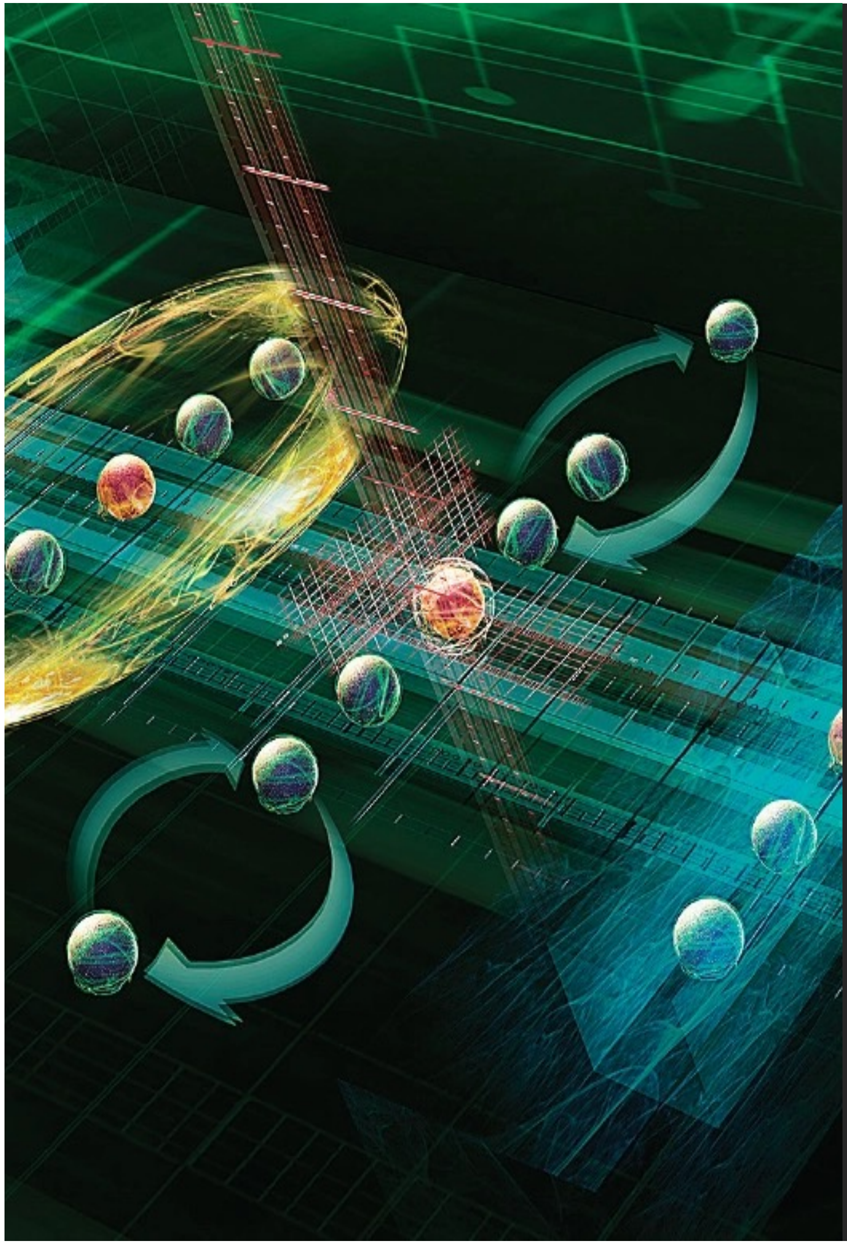


Lecture 8:

Quantum Error Correction

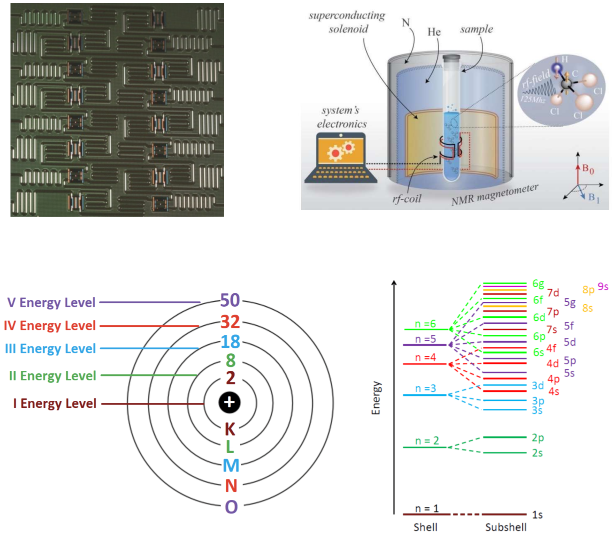
COMP3366
Quantum algorithms & computing architecture

Instructor: Yuxiang Yang

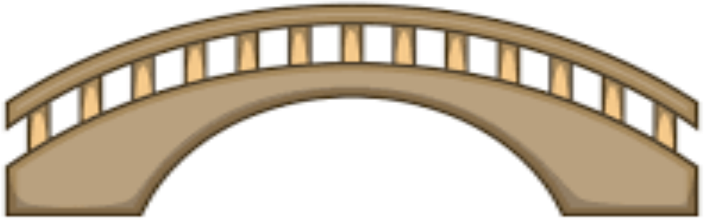
Department of Computer Science, HKU

Objectives:

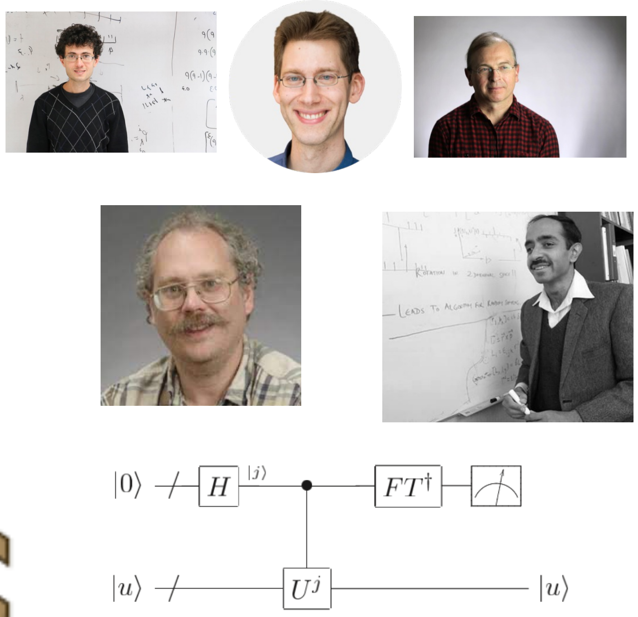
- **[O1] Concepts:** Errors, codes, error correction, code concatenation, syndrome detection, stabilizers, repetition codes, the Shor code.
- **[O2] Problem solving:** Analysis of error, syndrome, and performance of error correction codes.
- **[O3] Algorithm design:** Circuit implementation of quantum error correction.



Imperfect physical realization
(Lecture 7)



Quantum error correction
(Lectures 8 and 9)



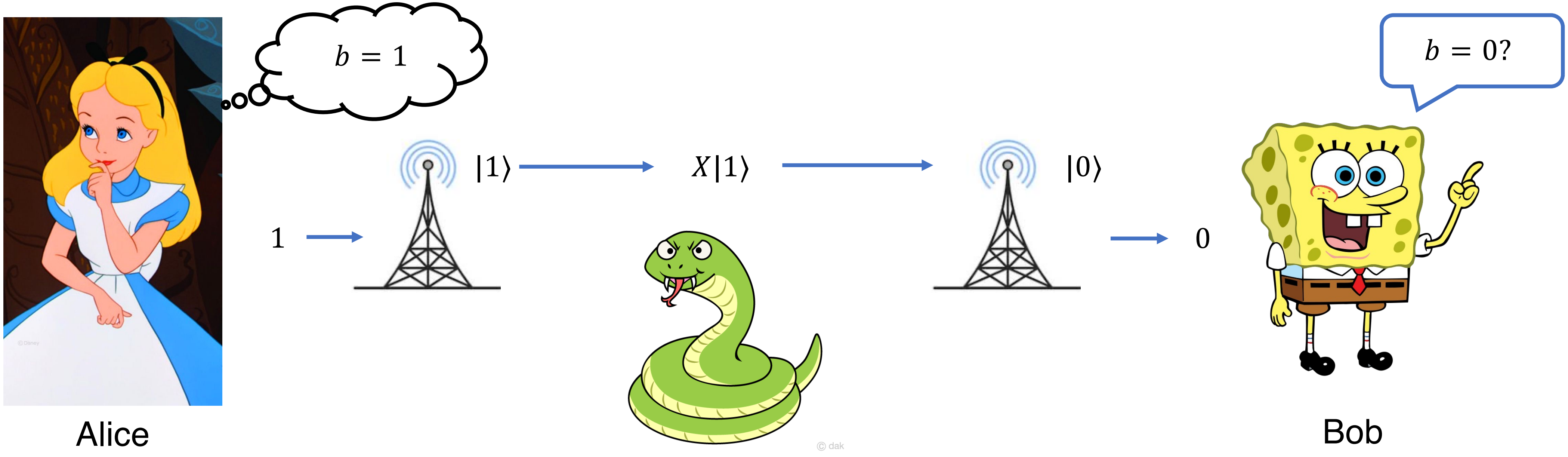
Noiseless quantum computations &
algorithms

Part I:
Error correction – a first taste

Quantum information vs. Classical errors

Communication under attack

- Alice wants to transfer a bit of information to a far away friend Bob, using qubit(s). They hired a communication company that can do QC.
- **Check!** There is a malicious snake who may flip one of the qubit(s) being sent. How could the company overcome this attack?



