# Introduction to Quantum Error Correction

Nielsen & Chuang

*Quantum Information and Quantum Computation*, CUP 2000, Ch. 10

Gottesman quant-ph/0004072

Steane quant-ph/0304016

Gottesman quant-ph/9903099

# Errors in QIP

- unitary $\alpha|0\rangle + \beta|1\rangle \xrightarrow{U} \alpha|0\rangle + \beta e^{i(\phi+\delta)}|1\rangle$
- non-unitary $\alpha|0\rangle + \beta|1\rangle \xrightarrow{M} p_\alpha|0\rangle$
- general: pure $\rightarrow$ mixed states

$$|\psi\rangle \rightarrow \rho_f \qquad tr\rho_f^{\ 2} < 1$$

$$\rho = |\psi\rangle\langle\psi| \rightarrow \rho_f = \sum_k E_k \rho E_k^\dagger = \sum_k E_k |\psi\rangle\underbrace{\langle\psi|E_k^\dagger}_{|\psi_k\rangle}$$

from $\rho_f = tr_{env}\left[U\rho \otimes \rho_{env} U^\dagger\right]$

$$= \sum_k \langle e_k|U\rho \otimes |e_0\rangle\langle e_0|U^\dagger|e_k\rangle$$

$$= \sum_k E_k \rho E_k^\dagger \quad E_k = \langle e_k|U|e_0\rangle, U(\text{sys+env})$$

trace preserving: $\sum_{\mathrm{k}} E_k E_k^\dagger = 1$

$\equiv$ take ρ and randomly replace by $E_k \rho E_k^\dagger = |\psi_k\rangle\langle\psi_k|$

with probability $p_k = tr\left(E_k \rho E_k^\dagger\right)$

# Quantum noise:

## channel representation

$$\rho \to \sum_k E_k \rho E_k^\dagger$$

Bit flip channel

$$E_0 = \sqrt{p}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, E_1 = \sqrt{1-p}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

Phase flip channel

$$E_0 = \sqrt{p}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, E_1 = \sqrt{1-p}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Bit-phase flip channel

$$E_0 = \sqrt{p}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, E_1 = \sqrt{1-p}Y = \sqrt{1-p}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

Amplitude damping channel

$$E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma^2} \end{pmatrix}, E_1 = \begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix}$$

Depolarizing channel

$$\varepsilon(\rho) = (1-p)\rho + \frac{p}{3}(X\rho X + Y\rho Y + Z\rho Z)$$

Geometrical interpretation: Bloch sphere in r-space (NC p. 376)

$$\rho = \frac{I + \bar{r}\cdot\bar{\sigma}}{2}, \bar{\sigma} = \{\sigma_x, \sigma_y, \sigma_z\}, \bar{r} = \{r_x, r_y, r_z\}$$

# Discrete errors as Pauli matrices

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

I|a>=|a>
X|a>=|a⊕1>
Y|a>=i$(-1)^a$|a ⊕1>
Z|a>=$(-1)^a$|a>

- N-qubit Pauli matrices

and ±1, ±i ≡ Pauli group, $P_n$: $4^{n+1}$ elements
(4n tensor products, overall phase ±1, ±i)

- notation: X⊗Y⊗I≡XYI
- eigenvalues +1, -1
- all pairs either commute or anticommute
  X, Y, Z, anticommute {X,Z}=0
  X, I etc commute [X,I]=0

$P_2$ spans 2x2 matrices
$P_n$ spans $2^n$x$2^n$ matrices
e.g. general phase error

$$R_{\theta/2} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} = e^{i\theta/2} \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}$$

$$= \cos(\theta/2) I - i \sin(\theta/2) Z$$

# Repetition codes

classical $0 \rightarrow 000$
$1 \rightarrow 111$

error, e.g. 010, corrected to majority value $\rightarrow$ 000
note: learned value of bits in doing so

prob. for bit error $p < 1$:

multi-bit error prob. $= 3p^2(1-p)+p^3=3p^2-2p^3$
$< p$ when $p < 0.5$

$0 \rightarrow 00000\ldots$
$1 \rightarrow 11111\ldots$

n bits, majority $n/2+1$
$\Rightarrow$ error prob. $\cong p^{n/2+1} + \ldots$
$\Rightarrow$ error prob. $\downarrow$ as $n \uparrow$ ($p < 0.5$)

quantum? $|\psi\rangle \xrightarrow{?} |\psi\rangle|\psi\rangle|\psi\rangle$

No cloning theorem!

