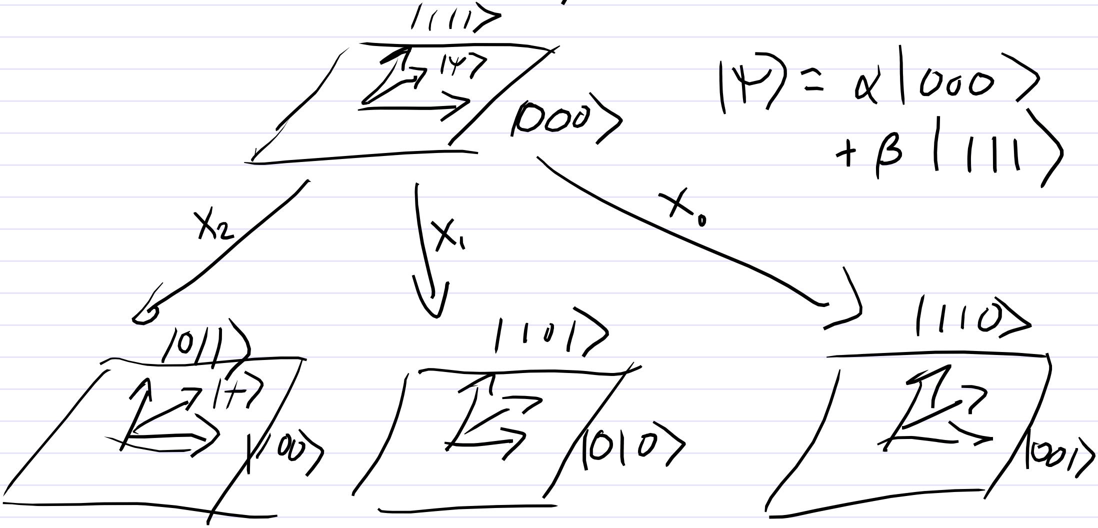
Lecture 20, 10 Nov 2020



$$|\psi\rangle = \alpha|000\rangle + \beta|111\rangle$$

"stabilizer formalism"

The New York Times

The Race Is On to Protect Data From the Next Leap in Computers. And China Has the Lead.

By Cade Metz and Raymond Zhong

Dec. 3, 2018

阅读简体中文版 · 閱讀繁體中文版

SAN FRANCISCO — The world's leading technology companies, from Google to Alibaba in China, are racing to build the first quantum computer, a machine that would be far more powerful than today's computers.

This device could break the encryption that protects digital information, putting at risk everything from the billions of dollars spent on e-commerce to national secrets stored in government databases.

An answer? Encryption that relies on the same concepts from the world of physics. Just as some scientists are working on quantum computers, others are working on quantum security techniques that could thwart the code-breaking abilities of these machines of the future.

It is a race with national security implications, and while building quantum computers is still anyone's game, China has a clear lead in quantum encryption. As it has with other cutting-edge technologies, like artificial intelligence, the Chinese government has made different kinds of quantum research a priority.

"China has a very deliberate strategy to own this technology," said Duncan Earl, a former researcher at Oak Ridge National Laboratory who is president and chief technology officer of Qubitekk, a company that is exploring quantum encryption. "If we think we can wait five or 10 years before jumping on this technology, it is going to be too late."

"Measure" an operator

$A^2 = 1$, A hermitian

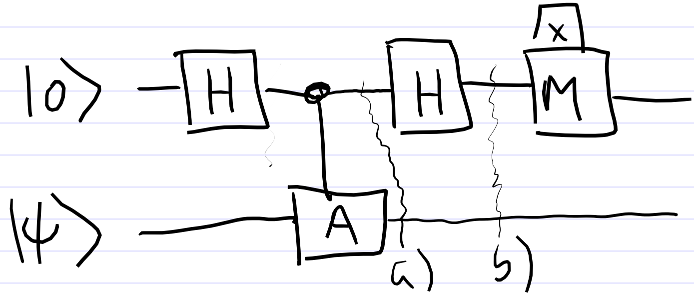
$\Rightarrow$ eigenvalues $= \pm 1$

$$A = \begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & -1 & & \\ & & & -1 & \\ & & & & \ddots \end{pmatrix} \qquad P_0^A = \frac{1+A}{2} = \begin{pmatrix} 1 & & & & \\ & 1 & & & \\ & & 0 & & \\ & & & 0 & \\ & & & & \ddots \end{pmatrix}$$