Beating the snake with the repetition code

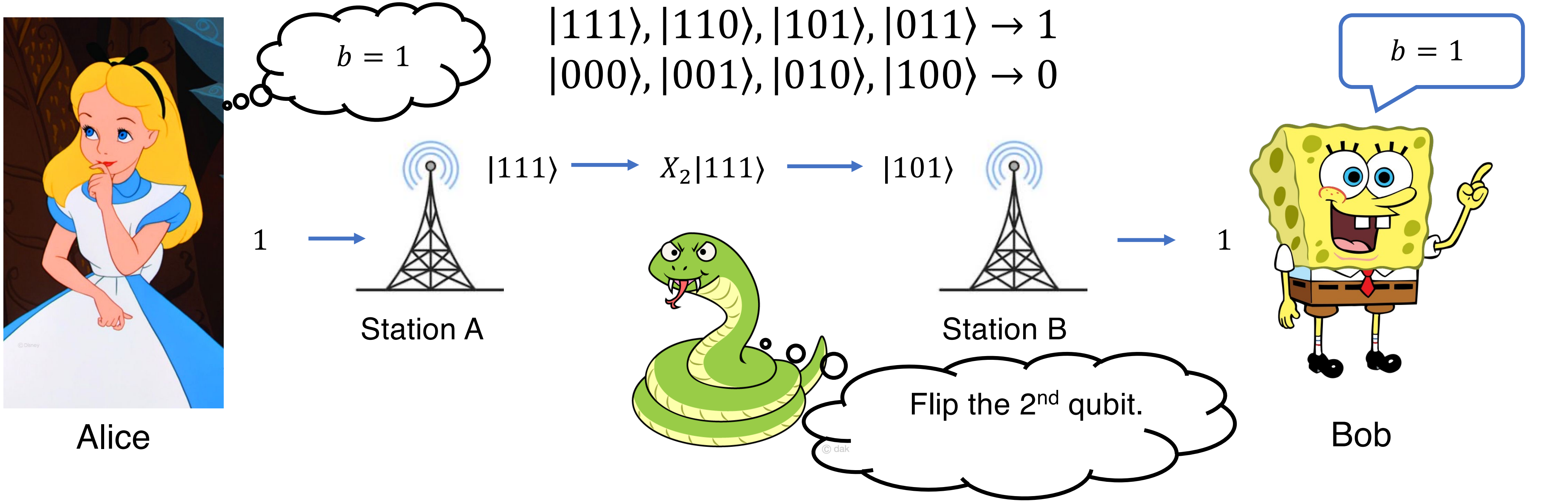
- Station A can encode the information into a 3-qubit codeword by making copies:

$$b \to |b_L\rangle = |bbb\rangle, \qquad b = 0,1.$$

"L" for "logical"; see later

- Station B can decode by measuring in the computational basis and adopt the majority voting rule:

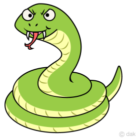
$$|111\rangle, |110\rangle, |101\rangle, |011\rangle \to 1$$
$$|000\rangle, |001\rangle, |010\rangle, |100\rangle \to 0$$



What does this have to do with quantum computers?

- In a quantum computer:

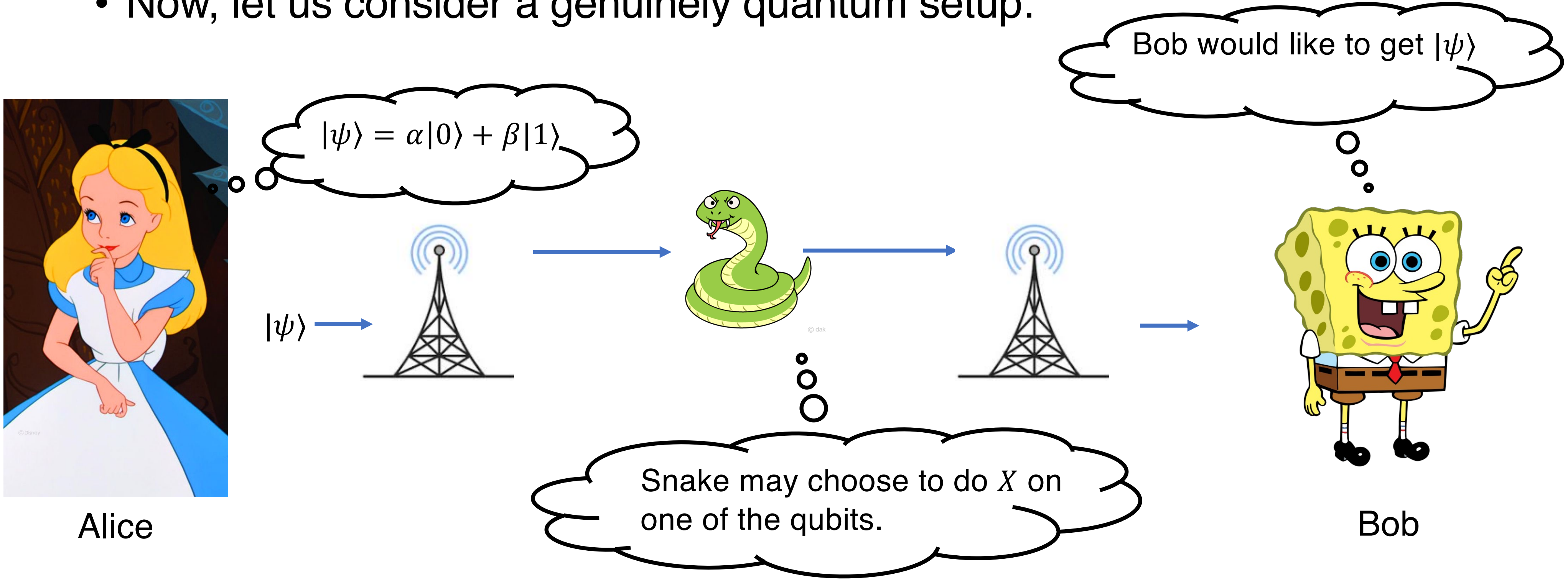
& = different stages of a quantum computation (e.g., Alice = QC's initial status,
Bob = QC's status after one second)

 = noises/errors in QC

- Why are there errors in a quantum computers:
  There are multiple sources of imperfection at each stage (state preparation, gates, measurements…) in the implementation (Lecture 7).
- In this example, 3 qubits are used to encode 1 (qu)bit of information.
- These 3 qubits are called physical qubits ("real" physical qubits in a QC that are subject to error) and the codeword is a logical (qu)bit (an "imaginary" noiseless system that contains 1-(qu)bit information).

Challenges for quantum error correction

- Everything so far is in fact “classical”.
  Indeed, we have been working in the computational basis $|0\rangle, |1\rangle$.
  No superposition, no entanglement.
- Now, let us consider a genuinely quantum setup:



Bob would like to get $|\psi\rangle$

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

$|\psi\rangle$

Snake may choose to do X on one of the qubits.

Alice

Bob

Challenges for quantum error correction

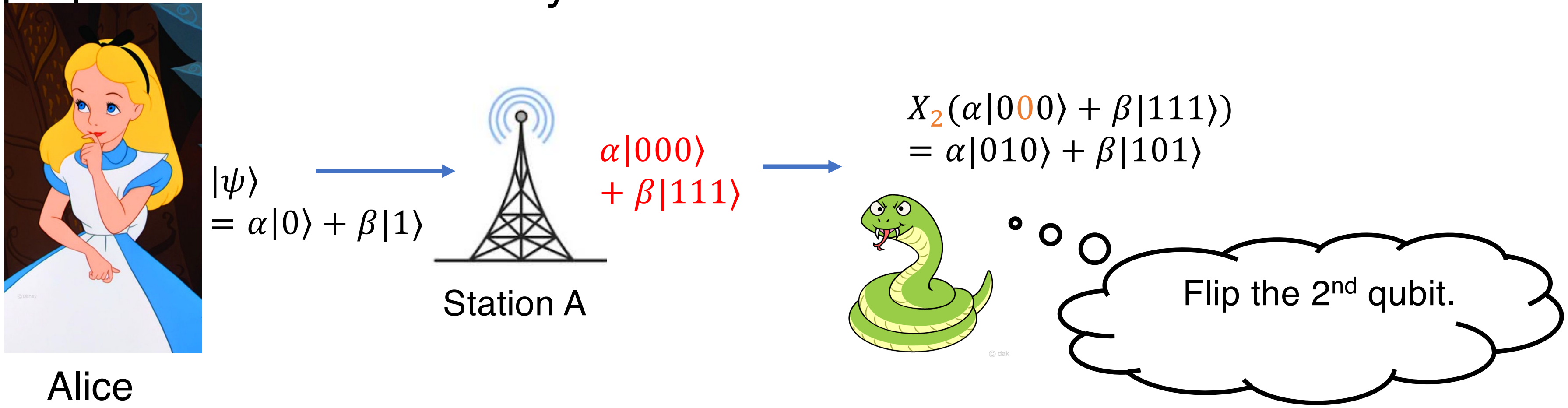
- Goal: design a scheme for the stations to transmit $|\psi\rangle$ faithfully.
- It is much harder to correct errors on a quantum computer:
  1. Quantum bits can be in superpositions of $|0\rangle$ and $|1\rangle$ (e.g., $|+\rangle$).
  2. "Looking at" quantum information without disturbance is impossible!
  3. Quantum errors are not just about bit flips!
- Moreover, you might be tempted to use copying $|\psi\rangle \rightarrow |\psi\rangle \otimes |\psi\rangle \otimes |\psi\rangle$
  Surprisingly, you cannot!
- No-copying/cloning theorem (see Assignment 3):
  For any n, there is no quantum gate U acting on n qubits, such that
  $$U\left(|\psi\rangle \otimes |0\rangle^{\otimes(n-1)}\right) = |\psi\rangle \otimes |\psi\rangle \otimes |\Psi(\psi)\rangle$$
  ($|\Psi(\psi)\rangle$ is an arbitrary $(n-2)$ qubit state that could depend on $|\psi\rangle$) holds for any qubit state $|\psi\rangle$.
- Station A cannot implement $|\psi\rangle \rightarrow |\psi\rangle \otimes |\psi\rangle \otimes |\psi\rangle$ without knowing $|\psi\rangle$.

Quantum repetition code

- Instead, we apply the same repetition code $|b_L\rangle = |bbb\rangle, b = 0,1$.
- Station A encodes $|\psi\rangle$ into 3 qubits by performing the 3-qubit gate $|b\rangle \otimes |00\rangle = |b\rangle \otimes |bb\rangle, b = 0,1$ on $|\psi\rangle \otimes |00\rangle$.
- By linearity of QC, $|\psi\rangle \rightarrow \alpha|000\rangle + \beta|111\rangle$.