suppose $|\psi\rangle \rightarrow |\psi\rangle|\psi\rangle$ and $|\phi\rangle \rightarrow |\phi\rangle|\phi\rangle$

then $\left(|\psi\rangle + |\phi\rangle\right) \rightarrow \left(|\psi\rangle + |\phi\rangle\right)\left(|\psi\rangle + |\phi\rangle\right)$

$= |\psi\psi\rangle + |\phi\phi\rangle + |\phi\psi\rangle + |\psi\phi\rangle$

but $|\psi\rangle + |\phi\rangle \rightarrow |\psi\psi\rangle + |\phi\phi\rangle$ by linearity

cannot copy <u>unknown</u> quantum states

# Encode/Error/Recovery

- quantum information is encoded into $\rho_C$
- an error occurs

$$\varepsilon(\rho_C) = \sum_k E_k \rho_C E_k^\dagger$$

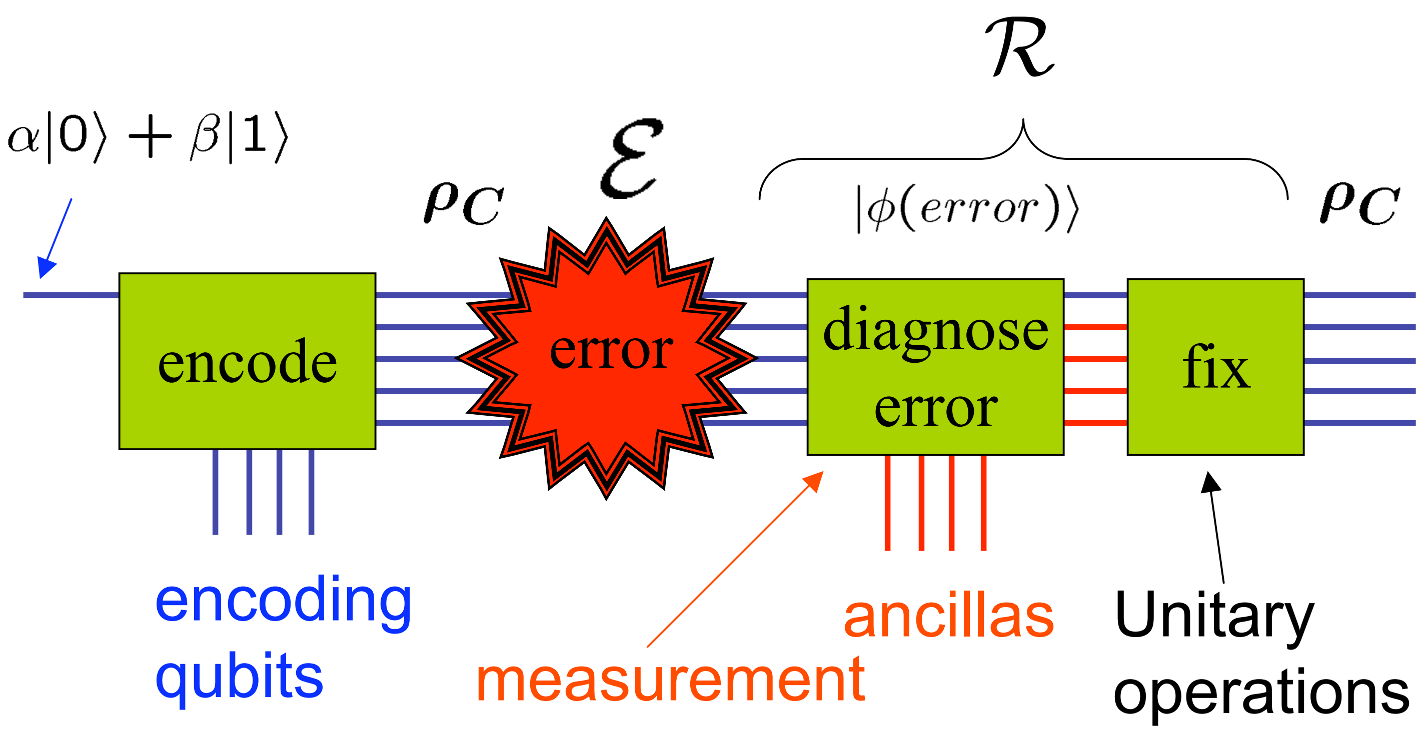
- recovery procedure undertaken

$$\mathcal{R}\left[\varepsilon(\rho_C)\right] = \sum_l R_l \sum_k E_k \rho_C E_k^\dagger R_l^\dagger$$

