Gottesman-Knill theorem

- a n-qubit state is a vector that has 2^n components
- its unitary evolution can be described by $2^n \times 2^n$ unitary matrices

→ exponentially large memory and extremely fast processors are required for large n

- How many qubits can we follow on a computer with a 16GB memory?

Gottesman-Knill theorem

- a n-qubit state is a vector that has 2^n components
- its unitary evolution can be described by $2^n \times 2^n$ unitary matrices

→ exponentially large memory and extremely fast processors are required for large n

- How many qubits can we follow on a computer with a 16GB memory?

$2 \cdot 32 \cdot (2^n)^2 < 16 \times 10^9 \times 8$ $\quad \therefore 2^{2n-1} < 10^9$ $\quad$ 1 byte=8 bit

$\therefore (2n-1)\log_{10} 2 < 9$ $\quad \therefore n \leq 15$ $\quad \log_{10} 2 = 0.30$

it is hard to simulate a large quantum system on a classical computer

Gottesman-Knill theorem

- In the Heisenberg representation, n-qubit quantum circuits composed of Clifford gates can be described by following the evolution of at most $2n$ logical operators $\{\bar{X}_1, \ldots, \bar{X}_n, \bar{Z}_1, \ldots \bar{Z}_n\}$
- since each logical operator is a Pauli product with ±, it can be described by $2n+1$ bits $(\pm(i^{\alpha_1\beta_1}X_1^{\alpha_1}Z_1^{\beta_1})\cdots(i^{\alpha_1\beta_1}X_n^{\alpha_n}Z_n^{\beta_n}),\ \alpha_i, \beta_i \in \{0,1\})$

→ the logical operators require at most $2n(2n+1)$ bits

Clifford circuits can be simulated on a classical computer in polynomial time of n

Gottesman-Knill theorem

Any quantum computer performing only Clifford group gates can be perfectly simulated in polynomial time on a classical computer.

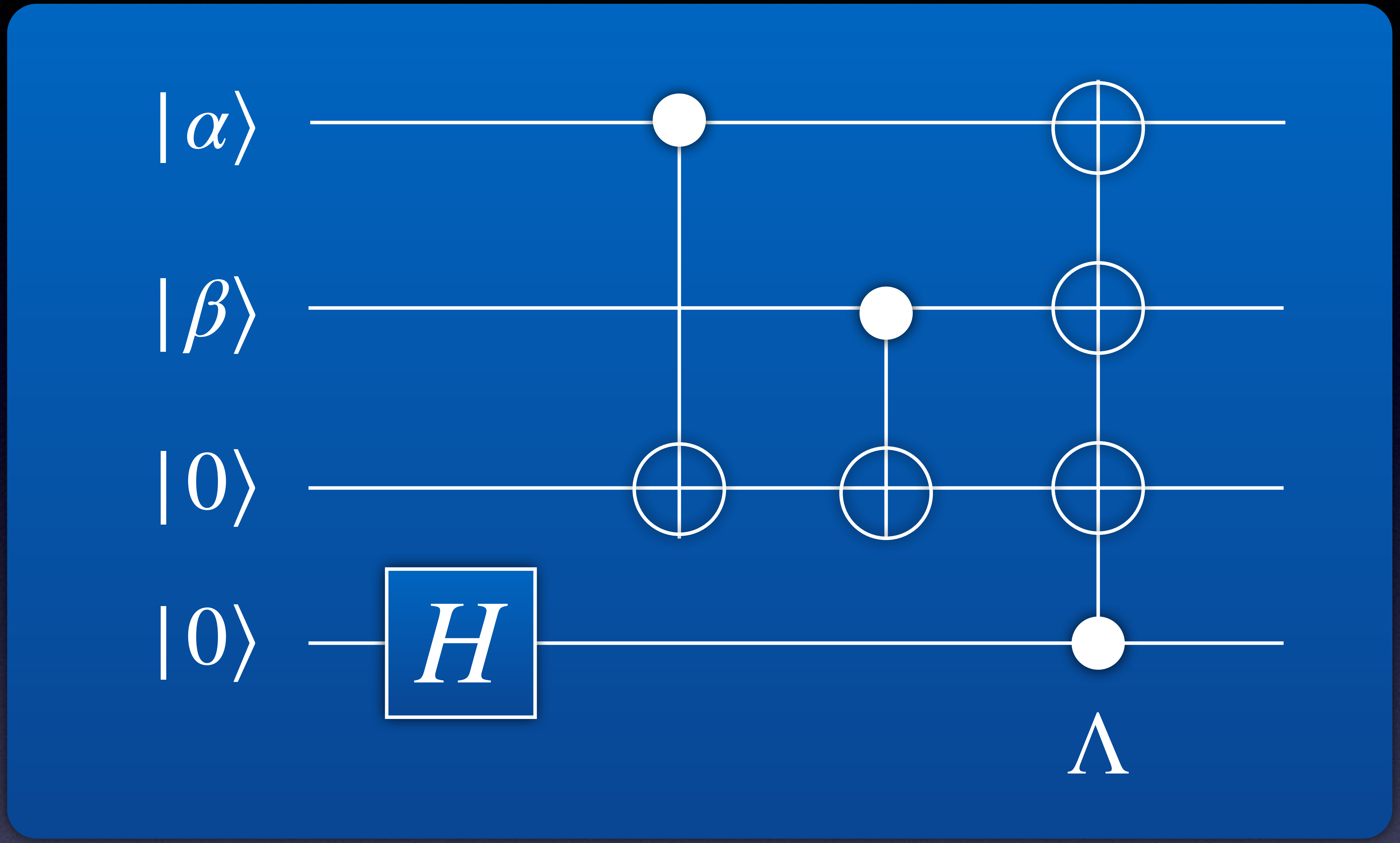
- Clifford group gates do not provide a universal set of gates, e.g., T is outside the Clifford group
- <u>the theorem implies that quantum computation is only more powerful than classical computation when it uses gates outside the Clifford group</u>