Exercise: Find the circuit implementation of this 3-qubit gates (using CNOT).

- When the snake performs a flip operation X, it flips both branches in the superposition simultaneously.



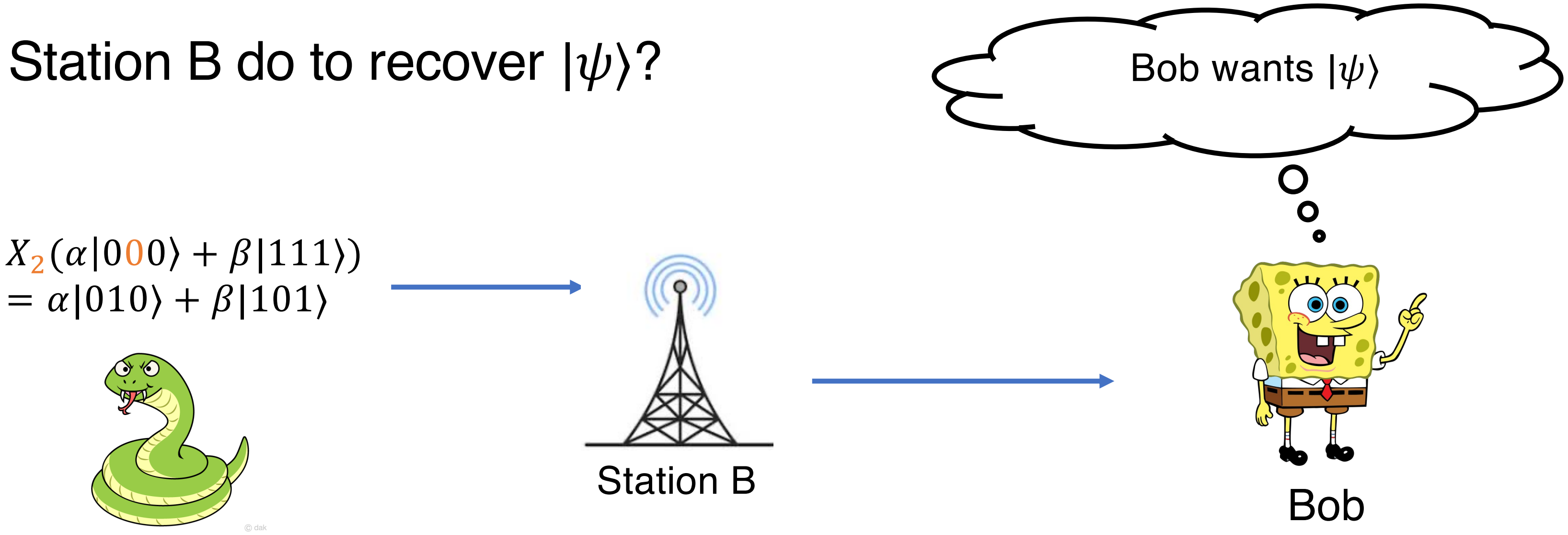
$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

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

$X_2(\alpha|000\rangle + \beta|111\rangle) = \alpha|010\rangle + \beta|101\rangle$

Quantum repetition code

- What should Station B do to recover $|\psi\rangle$?



$$X_2(\alpha|000\rangle + \beta|111\rangle) = \alpha|010\rangle + \beta|101\rangle$$

- Question: Can we measure in the computational basis (of 3 qubits)?
- No. This would collapse the superposition to, e.g., $|010\rangle$, and $|\psi\rangle$ cannot be recovered. The information about α, β is lost!
- Instead, Station B could perform a syndrome detection that learns the error without disturbing the encoded state!

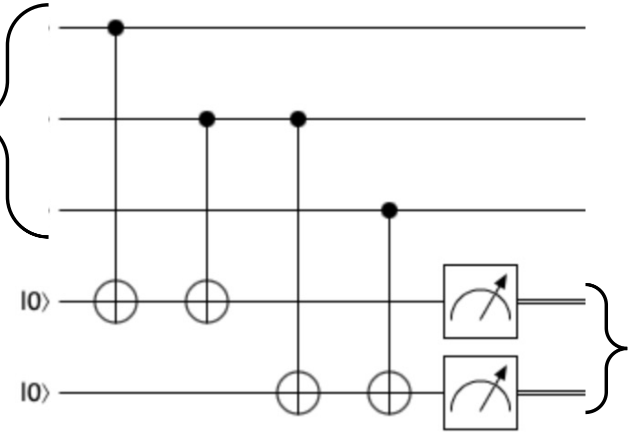
Syndrome detection

Exercise: Show how this circuit find out if the 1st or the 3rd qubit gets flipped.

- Syndrome detection is a useful gadget in quantum error correction to detect the errors without collapsing the state.
- We introduce 2 ancillary qubits as ”the doctor for repetition code”.
- Station B’s decoding consists of:

1. (Syndrome detection) Do CNOTs (as shown in the right circuit) and measure the 2 ancilla in computational basis,
2. (Correction):
   - If the measurement yields $(0,0)$, do nothing.
   - If the measurement yields $(1,0)$, do X_1.
   - If the measurement yields $(1,1)$, do X_2.
   - If the measurement yields $(0,1)$, do X_3.
3. (Decoding) Do inverse of encoding: $|bbb\rangle \rightarrow |b\rangle, b = 0{,}1$.

$\alpha|010\rangle + \beta|101\rangle$

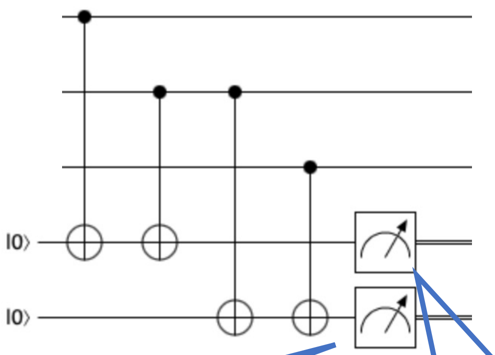


Error syndrome $= (1{,}1)$

Syndrome detection

- Question: Why does the gadget work?
- In the repetition code, each pair of the qubits have the same parity (both odd or even). This holds for both $|000\rangle$ and $|111\rangle$.
- A flip changes some of the parities, in the same way for both $|000\rangle$ and $|111\rangle$.
- The 2 measurements ask questions about the parities:
  - 1st measurement: 1st and 2nd qubits are the same?
  - 2nd measurement: 2nd and 3rd qubits are the same?
- Answers to these 2 questions uniquely determine the location of the error.

$\alpha|010\rangle + \beta|101\rangle$



2nd and 3rd qubits are not the same!

1st and 2nd qubits are not the same!

Exercise: Why don't we need a 3rd measurement?

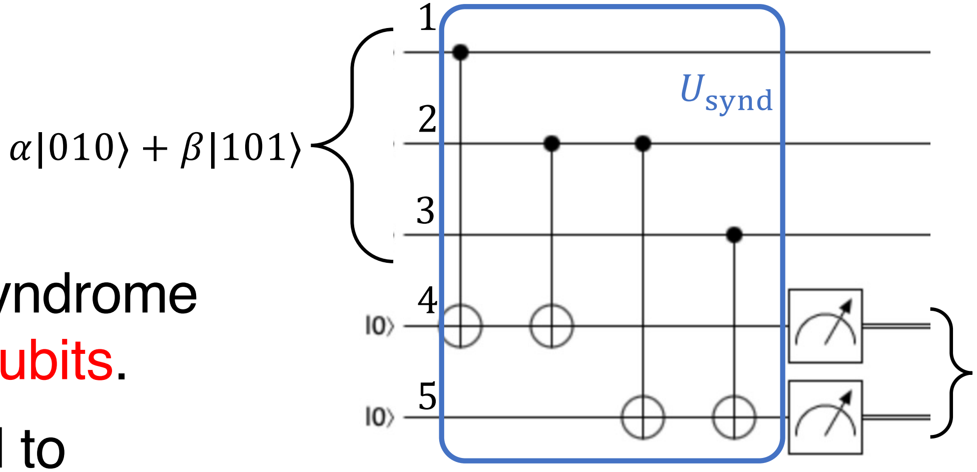
Technical details

Exercise: Show how this circuit find out if the 1st or the 3rd qubit gets flipped.

- Input state $\alpha|010\rangle + \beta|101\rangle$.
- Syndrome detection gate $U_{\text{synd}} = CNOT_{3,5}CNOT_{2,5}CNOT_{2,4}CNOT_{1,4}$.
- State evolution:

$$U_{\text{synd}}(\alpha|010\rangle + \beta|101\rangle) \otimes |00\rangle = \alpha|01011\rangle + \beta|10111\rangle$$
$$= (\alpha|010\rangle + \beta|101\rangle) \otimes |11\rangle.$$

- Syndrome detection gate U_{synd} acts like a controlled gate on the input state.
- The output is a product state. Measuring the last 2 qubits yields error syndrome without disturbing the state of the first 3 qubits.
- The syndrome measurements are related to Pauli observables (see next slides).