- regain the encoded state $\rho_C$

$$\mathcal{R}\left[\varepsilon(\rho_C)\right] = \rho_C$$

# Encoding and Recovery




error and recovery are superoperators

$$\rho = \mathbb{S}\left(|\psi\rangle\right) = \sum_k A_k \rho A_k^\dagger$$

Recovery operator $\mathcal{R}$ restores state to the code after error from environment

- encode into a subspace
- no meaurement of state, only of error
- achieve by adding ancilla qubits
- measure ancillas $\rightarrow$ syndrome of error
- perform unitaries conditional on syndrome to correct erroneous qubits

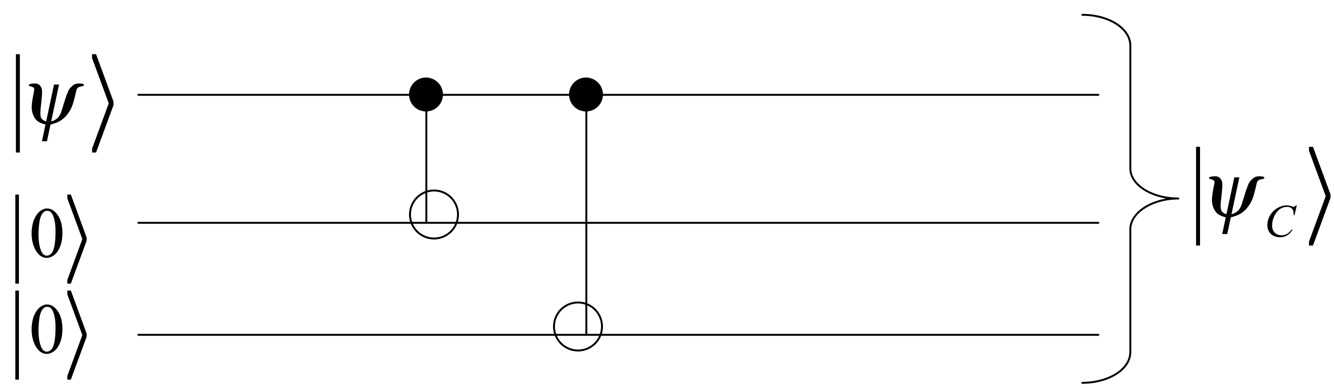
# Encoding

e.g., 3-qubit bit flip code

$|0_L\rangle = |000\rangle$

$|1_L\rangle = |111\rangle$

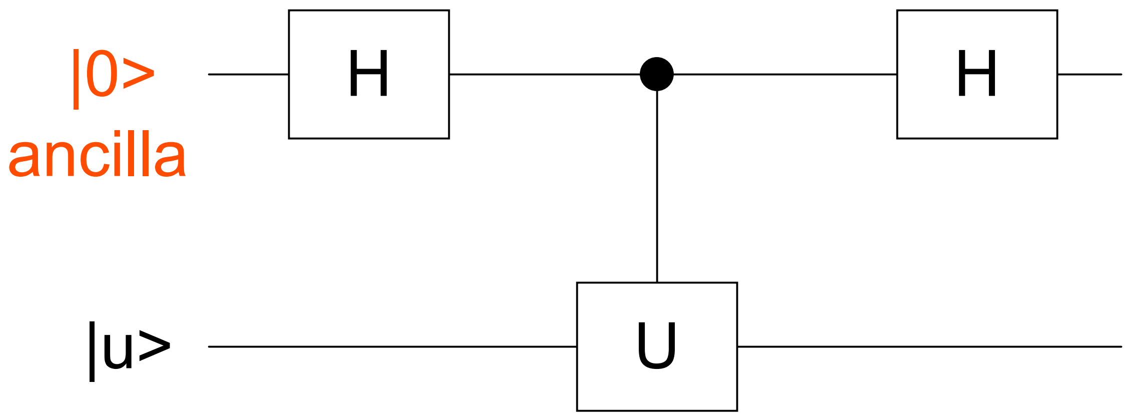
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \rightarrow |\psi_C\rangle = \alpha|0_L\rangle + \beta|1_L\rangle$$




$$(\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle \rightarrow \alpha|00\rangle + \beta|11\rangle$$

$$(\alpha|00\rangle + \beta|11\rangle) \otimes |0\rangle \rightarrow \alpha|000\rangle + \beta|111\rangle \equiv \alpha|0_L\rangle + \beta|1_L\rangle$$

