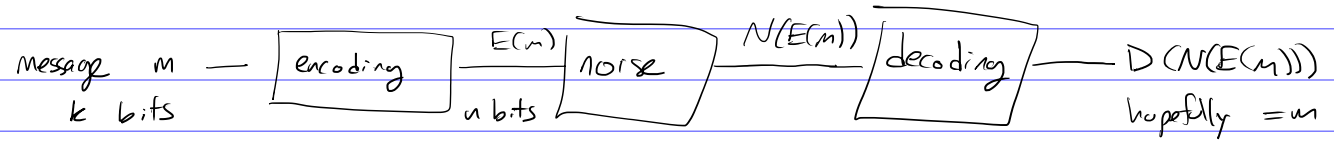
QUANTUM AND CLASSICAL ERROR CORRECTION

Classical error correction



noise can be random (flip each bit with prob p, aka BSC)
or worst-case (flip any subset of np bits)
These are pretty similar with subtle differences we won't explore.

What is possible here?
Let's look at examples
$k=1$ $n=3$ $0 \to 000$ $1 \to 111$
"repetition code"
Decoding is majority vote
Given the BSC the probability of logical error is
$3p^2 + p^3 = O(p^2)$. This is $< p$ if p is small.
$0 \to 0^{2l+1}$ $1 \to 1^{2l+1}$ $\Pr[j \text{ errors}] = \binom{2l+1}{j} p^j (1-p)^{2l+1-j}$

A key idea is to encode $k>1$ bits at once.
consider the alternative:

repetition code on more than one bit

Suppose p is constant, say 0.1
and we want to encode k bits
each one is encode into l bits, so $n = k \cdot l$
$x_1 \dots x_k \to x_1^l x_2^l \dots x_k^l$
prob of decoding error for each bit is
$\Pr[\underset{\text{binomial}}{\text{Bin}}_p(l, p) \geq \frac{l}{2}] \approx e^{-cl}$ (distribution)
Probability of any bit being wrong is $\approx k \cdot e^{-cl}$
For this to be $\ll 1$ we need $l \sim \log k$
So $n \sim k \log k$

General codes

$C \subseteq \{0,1\}^n$ is an $[n,k,d]$ code if

$|C| = 2^k$ (so it encodes k logical bits)

and $\min_{x,y \in C, x \neq y} \text{dist}(x,y) = d$

e.g. repetition code $C = \{0^n, 1^n\}$ $k=1$ $d=n$

codes with distance d can correct $d-1$ erasures or $\lfloor \frac{d-1}{2} \rfloor$ bit flips

"good codes" have $k/n, d/n > 0$ as $n \to \infty$

(Technically these are families of codes.)

Skip

we won't explore this in detail but here is a simple $[7,4,3]$ code that can correct one error

$(x_3, x_5, x_6, x_7) \to (x_3+x_5+x_7,\ x_3+x_6+x_7,\ x_3,\ x_5+x_6+x_7,\ x_5,\ x_6,\ x_7)$

$0\,1\,1 \quad 1\,0\,1 \quad 1\,1\,0 \quad 1\,1\,1$ — 1 2 3 4 5 6 7

Flipping one data bit means 2-3 parity bits will mismatch.

Flipping one parity bit also creates two discrepancies

rearranging

$$G = \begin{pmatrix} 1&0&0&0&0&1&1 \\ 0&1&0&0&1&0&1 \\ 0&0&1&0&1&1&0 \\ 0&0&0&1&1&1&1 \end{pmatrix}^T = \begin{pmatrix} I_4 & S \end{pmatrix}^T \qquad S = \begin{pmatrix} 0&1&1 \\ 1&0&1 \\ 1&1&0 \\ 1&1&1 \end{pmatrix}$$

message $m \to mG \in \mathbb{F}_2^7$

This is an example of a linear code

C is a k-dim subspace of $\mathbb{F}_2^n$

Random linear codes are good codes

choose $G \in \mathbb{F}_2^{n \times k}$ uniformly at random

$$d = \min_{x \neq y,\ x,y \in C} |x-y| = \min_{a,b \in \mathbb{F}_2^k,\ a \neq b} |G(a-b)| = \min_{a \in \mathbb{F}_2^k,\ a \neq 0} |Ga|$$

If $a \neq 0$, Ga is uniform in $\mathbb{F}_2^n$

$$\Pr_G[|Ga| \leq d] = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{d} \approx 2^{n H_2(d/n) - n}$$

$$H_2(p) = -p \log p - (1-p)\log(1-p)$$

$$\Pr_G[\exists a \ |Ga| \leq d] \leq \exp\left(k + n H_2(d/n) - n\right)$$

< 1 if $\frac{k}{n} < 1 - H_2(d/n)$ — Gilbert–Varshamov bound

Decoding?