Gottesman-Knill theorem

Any quantum computer performing only Clifford group gates can be perfectly simulated in polynomial time on a classical computer.

- however circuits using only Clifford group gates also have a number of important applications in the area of quantum communications - quantum error-correcting codes, quantum teleportation,…

Quantum Error-Correcting codes



start

$IIZI$	$IIZI$	$ZIZI$	$ZZZI$	$ZZZZ$
$IIIZ$	$IIIX$	$IIIX$	$IIIX$	$XXXX$

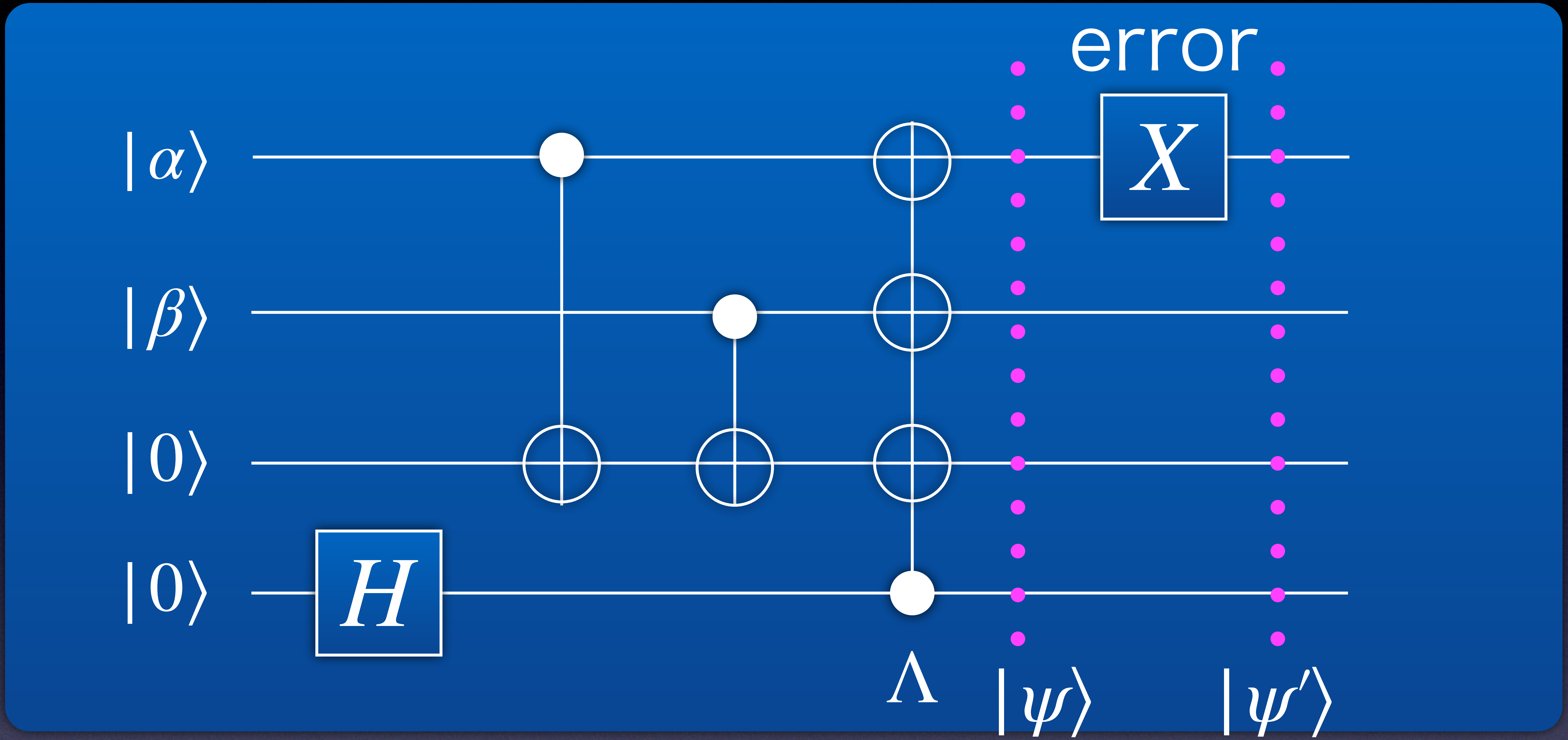
stabilizers

Exercise

Show
$$\Lambda(I \otimes I \otimes I \otimes X)\Lambda = X \otimes X \otimes X \otimes X$$
$$\Lambda(Z \otimes Z \otimes Z \otimes I)\Lambda = Z \otimes Z \otimes Z \otimes Z$$

using $\Lambda = I \otimes I \otimes I \otimes |0\rangle\langle 0| + X \otimes X \otimes X \otimes |1\rangle\langle 1|$