# Measurement (Pauli ops.)




$e_u$=eigenvalue of U

$$|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}\{|0\rangle+|1\rangle\}$$

$$\frac{1}{\sqrt{2}}\{|0\rangle+|1\rangle\}|u\rangle \xrightarrow{c-U} \frac{1}{\sqrt{2}}\{|0\rangle|u\rangle+|1\rangle e_u|u\rangle\}$$

$$= \frac{1}{\sqrt{2}}\{|0\rangle+e_u|1\rangle\}|u\rangle$$

$$\xrightarrow{H} \frac{1}{\sqrt{2}}\left\{\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)+\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)e_u\right\}|u\rangle$$

$$=\frac{1}{2}\{|0\rangle+|1\rangle+|0\rangle e_u-|1\rangle e_u\}|u\rangle$$

Measure qubit 1 (ancilla):

result |0> with prob. $\left[\frac{1}{2}(1+e_u)\right]^2$

syndromes

result |1> with prob. $\left[\frac{1}{2}(1-e_u)\right]^2$

unit eigenvalues of U ($\in P_n$)

$e_u=-1$: result 1 with prob. 1; result 0 with prob. 0

$e_u=+1$: result 1 with prob. 0; result 0 with prob. 1

# Continuous Errors

$$R_{\theta/2} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} = e^{i\theta/2} \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}$$

$$= \cos(\theta/2) I - i \sin(\theta/2) Z$$

add ancilla(s), transfer error info to ancilla (c-U)

$$Z\left(\alpha|0_L\rangle + \beta|1_L\rangle\right) \otimes |0_{anc}\rangle \rightarrow Z\left(\alpha|0_L\rangle + \beta|1_L\rangle\right) \otimes |Z_{anc}\rangle$$

$$I\left(\alpha|0_L\rangle + \beta|1_L\rangle\right) \otimes |0_{anc}\rangle \rightarrow I\left(\alpha|0_L\rangle + \beta|1_L\rangle\right) \otimes |no\, error_{anc}\rangle$$

ancilla → superposition

$$\cos\left(\frac{\theta}{2}\right) I\left(\alpha|0_L\rangle + \beta|1_L\rangle\right) \otimes |no\, error_{anc}\rangle$$

$$- i \sin\left(\frac{\theta}{2}\right) Z\left(\alpha|0_L\rangle + \beta|1_L\rangle\right) \otimes |Z_{anc}\rangle$$

measure ancilla

$$\text{prob. } \sin^2\left(\frac{\theta}{2}\right) \quad Z\left(\alpha|0_L\rangle + \beta|1_L\rangle\right) \otimes |Z_{anc}\rangle$$

