After correction, general conclusion:

state	probability
$(a\|000\rangle + b\|111\rangle)\|00\rangle$	$(1-p)^3$
$(a\|000\rangle + b\|111\rangle)\|11\rangle$	$p(1-p)^2$
$(a\|000\rangle + b\|111\rangle)\|10\rangle$	$p(1-p)^2$
$(a\|000\rangle + b\|111\rangle)\|01\rangle$	$p(1-p)^2$
$(a\|111\rangle + b\|000\rangle)\|01\rangle$	$p^2(1-p)$
$(a\|111\rangle + b\|000\rangle)\|10\rangle$	$p^2(1-p)$
$(a\|111\rangle + b\|000\rangle)\|11\rangle$	$p^2(1-p)$
$(a\|111\rangle + b\|000\rangle)\|00\rangle$	p^3

Overall probability to fail, i.e. get the wrong final state, is

$$3p^2(1-p)^2 + p^3 = O(p^2)$$

More general error:

$$
\begin{aligned}
R(\theta) &= \begin{pmatrix} \cos(\theta/2) & i\sin(\theta/2) \\ i\sin(\theta/2) & \cos(\theta/2) \end{pmatrix} \\
&= \cos(\theta/2) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + i\sin(\theta/2) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\
&= \cos(\theta/2)\, I \;\; + \;\; i\sin(\theta/2)\, X \\
&= cI + sX \qquad\qquad\qquad \text{where } \; c = \cos(\theta/2), \;\; s = i\sin(\theta/2)
\end{aligned}
$$

$$
\begin{aligned}
R_1R_2R_3 &= (cI + sX)(cI + sX)(cI + sX) \\
&= c^3 III + c^2 s(IIX + IXI + XII) + cs^2(XXI + XIX + IXX) + s^3 XXX
\end{aligned}
$$

$$
\begin{aligned}
\overset{\text{3−Qbit}}{|\psi\rangle} \otimes \overset{\text{ancilla}}{|00\rangle} \quad &\xrightarrow{\text{noise}} \quad (R_1R_2R_3|\psi\rangle) \otimes |00\rangle \\
&= \quad \big(c^3 + c^2 s(1 \text{ flip}) + cs^2(2 \text{ flip}) + s^3(3 \text{ flip})\big)\, |\psi\rangle \otimes |00\rangle \\
&\xrightarrow{\text{parity check}} \quad (c^3 III + s^3 XXX)|\psi\rangle \otimes |00\rangle \\
&\qquad + (c^2 sIIX + cs^2 XXI)|\psi\rangle \otimes |01\rangle \\
&\qquad + (c^2 sIXI + cs^2 XIX)|\psi\rangle \otimes |10\rangle \\
&\qquad + (c^2 sXII + cs^2 IXX)|\psi\rangle \otimes |11\rangle
\end{aligned}
$$

At this stage the state still has all possible errors:

$$(c^3 III + s^3 XXX)|\psi\rangle \otimes |00\rangle + cs(cIIX + sXXI)|\psi\rangle \otimes |01\rangle$$
$$+cs(cIXI + sXIX)|\psi\rangle \otimes |10\rangle + cs(cXII + sIXX)|\psi\rangle \otimes |11\rangle$$

Now measure the ancilla: **projection**

$$\begin{array}{lll} \rightarrow \text{either} & (c^3 III + s^3 XXX)|\psi\rangle \otimes |00\rangle & /\sqrt{c^6+s^6} \\ \text{or} & (cIIX + sXXI)|\psi\rangle \otimes |01\rangle & \text{probability } c^2s^2 \\ \text{or} & (cIXI + sXIX)|\psi\rangle \otimes |10\rangle & \text{probability } c^2s^2 \\ \text{or} & (cXII + sIXX)|\psi\rangle \otimes |11\rangle & \text{probability } c^2s^2 \end{array}$$

Apply corrective X depending on the syndrome:

$$\begin{array}{rll} \rightarrow \text{outcome either} & (c^3 III + s^3 XXX)|\psi\rangle & /\sqrt{c^6+s^6} \\ \text{or} & (cIII + sXXX)|\psi\rangle & (\text{Prob } = 3c^2s^2) \end{array}$$

Error term in the final state: either (s^6), or $(s^2$ with probability $3c^2s^2)$
Hence

$$P(\text{fail overall}) = O(s^4) = O(\sin^4\theta)$$

N.B. notice the *discretization* of errors: a continuous rotation error is projected by the syndrome measurement onto either the identity or a bit flip (Pauli X): a discrete set of errors.

