Lecture 1.

Classical coding theory

Summary

Central problem of communication: *Communication in the presence of noise*

$$
\begin{array}{ccccccc}
\text{message} & \text{encode} & & \text{error } e & & \text{decode} & \\
m & \rightarrow & u & \rightarrow & u+e & \rightarrow & m' \\
 & & & & & & \\
0 & \rightarrow & 000 & \rightarrow & 001 & \rightarrow & 0 \\
1 & \rightarrow & 111 & \rightarrow & 110 & \rightarrow & 1
\end{array}
$$

$P(\text{fail}) = P(2 \text{ or } 3 \text{ errors}) = 3p^2(1-p) + p^3$

Code **rate** $= \dfrac{k}{n} = \dfrac{1}{3.}$

In general

$$
\begin{aligned}
P(\text{fail}) &= \binom{n}{t+1} p^{t+1}(1-p)^{n-t-1} + \cdots \\
&\simeq \frac{n!}{(t+1)!(n-t-1)!} p^{t+1}
\end{aligned}
$$

Galois Field GF(2)

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \qquad \begin{array}{c|cc} \times & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$$

bit string = binary **vector**

length = n. dimensions

addition:

$$\begin{array}{cc} & (1011) \\ + & (0110) \\ \hline = & (1101) \end{array}$$

inner product:

$$\begin{aligned} (1011) \cdot (0110) = (1011)\begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} &= 0 + 0 + 1 + 0 \\ &= 1 \end{aligned}$$

$$u \cdot v = uv^T$$

This is also a "parity check"

$$\begin{array}{l} 1\,\underbrace{0\;1}\,1 \\ 0\,\overbrace{1\;1}\,0 \;\; \Rightarrow \;\; \mathit{odd} \end{array}$$

Note

$$\begin{aligned} u \cdot v &= v \cdot u \\ u \cdot (v + w) &= u \cdot v + u \cdot w \end{aligned}$$

A vector can be "orthogonal" to itself: $0110 \cdot 0110 = 0$

Weight = number of non-zero components: $\mathrm{wt}(1011) = 3$

Distance = number of bit-flips to go from u to v.
e.g.

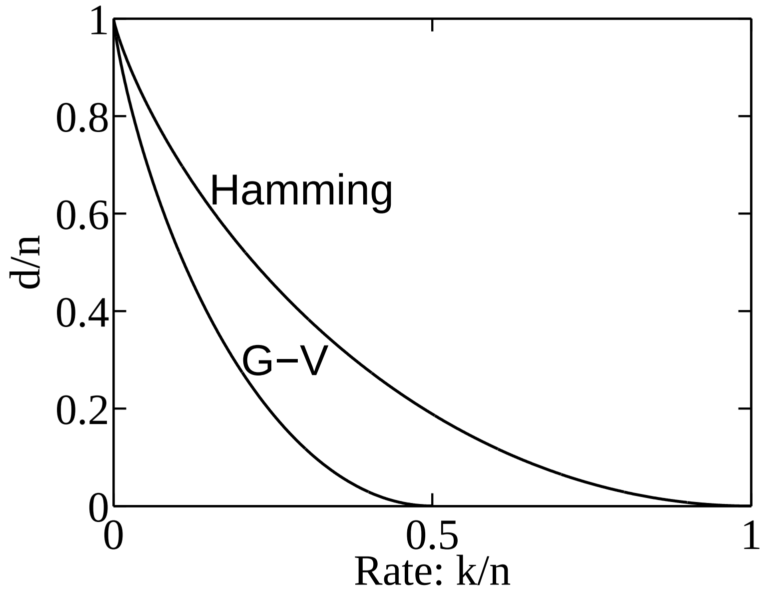
$$\begin{array}{l} 1011 \\ 0110 \\ {*}{*}\ {*} \quad \Rightarrow \quad 3 \end{array}$$

$$d_{u,v} = \mathrm{wt}(u+v)$$

Upper limit on correctable errors t:
If
n = length of codewords
m = number of vectors in the code (thus encode $\log_2 m$ bits)
Then

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

="*Hamming Bound*".