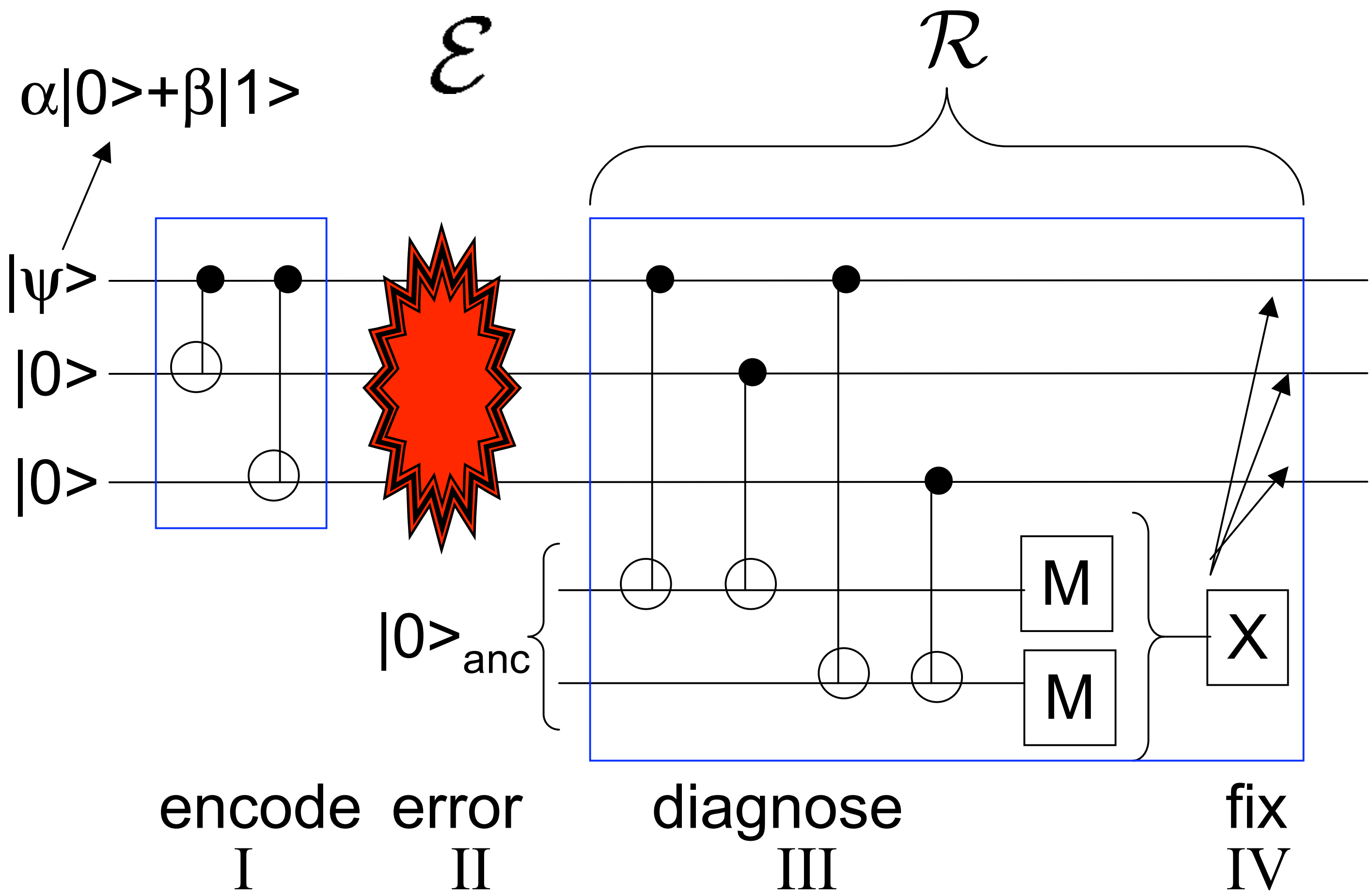
$$\text{prob. } \cos^2\left(\frac{\theta}{2}\right) \quad I\left(\alpha|0_L\rangle + \beta|1_L\rangle\right) \otimes |no\, error_{anc}\rangle$$

invert either one → restore initial state

# 3-qubit Bit Flip Code

$|0_L\rangle = |000\rangle$
$|1_L\rangle = |111\rangle$

Error X with prob. p




I: $(\alpha|0\rangle+\beta|1\rangle)\otimes|0\rangle \otimes|0\rangle \rightarrow \alpha|000\rangle+\beta|111\rangle$

II: 8 possibilities from errors XII, IXI, IIX, XXI, XIX, IXX, XXX, III

| state after error | Prob. of getting state |
|---|---|
| $\alpha\|000>+\beta\|111>$ | $(1-p)^3$ |
| $\alpha\|100>+\beta\|011>$ | $p(1-p)^2$ |
| $\alpha\|010>+\beta\|101>$ | $p(1-p)^2$ |
| $\alpha\|001>+\beta\|110>$ | $p(1-p)^2$ |
| $\alpha\|110>+\beta\|001>$ | $p^2(1-p)$ |
| $\alpha\|101>+\beta\|010>$ | $p^2(1-p)$ |
| $\alpha\|011>+\beta\|100>$ | $p^2(1-p)$ |
| $\alpha\|111>+\beta\|000>$ | $p^3$ |

1 or no error

III: a) perform CNOT between qubits 1 & 2 with ancilla 1
b) perform CNOT between qubits 1 & 3 with ancilla 2

$\rightarrow$

| | |
|---|---|
| $\alpha\|000>+\beta\|111>\|00>$ | $(1-p)^3$ |
| $\alpha\|100>+\beta\|011>\|11>$ | $p(1-p)^2$ |
| $\alpha\|010>+\beta\|101>\|10>$ | $p(1-p)^2$ |
| $\alpha\|001>+\beta\|110>\|01>$ | $p(1-p)^2$ |
| $\alpha\|110>+\beta\|001>\|01>$ | $p^2(1-p)$ |
| $\alpha\|101>+\beta\|010>\|10>$ | $p^2(1-p)$ |
| $\alpha\|011>+\beta\|100>\|11>$ | $p^2(1-p)$ |
| $\alpha\|111>+\beta\|000>\|00>$ | $p^3$ |