$$P_1^A = \frac{1-A}{2} = \begin{pmatrix} 0 & & & & \\ & 0 & & & \\ & & 1 & & \\ & & & 1 & \\ & & & & \ddots \end{pmatrix}$$

Projectors onto ± 1 eigenspaces.

eigenvalue of P_x^A is $(-1)^x$



$$\frac{P_x^A|\psi\rangle}{\sqrt{\langle\psi|P_x^A|\psi\rangle}}$$

a) $C^A \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|\psi\rangle + |1\rangle A|\psi\rangle\right)$

b) $\frac{1}{2}\left((|0\rangle+|1\rangle)|\psi\rangle + (|0\rangle-|1\rangle)A|\psi\rangle\right)$

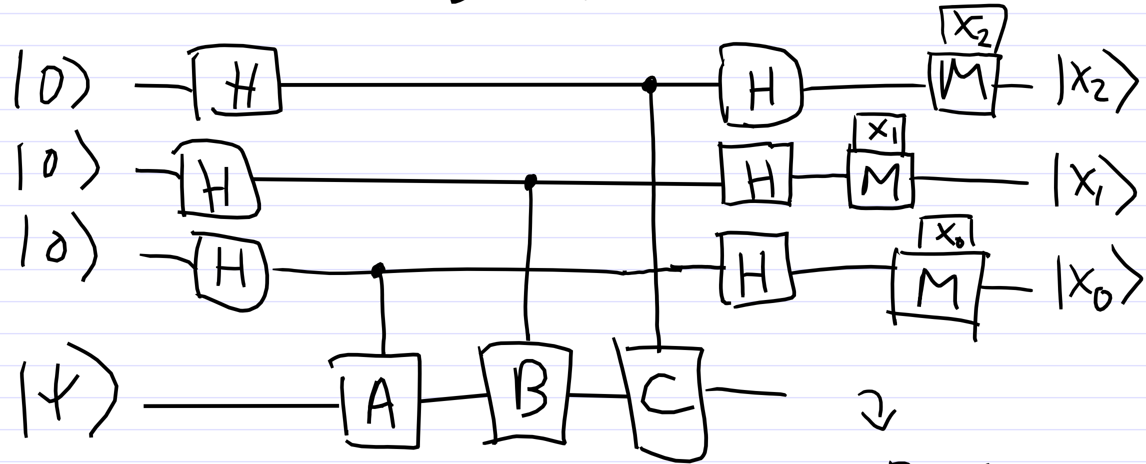
$= \frac{1}{2}|0\rangle(1+A)|\psi\rangle + \frac{1}{2}|1\rangle(1-A)|\psi\rangle$

$= |0\rangle P_0^A|\psi\rangle + |1\rangle P_1^A|\psi\rangle$

Note: if $A = Z$ for single qubit, coincides with usual notion of measurement

Multiple operator measurements

$$A^2 = B^2 = C^2 = 1$$



$$\sum_{x_2, x_1, x_0} |x_2\rangle |x_1\rangle |x_0\rangle \, P^{C}_{x_2} P^{B}_{x_1} P^{A}_{x_0} |\psi\rangle$$

⇒ If A, B, C are mutually commuting, then measuring X_0, X_1, X_2 projects onto their joint eigenspaces.

