the probabilities must sum to 1.

$$|\psi\rangle = c_1|e_1\rangle + c_2|e_2\rangle \quad \text{w/} \quad |c_1|^2 + |c_2|^2 = 1$$

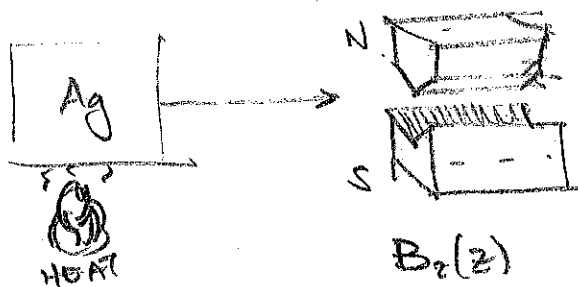
write $c_1 = c_1$, $c_2 = c_2$
AND CAN ASSUME $c_{1,2} \in \mathbb{R}$

WHAT BASIS? \leftrightarrow (set of observables)

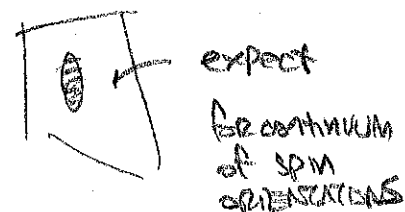
eg. Stern-Gerlach expt

5_z state

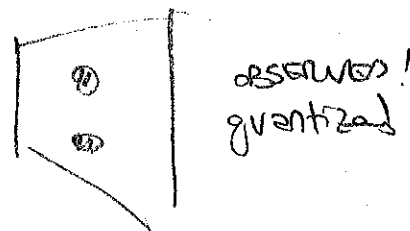
consider SILVER ATOMS \leftarrow 47 electrons
(46 are spherically symmetric)
↳ leftover electron intrinsic spin gives angular momentum.



$B_z(z)$
(inhomogeneous: $\partial_z B_z \neq 0$)



expect
a continuum
of spin
orientations



observed!
quantized

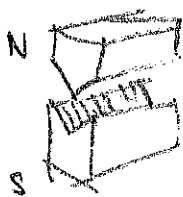
what's going on? MAGNETIC MOMENT of Ag atom \sim SPIN of electron

$$\mu \propto S$$

there is a force in z-dir: $F_z = \partial_z (\mu \cdot B)$

$$= \mu_z (\partial_z B_z)$$

\uparrow some const



$$= S_z$$

MEASUREMENT

evidently, some atoms have $\mu_z = \pm$ \leftarrow in fact: $S_z = \pm \hbar/2$
quantized spin!

(*)

$$|\psi\rangle = c_1 |\uparrow\rangle + c_2 |\downarrow\rangle$$

\swarrow
a nice basis:

$$|\uparrow\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \leftarrow \text{spin up } (S_z = \hbar/2)$$

$$|\downarrow\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \leftarrow \text{spin down } (S_z = -\hbar/2)$$

RULE: MEASUREMENT of STATE "COLLAPSES" the wavefunction

UPON MEASUREMENT, (*) BECOMES EITHER $|\uparrow\rangle$ or $|\downarrow\rangle$

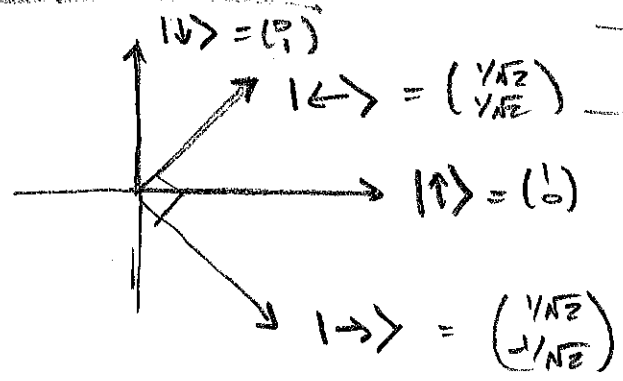
$$|\psi\rangle \big|_{\text{before MEAS}} = \frac{1}{\sqrt{2}} |\uparrow\rangle + \frac{1}{\sqrt{2}} |\downarrow\rangle \xrightarrow{\text{MEAS}} \frac{1}{\sqrt{2}} |\uparrow\rangle \quad \text{if measured } \uparrow$$

100% spin up!
if we measure again,
100% going to be
spin up.