syndrome

syndrome redundant for 1 and 2 (0 and 3) errors, but unequal probabilities

III. c) M = measure ancillas:
assume only 1 (or 0) error $\Rightarrow$ syndrome uniquely identifies error

failure rate of code = rate of $\geq$ 2 errors

$$= 3p^2(1-p)+p^3$$
$$= 3p^2-2p^3$$
$$< p \text{ for } p < 0.5$$

IV. fix by applying unitary conditional on M

| syndrome: | |
|---|---|
| 00 | do nothing |
| 01 | apply $\sigma_x$ to 3rd qubit |
| 10 | apply $\sigma_x$ to 2nd qubit |
| 11 | apply $\sigma_x$ to 1st qubit |

$\alpha|000\rangle+\beta|111\rangle|00\rangle$
$\alpha|100\rangle+\beta|011\rangle|11\rangle$
$\alpha|010\rangle+\beta|101\rangle|10\rangle$
$\alpha|001\rangle+\beta|110\rangle|01\rangle$

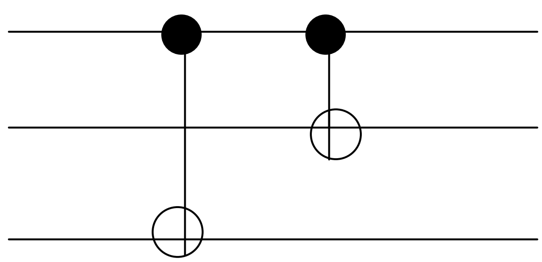
} recover encoded state $\alpha|000\rangle+\beta|111\rangle$

# Decoding

e.g. from syndrome 10

after IV. have $\alpha|000\rangle+\beta|111\rangle$ with $p(1-p)^2$

extract original qubit $\alpha|0\rangle+\beta|1\rangle$ with circuit:



i) ii)

i) $\alpha|000\rangle+\beta|111\rangle \rightarrow \alpha|0\rangle|00\rangle+\beta|1\rangle|10\rangle$

ii) $\alpha|0\rangle|00\rangle+\beta|1\rangle|10\rangle \rightarrow \alpha|0\rangle|00\rangle+\beta|1\rangle|00\rangle$