1
0.8
0.6
0.4
0.2
0
d/n
Hamming
G−V
0
0.5
1
Rate: k/n

Linear code

$$\begin{aligned} C &= \{u\} \quad \text{such that} \quad (u+v) \in C \quad \forall\, u, v \in C \\ &= \text{linear vector space} \end{aligned}$$

Properties

1. size $m = 2^k$
2. any linearly independent set of k vectors can span the space

$$\text{e.g.} \qquad G = \begin{pmatrix} 0011 \\ 1100 \end{pmatrix} \qquad \textbf{Generator matrix}$$

3. form H having $n-k$ rows such that

$$HG^T = 0$$

$\Rightarrow$ all u satisfy the "parity checks" in H,

$$Hu^T = 0 \qquad \textbf{Parity check matrix}$$

4. Dual code

$$C^{\perp} \;=\; \{v\} \quad \text{such that} \quad (v \cdot u) = 0 \quad \forall\, u \in C$$

N.B. C and $C^{\perp}$ overlap (e.g. both contain $00\cdots 0$)

$$\begin{aligned} H_C &= G_{C^{\perp}} \\ G_C &= H_{C^{\perp}} \end{aligned}$$

5. Minimum distance $\quad d(u,v) = \mathrm{wt}(u+v) = \text{minimum weight}$

Parity checking and syndrome

Recall $Hu^T = 0; \;\; \forall u \in C$

error e : $\qquad u \rightarrow u + e$

$$\begin{aligned} H(u+e)^T &= Hu^T + He^T \\ &= 0 + He^T \\ &= He^T \\ &= \text{error } \textbf{syndrome} \end{aligned}$$

Can we deduce e from He^T ?

Ans.: no, since consider $e' = e + v$:

$$\begin{aligned} H(u+e')^T &= Hu^T + He^T + Hv^T \\ &= 0 + He^T + 0 \\ &= He^T \end{aligned}$$

$\Rightarrow$ each e is a member of a *coset*, all having the same syndrome

We can pick 1 error from each coset and call it correctable
$\Rightarrow$ there are 2^{n-k} correctable errors (with 2^{n-k} syndromes).

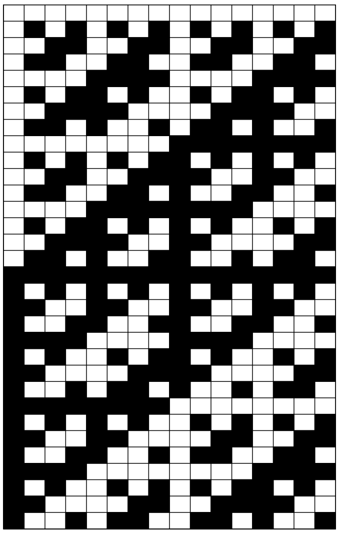


Figure 1: $[16, 5, 8]$ Reed-Muller code.

Existence of good codes: Gilbert-Varshamov bound

There exists a linear $[n, k, d]$ code if

$$1+\binom{n-1}{1}+\binom{n-1}{2}+\cdots+\binom{n-1}{d-2}<2^{n-k}$$

Proof:
1. Distance d if and only if every set of $(d-1)$ cols of H is linearly independent
2. Build H as follows:

Let $r = n - k =$ number of rows

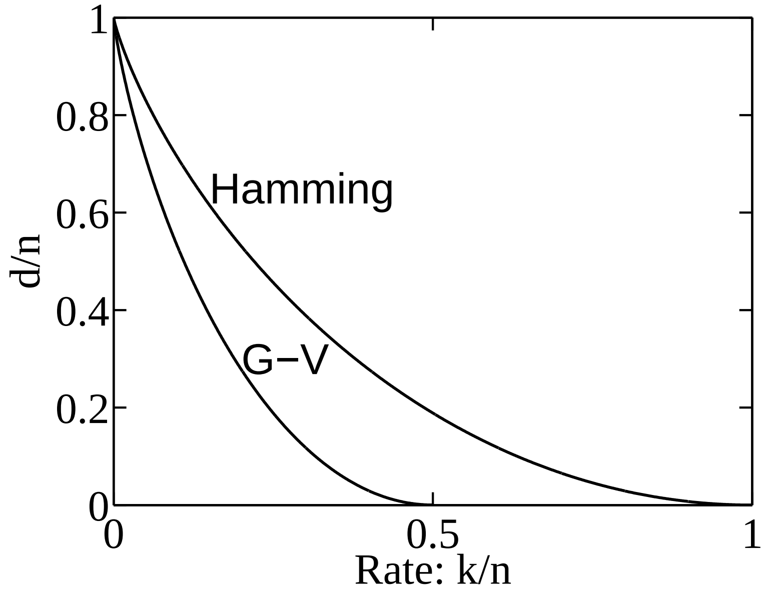
Suppose we have formed i cols, such that every set of $(d-1)$ is lin. ind.

Form col. vectors by picking $(d-2)$ or fewer of these: how many can be formed?

$$\text{ans. :} \qquad \binom{i}{1}+\binom{i}{2}+\cdots+\binom{i}{d-2}$$

If this is $< 2^r - 1$ then can pick a vector not yet appearing

$\Rightarrow$ get new col. such that any $(d-1)$ still lin. ind.	Keep going until $i+1=n$
$\Rightarrow$ now have $i+1$ cols. of H	$\rightarrow$ hence condition as claimed.



1
0.8
0.6
0.4
0.2
0
d/n
Hamming
G−V
0
0.5
1
Rate: k/n

Lecture 2.

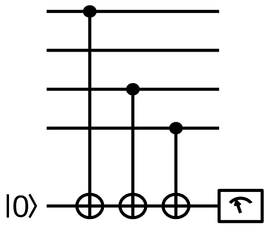
Principles of quantum error correction

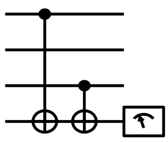
Quantum Error Correction: introducing main ideas

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





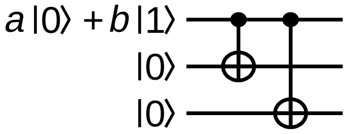
3 bit code

$$
\begin{matrix} 000 \\ 111 \end{matrix} \qquad \text{check matrix} \quad H = \begin{pmatrix} 110 \\ 101 \end{pmatrix}
$$

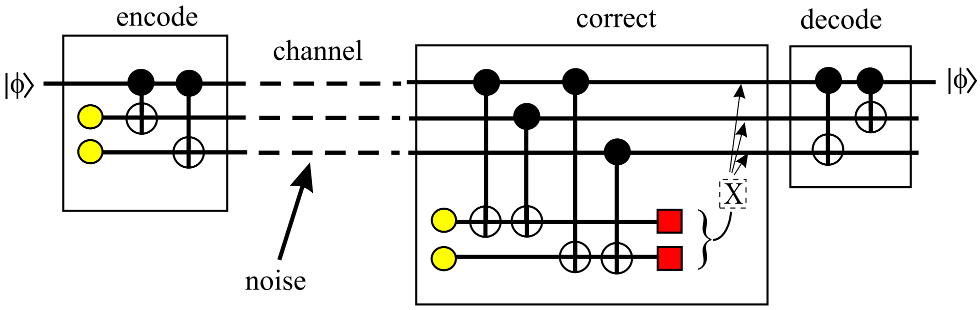
Quantum case

$$
\begin{aligned}
|0\rangle &\rightarrow |000\rangle \\
|1\rangle &\rightarrow |111\rangle
\end{aligned}
$$

Encoding network:

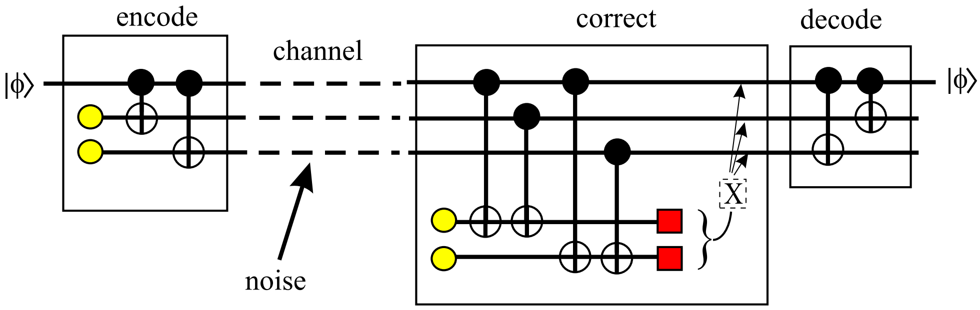


$$
\begin{aligned}
(a|0\rangle + b|1\rangle)|0\rangle|0\rangle &= a|000\rangle + b|100\rangle \\
&\xrightarrow{\text{CNOT}} a|000\rangle + b|110\rangle \\
&\xrightarrow{\text{CNOT}} a|000\rangle + b|111\rangle
\end{aligned}
$$



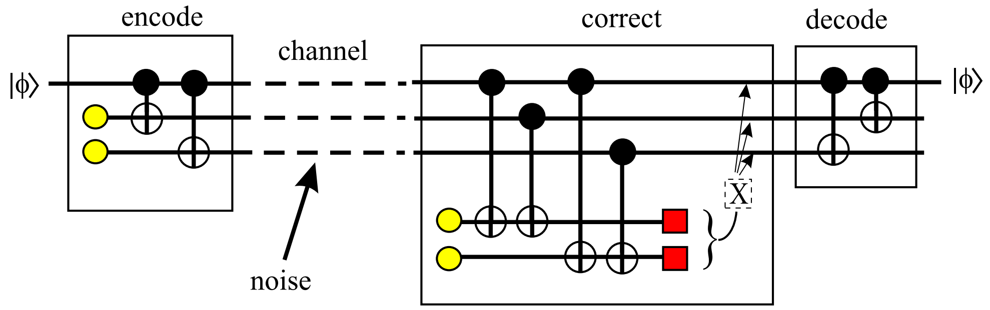
Noise in the channel: random bit flips: operator X with probability p

state	probability
$a\|000\rangle + b\|111\rangle$	$(1-p)^3$
$a\|100\rangle + b\|011\rangle$	$p(1-p)^2$
$a\|010\rangle + b\|101\rangle$	$p(1-p)^2$
$a\|001\rangle + b\|110\rangle$	$p(1-p)^2$
$a\|110\rangle + b\|001\rangle$	$p^2(1-p)$
$a\|101\rangle + b\|010\rangle$	$p^2(1-p)$
$a\|011\rangle + b\|100\rangle$	$p^2(1-p)$
$a\|111\rangle + b\|000\rangle$	p^3



Include ancilla bits in the notation (still at time just after channel):

state	probability
$(a\,\lvert 000\rangle + b\,\lvert 111\rangle)\,\lvert 00\rangle$	$(1-p)^3$
$(a\,\lvert 100\rangle + b\,\lvert 011\rangle)\,\lvert 00\rangle$	$p(1-p)^2$
$(a\,\lvert 010\rangle + b\,\lvert 101\rangle)\,\lvert 00\rangle$	$p(1-p)^2$
$(a\,\lvert 001\rangle + b\,\lvert 110\rangle)\,\lvert 00\rangle$	$p(1-p)^2$
$(a\,\lvert 110\rangle + b\,\lvert 001\rangle)\,\lvert 00\rangle$	$p^2(1-p)$
$(a\,\lvert 101\rangle + b\,\lvert 010\rangle)\,\lvert 00\rangle$	$p^2(1-p)$
$(a\,\lvert 011\rangle + b\,\lvert 100\rangle)\,\lvert 00\rangle$	$p^2(1-p)$
$(a\,\lvert 111\rangle + b\,\lvert 000\rangle)\,\lvert 00\rangle$	p^3