MEASUREMENT is HERMITIAN op: $S_z = \frac{\hbar}{2} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
eigenvals are observed vals: $\lambda = \pm \hbar/2$

\hookrightarrow output of MEAS is $|\psi\rangle \rightarrow |\pm\rangle$ (eigenvector)
w/ probability $|c_{\pm}|^2$

OTHER BASES



EIGENBASIS of S_z

eigenbasis of S_x

$$S_x = \frac{\hbar}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

OBSERVE:

$$|↖> = \frac{1}{\sqrt{2}} |↑> - \frac{1}{\sqrt{2}} |↓>$$

$$|↘> = \frac{1}{\sqrt{2}} |↑> + \frac{1}{\sqrt{2}} |↓>$$

$|↖>$ is a linear comb. of $|↑>$

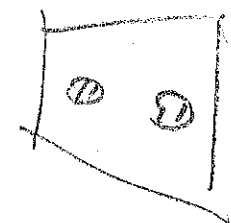
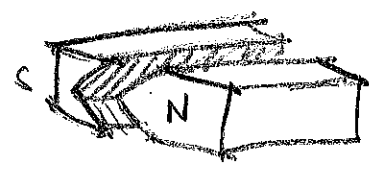
quantum superposition
NEITHER ↑ NOR ↓ UNTIL OBSERVED

similarly:

$$|↑> = \frac{1}{\sqrt{2}} |↖> + \frac{1}{\sqrt{2}} |↘>$$

$$|↓> = -\frac{1}{\sqrt{2}} |↖> + \frac{1}{\sqrt{2}} |↘>$$

What is $|↖>$ basis? ROTATE SG APPARATUS 90°:

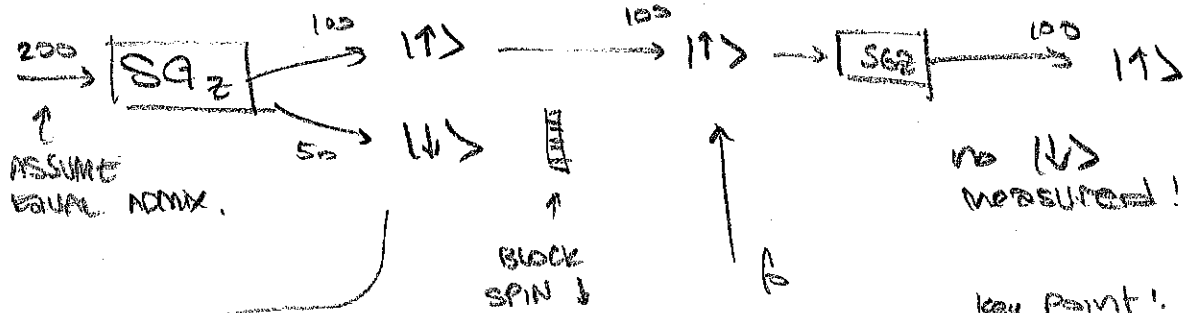


SPITS IN HORIZ DIR
VS. VERT DIR

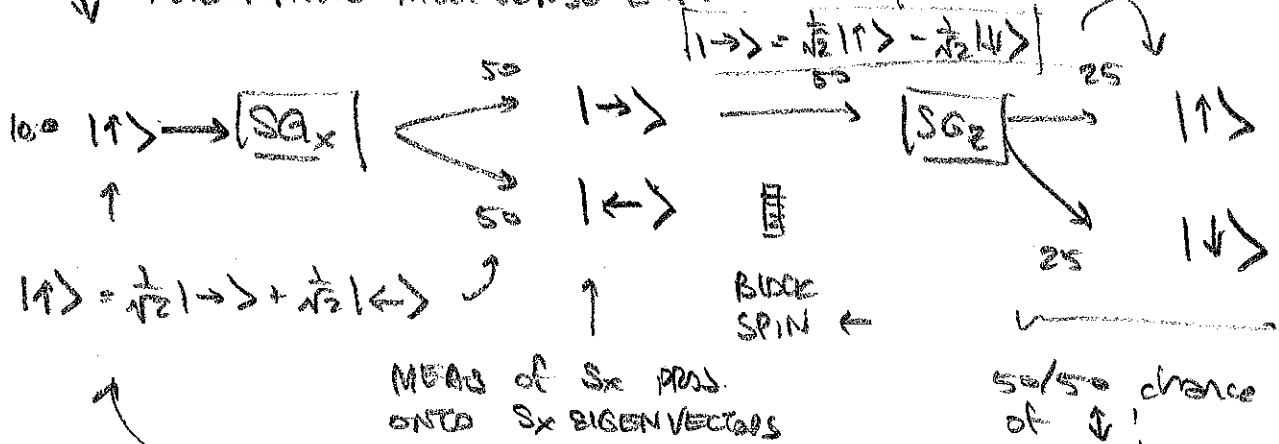
"measures spin in x-dir"

nb: collapsing to eigenstate of S_x mixes up information about S_z meas! $[S_x, S_z] \neq 0$.

SUCCESSIVE SG MEASUREMENTS: (ENSEMBLE)

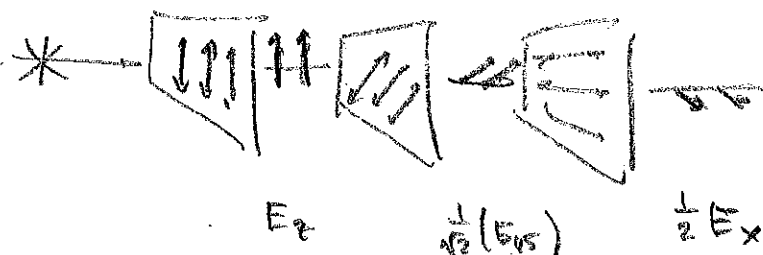
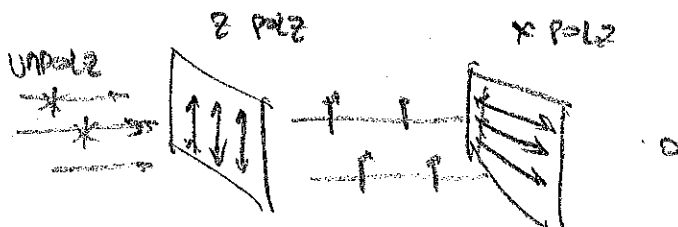


ALTERNATIVE MULTIVERSE EXPT.

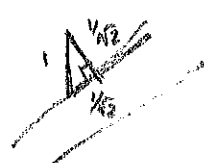


even though @ this point there was no ↓ comp!

ANALOG W/ POLARIMETERS (try this w/ 3 sets of polarized sunglasses)



JUST INSERTED AN INTERMED FILTER.



equivalence of state vectors

obpm: $|\uparrow\rangle \cong -|\uparrow\rangle$ (or in gen: $|\uparrow\rangle = e^{i\theta} |\uparrow\rangle$)

is there any measurement that can distinguish? NO

PICK SOME BASIS, not necessarily $|\uparrow\rangle : |e_1\rangle, |e_2\rangle$

MEASURE $|\uparrow\rangle = a|e_1\rangle + b|e_2\rangle$

$$P(\text{obs } \textcircled{1}) = |a|^2$$

$$P(\text{obs } \textcircled{2}) = |b|^2$$

MEASURE $-|\uparrow\rangle = (-a)|e_1\rangle + (-b)|e_2\rangle$

(SAME!)