Quantum Error-Correcting codes



Λ	X
$XXXX$	$XXXX$
$ZZZZ$	$-ZZZZ$

$$|\psi'\rangle = X_1|\psi\rangle$$

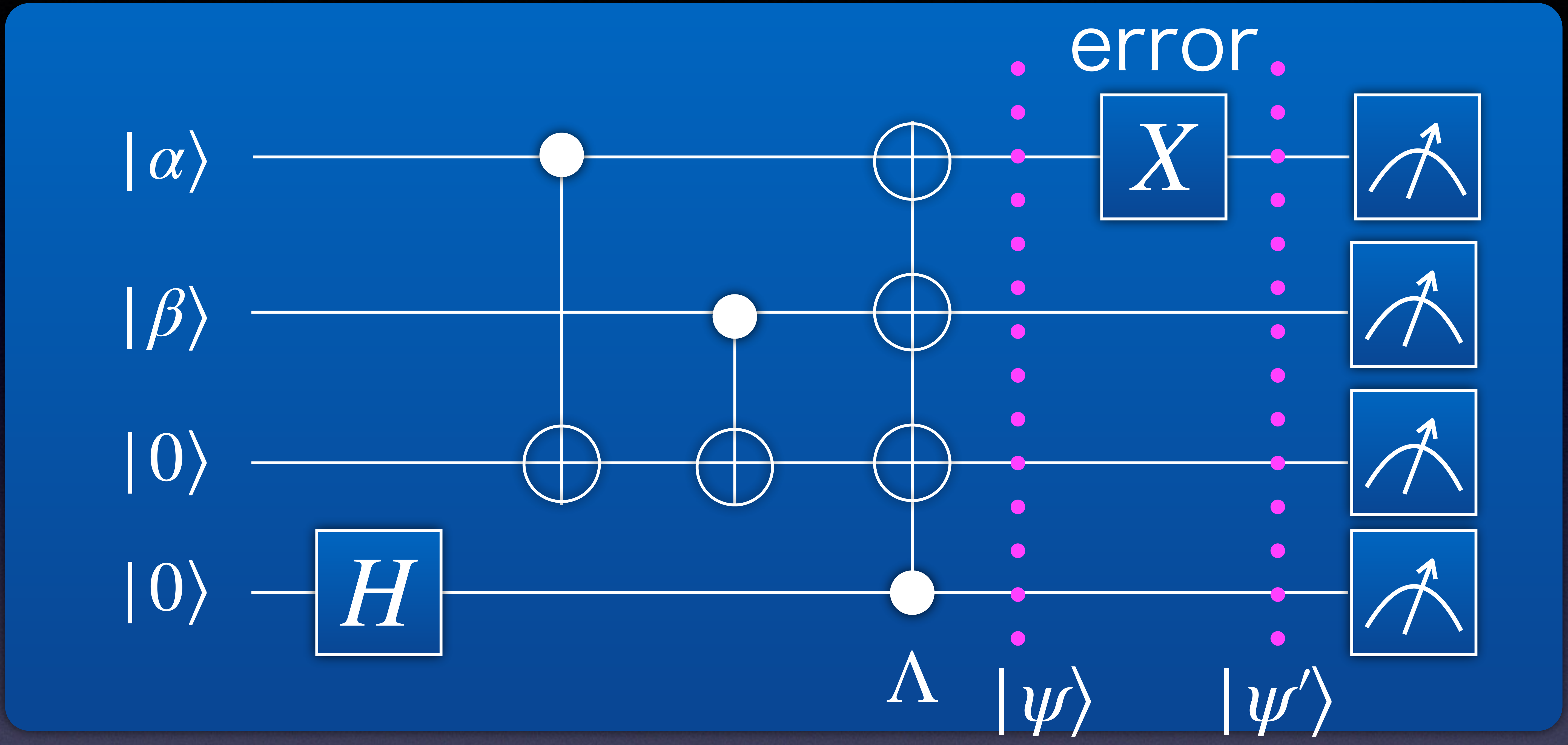
no error

$$XXXX|\psi\rangle = |\psi\rangle$$
$$ZZZZ|\psi\rangle = |\psi\rangle$$

X error

$$XXXX|\psi'\rangle = |\psi'\rangle$$
$$ZZZZ|\psi'\rangle = -|\psi'\rangle \quad \{ZZZZ, XIII\} = 0$$