$= (\alpha|0\rangle+\beta|1\rangle)|00\rangle$

$\Rightarrow$ get correct qubit state with prob. > 1-p

prob. of failure = $3p^2-2p^3 < p$ for $p < 0.5$

success = 100% if no 2 or 3 errors

error prob. reduced from p to $O(p^2)$

# 3-bit Phase Code

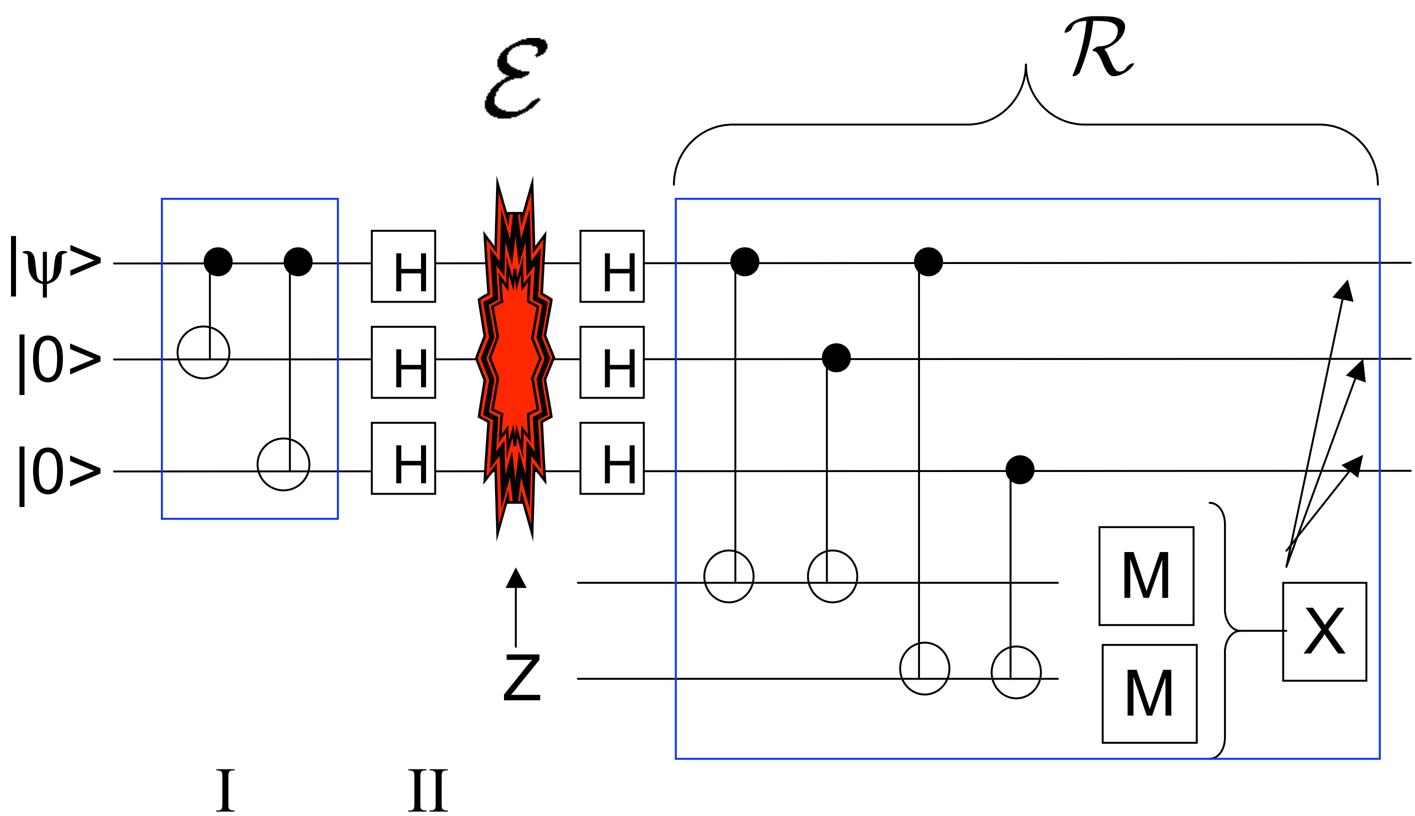
$\sigma_z(\alpha|0>+\beta|1>) = \alpha|0>-\beta|1>$ not classical!

change basis: $|+> =1/\sqrt{2}(|0>+|1>)$
$|-> =1/\sqrt{2}(|0>-|1>)$

$$\begin{pmatrix} + \\ - \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = H \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

then $\sigma_z|+>=|->$
$\sigma_z|->=|+>$
like bit flip!

$H\sigma_z H=\sigma_x$ or $H=|+><0|+|-><1|$



effectively encoded into $|0_L>=|+++>$, $|1_L>=|--->$

$$I, II \rightarrow \alpha|+++> + \beta|--->$$

phase errors ZII, IZI, ZII act as Z on |000>, |111>

e.g., ZII|000> = |000>
ZII|111> = -1|111>

but as X on |+++>, |--->

# Both bit flip and phase errors:

concatenate these two codes:

$|0_L\rangle = (|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$
$|1_L\rangle = (|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)$

inner layer corrects bit flips 000, 111
outer layer corrects phase flips +++, ----

Shor PRA **52**, R2493 (1995)

define Bell basis:

$|000\rangle \pm |111\rangle$
$|001\rangle \pm |110\rangle$
$|010\rangle \pm |101\rangle$
$|100\rangle \pm |011\rangle$

consider decoherence of qubit 1:

$e|0\rangle \rightarrow a_0|0\rangle + a_1|1\rangle$
$e|1\rangle \rightarrow a_2|0\rangle + a_3|1\rangle$

$e, a_0, \ldots a_3$ = states of env

first triple:

$|000\rangle + |111\rangle \rightarrow (a_0|0\rangle + a_1|1\rangle)|00\rangle + (a_2|0\rangle + a_3|1\rangle)|11\rangle$
$= a_0|000\rangle + a_1|100| + a_2|011\rangle + a_3|111\rangle$

put in Bell basis $\rightarrow$

$$=1/2\ (a_0+a_3)\ (|000> + |111>)$$
$$+1/2\ (a_0-a_3)\ (|000> - |111>)$$
$$+1/2\ (a_1+a_2)\ (|100> + |011>)$$
$$+1/2\ (a_1-a_2)\ (|100> - |111>)$$

similarly |000> - |111> goes to

$$=1/2\ (a_0+a_3)\ (|000> - |111>)$$
$$+1/2\ (a_0-a_3)\ (|000> + |111>)$$
$$+1/2\ (a_1+a_2)\ (|100> - |011>)$$
$$+1/2\ (a_1-a_2)\ (|100> + |111>)$$

output 2 (syndrome 2)

assume 1 error only:

compare all 3 triples, see which differs

majority sign indicates $|0_L>$ or $|1_L>$

find which qubit decohered

(measure 9 ancillas $\rightarrow$ which syndrome)

restore qubit state with a unitary operation

e.g. from |000> - |111>)

