Lecture 18

Simple quantum error-correcting codes

Binary symmetric channel

The classical **binary symmetric channel** is

input: $b \in \{0,1\}$

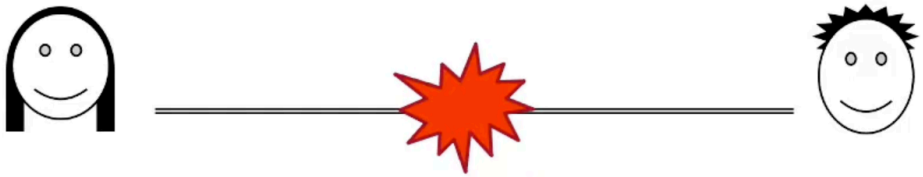
output: $\begin{cases} b & \text{with prob. } 1-\varepsilon \\ \neg b & \text{with prob. } \varepsilon \end{cases}$

This channel (called BSC_ε) is a classical analogue of the depolarizing channel

output: $\begin{cases} b & \text{with prob. } 1-2\varepsilon \\ \begin{bmatrix} 1/2 \\ 1/2 \end{bmatrix} & \text{with prob. } 2\varepsilon \end{cases}$

"maximally mixed" state $\begin{cases} 0 & \text{with prob. } 1/2 \\ 1 & \text{with prob. } 1/2 \end{cases}$

Suppose that Alice wants to communicate to Bob but their communication channel is ***noisy***



binary symmetric channel

How can they reduce the noise level?

1. Get a better communication channel (a BCS with smaller ε)

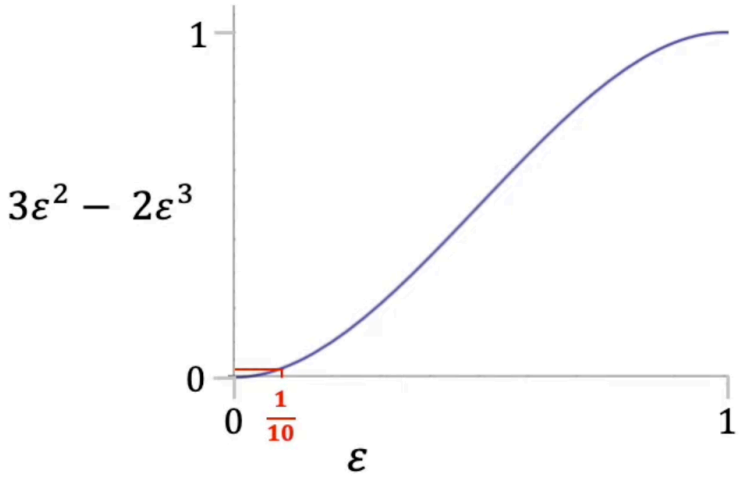
1 3-bit repetition code

Alice **encodes** $b \in \{0,1\}$ as bbb and sends the three bits through the channel

Bob **decodes** the three bits that he receives by taking the majority value

Assumption: the channel behaves independently each time it's used

Then the failure probability is $3\varepsilon^2(1-\varepsilon) + \varepsilon^3 = 3\varepsilon^2 - 2\varepsilon^3$



if $\varepsilon = \frac{1}{10}$ then the failure probability is $< \frac{1}{35}$

if $\varepsilon = \frac{1}{1000}$ then the failure probability is $< \frac{1}{300{,}000}$

Overhead: need to send three times as many bits
(the **rate** of the code is $1/3$)

Error-correcting codes

If the data is a long string of bits then, using the 3-bit repetition code, there will be errors:

$$1000100\mathbf{1}00100111011111\mathbf{0}1000101011101011010001101100101011010\mathbf{0}1100111010110001011001\mathbf{0}110\cdots$$

- using no code, the fraction of errors is ε
- using the three-bit repetition code, the fraction of errors is $3\varepsilon^2 - 2\varepsilon^3$

For a Gigabyte (~8.5 billion bits) with $\varepsilon = 1/100$, the expected number of errors is around:
85 million without the code, and 24,000 with the code

Are there codes that succeed without **any** errors, with high probability?