Generalize:

$\{000, 111\} \longrightarrow$ any classical code $\mathcal{C}$
$G_{\mathcal{C}} \rightarrow$ logic gate network to create the quantum states
$H_{\mathcal{C}} \rightarrow$ logic gate network to perform the parity check (syndrome) measurements.

These are "quasi classical" codes.

Phase errors, also known as decoherence (random ϕ):

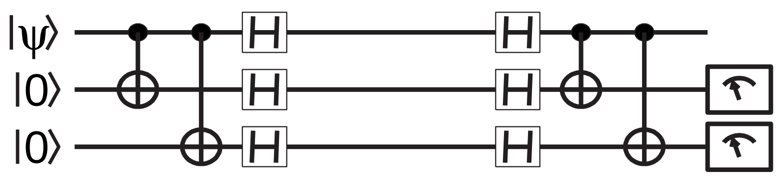
$$\begin{pmatrix} e^{i\phi/2} & 0 \\ 0 & e^{-i\phi/2} \end{pmatrix} = \cos(\phi/2)\, I + i\sin(\phi/2)\, Z \qquad \left[Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right]$$

Notice:

$$HZH = X$$

So perform Hadamards before and after the channel
$\Rightarrow$ convert phase noise to bit-flip noise
$\Rightarrow$ correct as before!

Simplest experiment:

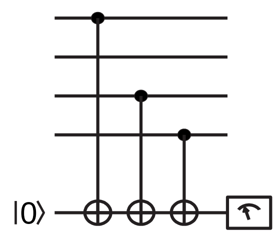


Quantum Error Correction: introducing main ideas

Pauli group

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Parity check



Discretization of errors: a continuous error is projected by a syndrome measurement onto one of a discrete set of errors.

We already noticed

$$
\begin{array}{ccc}
HHH(|000\rangle + |111\rangle) & = & |000\rangle + |011\rangle + |101\rangle + |110\rangle \\
\text{repetition code} & \stackrel{HHH}{\leftrightarrow} & \text{even weight code} \\
\mathcal{C} & \leftrightarrow & \mathcal{C}^{\perp}
\end{array}
$$

. . . more generally: **Dual code theorem**: (Steane 1996)

$$
HH \cdots H \sum_{u \in \mathcal{C}} |u\rangle = \sum_{v \in \mathcal{C}^{\perp}} |v\rangle
$$

This gives us a very useful hint: form states consisting of equal superposition of *all* members of a linear code.

e.g.

$$
\begin{aligned}
|0\rangle_L &= \sum_{u \in \mathcal{C}_0} |u\rangle \\
&= |0000000\rangle + |1010101\rangle + |0110011\rangle + |1101010\rangle + |0001111\rangle + |1011010\rangle + |0111100\rangle + |0010101\rangle
\end{aligned}
$$

However, we want more than one quantum state.

But suppose C_0 is itself just part of a larger code $\mathcal{C}_K$:

$$\mathcal{C}_0 \subset \mathcal{C}_K$$

then we can form

$$
\begin{aligned}
|1\rangle_L &= \sum_{u \in (\mathcal{C}_K \setminus \mathcal{C}_0)} |u\rangle \\
&= |1111111\rangle + |0101010\rangle + |1001100\rangle + |0010101\rangle + |1110000\rangle + |0100101\rangle + |1000011\rangle + |1101010\rangle
\end{aligned}
$$