Error syndrome = (1,1)

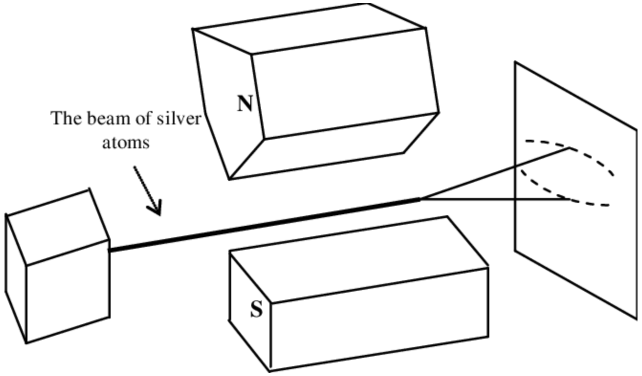
Brought over from Lecture 1: Measurement of an observable

- Any Hermitian matrix A corresponds to a physical observable.
- The expectation of A, denoted by $\langle A\rangle$, with respect to a quantum state $|\psi\rangle$ equals $\langle\psi|A|\psi\rangle$ and can be effectively measured:
- We can write $A = \sum_i a_i|\phi_i\rangle\langle\phi_i|$ for ONB $\{|\phi_i\rangle\}$, and thus the expectation of H can be estimated by measuring in the eigenbasis $\{|\phi_i\rangle\}$:

$$\langle\psi|A|\psi\rangle = \sum_i a_i p_i \qquad\qquad p_i = |\langle\psi|\phi_i\rangle|^2$$

- Example (Stein-Gerlach experiment):

$$|\psi\rangle = |+\rangle$$
$$A = Z/2 = (|0\rangle\langle 0| - |1\rangle\langle 1|)/2$$



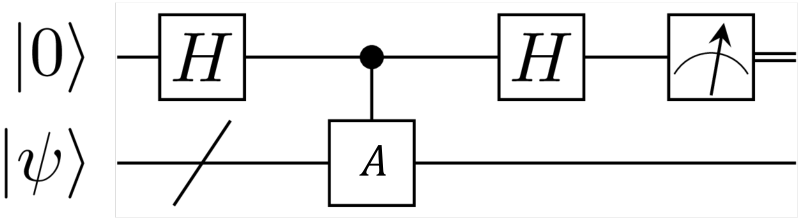
Measurement of Pauli observables

Exercise: Show that the eigenvalues of such an A are either 1 or -1.

- If A is both Hermitian and unitary, it is both an observable and a gate. This is true when A is a Pauli string, e.g., $A = Z_1 Z_2$.

$Z_i \coloneqq Z$ on the i-th qubit and I on the others

- When $|\psi\rangle$ is an eigenstate, the expectation $\langle A\rangle$ (= eigenvalue of $|\psi\rangle$) can be measured via the Hadamard test without changing $|\psi\rangle$:



Outcome $0 \mapsto$ *eigenvalue* $+1$.
Outcome $1 \mapsto$ *eigenvalue* -1

- Exercise: Prove the above statement (Hint: phase kickback trick!).
- This approach is better than the previous one. For example, when $A = Z_1 Z_2$, if we measure in the computational basis, an eigenstate $|B_0\rangle$ (the Bell state) will be collapsed to $|00\rangle$ or $|11\rangle$, but the Hadamard test is non-demolition (keeps $|B_0\rangle$ as it is)!

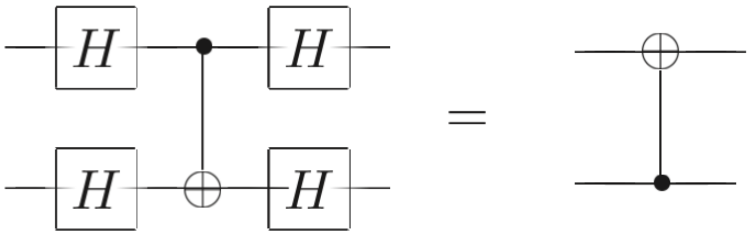
Syndrome detection as Hadamard tests

Eigenvalues = $(-1,-1)$

Eigenvalues = $(+1,+1)$

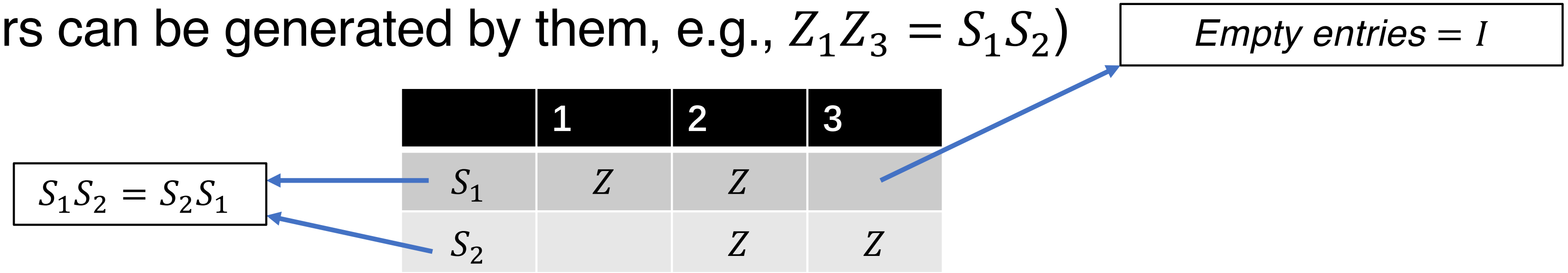
- How is the Hadamard test related to syndrome detection?
- Observation: the codeword $\alpha|000\rangle + \beta|111\rangle$ and the distorted codeword $\alpha|010\rangle + \beta|101\rangle$ are both eigenstates of Z_1Z_2 and Z_2Z_3.
- No error → codeword has eigenvalues $+1$ for both observables;
  Error → state has -1 eigenvalue(s) depending on error's location.
- To detect the error syndrome, it is enough to perform 2 Hadamard tests for Z_1Z_2 and Z_2Z_3, respectively!

Exercise: Show that the syndrome detection circuit is equivalent to two Hadamard tests:
[Hint: use the circuit equivalence in the right-hand side]



General theory: Stabilizers

- What is special about Z_1Z_2, Z_2Z_3? Answer: they are stabilizers!
- A stabilizer S is a Pauli string (e.g., $X \otimes Z \otimes I$) such that $S|b_L\rangle = |b_L\rangle, b = 0,1$. That is, they are +1 eigenstates of S.
- The repetition code has two independent stabilizers:
  (and others can be generated by them, e.g., $Z_1Z_3 = S_1S_2$)



	1	2	3
S_1	Z	Z	
S_2		Z	Z

Empty entries $= I$

$S_1S_2 = S_2S_1$

- In a quantum error correction code, stabilizers commute with each other:

$$S_iS_j = S_jS_i, \qquad \forall i, j.$$

- For a complete theory of stabilizers, see bonus material.

Detecting errors with stabilizers

- When a bit flip error occurs, since $XZ = -ZX$, the codewords may become a -1 eigenstate of S_i, if S_i has a Z at this location.

- For example, when X_1 occurs, $S_1(X_1|b_L\rangle) = -X_1|b_L\rangle$, since $S_1 = Z_1Z_2$.
  For $S_2 = Z_2Z_3$, we have $S_2(X_1|b_L\rangle) = X_1|b_L\rangle$.
  ⇒ The erroneous state $X_1|b_L\rangle$ is still an eigenstate, but with different eigenvalues!

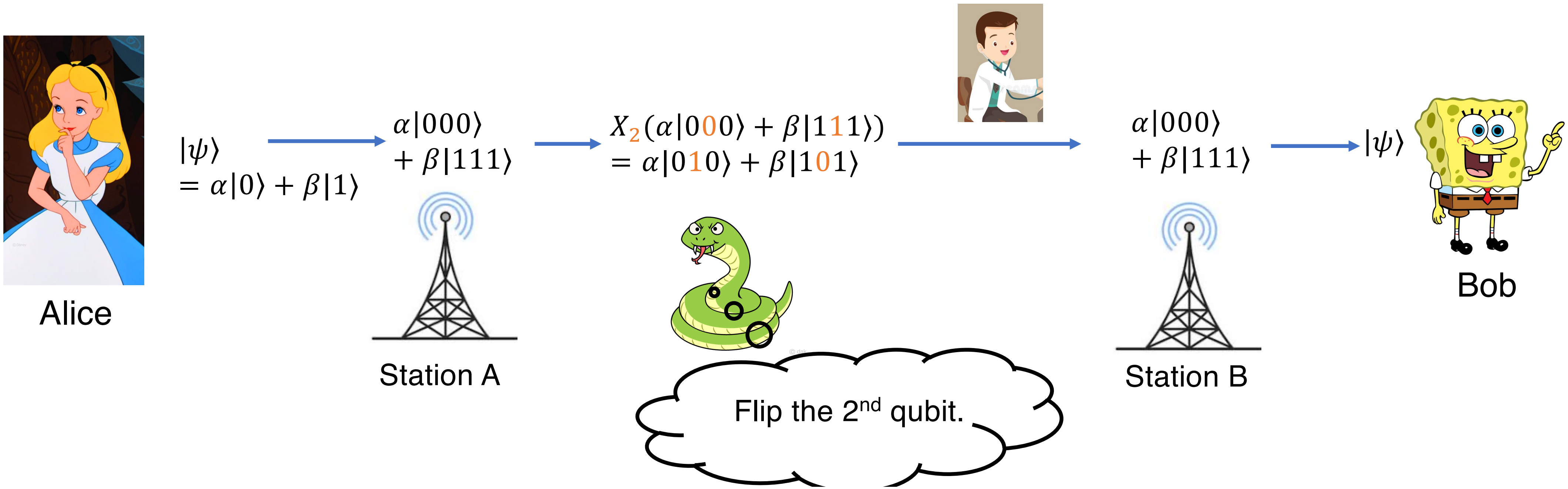
- If we now measure S_1, S_2, we will get $(-1, +1)$.
  So, we know the error's location!

Exercise: Complete the details of these derivations.

- The syndrome detection = measuring the stabilizers.

Quantum repetition code: complete version

- Station A encodes $|\psi\rangle$ into a codeword $|\psi_C\rangle$ by performing the 3-qubit gate $U: |b\rangle \otimes |00\rangle = |b\rangle \otimes |bb\rangle, b = 0{,}1$ on $|\psi\rangle \otimes |00\rangle$.
- Station B decodes by first measuring the stabilizers + correction to recover $|\psi_C\rangle$, and then $U^\dagger$ to recover $|\psi\rangle$ (the 2nd and the 3rd qubits are in $|00\rangle$ and can be discarded).



Alice

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

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

Station A

$X_2(\alpha|000\rangle + \beta|111\rangle) = \alpha|010\rangle + \beta|101\rangle$

Flip the 2nd qubit.