A larger repetition code reduces the error probability per bit — but this also reduces the rate

But there are much better error-correcting codes than this …

Amazing result about "good multi-bit codes"

For the binary symmetric channel with error parameter $\varepsilon < 1/2$, the success probability for long strings can be arbitrarily close to 1, *while maintaining a constant rate*

⑦ Error-correcting codes

Encode blocks of size n into blocks of size m

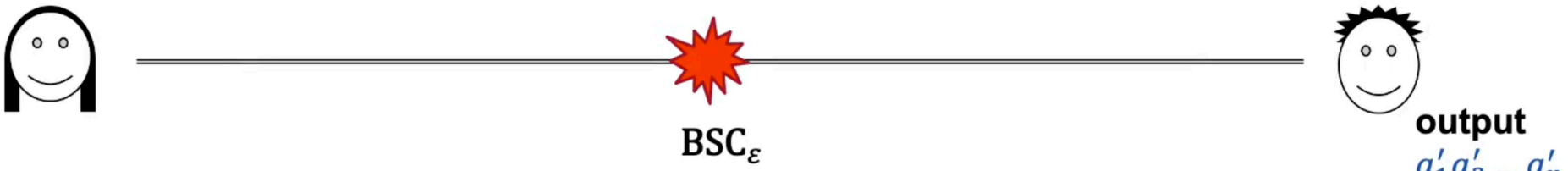
Encoding function $E: \{0,1\}^n \longrightarrow \{0,1\}^m$

Decoding function $D: \{0,1\}^m \longrightarrow \{0,1\}^n$

rate of the code: n/m

Let $\mathrm{BSC}_\varepsilon(b_1 b_2 \ldots b_m)$ denote the output of the binary symmetric channel on the string $b_1 b_2 \ldots b_m$
(it will be a probability distribution on the set of m-bit strings)

input
$a_1 a_2 \ldots a_n$



output
$a'_1 a'_2 \ldots a'_n$

Error probability $\Pr[D(\mathrm{BSC}_\varepsilon(E(a_1 a_2 \ldots a_n))) \neq a_1 a_2 \ldots a_n$

Good error-correcting codes

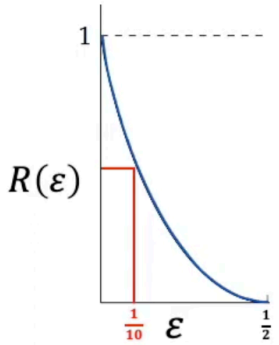
What's the best rate possible if the noise level per bit is ε?

Shannon entropy function

$$H(\varepsilon, 1-\varepsilon) = -\varepsilon \log \varepsilon - (1-\varepsilon)\log(1-\varepsilon)$$

Define

$$R(\varepsilon) = 1 - H(\varepsilon, 1-\varepsilon)$$



Result about good multi-bit codes:

For any noise level $\varepsilon < 1/2$, we can select any rate $r < R(\varepsilon)$ and any failure error probability $\delta > 0$ and then there exists an error-correcting code with $n/m \geq r$, whose success probability is $\geq 1 - \delta$

Some further considerations:

- Block length n (need large n to achieve small δ)
- Computational cost of computing E and D (efficient error-correcting codes exist)

Are there *quantum* error-correcting codes?

Is there a quantum repetition code?

Encoding: 

Decoding: take the majority of the three qubits

Anything wrong with this?

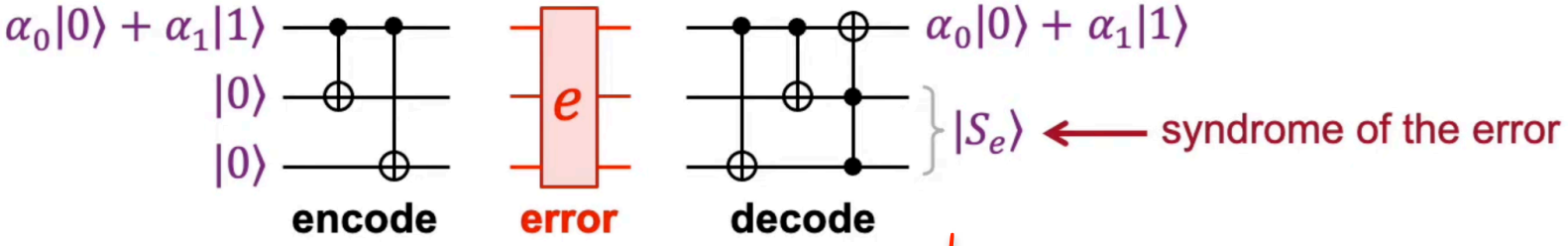
Violates no-cloning theorem

How do you take the majority of three qubits?

Is there a fundamental obstacle to quantum error-correcting codes?