IM. COMB.
WHAT ABOUT SUPERPOSITIONS?

$$\frac{1}{\sqrt{2}} (|\uparrow\rangle + |\downarrow\rangle)$$

$$\frac{1}{\sqrt{2}} (-|\uparrow\rangle - |\downarrow\rangle)$$

$$\frac{1}{\sqrt{2}} (|\uparrow\rangle - |\downarrow\rangle)$$

$$\frac{1}{\sqrt{2}} (-|\uparrow\rangle + |\downarrow\rangle)$$

} overall phase... these
are identical

} these are identical

are these identical??

is there any measurement to
distinguish

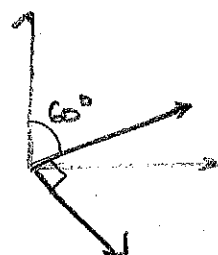
$$\frac{1}{\sqrt{2}} (|\uparrow\rangle + |\downarrow\rangle) \text{ from } \frac{1}{\sqrt{2}} (|\uparrow\rangle - |\downarrow\rangle) ??$$

ANSWER YES : $\frac{1}{\sqrt{2}}(|\uparrow\rangle + |\downarrow\rangle) = |\leftarrow\rangle$

$$\frac{1}{\sqrt{2}}(|\uparrow\rangle - |\downarrow\rangle) = |\rightarrow\rangle$$

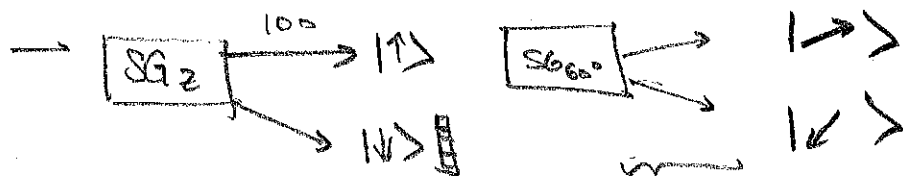
So if we do ANY (SGX) MEASUREMENT
("measure spin in x dir")

THIRD BASIS (op on #1)



$$|\leftarrow\rangle = \begin{pmatrix} \sqrt{3}/2 \\ 1/2 \end{pmatrix} = \frac{\sqrt{3}}{2}|\uparrow\rangle + \frac{1}{2}|\downarrow\rangle$$

$$|\rightarrow\rangle = \begin{pmatrix} 1/2 \\ -\sqrt{3}/2 \end{pmatrix} = \frac{1}{2}|\uparrow\rangle - \frac{\sqrt{3}}{2}|\downarrow\rangle$$



HOW MANY?

$$\begin{pmatrix} 1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & 1/2 \end{pmatrix} \begin{pmatrix} |\uparrow\rangle \\ |\downarrow\rangle \end{pmatrix} = \begin{pmatrix} |\rightarrow\rangle \\ |\leftarrow\rangle \end{pmatrix}$$

$$\begin{pmatrix} |\uparrow\rangle \\ |\downarrow\rangle \end{pmatrix} = \begin{pmatrix} 1/2 & \sqrt{3}/2 \\ -\sqrt{3}/2 & 1/2 \end{pmatrix} \begin{pmatrix} |\rightarrow\rangle \\ |\leftarrow\rangle \end{pmatrix}$$

$$\Rightarrow |\uparrow\rangle = \left(\frac{1}{2}\right)|\rightarrow\rangle + \left(\frac{\sqrt{3}}{2}\right)|\leftarrow\rangle$$

$$P(\rightarrow) = 1/4$$

$$P(\leftarrow) = 3/4$$

BB84 ← Bennett & Brassard 1984

CRYPTOGRAPHY: A → B want to share secret messages

↳ requires a KEY; ideally as long as message
to decrypt message. Avoid eavesdroppers!