$C = \operatorname{Im} G = \ker H$

H = parity check matrix e.g. $\begin{pmatrix} 1 & 1 \end{pmatrix}^T$ for the parity code

or $\begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}^T = H$ for the Hamming code

It satisfies $HG = 0$

Given a message m the encoding is Gm
After noise we get $Gm + e$
where e is the error pattern

To diagnose the error we check parities by multiplying by H
$\Rightarrow H(Gm + e) = \underbrace{HGm}_{=0} + He = He$

He is the syndrome

Maximum likelihood decoding means finding
$\arg\min \operatorname{wt}(\hat{e})$ s.t. $\underbrace{H\hat{e}}_{\text{find this}} = \underbrace{He}_{\text{we observe this}}$

This is NP-complete but can be done efficiently for the right choice of code.

Quantum codes

$|\psi\rangle \to |\psi\rangle|\psi\rangle|\psi\rangle$ is no good

We need encoding to be an isometry

meaning $E^\dagger E = I$

e.g. $E|0\rangle = |000\rangle$ $\quad E|1\rangle = |111\rangle$

$E(\alpha|0\rangle + \beta|1\rangle) = \alpha|000\rangle + \beta|111\rangle$

Worries about quantum codes

- no-cloning
- measurement destructive
- continuous errors

can correct one X error

say one of $\{I, X_1, X_2, X_3\}$ occurs

subspaces spanned by $|000\rangle, |111\rangle$

$|100\rangle, |011\rangle$

$|010\rangle, |101\rangle$

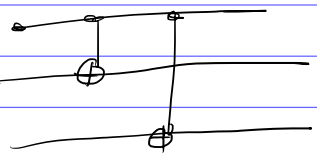
$|001\rangle, |110\rangle$

encoding

$\alpha|0\rangle + \beta|1\rangle$

$|0\rangle$

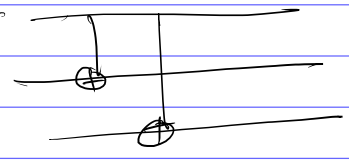
$|0\rangle$



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

decoding

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

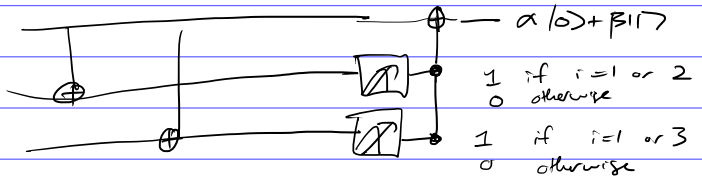


$\alpha|0\rangle + \beta|1\rangle$

$|0\rangle$

$|0\rangle$

$X_i(\alpha|000\rangle + \beta|111\rangle) = X_i E|\psi\rangle$

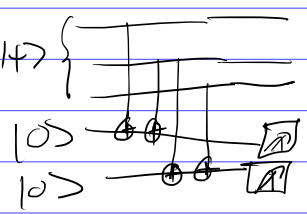


good: decodes, corrects 0 or 1 errors, corrects superpositions like $e^{i\theta X_i}$

corrects $(e^{i\delta X})^{\otimes 3}$ to 1st order in δ

bad: outputs unprotected qubit (this may or may not be desirable)

$X_1^{e_1} X_2^{e_2} X_3^{e_3} E|\psi\rangle$



$X_1^{e_1} X_2^{e_2} X_3^{e_3} E|\psi\rangle$

can diagnose error if $\|e\|_1 = \sum_i e_i = 0$ or 1

What about Z errors?

$E|0\rangle = |+++\rangle$ $\quad E|1\rangle = |---\rangle$

$Z_1 \to |-++\rangle$ or $|+--\rangle$ etc...

4 errors? hmm...

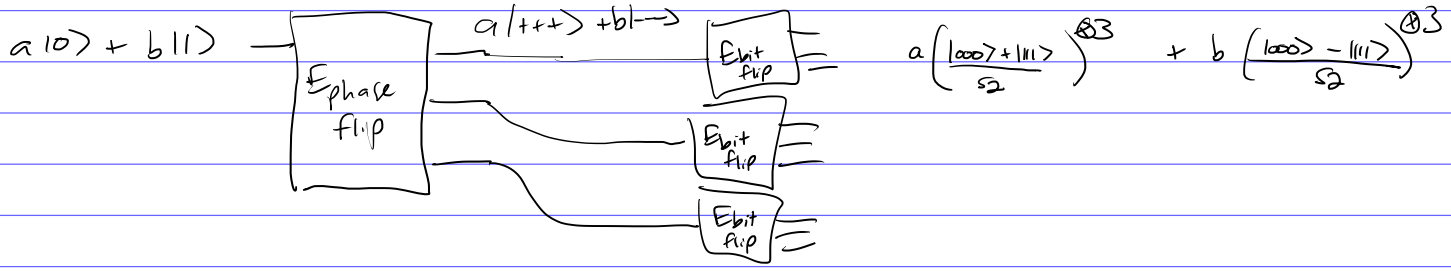
Use the 3-qubit phase-flip code

Note that the 3-qubit bit flip code makes Z errors worse since Z_1, Z_2 or Z_3 all cause logical Z errors.
However the protection against X errors is greater.
Suppose the Z error rate is $p_z \ll 1$, $\Pr[\text{logical } Z \text{ error}] \approx 3p_z = O(p_z)$
and the X error rate is $p_x \ll 1$ $\Pr[\text{logical } X \text{ error}] \approx 3p_x^2 = O(p_x^2)$
This means the code can be net beneficial despite magnifying Z errors.