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

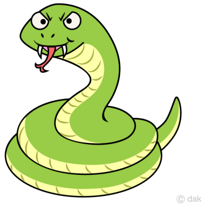
Station B

$|\psi\rangle$

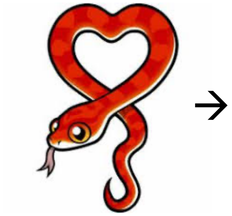
Bob

Quantum bit & phase flip errors

- … even more challenges in the quantum case:
  1. Quantum bits can be in superpositions of $|0\rangle$ and $|1\rangle$!
  2. "Looking at" quantum information without disturbance is impossible!
  3. Quantum information cannot be copied!
  4. Quantum errors are not just about bit flips!
- There are more than one snake in the quantum zone!



→ bit flips



→ phase flips

- For qubits, we must also deal with phase flips, which correspond to the Pauli gate $Z|1\rangle \rightarrow (-1)|1\rangle$!

Discussion: Can repetition code deal with both errors?

- Suppose we use the repetition code $|\psi_C\rangle = \alpha|000\rangle + \beta|111\rangle$.
- An error, being either X or Z, could have happened to one qubit. But we don't know its type and location.
- Can we still correct the error in this case?

Part II:
QEC for quantum errors

Quantum information vs. Quantum errors

Repetition code for phase flips

- The repetition code for X error cannot deal with Z errors.
- Let us focus on Z error first. How to deal with Z (phase flip)?
- Observation: $Z = HXH$, so another repetition code:

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

  can handle phase flips!

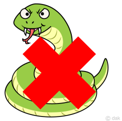
Exercise: Show that the stabilizers are X_1X_2 and X_2X_3. Further show that how you detect a Z error.

- Procedure:

  First do $|\psi\rangle \overset{H}{\rightarrow} \alpha|+\rangle + \beta|-\rangle$, and then do the repetition code encoding & decoding in the Hadamard basis, and finally do $\alpha|+\rangle + \beta|-\rangle \overset{H}{\rightarrow} |\psi\rangle$.
- But the repetition code for phase flip, again, does not work for bit flip. Can we handle phase and bit flips simultaneously?

Solution: code concatenation

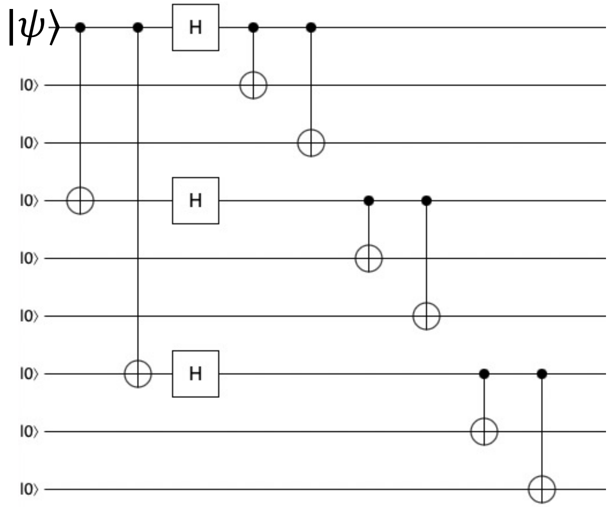
- Target: to handle phase and bit flips simultaneously!
- Idea: (2-level encoding)
  bottom level = repetition code for bit flip,
  top level = repetition code for phase flip on top of the 1st level code



- This is the Shor 9-qubit code:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \mapsto |\psi_C\rangle \propto \alpha(|000\rangle + |111\rangle)^{\otimes 3} + \beta(|000\rangle - |111\rangle)^{\otimes 3}$$

"It's me again who saves the day ..."



Circuit for encoding in Shor's code

Construction of the Shor code

- How the Shor code is derived:
  bottom level = repetition code for bit flip $\left|\tilde{0}_L\right\rangle = |000\rangle, \left|\tilde{1}_L\right\rangle = |111\rangle$.
  top level = repetition code for phase flip on top of the bottom level code:
  $$|0_L\rangle = |\tilde{+}_L\rangle|\tilde{+}_L\rangle|\tilde{+}_L\rangle, |1_L\rangle = |\tilde{-}_L\rangle|\tilde{-}_L\rangle|\tilde{-}_L\rangle,$$
  with $\left|\tilde{\pm}_L\right\rangle := \frac{1}{\sqrt{2}}\left(\left|\tilde{0}_L\right\rangle \pm |\tilde{1}_L\rangle\right)$.
- Therefore, we obtain the Shor 9-qubit code:
  $$|0_L\rangle = \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)^{\otimes 3}$$
  $$|1_L\rangle = \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle)^{\otimes 3}$$
- How to correct errors with the Shor code?

Exercise: Show how the 9-qubit code can correct any single-qubit X, Z error, and work out the syndrome measurement.

Stabilizer formalism of error correction

- To construct a QEC code, we first find a set of commuting Pauli strings $\{S_i\}$ as the stabilizers.
- The codewords are designed to be the $(+1)$-eigenstates of all $\{S_i\}$.
- An erroneous state (subject to a correctable error) is still an eigenstate but with some of the eigenvalues changed to -1.
- The syndrome detection = measuring the stabilizers.

  Stabilizers can be measured via the Hadamard tests.

  These tests will not disturb each other
  (i.e., the order of execution does not matter).
- Errors will be identified and corrected.

Stabilizers for the Shor code

	1	2	3	4	5	6	7	8	9
S_1	Z	Z							
S_2		Z	Z						
S_3				Z	Z				
S_4					Z	Z			
S_5							Z	Z	
S_6								Z	Z
S_7	X	X	X	X	X	X			
S_8				X	X	X	X	X	X

Empty entries $= I$

They are independent!

$S_iS_j = S_jS_i$ for any i, j

$= \widetilde{X_1}$ after the first layer of encoding

Exercise: Verify that the stabilizers commute with each other.

Correct an X error in the Shor code

- First consider bit flip errors.
- The syndrome detection for bit flips for the Shor code is just 3 syndrome detection for the 3-qubit repetition code, applied to qubits $\{1,2,3\}, \{4,5,6\}, \{7,8,9\}$, respectively.
- If a bit flip, e.g., X_3 occurs, we get $\langle Z_2 Z_3 \rangle = -1$ while other stabilizers are measured to $+1$.

Exercise: Show this fact.

- Based on this, we can perform X on the 3rd qubit to correct the error.
- In general, observe that the encoded state, under a single X error, remains a joint eigenstate of $Z_1 Z_2, Z_2 Z_3, Z_4 Z_5, Z_5 Z_6, Z_7 Z_8, Z_8 Z_9$. The syndrome detection can be done via 6 Hadamard tests:
- What about phase flip errors?

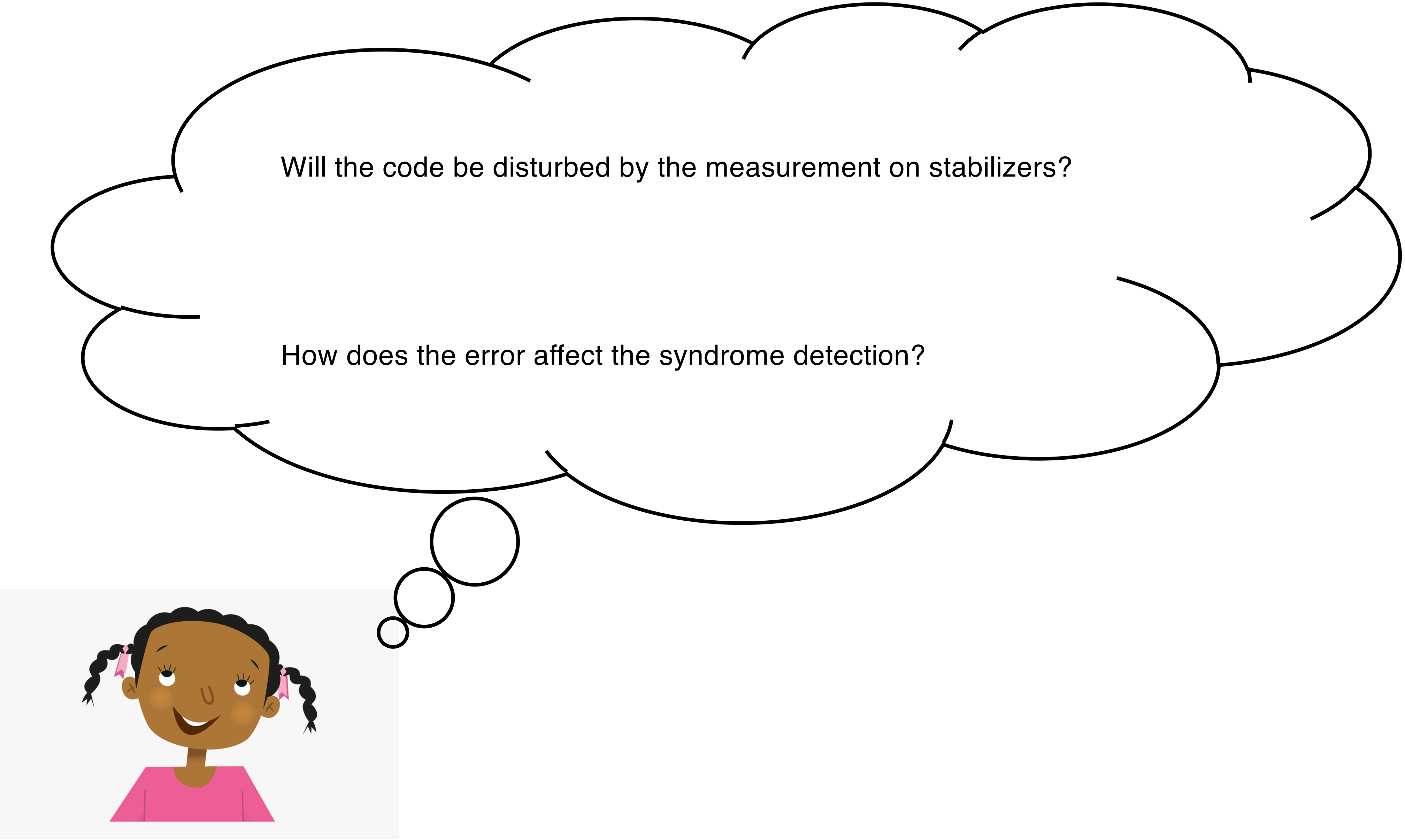
Correct a Z error in the Shor code

- Let us now consider phase flip errors.
- Observe that the codeword $|\psi_C\rangle = \alpha|0_L\rangle + \beta|1_L\rangle$, under a single Z error, remains a joint eigenstate of $X_1X_2X_3X_4X_5X_6$ and $X_4X_5X_6X_7X_8X_9$. The syndrome detection can be done via 2 Hadamard tests for these 2 observables.
- For example, if Z_2 occurs, we have

$$\langle X_1X_2X_3X_4X_5X_6\rangle = -1$$
$$\langle X_4X_5X_6X_7X_8X_9\rangle = +1$$

- Then, we can apply Z to any of the first 3 qubits to correct the error.