$$a\,|0\rangle_L + b\,|1\rangle_L =$$

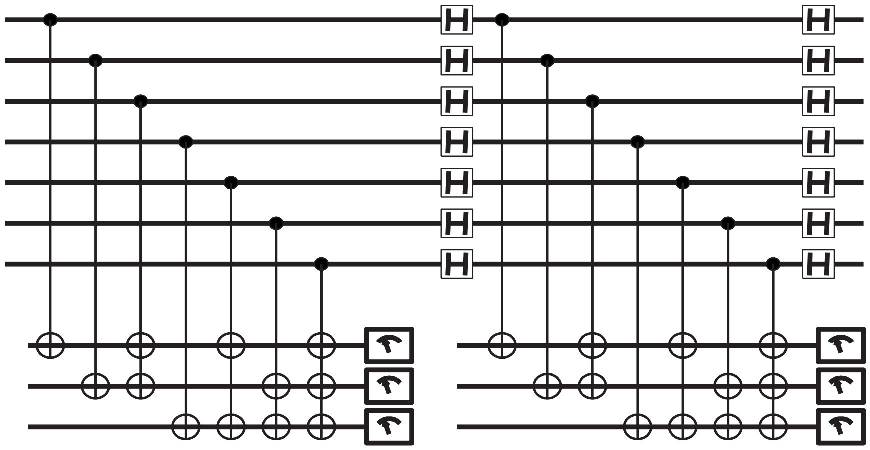
$$a\Big(|0000000\rangle + |1010101\rangle + |0110011\rangle + |1101010\rangle + |0001111\rangle + |1011010\rangle + |0111100\rangle + |0010101\rangle\Big)$$
$$+b\Big(|1111111\rangle + |0101010\rangle + |1001100\rangle + |0010101\rangle + |1110000\rangle + |0100101\rangle + |1000011\rangle + |1101010\rangle\Big)$$

What ‘beast’ have we got here?

1. We can measure all the parity checks of the larger code $\mathcal{C}_K$: both $|0\rangle_L$ and $|1\rangle_L$ are eigenstates of $ZIZIZIZ$, $IZZIIZZ$, $IIIZZZZ$.
$\longrightarrow$ thus deduce bit-flips (up to the correction ability of $\mathcal{C}_K$).

2. What about phase flips (Pauli Z)?
To see their effect, use $Z = HXH$,
$\longrightarrow$ they give ‘bit flips’ in the other basis
but $|0\rangle_L$ transforms into another code in the other basis (namely $\mathcal{C}_0^\perp$)
AND $|1\rangle_L$ transforms into that SAME code $\mathcal{C}_0^\perp$ (with some sign changes)
$\longrightarrow$ we can do FURTHER parity measurements, now in the other basis
(equivalent to measuring the observables $XIXIXIX$, $IXXIIXX$, $IIIXXXX$)
$\longrightarrow$ deduce phase-flip syndrome

Complete parity checking for 7-bit code:



This example has:
$\mathcal{C}_K = [7, 4, 3]$ single-error correcting code,
$|0\rangle_L$ constructed from $\mathcal{C}_0 = [7, 3, 4] = (\mathcal{C}_K$ with a further overall parity check),
and the code $\mathcal{C}_0^{\perp}$ appearing in the second basis is also $\mathcal{C}_K$ (an example of a code that contains its dual)
$\Rightarrow$ single-error correction of BOTH bit flips AND phase flips

We now have 2 "quantum codewords" $|0\rangle_L$ and $|1\rangle_L$. This is a code encoding 1 qubit into 7. It can recover from a bit flip of an arbitrary qubit, and from a phase flip of an arbitrary qubit, *and from both at once.*

General Noise

Any interaction of a qubit with another system can be described by some transformation

$$(a|0\rangle + b|1\rangle)|\phi\rangle_e \to T[(a|0\rangle + b|1\rangle)|\phi\rangle_e]$$

where T may be written

$$T = \left(\begin{array}{c|c} T_1 & T_2 \\ \hline T_3 & T_4 \end{array}\right) = \left(\begin{array}{c|c} T_I & 0 \\ \hline 0 & T_I \end{array}\right) + \left(\begin{array}{c|c} 0 & T_X \\ \hline T_X & 0 \end{array}\right) + \left(\begin{array}{c|c} 0 & -T_Y \\ \hline T_Y & 0 \end{array}\right) + \left(\begin{array}{c|c} T_Z & 0 \\ \hline 0 & -T_Z \end{array}\right)$$

$$= \quad T_I \otimes I \quad + \quad T_X \otimes X \quad + \quad T_Y \otimes Y \quad + \quad T_Z \otimes Z$$

with $T_I = (T_1 + T_4)/2, \qquad T_Z = (T_1 - T_4)/2, \qquad$ etc.