3-qubit code for one X-error

The following 3-qubit quantum code protects against up to one X error (bit-flip)



The data $\alpha_0|0\rangle + \alpha_1|1\rangle$ is shielded from each of these errors:

$I\otimes I\otimes I$	$X\otimes I\otimes I$	$I\otimes X\otimes I$	$I\otimes I\otimes X$
$\|00\rangle$	$\|11\rangle$	$\|10\rangle$	$\|01\rangle$

Exercise: verify this

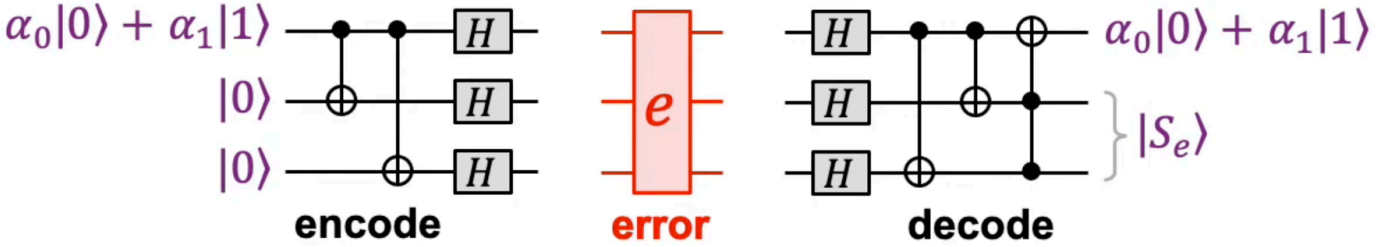
← syndromes

What about Z errors?

They are passed through: one Z error is equivalent to applying Z to the original data

3-qubit code for one Z-error

We can adapt the code to protect against Z-errors instead of X-errors



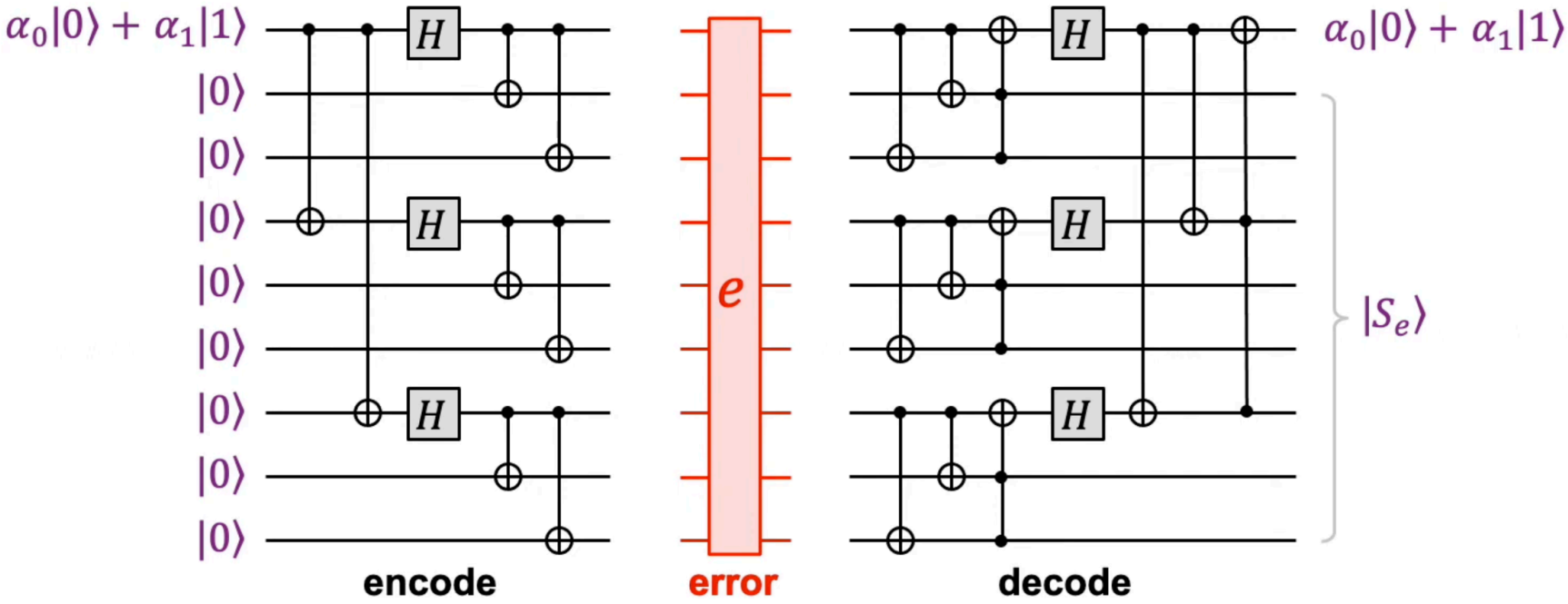
Since $HZH = X$, the data $\alpha_0|0\rangle + \alpha_1|1\rangle$ is shielded from each of these errors:

$I\otimes I\otimes I$	$Z\otimes I\otimes I$	$I\otimes Z\otimes I$	$I\otimes I\otimes Z$	
$\|00\rangle$	$\|11\rangle$	$\|10\rangle$	$\|01\rangle$	← syndromes

Is there a code that protects against arbitrary one-qubit errors?

$X = HZH$

Shor's 9-qubit quantum code



The "inner" part corrects any one-qubit X-error (and passes through a Z-error)

The "outer" part corrects any one-qubit Z-error

Since $Y = iXZ$, one-qubit Y-errors are also corrected

Shor's 9-qubit quantum code

Since, any one-qubit unitary is expressible as

$$U = \eta_0 I + \eta_x X + \eta_y Y + \eta_z Z$$

this code corrects any one-qubit unitary error

Exercise: confirm this

Consider the quantum channel that applies

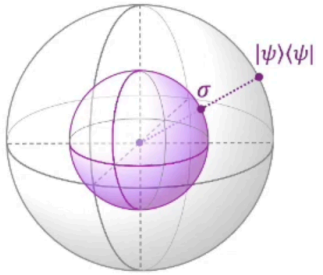
$$\begin{cases} I & \text{with prob. } 1-\varepsilon \\ X & \text{with prob. } \varepsilon/3 \quad \text{(bit flip)} \\ Y & \text{with prob. } \varepsilon/3 \quad \text{(bit+phase flip)} \\ Z & \text{with prob. } \varepsilon/3 \quad \text{(phase flip)} \end{cases}$$

← this is actually the **depolarizing channel**

$$\rho \longmapsto p\rho + (1-p)\begin{bmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{bmatrix}$$

for some parameter p

Exercise: prove this



This code reduces the failure probability from ε to less than $c\varepsilon^2$ (where $c \leq 36$)

For sufficiently small ε, this is an improvement

Are there good multi-qubit quantum codes?

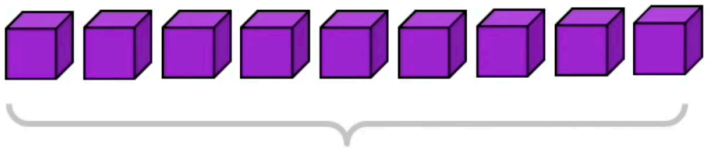
redundancy ≠ copying

Data $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$

Encoding

$$\alpha_0(|000\rangle + |111\rangle)^{\otimes 3} + \alpha_1(|000\rangle - |111\rangle)^{\otimes 3}$$

$|0\rangle_L$ $|1\rangle_L$

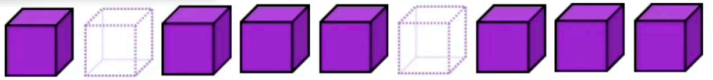


can recover $|\psi\rangle$ from any 1-qubit **error**
(in an ***unknown position***)

Is there a shorter code for one error?

Stay tuned for the next lecture

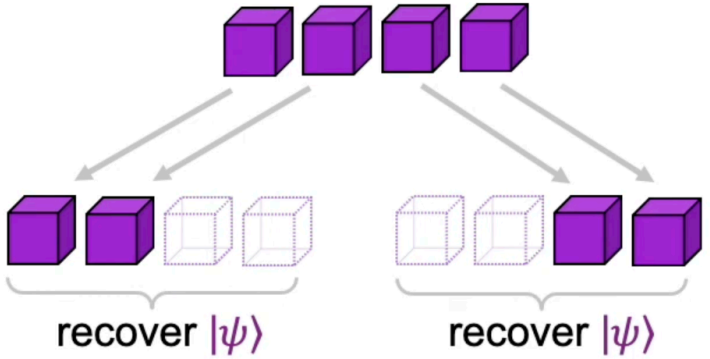
Erasure errors: errors in ***known*** positions



The Shor code can recover from any 2 erasure errors

Theorem: there's no 4-qubit code for 2 erasure errors

Proof:



This would contradict the no-cloning theorem