Show that Z_1 and Z_2 errors have the same syndrome. Further show that we can still properly correct them.



Will the code be disturbed by the measurement on stabilizers?

How does the error affect the syndrome detection?

- Question 1: Will the stabilizer measurements disturb each other?

- Answer: No!

- The stabilizers commute with each other (e.g., $[Z_1Z_2, Z_2Z_3] = 0$ for the repetition code) and can be measured simultaneously without disturbing each other.
- The measurements are Hadamard tests that does not disturb the code state.

- Question 2: What if an error occurs?
- Answer: An error (X or Z) either commutes or anti-commutes with the stabilizers.

Recall: $XZ = -ZX$

- $|\psi_L\rangle$ is a-$(+1)$ eigenstate of all stabilizers $\{S_i\}$.
  Now an error, e.g., Z_j, happens. The code state is $E|\psi_L\rangle$.
- For any S_i, since $S_iE = ES_i$ or $S_iE = -ES_i$, we have
  $S_i(E|\psi_L\rangle) = \pm ES_i|\psi_L\rangle = \pm(E|\psi_L\rangle)$.

Since $S_i|\psi_L\rangle = |\psi_L\rangle$

- The erroneous state $E|\psi_L\rangle$ is still an eigenstate of all $\{S_i\}$.
- Therefore, we can measure the stabilizers without disturbing it!

Example

- Suppose a phase-flip error happens at the 5th qubit, i.e., $E = Z_5$.
- 8 stabilizers:

$$X_1X_2X_3X_4X_5X_6, X_4X_5X_6X_7X_8X_9, Z_1Z_2, Z_2Z_3, Z_4Z_5, Z_5Z_6, Z_7Z_8, Z_8Z_9.$$

- The error commutes with all the Z-stabilizers, e.g., Z_1Z_2, Z_4Z_5.
- The error anti-commutes with both X-stabilizers $X_1X_2X_3X_4X_5X_6, X_4X_5X_6X_7X_8X_9$. Because $X_1X_2X_3X_4X_5X_6Z_5 = X_1X_2X_3X_4(X_5Z_5)X_6 = X_1X_2X_3X_4(-Z_5X_5)X_6 = (-1)Z_5X_1X_2X_3X_4X_5X_6$
- Syndrome detection + correction:
  - $\langle X_1X_2X_3X_4X_5X_6\rangle = \langle X_4X_5X_6X_7X_8X_9\rangle = -1 \Rightarrow$ apply a Z to the 5th qubit.
  - The other stabilizers → $+1 \Rightarrow$ no correction needed.

Exercise: Show that the same syndrome appears for the errors Z_4 and Z_6. Both errors can be corrected in the same way as we did for Z_5.

Summary of the Shor code

- The Shor code is a 9-qubit code that is the concatenation of two repetition codes, one for X errors and the other for Z errors.

- Error correction capability:
  The Shor code can correct a single X error or a single Z error happened to any of the 9 physical qubits.

- Syndrome detection:
  --- consists of 8 Hadamard tests for the stabilizers:

$$X_1X_2X_3X_4X_5X_6, X_4X_5X_6X_7X_8X_9, Z_1Z_2, Z_2Z_3, Z_4Z_5, Z_5Z_6, Z_7Z_8, Z_8Z_9.$$

Part III:
Effectiveness of QEC

Are quantum errors just X and Z?

No!
For instance, it can be a unitary U that is not X, Z.

Then how can we correct other errors?

If we can correct $A, B, C, \ldots$ we can correct any linear span of $A, B, C, \ldots$

Correcting Y error

- For concreteness, let us consider the Shor code, but the argument here works for any code.
- Question: can we correct the Pauli Y error with the Shor code?
- Suppose Y_1 occurs in the (9-qubit) Shor code: $|0/1_L\rangle = \frac{1}{2\sqrt{2}}(|000\rangle +/- |111\rangle)^{\otimes 3}$.
- Observation: $Y = iXZ$, and Y_1 is (up to a global phase) Z_1 followed by X_1.
- When a phase flip and a bit flip happen to the same qubit in the Shor code, one round of syndrome detection + correction will first correct the bit flip and then the phase flip.

Exercise: Verify this for Y_1.

- Therefore, the Shor code is robust against a single Y error at any one of the 9 physical qubits.

Correcting Continuous Rotations

- Quantum errors can even be more general than X, Y, Z.
- Suppose a continuous rotation $R_Z(\theta)$ occurs on the kth qubit of codeword:

$$R_{Z,k}(\theta)|\psi_C\rangle = \cos\frac{\theta}{2}|\psi_C\rangle - i\sin\frac{\theta}{2}Z_k|\psi_C\rangle$$

- Applying the syndrome detection gate U_{synd} :
  Before the measurement of the syndrome, we get

Ancilla state corresponding to the outcome "no error"

Computational basis of the multi-qubit ancilla.

$$U_{\text{synd}}R_{Z,k}(\theta)|\psi_C\rangle|0\rangle = \cos\frac{\theta}{2}|\psi_C\rangle|I\rangle - i\sin\frac{\theta}{2}Z_k|\psi_C\rangle|Z_k\rangle.$$

Ancilla state corresponding to the outcome "Z error at qubit k"

- Measuring the ancilla collapses the state; 2 cases:
  1. With prob. $\left(\cos\frac{\theta}{2}\right)^2$ we get $|\psi_C\rangle$, and no correction is needed!
  2. With prob. $\left(\sin\frac{\theta}{2}\right)^2$ we get $Z_k|\psi_C\rangle$, and we can get back $|\psi_C\rangle$ by applying Z_k.
- Either way, we can correct the error perfectly! $R_{Z,k}(\theta)$ (for any θ) is not a problem.
- Similarly, we can also correct $R_{X,k}(\theta)$.

Correcting general errors

- **Theorem:**
  If a quantum error correction code corrects errors $A_1, \ldots, A_k$, it also corrects any linear combination $\alpha_1 A_1 + \cdots + \alpha_k A_k$ of them.
- Facts:
  1. The Shor 9-qubit code can correct single-qubit X, Z
  2. (Implied by step 1) Shor 9-qubit code can also correct single-qubit Y.
  3. (Linear algebra) Any 2×2 unitary can be written as $\alpha I + \beta X + \gamma Y + \delta Z$.
- **Corollary:**
  The Shor 9-qubit code can correct any single-qubit error[*]!

$*$: In fact, single-qubit errors are a bit more general than random unitaries, but our argument still works ~

Correcting small errors on every qubit

- Suppose there is a small error $U_\epsilon = I + \epsilon X$ (or Y, Z) on every qubit, instead of on one of them. The overall error effect is $U_\epsilon^{\otimes n}$.
- Observe that (by Taylor expansion)

$$U_\epsilon^{\otimes n} = I^{\otimes n} + \underbrace{\epsilon(E_1 + E_2 + \cdots + E_n)}_{\text{Correctable single-qubit errors.}} + O(\epsilon^2)$$

- The Shor 9-qubit code can still correct the error very well, up to a tiny term that scales at most as ϵ^2!

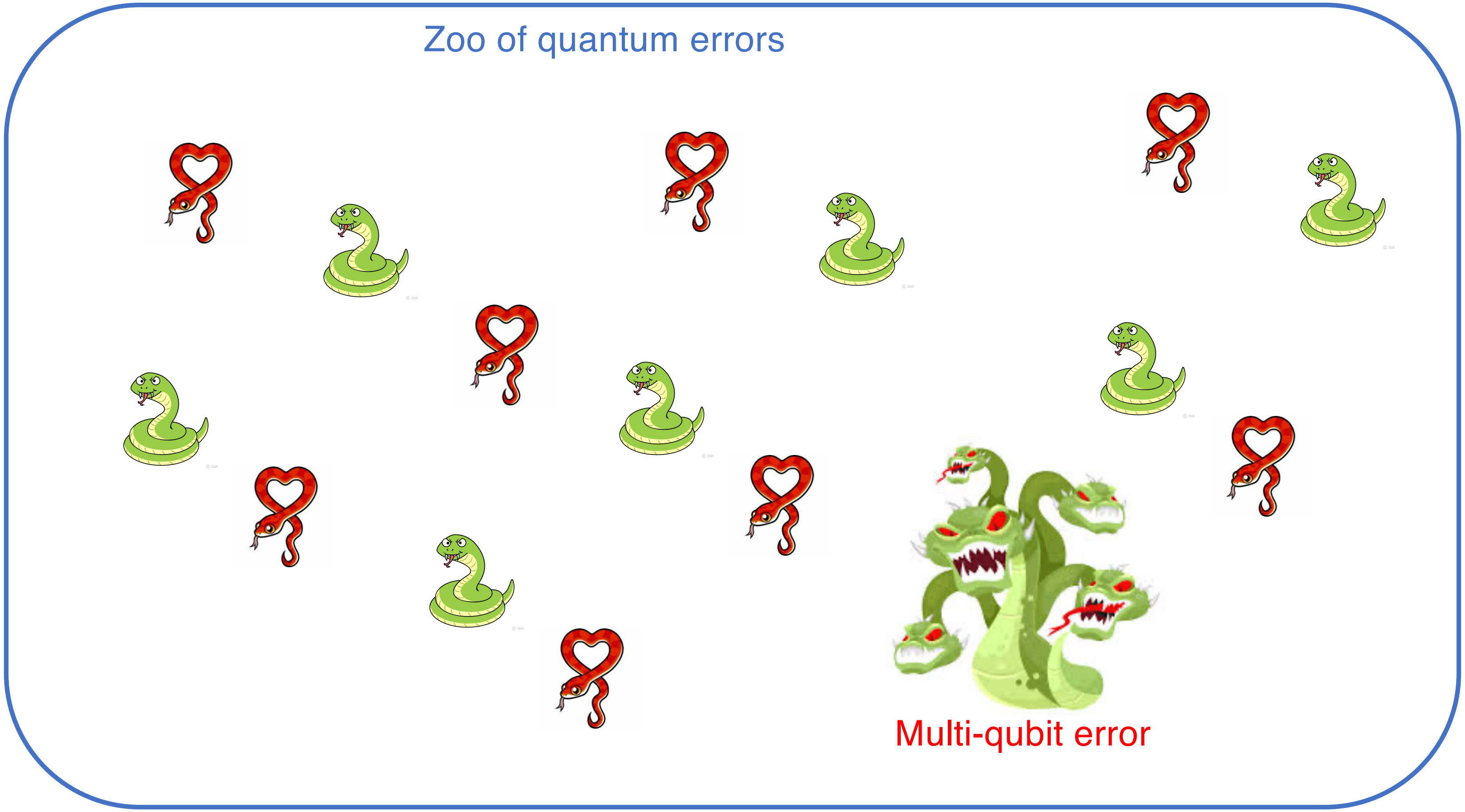
What if more than one error occur?