Quantum Error-Correcting codes



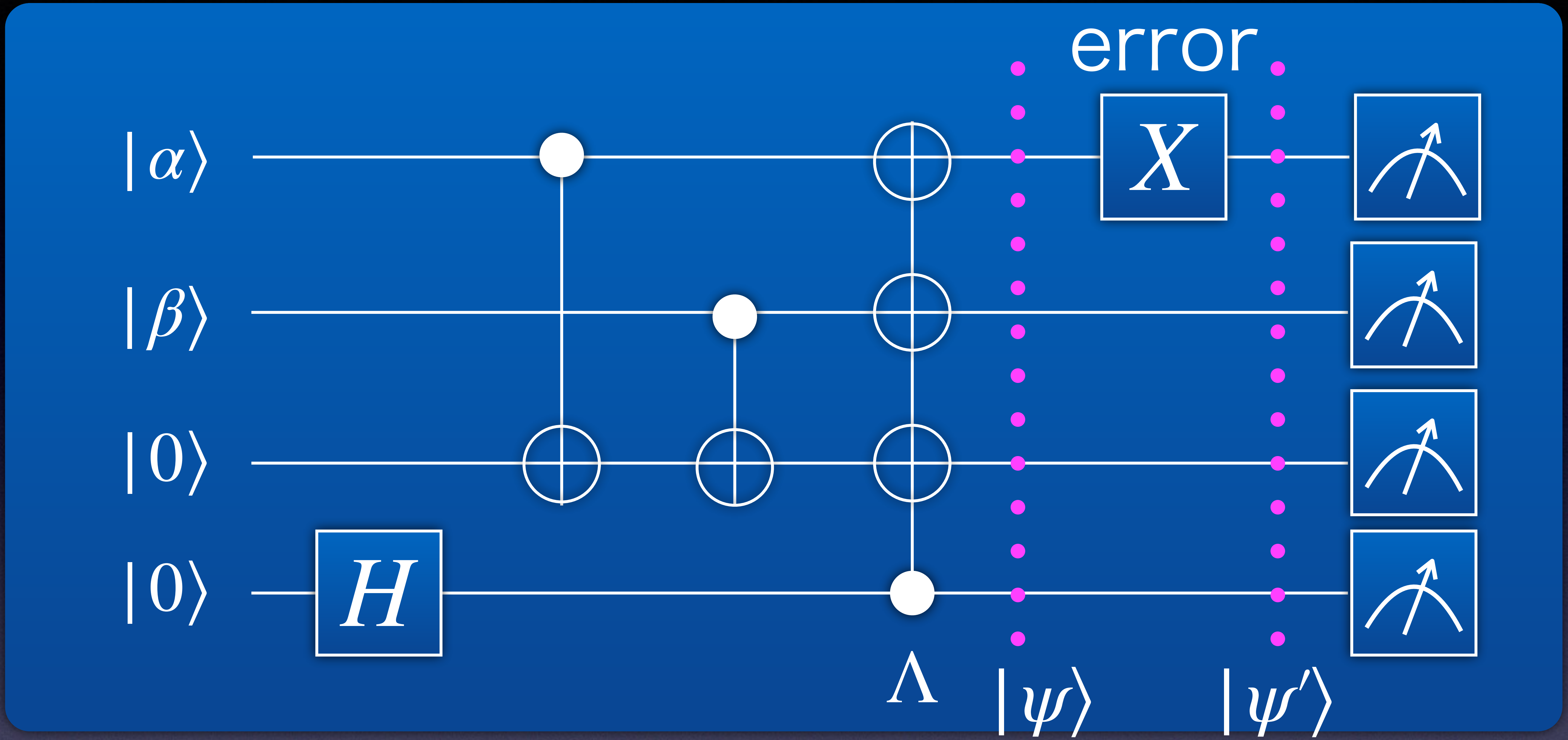
Λ	X
$XXXX$	$XXXX$
$ZZZZ$	$-ZZZZ$

$$|\psi'\rangle = X_1|\psi\rangle$$

	no error	X error
	$XXXX|\psi\rangle = |\psi\rangle$	$XXXX|\psi'\rangle = |\psi'\rangle$
	$ZZZZ|\psi\rangle = |\psi\rangle$	$ZZZZ|\psi'\rangle = -|\psi'\rangle$
outcome of $ZZZZ$	+1	-1