± 1

$$V\left(\frac{1+(-1)^x V}{2}\right) = (-1)^x\left(\frac{1+(-1)^x V}{2}\right)$$

$$P_x^V$$

Specify 5 qubit code

$$M_0 = Z_1 X_2 X_3 Z_4 \qquad \underline{M_i^2 = 1}$$

$$M_1 = Z_2 X_3 X_4 Z_0$$

$$M_2 = Z_3 X_4 X_0 Z_1$$

$$M_3 = Z_4 X_0 X_1 Z_2$$

$$[X_i, Z_j] = 0 \quad i \neq j$$

Commutator

$$[A,B] = AB - BA$$

$$[M_i, M_j] = 0$$

$$M_4 = Z_0 X_1 X_2 Z_3 \ ?$$

not independent $= M_0 M_1 M_2 M_3$

Code words

$$|\bar{0}\rangle = \frac{1}{4}(1+M_0)(1+M_1)(1+M_2)(1+M_3)|00000\rangle$$

$$|\bar{1}\rangle = \frac{1}{4}(1+M_0)(1+M_1)(1+M_2)(1+M_3)|11111\rangle$$

Normalized? $\quad (1+M_i)^2 = 2(1+M_i)$

$$\langle\bar{0}|\bar{0}\rangle = \frac{1}{16} 16 \langle 0^5 | \prod_i (1+M_i) | 0^5\rangle = \underline{1}$$

$$\langle\bar{1}|\bar{1}\rangle = \underline{1} \qquad \bar{X} = X_0 X_1 X_2 X_3 X_4$$

$$\langle\bar{1}|\bar{0}\rangle = \langle\bar{0}|\bar{1}\rangle = 0 \qquad \bar{Z} = Z_0 Z_1 Z_2 Z_3 Z_4$$

$$|\bar{1}\rangle = \bar{X}|\bar{0}\rangle \qquad \bar{Z}|\bar{0}\rangle = |\bar{0}\rangle \qquad [\bar{X}, M_i] = 0$$

$$|\bar{0}\rangle = \bar{X}|\bar{1}\rangle \qquad \bar{Z}|\bar{1}\rangle = -|\bar{1}\rangle \qquad [\bar{Z}, M_i] = 0$$

$M_0 = Z_1 X_2 X_3 Z_4$ $\qquad$ $M_2 = Z_3 X_4 X_0 Z_1$

$M_1 = Z_2 X_3 X_4 Z_0$ $\qquad$ $M_3 = Z_4 X_0 X_1 Z_2$

Now see that the M_i characterize the 16 spaces $\underset{\text{uncorrupted}}{\mathbb{1}}$ $\underbrace{X_i \; Y_i \; Z_i}_{\text{15 corruptions}}$:

	X_0	Y_0	Z_0	X_1	Y_1	Z_1	X_2	Y_2	Z_2	X_3	Y_3	Z_3	X_4	Y_4	Z_4	$\mathbb{1}$
M_0	+	+	+	−	−	+	+	−	−	+	−	−	−	−	+	+
M_1	−	−	+	+	+	+	−	−	+	+	−	−	+	−	−	+
M_2	+	−	−	−	−	+	+	+	+	−	−	+	+	−	−	+
M_3	+	−	−	+	−	−	−	−	+	+	+	+	−	−	+	+

each column is a unique error signature. Just look at whether the given operator commutes or anti-commutes with M_i.

e.g., (start of 1st column)

$$M_0 X_0 |\psi\rangle = X_0 M_0 |\psi\rangle = +X_0|\psi\rangle$$

$$M_1 X_0 |\psi\rangle = -X_0 M_1 |\psi\rangle = -X_0|\psi\rangle$$

Recall $|\bar{0}\rangle = \frac{1}{4}\prod_i (1+M_i)\,|0^5\rangle$

$|\bar{1}\rangle = \frac{1}{4}\prod_i (1+M_i)\,|1^5\rangle$

have $M_0, M_1, M_2, M_3 = +1, +1, +1, +1$

Suppose: measure M_0, M_1, M_2, M_3

as $+1, -1, +1, -1$

How to correct error?

Well $+-+-$ is the X_2 column,

so the state has an X_2 error

$$X_2|\psi\rangle$$

To correct, apply X_2

$$X_2 X_2|\psi\rangle = |\psi\rangle$$