- The Shor 9-qubit code:
  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \mapsto |\psi_C\rangle \propto \alpha(|000\rangle + |111\rangle)^{\otimes 3} + \beta(|000\rangle - |111\rangle)^{\otimes 3}$
  can correct a single error X or Z happened to any of its 9 physical qubits.
- It cannot correct all k-qubit errors with $k \geq 2$.

- For instance, suppose the original state is in the logical zero:
  $$|0_L\rangle \propto (|000\rangle + |111\rangle)^{\otimes 3}.$$
  Now, if Z_1Z_4 (i.e., phase to the 1st and 4th qubits) happens, the state will be $\propto (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle + |111\rangle)$.

- The syndrome detection will mistakenly conclude that Z_7, Z_8 or Z_9 happened, and apply a phase flip to one of the last registers. We then get $\propto (|000\rangle - |111\rangle)^{\otimes 3}$ which is the logical one.

- Luckily, as discussed previously, multi-qubit errors are much rarer if our qubits have high enough quality (error effect: $U_\epsilon^{\otimes n}$ for $\epsilon \ll 1$)



Zoo of quantum errors

Multi-qubit error

So … my code corrects all single-qubit errors, but collapses when there are more than 2 Pauli errors happening simultaneously.

Don’t be sad, my friend ~

First, there is a way to make a code more powerful and more robust.

Second, this is a law of nature rather than a technical drawback … There is no error correction code that corrects all errors.

For both, please follow our next lecture on fault-tolerance!

The Steane code

- The Shor code is not the only QEC code. Consider the encoding:

$$|0_L\rangle = \frac{|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle + |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle}{2\sqrt{2}}$$

$$|1_L\rangle = \frac{|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle + |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle}{2\sqrt{2}}$$

- It has 7 physical qubits, 1 logical qubit, and correct 1-qubit errors. Its syndrome detection is defined by the following observables:

	1	2	3	4	5	6	7
S_1				Z	Z	Z	Z
S_2		Z	Z			Z	Z
S_3	Z		Z		Z		Z
S_4				X	X	X	X
S_5		X	X			X	X
S_6	X		X		X		X

- It is obtained by a more general procedure of “code concatenation” (it is an example of **CSS codes**) beyond this course.
- It will replace the Shor code and be our focus in the next lecture.

Summary

- In quantum error correction, it is enough to consider the bit (flip) error X and the phase (flip) error Z!
- In practice, errors are more likely to involve only a single or a few qubits at each time.
- The Shor 9-qubit code (and, similarly, other codes) can:

1. Correct any single-qubit error. ✅
2. Correct small errors that happen simultaneously on multiple qubits. ✅
3. Detect errors and correct them without collapsing the state or deteriorating its quantum information. ✅

- We assumed that the encoding/decoding, syndrome detection and correction do not generate extra errors. In practice, this is a strong assumption (see Lecture 9).

Homework

- Review the lecture slides;

  you may find the review questions in the next slides helpful.

  Try the exercises in the slides and discuss with your classmates.

- Review the Linear Algebra Note (bonus material)

- Attempt Q3 and Q4 in Assignment 3.

- Optional: Read p426-434 of *Quantum Computation and Quantum Information* by Nielsen and Chuang.

Review questions

- What is the difference between physical and logical qubits?
- Try to recover the proof of no-copying theorem by yourself.
- In the syndrome detection for the 3-qubit repetition code, why can't we introduce 3 (instead of 2) ancillary qubits, and do 1 CNOT on each pair of 1 code qubit + 1 ancillary qubit (in total 3 CNOTs)?
  (That is, can't we measure Z_1, Z_2, Z_3?)
- Why must the stabilizers commute with each other? What if they do not?
- To detect errors, we made (syndrome) detection, which extracts information about a quantum state. Why (and under what condition) can we do this without collapsing the state?

Part III*: Stabilizer formalism

– a general recipe for finding more QECCs

*: bonus content

(Warning: advanced math ahead)

OK. Quantum error correction codes are indeed cool and important …

But are there any more codes than the 9-qubit, and how do we find them?

We need a general formalism called the stabilizer formalism!

The Pauli group

- The Pauli group P_n on n qubits is defined to be the set of operations generated by $\{X_i, Z_i, Y_i : i = 1,2, \ldots, n\}$. (Note that $Y = iXZ$.)
- Group is a set $G = \{g_1, g_2, \ldots\}$ with a “multiplication” operation satisfying:
  1. Closure: $g_1 g_2 \in G$ for any $g_1, g_2 \in G$.
  2. Associativity: $(g_1 g_2) g_3 = g_1 (g_2 g_3)$
  3. Identity: there is an element $e \in G$ such that $eg = ge = g$ for any $g \in G$
  4. Inverse: for any $g \in G$ there is a $g \in G^{-1}$ such that $gg^{-1} = g^{-1}g = e$.
- A group G is generated by elements $g_1, \ldots, g_k$ (denoted by $G = \langle g_1, \ldots, g_k \rangle$) if every $g \in G$ can be represented as a sequence of elements drawn from $\{g_1, \ldots, g_k\}$.
- Example: $\{I, Z_1 Z_2, Z_1 Z_3, Z_2 Z_3\} = \langle Z_1 Z_2, Z_2 Z_3 \rangle$ since $I = (Z_1 Z_2)^2$ and $Z_1 Z_3 = (Z_1 Z_2)(Z_2 Z_3)$.

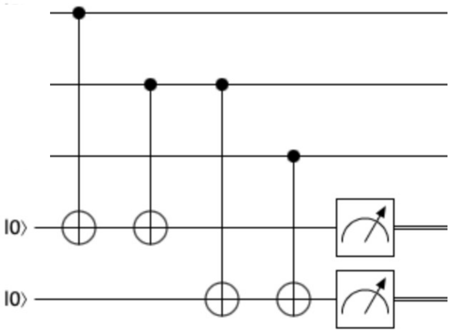
The Pauli group

- The Pauli group P_n on n qubits is defined as $P_n \coloneqq \langle X_1, Z_1, Y_1, \ldots, X_n, Z_n, Y_n \rangle$.
- P_n contains all operators of the form $X \otimes Y \otimes X \otimes I \otimes Z \otimes \cdots$ up to a phase $\in \{\pm 1, \pm i\}$. (The phase i comes from $YZX = i$.)
- The weight of any $M \in P_n$ is the number of qubits where M acts as non-identity. For instance, $w(X \otimes I \otimes Z \otimes Y \otimes I) = 3$.
- Fact:
  Any $M, N \in P_n$ either commutes ($MN = NM$) or anti-commutes ($MN = -NM$).

Exercise: Does X commute or anti-commute with Z?
What about $X \otimes X$ and $Z \otimes Z$?

Syndrome detection revisited

- Why does the error syndrome detection for the 3-(qu)bit repetition code work in this way?



= 1st and 2nd qubits have the same parity?

= 2nd and 3rd qubits have the same parity?

- Answer: They are parity checks!
- Consider 2 elements in P_3: $Z_1 Z_2 = Z \otimes Z \otimes I$ and $Z_2 Z_3 = I \otimes Z \otimes Z$.
- A codeword (000/111) is a $+1$ eigenstate of $Z_1 Z_2$ and $Z_2 Z_3$
  An erroneous state (e.g., 101,001) is a -1 eigenstate of $Z_1 Z_2$ or $Z_2 Z_3$.

Syndrome detection revisited

- Similarly, phase error can be detected by $X_1X_2, X_2X_3 \in P_3$. In summary:
  Measuring $X \otimes X$ detects phase flip (Z) errors.
  Measuring $Z \otimes Z$ detects bit flip (X) errors!
- In the Shor 9-qubit code:

	1	2	3	4	5	6	7	8	9
S_1	Z	Z							
S_2		Z	Z						
S_3				Z	Z				
S_4					Z	Z			
S_5							Z	Z	
S_6								Z	Z
S_7	X	X	X	X	X	X			
S_8				X	X	X	X	X	X

$= \widetilde{X_1}$ after the first layer of encoding

Empty entries $= I$

They are independent!