Now after parity checks (*syndrome extraction*)

state	probability
$(a\|000\rangle + b\|111\rangle)\|00\rangle$	$(1-p)^3$
$(a\|100\rangle + b\|011\rangle)\|11\rangle$	$p(1-p)^2$
$(a\|010\rangle + b\|101\rangle)\|10\rangle$	$p(1-p)^2$
$(a\|001\rangle + b\|110\rangle)\|01\rangle$	$p(1-p)^2$
$(a\|110\rangle + b\|001\rangle)\|01\rangle$	$p^2(1-p)$
$(a\|101\rangle + b\|010\rangle)\|10\rangle$	$p^2(1-p)$
$(a\|011\rangle + b\|100\rangle)\|11\rangle$	$p^2(1-p)$
$(a\|111\rangle + b\|000\rangle)\|00\rangle$	p^3

Next, measure the ancilla
in $|0\rangle$, $|1\rangle$ basis.
Nothing happens here, except we learn the syndrome

state	probability
$(a\,|000\rangle + b\,|111\rangle)\,|00\rangle$	$(1-p)^3$
$(a\,|100\rangle + b\,|011\rangle)\,|11\rangle$	$p(1-p)^2$
$(a\,|010\rangle + b\,|101\rangle)\,|10\rangle$	$p(1-p)^2$
$(a\,|001\rangle + b\,|110\rangle)\,|01\rangle$	$p(1-p)^2$
$(a\,|110\rangle + b\,|001\rangle)\,|01\rangle$	$p^2(1-p)$
$(a\,|101\rangle + b\,|010\rangle)\,|10\rangle$	$p^2(1-p)$
$(a\,|011\rangle + b\,|100\rangle)\,|11\rangle$	$p^2(1-p)$
$(a\,|111\rangle + b\,|000\rangle)\,|00\rangle$	p^3

Measurement of the ancilla
case where measurement result is 00:

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

action: do nothing

Measurement of the ancilla
case where measurement result is 01:

state	probability
$(a\|001\rangle + b\|110\rangle)\|01\rangle$	$p(1-p)^2$
$(a\|110\rangle + b\|001\rangle)\|01\rangle$	$p^2(1-p)$

action: apply X to 3rd qubit

Result
after correction:

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

Result: wrong state with probability $p^2(1-p)$.

Measurement of the ancilla
case where measurement result is 10:

state	probability
$(a\|010\rangle + b\|101\rangle)\|10\rangle$	$p(1-p)^2$
$(a\|101\rangle + b\|010\rangle)\|10\rangle$	$p^2(1-p)$

action: apply X to 2nd qubit

Result
after correction:

state	probability
$(a\,\lvert 000\rangle + b\,\lvert 111\rangle)\,\lvert 10\rangle$	$p(1-p)^2$
$(a\,\lvert 111\rangle + b\,\lvert 000\rangle)\,\lvert 10\rangle$	$p^2(1-p)$

Result: wrong state with probability $p^2(1-p)$.

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

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

More general error:

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

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

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

At this stage the state still has all possible errors:

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

Now measure the ancilla: **projection**

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

Apply corrective X depending on the syndrome:

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

Overall error in the final state: either s^6, or s^2 with probability $3c^2 s^2$
Hence

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

N.B. notice the *discretization* of errors: a continuous rotation error is projected by the syndrome measurement onto one of a discrete set of errors.

Generalize $\longrightarrow$ any classical code
$G \rightarrow$ generator network
$H \rightarrow$ parity check network.

These are "quasi classical" codes.