$\{ZZZZ, XIII\} = 0$

Quantum Error-Correcting codes



Λ	X
$XXXX$	$XXXX$
$ZZZZ$	$-ZZZZ$

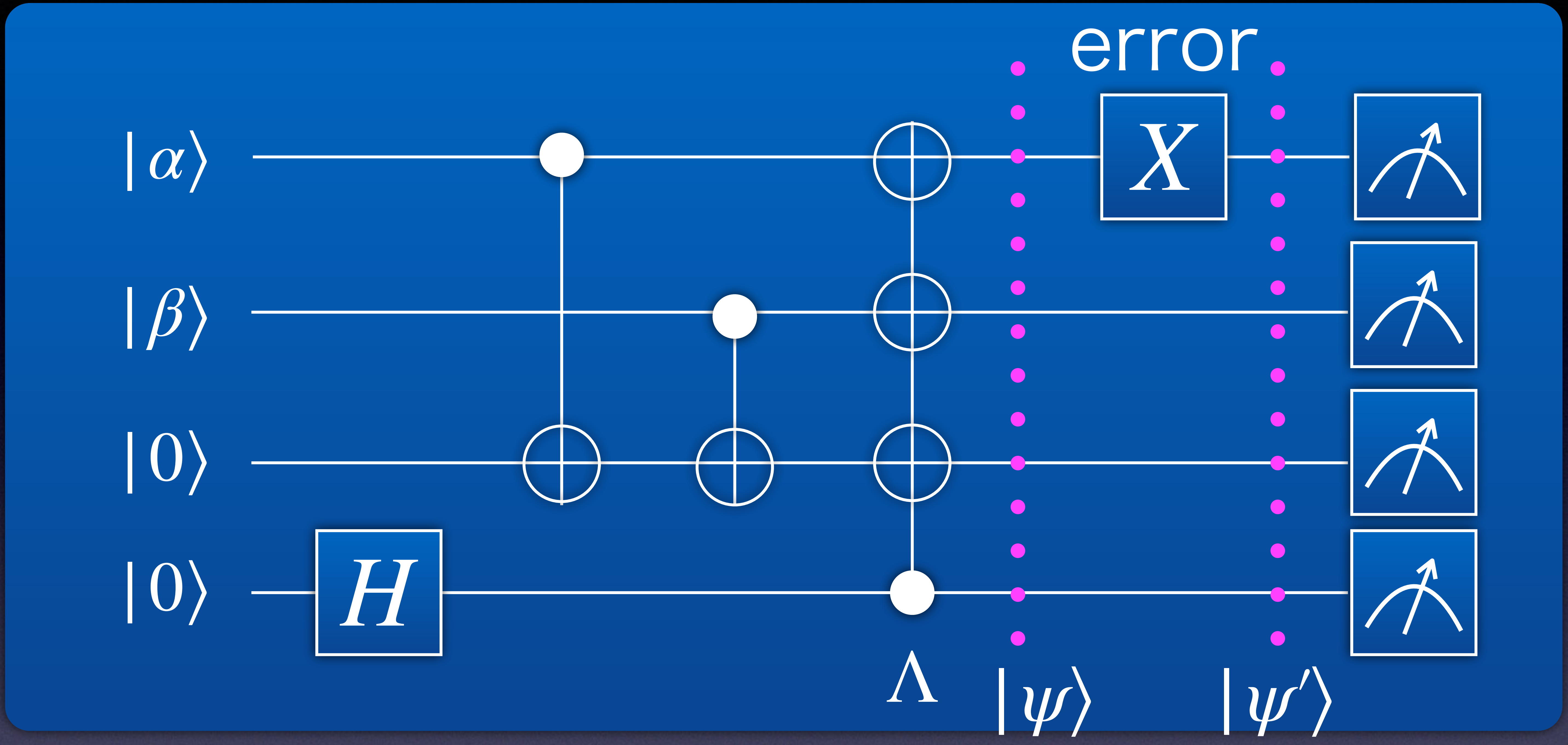
$$|\psi'\rangle = X_1|\psi\rangle$$

	no error	X error
	$XXXX|\psi\rangle = |\psi\rangle$	$XXXX|\psi'\rangle = |\psi'\rangle$
	$ZZZZ|\psi\rangle = |\psi\rangle$	$ZZZZ|\psi'\rangle = -|\psi'\rangle$
outcome of $ZZZZ$	+1	-1

$\{ZZZZ, XIII\} = 0$

an error anticommuting with a stabilizer can be detected !