Hence **any** evolution can be written

$$|\psi\rangle|\phi\rangle_e \to |\psi\rangle|\alpha\rangle_e + (X|\psi\rangle)|\beta\rangle_e + (Y|\psi\rangle)|\gamma\rangle_e + (Z|\psi\rangle)|\delta\rangle_e$$

= combination of I, X, $Y = XZ$, and Z errors.
$\Rightarrow$ **we only need to correct Pauli errors**

$\Rightarrow$ our 7-qubit encoding can recover from a *completely arbitrary* corruption of any single qubit, *including relaxation, entanglement with environment, etc.*

This is called a *single-error-correcting* quantum code.

Extension to larger codes

The generalization to correct more errors is immediate:

- start from any self-dual classical code, e.g. [24,12,8] Golay code
- 'puncture' (knock off 1 bit and 1 line from the generator)
  $\rightarrow$ obtain $\mathcal{C}_0 = [23, 11, 8] \subset \mathcal{C}_K = [23, 12, 7] = \mathcal{C}_0^{\perp}$
- Thus encode 1 qubit into 23 qubits with 3-error-correcting code, etc.
- Explicit construction for encoding and correction gate networks from the generator and parity check matrices.

Can we also generalize to "good codes", i.e. *efficient* codes?

Yes!

- seek $\mathcal{C}_0 \subset \mathcal{C}_K$ with larger $\mathcal{C}_K$, so that $\mathcal{C}_0$ is one of many (i.e. 2^K) subsets (cosets)

Hence

Theorem (CSS codes): (Calderbank, Shor, Steane 1996)
A pair of classical codes $\mathcal{C}_1 = [n, k_1, d_1]$, $\mathcal{C}_2 = [n, k_2, d_2]$ with

$$\mathcal{C}_2^{\perp} \subset \mathcal{C}_1$$

can be used to construct a quantum code of size $k_1 - (n - k_2) = k_1 + k_2 - n$ with minimum distance d_1 for X errors, d_2 for Z errors.

e.g. If $\mathcal{C}_1$ contains its dual, then $\mathcal{C}_2 = \mathcal{C}_1$ and we have

$$K = 2k_1 - n$$

$\longrightarrow$ existence of *good quantum codes* (since there exist self-dual classical codes above the Gilbert-Varshamov bound).

$\longrightarrow$ "Shannon theorem" for perfect communication through a noisy quantum channel.

Evolution in the presence of noise.

Hamiltonian for evolution of a system of qubits, interacting with each other and with anything else:

$$H_I = \sum_i E_i \otimes H_i^e$$

Evolution of the reduced density matrix of the qubits:

$$\begin{array}{lrl} & \rho_0 & \rightarrow \; \sum_{ij} a_{ij}\, E_i\, \rho_0 E_j \\ \text{QEC:} & & \rightarrow \; f\rho_0 + \sum_{\text{uncorrectable } E_i, E_j} a_{ij}\, E_i'\, \rho_0\, E_j' \end{array}$$

$$\begin{array}{lrcl} \text{where fidelity} & f & = & 1 - \mathrm{Tr}\left[\sum_{\text{uncorrectable } E_i, E_j} a_{ij}\, E_i'\, \rho_0\, E_j'\right] \\ & & \geq & 1 - \sum_{\text{uncorrectable } E_i, E_j} |a_{ij}| \end{array}$$

a_{ii} = 'the probability that error E_i occurs'
= the probability that the syndrome extraction projects the state onto one which differs from the noise-free state by error operator E_i

We can always write

$$H_I = \sum_{\mathrm{wt}(E)=1} E \otimes H_E^e + \sum_{\mathrm{wt}(E)=2} E \otimes H_E^e + \sum_{\mathrm{wt}(E)=3} E \otimes H_E^e + \dots$$

Independent noise: only weight 1 terms.
More generally: coupling constants usually of order $\epsilon^t/t!$.