Phase errors, also known as decoherence

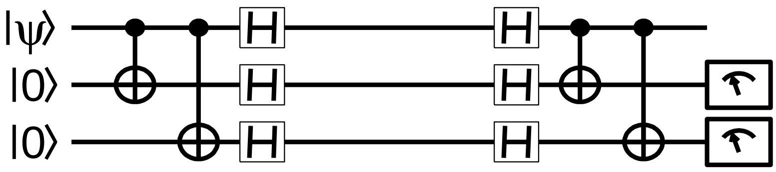
$$\begin{pmatrix} e^{i\phi/2} & 0 \\ 0 & e^{-i\phi/2} \end{pmatrix} = \cos(\phi/2)I + i\sin(\phi/2)Z$$

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:



General Noise

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

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

where T may be written

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

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

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

Hence **any** evolution can be written

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

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

Consider the following:

$$\begin{aligned} \text{bit flip} \quad |0\rangle &\rightarrow |1\rangle \\ \text{phase flip} \quad |\bar{0}\rangle &\rightarrow |\bar{1}\rangle \end{aligned}$$

where

$$\begin{aligned} |\bar{0}\rangle &= H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2} \\ |\bar{1}\rangle &= H|1\rangle = (|0\rangle - |1\rangle)/\sqrt{2} \end{aligned}$$

Notice

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

…more generally: **Dual code theorem**:

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

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 $\mathcal{C}_1$:

$$\mathcal{C}_0 \subset \mathcal{C}_1$$

e.g.

$$G_1 = \begin{pmatrix} 1010101 \\ 0110011 \\ 0001111 \\ 1110000 \end{pmatrix} \quad \left.\begin{matrix} \\ \\ \\ \end{matrix}\right\} G_0$$

$\mathcal{C}_1$ has $[n = 7, k = 4]$, $\mathcal{C}_0$ has $[n = 7, k = 3]$.

The code $\mathcal{C}_1$ allows bit errors to be corrected for both $|0\rangle_L$ and $|1\rangle_L \equiv XXXIIII\,|0\rangle_L$ and combinations thereof.

The code $\mathcal{C}_0^\perp$ allows phase errors to be corrected, at least for the state we started with, $|0\rangle_L$.

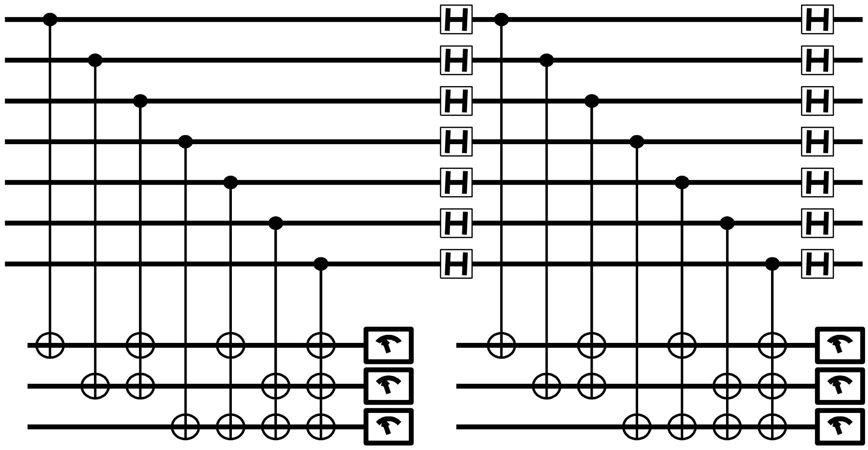
Now check that $|1\rangle_L$ can also be phase-error corrected.
Use

$$\mathbf{H}\,XXXIIII = ZZZIIII\,\mathbf{H} \qquad \text{where } \mathbf{H} \equiv HH\cdots H$$

$$\begin{aligned}\Rightarrow \mathbf{H}\,XXXIIII \sum_{u\in\mathcal{C}_0} |u\rangle &= ZZZIIII \sum_{v\in\mathcal{C}_0^\perp} |v\rangle \\ &= \text{still satisfies all the checks of } \mathcal{C}_0^\perp\end{aligned}$$

It works! Therefore we now have 2 quantum states, $|0\rangle_L$ and $|1\rangle_L$ called *quantum codewords*, which can be corrected for X and Z errors, and hence also for Y errors. This is a quantum code for encoding 1 qubit into 7.