Quantum Error-Correcting codes



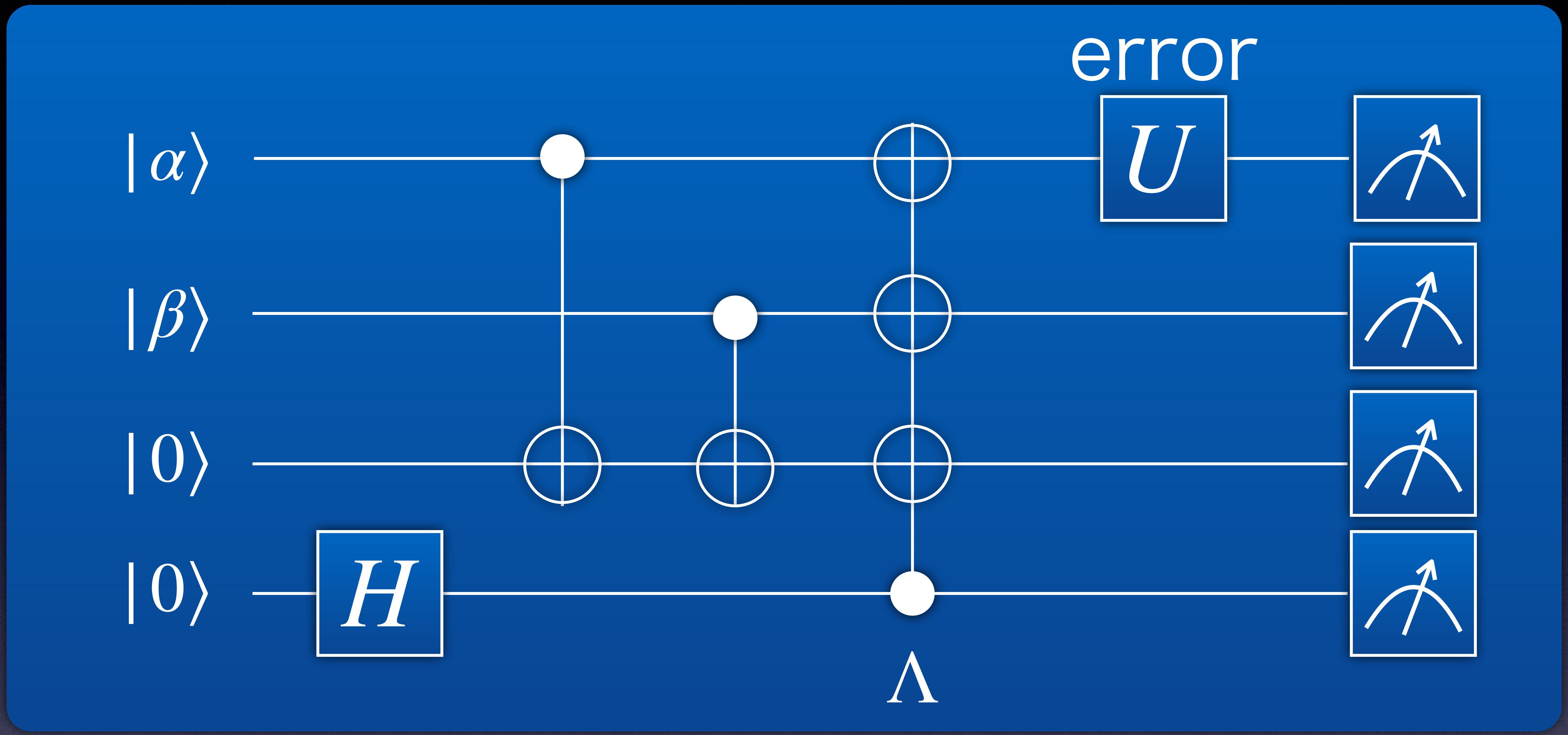
Λ	X
$XXXX$	$XXXX$
$ZZZZ$	$-ZZZZ$

$$|\psi'\rangle = X_1|\psi\rangle$$

	no error	X error
	$XXXX|\psi\rangle = |\psi\rangle$	$XXXX|\psi'\rangle = |\psi'\rangle$
	$ZZZZ|\psi\rangle = |\psi\rangle$	$ZZZZ|\psi'\rangle = -|\psi'\rangle$ $\{ZZZZ, XIII\} = 0$
outcome of $ZZZZ$	+1	-1

the state does not collapse, because it's an eigenstate of the stabilizer!