BB84: Key Generation using QM

perfectly random → EAVESDROP-PROOF
OBSERVER

UNCD 2 state quantum system: QUBIT

A: BASIS $|a_0\rangle, |a_1\rangle$ ← 0 & 1 for A

B: BASIS $|b_0\rangle, |b_1\rangle$ ← 0 & 1 for B

$|b_0\rangle \neq |a_0\rangle$ in general
 $|b_1\rangle \neq |a_1\rangle$ (any orientation)

if A sends $|a_0\rangle$ = $d_0|b_0\rangle + d_1|b_1\rangle$
one bit

some linear combination
of Bob's qubit basis

When B measures,

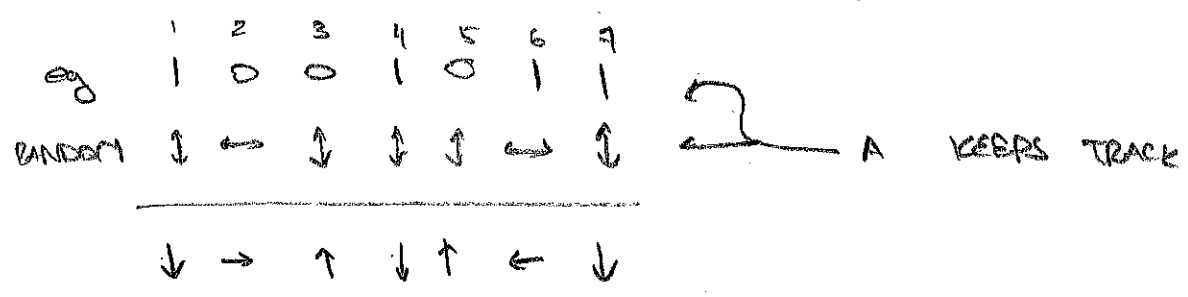
$$P(0) = |d_0|^2$$

$$P(1) = |d_1|^2$$

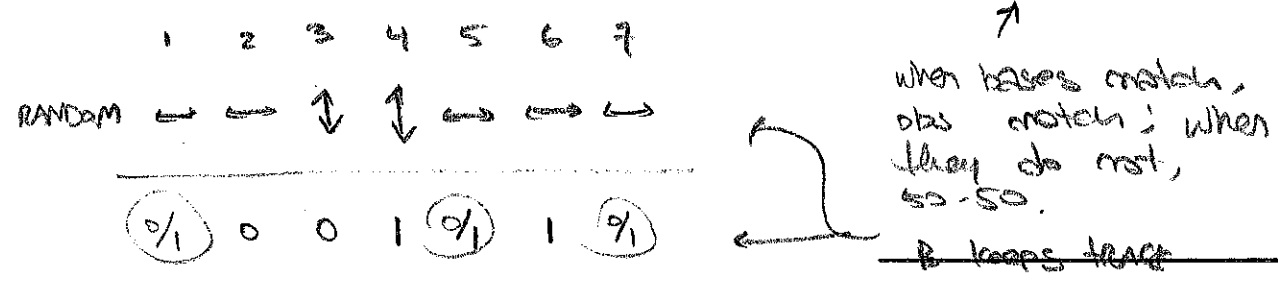
(not obviously useful for
sending info!)