Complete parity checking for 7-bit code:



Hence

Theorem (CSS codes):
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).

$\longrightarrow$ $\boxed{\text{“Shannon theorem” for perfect communication through a noisy quantum channel.}}$

Examples:

- 7-bit code: Hamming code contains its dual (every row of H satisfies all the checks in H)
- $[127, 85, 13]$ classical BCH code $\to$ $[[127, 43, 13]]$ quantum BCH code
- $[23, 12, 7]$ classical Golay code $\to$ $[[23, 1, 7]]$ quantum code

e.g. 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.

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

$P(\text{uncorrectable error}) \simeq 8855 \times (0.001)^4 \simeq 10^{-8}$

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

Lecture 3.

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!

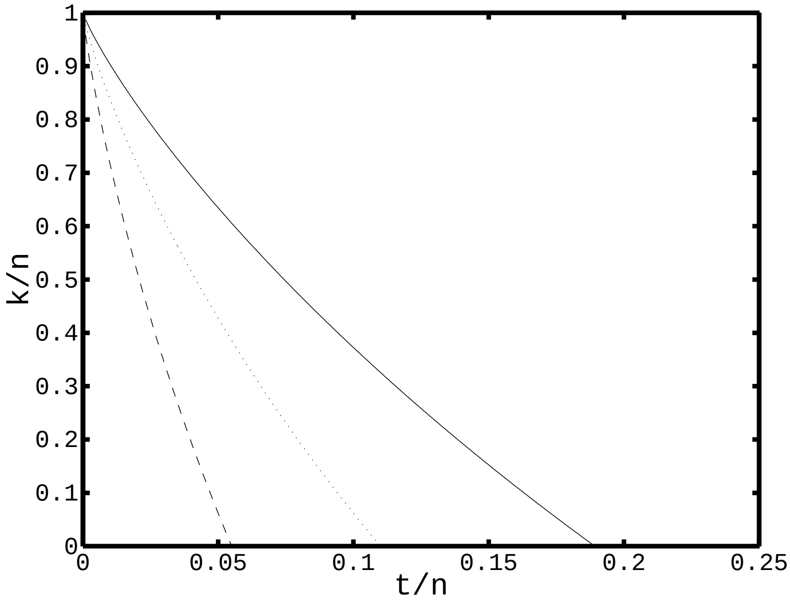
$$H = \left(\begin{array}{c|c} 11000 & 00101 \\ 01100 & 10010 \\ 00110 & 01001 \\ 00011 & 10100 \end{array} \right), \qquad G = \left(\begin{array}{c|c} H_x & H_z \\ 11111 & 00000 \\ 00000 & 11111 \end{array} \right).$$

One possible choice of the two codewords is

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

$$|1\rangle_L = X_{11111} |0\rangle_L .$$

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.

Resulting error is:

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

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

Therefore use stabilizer $-Z_1Z_2$,

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

Both states have the same energy $\Rightarrow$ they both aquire 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.

(2.) General errors.

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:

$$\begin{aligned} \rho_0 \;&\rightarrow\; \sum_{ij} a_{ij}\, E_i\, \rho_0 E_j \\ \text{QEC:} \qquad &\rightarrow\; F\rho_0 + \sum_{\text{uncorrectable}} a_{ij}\, E_i'\, \rho_0\, E_j' \end{aligned}$$

$$\text{fidelity} \qquad F = 1 - \mathrm{Tr}\left[\sum_{\text{uncorrectable}} a_{ij}\, E_i'\, \rho_0\, E_j'\right]$$

$$\sim\; 1 - \sum_{\text{uncorrectable}} |a_{ij}|$$

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.