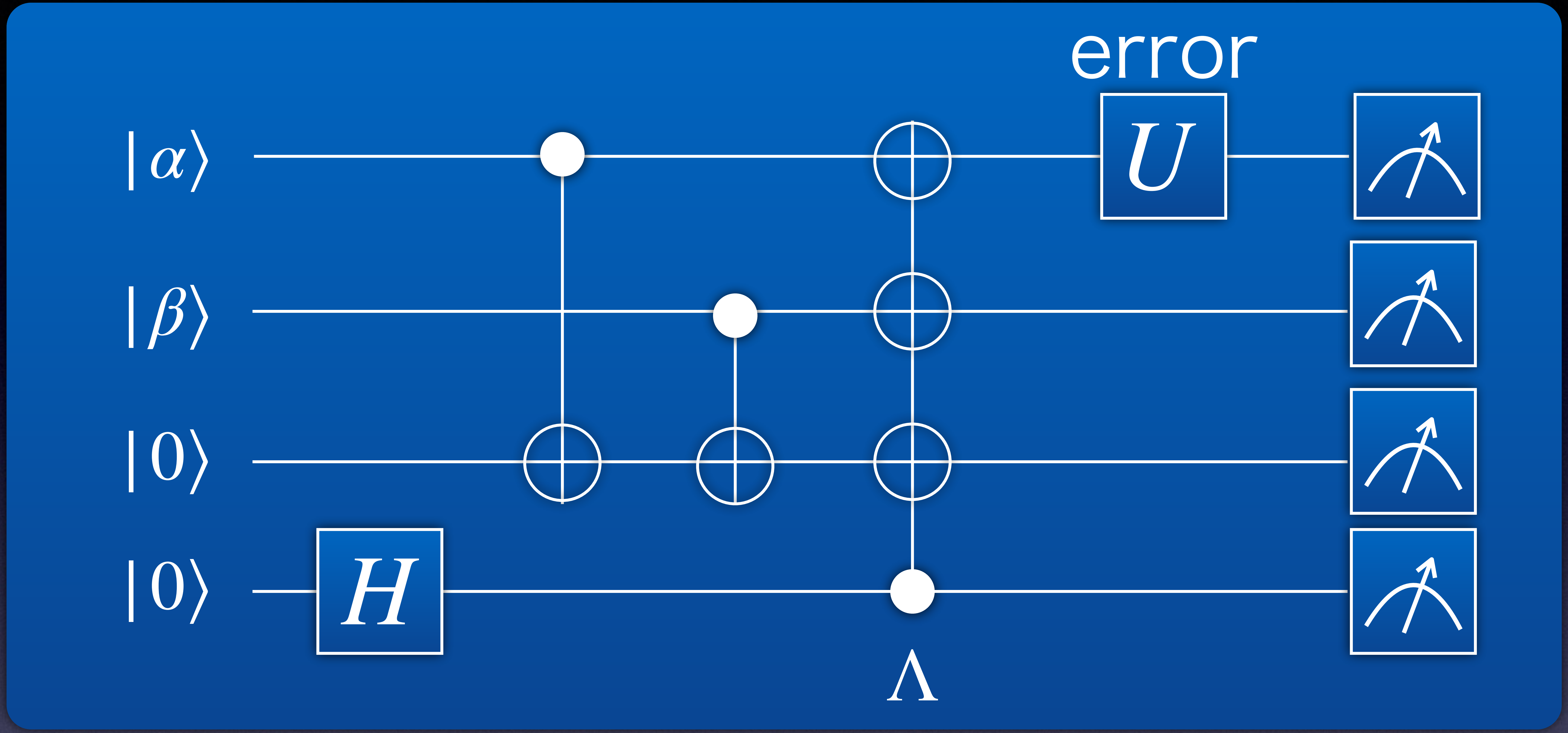
Quantum Error-Correcting codes



	$U = X$	Z	Y
$XXXX$	$XXXX$	$-XXXX$	$-XXXX$
$ZZZZ$	$-ZZZZ$	$ZZZZ$	$-ZZZZ$

- any 1-qubit Pauli error can be detected by stabilizers $XXXX$ and $ZZZZ$
- 2-qubit errors that commute with them cannot be detected 🙆 XZ, YX, 🙅 XX, YY, ZZ