$S_iS_j = S_jS_i$ for any i, j

Stabilizers

- In Shor 9-qubit code:
  - Codewords/Erroneous states are eigenstates of the syndrome observables $S_1, \dots, S_8$, with different eigenvalues.
  - Codewords are stabilized by $S_1, \dots, S_8$ (eigenvalue = +1).
  - Different syndrome observables commute $S_i S_j = S_j S_i$ for any i, j.
  - $S_1, \dots, S_8$ are independent:
    Take any subset, any element outside the subset cannot be generated by elements in the subset.
- Consider $S \subset P_n$ that contains any operator stabilizing all codewords.
- Facts:
  1. $S = \langle S_1, \dots, S_8 \rangle$ is an Abelian group!
  2. By linear algebra, commuting operators can be diagonalized simultaneously.

Exercise: Verify Fact 1.

- This gives us a way to find quantum error correction codes:

A general way of finding quantum error correction codes

- To find an n-qubit code:
  1. Find a subset $\{S_1, \dots, S_m\}$ of P_n, where the elements are independent and commute with each other.
  2. Define the stabilizer group $S \coloneqq \langle S_1, \dots, S_m \rangle$.
  3. Define the codewords to be the (common) $+1$ eigenstates of every element in S.
- Some questions follow:
  1. How large is the code? (i.e., how many logical qubits are there in the code)
  2. What kinds of errors can the code correct?
     ($S = \langle Z_1 \rangle$ is also a stabilizer group but the code cannot correct too many errors.)

Exercise:
Show that it is a bad idea to add the element $-I$ to a stabilizer group. Therefore, we focus on S that does not contain $-I$.

Size of a stabilizer code

- Question:
  Given a stabilizer group $S \coloneqq \langle S_1, \dots, S_m \rangle$ and its associated code, how many logical qubits do we have?
- Dimension of the n-qubit Hilbert space = 2^n.
- Fact: If $-I \notin S$ then the codeword space is 2^{n-m} dimensional.
- The number of logical qubits of a stabilizer code is $n - m$, where m is the number of independent generators of the stabilizer!

Error correction capability

- Question: When is an error uncorrectable?
- For any n-qubit state, measuring the stabilizer (generators) $S_1, \dots, S_m$ yields a binary string $\vec{s} \in (s_1, \dots, s_m) \in \{0,1\}^m$.
- Let $\mathcal{H}_C$ be the code space.
  For any $|\psi\rangle \in \mathcal{H}_C$, we have $\vec{s}(|\psi\rangle) = \vec{1} = (1,1, \dots, 1)$.
- Fact: For any $M \in P_n$, $\vec{s}(M|\psi\rangle)$ is the same for any $|\psi\rangle \in \mathcal{H}_C$.
- Therefore, we can denote by $\vec{s}(M)$ for the outcomes of measuring the stabilizers after an error $M \in P_n$ occurred.
- For instance, $\vec{s}(M) = \vec{1}$ for any $M \in S$.
- What about $M \notin S$?

Error correction capability

Exercise:
Show that $S \subset N(S)$

- Define $N(S) \coloneqq \{g \in P_n : [g, M] = 0\ \forall M \in S\}$ (the centralizer of S).
- For any $M, N \in P_n$:

$$\vec{s}(M) = \vec{s}(N) \Leftrightarrow \left[S_i, M^\dagger N\right] = 0, \forall\, i \Leftrightarrow M^\dagger N \in N(S).$$

  Two errors show the same syndrome if and only if $M^\dagger N \in N(S)$.
  Two errors show different syndromes if and only if $M^\dagger N \notin N(S)$.

- To correct errors in a stabilizer code:
  1. Measure the generators to obtain $\vec{s}$
  2. If $\vec{s} \neq \vec{1}$, apply the inverse of M, where $M \in P_n$ has syndrome $\vec{s}$, for correction.

Since we know only $\vec{s}$ but not the actual error, M is an arbitrary fixed operation.

- The error correction works if $M^\dagger N|\psi\rangle = |\psi\rangle$ for any codeword $|\psi\rangle$.
  In another word, $M^\dagger N \in S$!

Error correction capability

- For error correction to work, it requires $M^\dagger N \in S$ for any errors M, N with the same syndrome!
- In general, two errors show the same syndrome if and only if $M^\dagger N \in N(S)$.
- (Error-correction condition for stabilizer codes)
  A set $\{E_k\} \subset P_n$ of errors are correctable by a stabilizer code S, if and only if $E_j^\dagger E_k \notin N(S) - S$ for any j, k.

Error classification

- For any error $M \in P_n$, there are 3 cases:
    1. (**No correction needed**) If $M \in S$, M has no effect on codewords since $M|\psi\rangle = |\psi\rangle$ for any codeword $|\psi\rangle$. We don't need to do anything!
    2. (**Error can be perfectly corrected**) If $N^\dagger M \notin N(S)$, where N is a fixed recovery operation associated with $\vec{s}(M)$. We can correct M by measuring the stabilizers and applying N!
    3. (**Uncorrectable**) If $N^\dagger M \in N(S) \setminus S,$ M cannot be corrected! For example, $Z_1Z_2Z_3Z_4Z_5Z_6$ is uncorrectable for the Shor 9-qubit code.

$\}$ correctable errors 😎

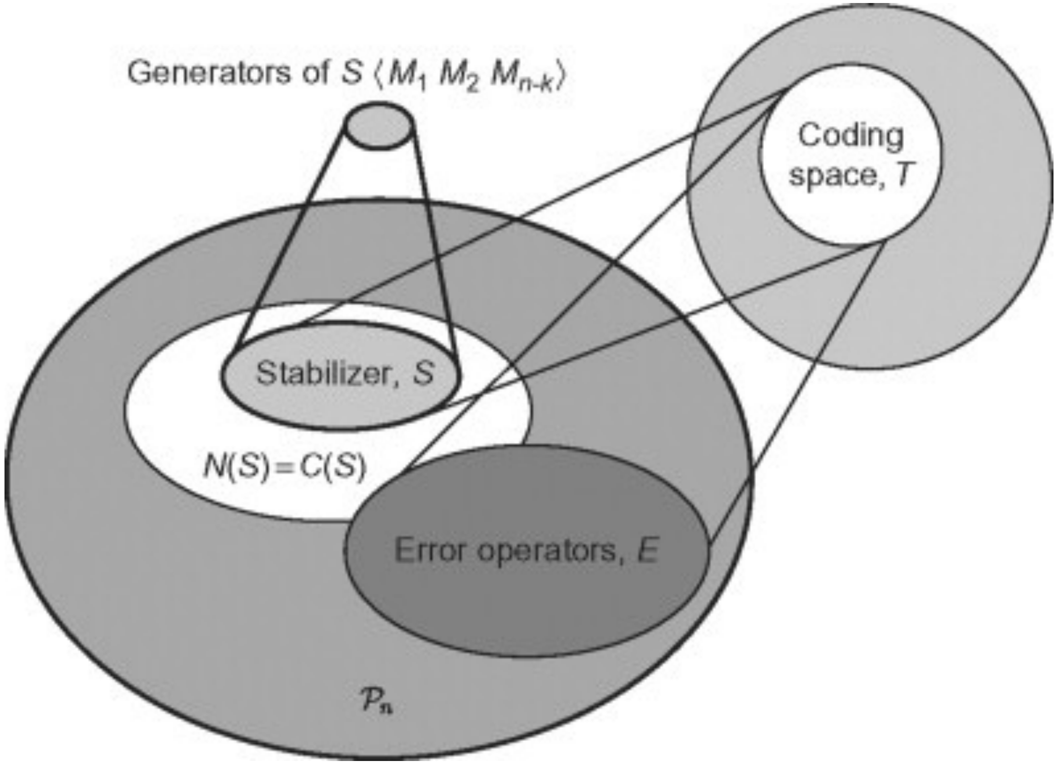
uncorrectable errors 🥲

- Uncorrectable errors are those that are indistinguishable from logical operations.
- As long as you are doing meaningful quantum computations, there must be some uncorrectable errors!

Distance of a stabilizer code

- The distance d of a stabilizer code is the smallest weight of Pauli operator in $N(S) \setminus S$.
- A stabilizer code of distance d will correct $\lfloor (d-1)/2 \rfloor$ errors.
  To correct t-qubit errors, we need distance $2t+1$.
- Why? Because:
  1. an error becomes uncorrectable if it is in $N(S) \setminus S$.
  2. For two arbitrary t-qubit errors N, M, $N^{\dagger}M$ is at most $2t$ qubits.
  3. The errors N, M are correctable if $d > 2t$.

Geometry of stabilizer codes



Example: CSS codes

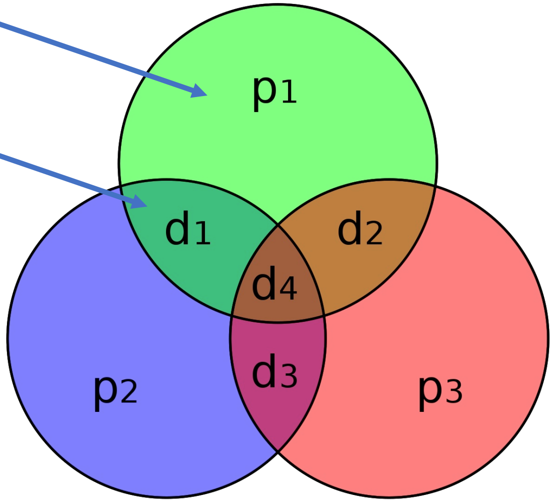
- CSS codes use two classical error correction codes that are concatenated together. One for bit flips and one for phase flips.
- Example: a [[7,1,3]] code (aka the Steane code):
  (We use "[, ,] " ("[[, ,]]") to denote classical (quantum) codes)

	1	2	3	4	5	6	7
S_1				Z	Z	Z	Z
S_2		Z	Z			Z	Z
S_3	Z		Z		Z		Z
S_4				X	X	X	X
S_5		X	X			X	X
S_6	X		X		X		X

1st [7,4,3] Hamming code

2nd [7,4,3] Hamming code

Idea of Hamming [7,4,3]



A parity bit = $d_1 \oplus d_2 \oplus d_4$

A free bit

Example: The smallest code!

- The minimal number of physical qubits in a QEC code is 5.

- This is a [[5,1,3]] code:

	1	2	3	4	5
S_1	X	Z	Z	X	
S_2		X	Z	Z	X
S_3	X		X	Z	Z
S_4	Z	X		X	Z