Then in the worst case (a_{ij} adding in phase):

$$1 - F \simeq P(t+1) \simeq \left(3^{t+1} \binom{n}{t+1} \epsilon^{t+1}\right)^2$$

or very often:

$$1 - F \simeq P(t+1) \simeq 3^{t+1} \binom{n}{t+1} \epsilon^{2(t+1)}$$

The evolution of a multiply-entangled system coupled to an uncontrolled environment is a non-trivial problem!

QEC will directly reveal the high-order correlations in the evolution of many-body entangled quantum systems. These terms are either small enough to permit quantum computing, or else they will reveal physics which is not currently understood.

Examples:

- 7-bit code: $[n = 7, k = 4, d = 3]$ classical Hamming code
  $\rightarrow [[n = 7, K = 1, d = 3]]$ (1-error-correcting) quantum code
- $[23, 12, 7]$ classical Golay code $\rightarrow [[23, 1, 7]]$ (3-err-corr.) quantum code
- $[127, 85, 13]$ classical BCH code $\rightarrow [[127, 43, 13]]$ (6-err-corr.) quantum BCH code

e.g. Golay code: suppose we have 23 atoms, each decaying by spontaneous emission, with lifetime 1 s.

suppose processor has 'clock rate' 100 kHz (i.e. 2-bit gate takes 10 μs)

$2 \times 88 = 176$ gates to extract parity checks, completed in 8 steps.

hence correct the atoms every ms $\Rightarrow$ error probability for each atom $\simeq 0.001$

$P(\text{uncorrectable error}) \simeq \begin{pmatrix} 23 \\ 4 \end{pmatrix} \times (0.001)^4 \simeq 10^{-8}$

Repeat 10^8 times: **preserve the encoded qubit for 10^8 ms = 1 day!**

Further remarks on error correction

Conditions for a quantum error correcting code:

Code C can correct a set of errors $\mathcal{E}$ if and only if

$$\begin{aligned} \langle u| E_1 E_2 |v\rangle &= 0 \\ \langle u| E_1 E_2 |u\rangle &= \langle v| E_1 E_2 |v\rangle \end{aligned}$$

for all $E_1, E_2 \in \mathcal{E}$ and $|u\rangle, |v\rangle \in \mathcal{C}$, $|u\rangle \neq |v\rangle$.

Quantum Hamming bound

For nondegenerate codes, where $\langle u| E_1 E_2 |u\rangle = 0$:

$$m\left(1 + 3\binom{n}{1} + 9\binom{n}{2} + \cdots + 3^t\binom{n}{t}\right) \leq 2^n$$

e.g. single-error correcting:

$$\begin{aligned}
1 \text{ qubit} &\rightarrow 4 \text{ errors} \Rightarrow \text{no correction} \\
2 \text{ qubit} &\rightarrow 7 \text{ errors} \\
3 \text{ qubit} &\rightarrow 10 \text{ errors} \\
4 \text{ qubit} &\rightarrow 13 \text{ errors} \\
5 \text{ qubit} &\rightarrow 16 \text{ errors} \Rightarrow \text{code may exist}
\end{aligned}$$