BB84

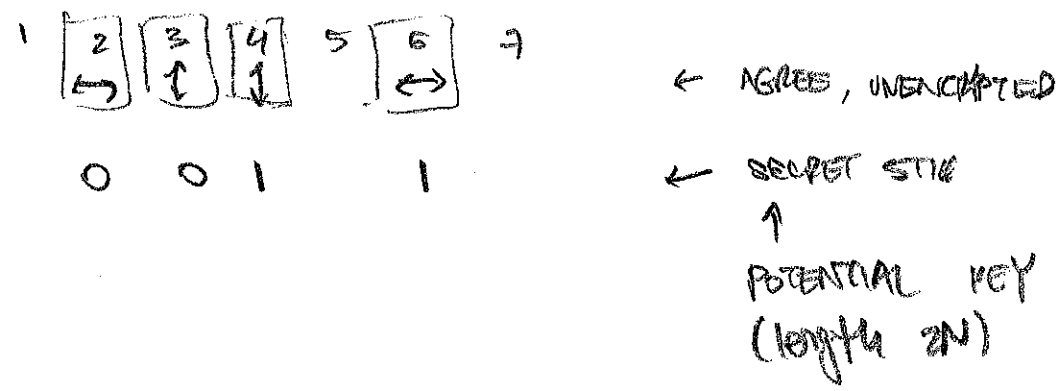
① ALICE WANTS TO SEND A (PROTO-)KEY to BOB
 ↳ 4n bits, for each bit, RANDOM PICK BASIS
 factor of 4 for convenience
 $n \gg 1$
 eg $| \uparrow \rangle$ or $| \leftrightarrow \rangle$



② BOB RECEIVES PROTO-KEY & READS IT
 FOR EA. BIT, RANDOM PICK BASIS, OBSERVES



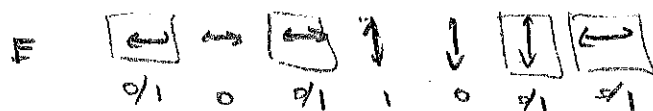
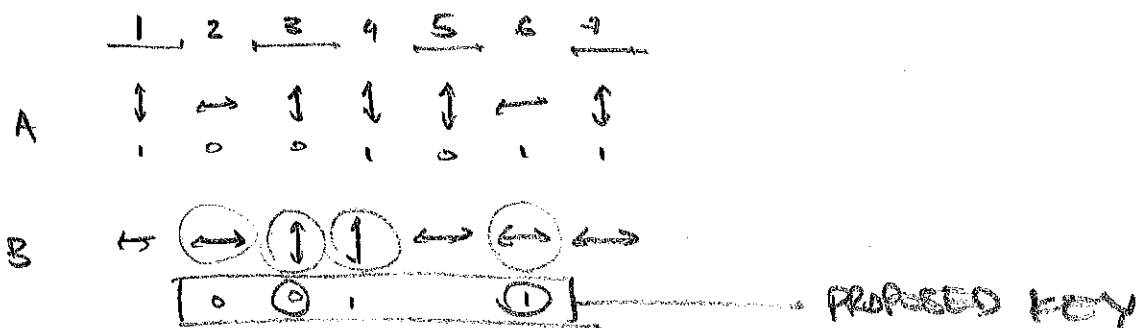
③ ROUGHLY 1/2 of ALL BITS HAVE SAME BASIS (~2n)
 ↳ A & B share their BASES over an UNENCRYPTED LINE
 ↳ RECORD WHICH ELEMENTS of the LIST HAD THE SAME BASIS



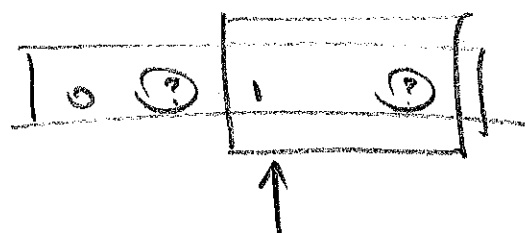
④ test for EAVESDROPPER

E wants to clone key.
 ↓
 means ^{intercepting} measuring qubits

BEST E can do: RANDOMLY PICK BASIS
 for EACH QUBIT, MEASURE,
 PASS ALONG TO BOB



E chooses wrong basis
 w/rt A half the time



half of these will
 pass the wrong
 state to B.

UNENCRYPTED:

A & B PICK half of the n
 QUBITS THAT THEY SHOULD AGREE on.

↳ n qubits for testing

they then compare out loud

↳ if they agree → SAFE

if they disagree on any → COMPROMISED
 (they re-encrypt)

for large n, E has to be
 improbably lucky to avoid detection.