Challenges		Solutions
No-cloning	→	isometric encoding
Measurement destructive	→	learn about errors, not logical qubits
Continuous errors	→	collapsed by syndrome measurement

We've addressed everything except for correcting X and Z errors at the same time

For this we introduce a concatenated code, namely
The 9-qubit Shor code



To decode we first correct X errors on each block,
then Z errors on the outer code.
This can correct any single-qubit error
$\{I, X_1, X_2, \ldots, X_9, Y_1, \ldots, Y_9, Z_1, \ldots, Z_9\}$

QECC conditions

a code has a set of correctable errors

e.g. I, X_1, X_2, X_3

or $I, X_1, \dots, X_9, Y_1, \dots, Y_9, Z_1, \dots Z_9$

This is a linear subspace and Kraus ops within this space are corrected

e.g. $\mathcal{E}(\rho) = |+X+|\,\rho\,|+X+| + |-X-|\,\rho\,|-X-|$

$= \frac{\rho + X\rho X}{2}$

$|\psi\rangle \to |\psi\rangle_Q \otimes |0\rangle_E + X|\psi\rangle_Q \otimes |1\rangle_E$ / $\sqrt{2}$

$\to \frac{|\psi\rangle_Q \otimes |0\rangle_S \otimes |0\rangle_E + X|\psi\rangle_Q \otimes |1\rangle_S \otimes |1\rangle_E}{\sqrt{2}}$

$\to |\psi\rangle_Q \otimes \left(\frac{|0\rangle_S \otimes |0\rangle_E + |1\rangle_S \otimes |1\rangle_E}{\sqrt{2}} \right)$

e.g. ampl damping

$\begin{pmatrix} 1 & \\ & \sqrt{1-\gamma} \end{pmatrix} \in \text{span}\{I, Z\}$ $\quad \begin{pmatrix} 0 & 0 \\ \sqrt{\gamma} & 0 \end{pmatrix} \in \text{span}\{X, Y\}$

$C = \text{span}\{|000\rangle, |111\rangle\}$

$X_1 C = \text{span}\{|100\rangle, |011\rangle\}$

$X_2 C = \text{span}\{|010\rangle, |101\rangle\}$

$X_3 C = \text{span}\{|001\rangle, |110\rangle\}$

correctable b/c subspaces are orthogonal

classical codes $\supset$ classical linear codes $\subset$ q stabilizer codes $\supset$ CSS codes $\supset$ topological codes

$$C = \{ x \in \mathbb{F}_2^n : \langle h, x \rangle = 0 \quad \forall h \in \mathrm{Im}\, H \}$$

$$\Updownarrow$$

$$Hx = 0 \iff \langle h_1, x \rangle = \cdots = \langle h_m, x \rangle = 0$$

where $\mathrm{span}\{h_1, \ldots, h_m\} = \mathrm{Im}\, H$

towards quantum

classical check $h \in \mathbb{F}_2^n$

$\Rightarrow$ quantum check $Z^h := Z_1^{h_1} Z_2^{h_2} \cdots Z_n^{h_n}$

$$Z^h |z\rangle = (-1)^{h \cdot z} |z\rangle$$

checks $h^{(1)}, \ldots, h^{(m)} \Rightarrow S = \langle Z^{h^{(1)}}, \ldots, Z^{h^{(m)}} \rangle$

$$C = \{ |\psi\rangle : g|\psi\rangle = |\psi\rangle \quad \forall g \in S \}$$

errors are bit flips $X^e = X_1^{e_1} \cdots X_n^{e_n}$

X^e detected by Z^h if $Z^h X^e |\psi\rangle = -X^e |\psi\rangle$ $\forall |\psi\rangle \in C$

$XZ = -ZX$ $\quad Z^h X^e |\psi\rangle = (-1)^{h \cdot e} X^e Z^h |\psi\rangle = (-1)^{he} X^e |\psi\rangle$

undetected set = $\ker H$ = code space AND logical operators

now quantum

$P_n = \langle X_1, Z_1, \ldots, X_n, Z_n \rangle$ n-qubit Paulis

$S \subset P_n$ is a stabilizer group if S is abelian and $-I \notin S$

$$C(S) = \{ |\psi\rangle : g|\psi\rangle = |\psi\rangle \quad \forall g \in S \}$$

$N(S) = \{ U \in P_n : UgU^\dagger \in S \ \forall g \in S \}$

$Z(S) = \{ U : UgU^\dagger = g \ \forall g \in S \}$ same as $[U, g] = 0$

S = stabilizers = check operators

$N(S)/S$ = logical operators or undetected errors

$Z(S) = N(S)$ $\quad nsn^\dagger = \pm s \in S$ can't be $-S$