5-bit code

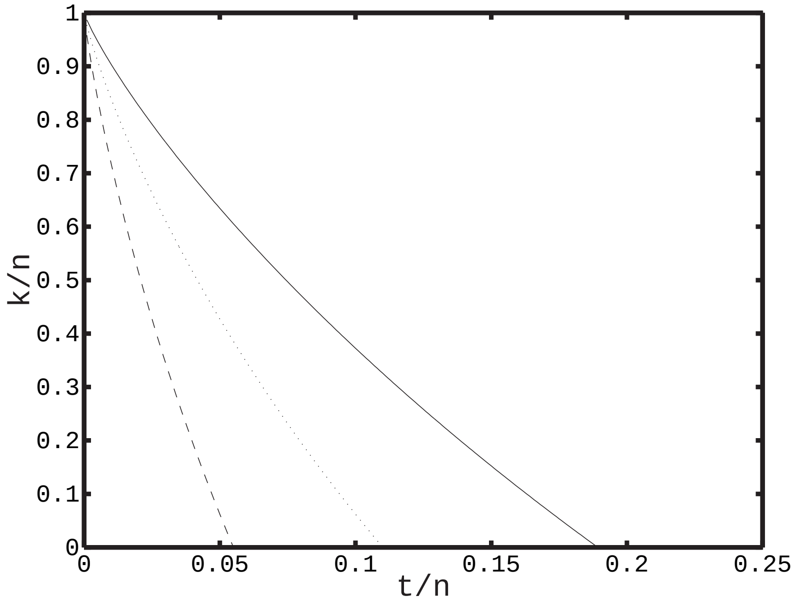
It does exist!

$$H = \left(\begin{array}{c|c} 11000 & 00101 \\ 01100 & 10010 \\ 00110 & 01001 \\ 00011 & 10100 \end{array} \right), \qquad G = \left(\begin{array}{c|c} H_x & H_z \\ 11111 & 00000 \\ 00000 & 11111 \end{array} \right).$$

One possible choice of the two codewords is

$$\begin{aligned} |0\rangle_L &= |00000\rangle + |11000\rangle + |01100\rangle - |10100\rangle \\ &+ |00110\rangle - |11110\rangle - |01010\rangle - |10010\rangle \\ &+ |00011\rangle - |11011\rangle - |01111\rangle - |10111\rangle \\ &- |00101\rangle - |11101\rangle - |01001\rangle + |10001\rangle, \\ |1\rangle_L &= X_{11111} |0\rangle_L . \end{aligned}$$

Hamming and G-V bounds in limit of large codeword length n



Decoherence-free subspace

What if the noise is such that the errors are all in the stabilizer?

Then no correction is needed! The codespace is simply unaffected by the noise.

Example: the energy gap of all the qubits gets shifted by the same amount.

Error:

$$\begin{aligned} e^{i\Delta E Z_1 t/2\hbar} e^{i\Delta E Z_2 t/2\hbar} &= e^{i\Delta E (Z_1+Z_2)t/2\hbar} \\ &= I + i\frac{\Delta E t}{2\hbar}(Z_1+Z_2) - \frac{1}{2}\left(\frac{\Delta E t}{2\hbar}\right)^2 (Z_1+Z_2)^2 + \cdots \end{aligned}$$

Need

$$\begin{aligned} (Z_1+Z_2)\,|\psi\rangle &= 0 \\ \Rightarrow \qquad Z_1\,|\psi\rangle &= -Z_2\,|\psi\rangle \\ \Rightarrow \qquad Z_1 Z_2\,|\psi\rangle &= -\,|\psi\rangle \end{aligned}$$

Therefore use stabilizer $-Z_1 Z_2$,

$$\text{code} \;= |01\rangle\,,\; |10\rangle\,.$$

Both states have the same energy $\Rightarrow$ they both acquire the same extra phase

$\Rightarrow$ it appears as a global phase $\Rightarrow$ no effect.

Noise again

(1.) Unitary errors.

Define the norm of a vector:

$$|| \, |v\rangle \, || \equiv \sqrt{\langle v \mid v\rangle}$$

Let

$$E(U,V) \;\equiv\; \max_{|\psi\rangle} ||(U-V)\,|\psi\rangle\,||$$

This is a measure of how bad the state is if operation V is implemented when U was intended.

It can be shown that

$$E(U_m U_{m-1} \cdots U_1, V_m V_{m-1} \cdots V_m) \leq \sum_{j=1}^{m} E(U_j, V_j)$$

i.e. errors add.