$1/2\ (a_0+a_3)\ (|000> - |111>) \Rightarrow$ no error

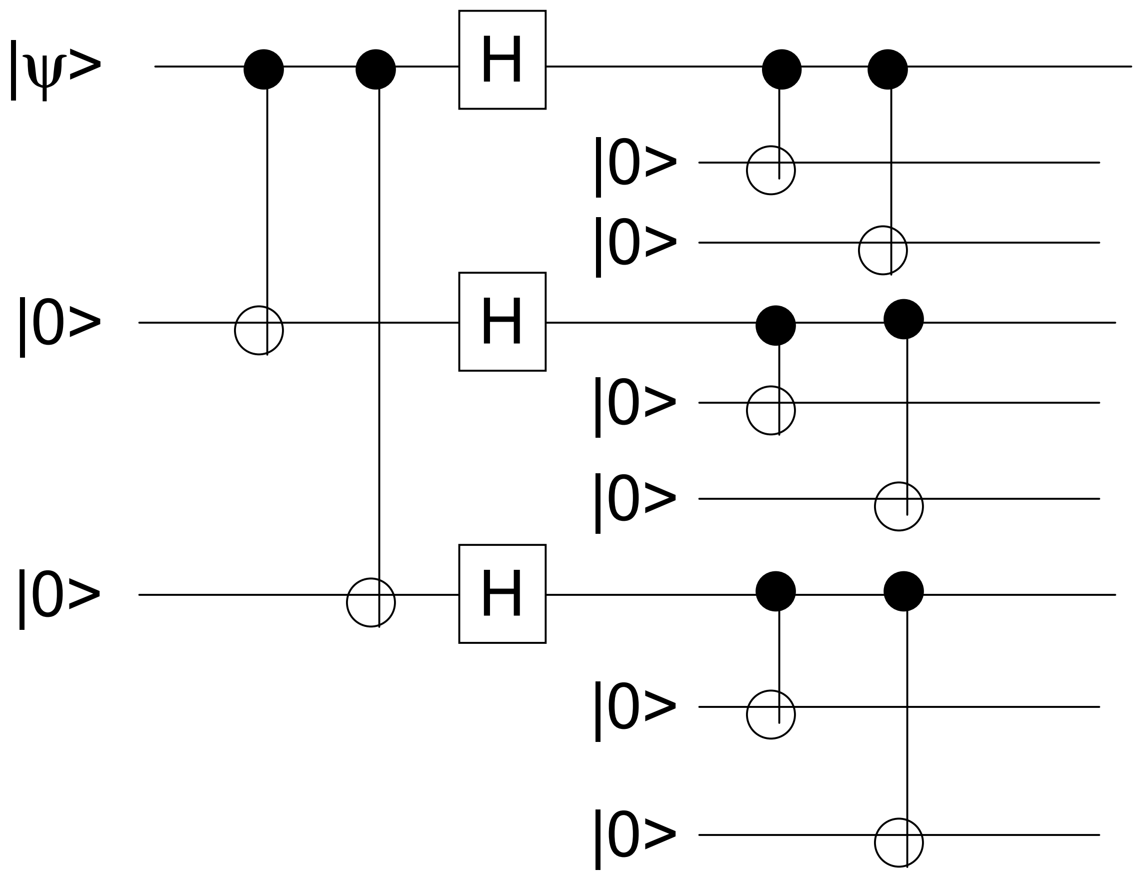
output 2 $1/2\ (a_0-a_3)\ (|000> + |111>) \Rightarrow$ Z error

$1/2\ (a_1+a_2)\ (|100> + |011>) \Rightarrow$ X error

$1/2\ (a_1-a_2)\ (|100> - |011>) \Rightarrow$ ZX=Y error

have diagnosed error on 1st qubit
$\rightarrow$ correct with appropriate unitary

Encoder:




[9,1,3] code: 9 physical qubits
1 logical qubit
(3-1)/2=1 arbitrary error corrected

not most efficient code: [7,1,3] and [5,1,3]
cannot compute easily (logical X, Z OK
logical H, CNOT, T hard)