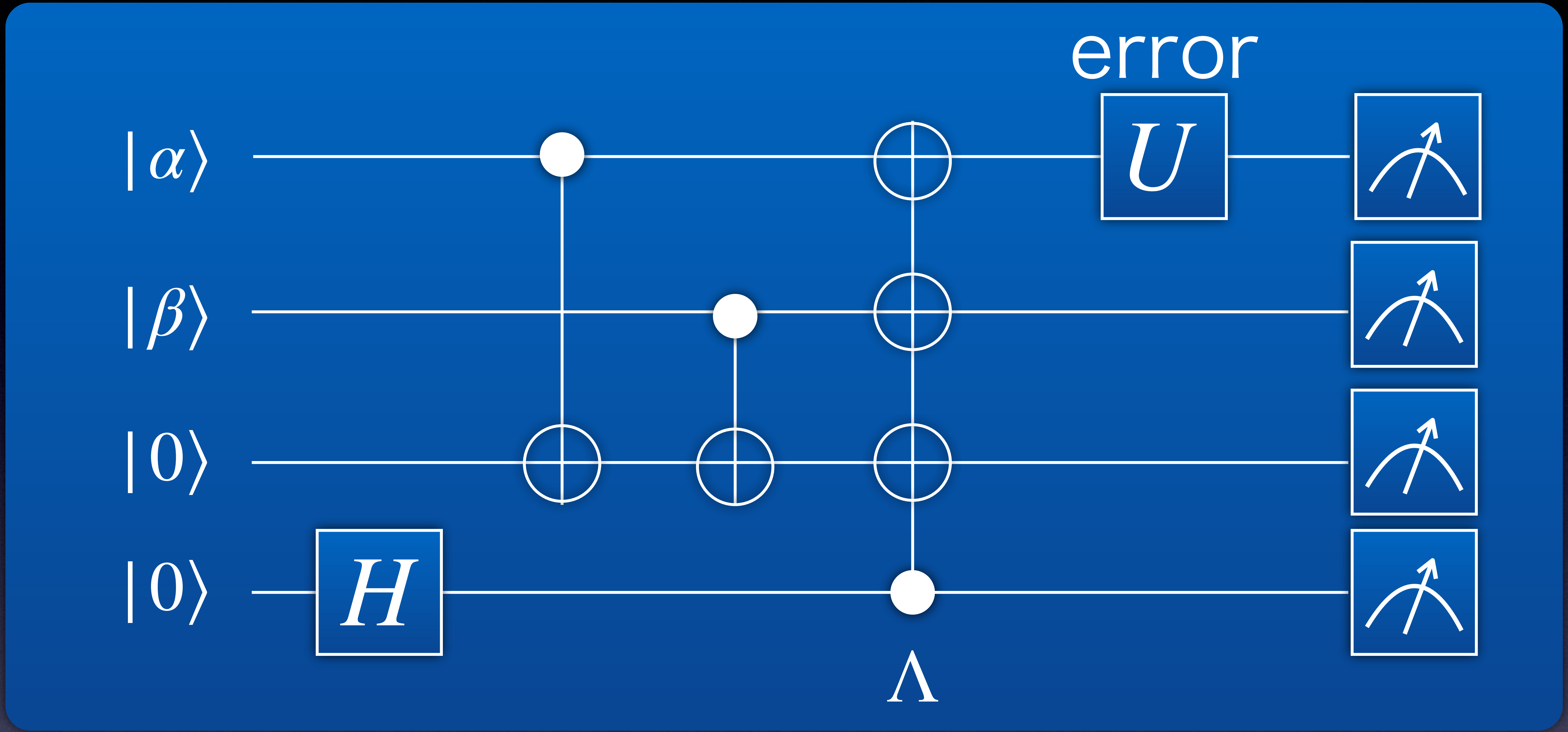
Quantum Error-Correcting codes



general error: $U = aI + bX + cY + dZ$ $\quad |\psi\rangle \rightarrow a|\psi\rangle + bX_1|\psi\rangle + cY_1|\psi\rangle + dZ_1|\psi\rangle$

	$\vert\psi\rangle$	$X_1\vert\psi\rangle$	$Z_1\vert\psi\rangle$	$Y_1\vert\psi\rangle$
$XXXX$	+1	+1	-1	-1
$ZZZZ$	+1	-1	+1	-1

Quantum Error-Correcting codes

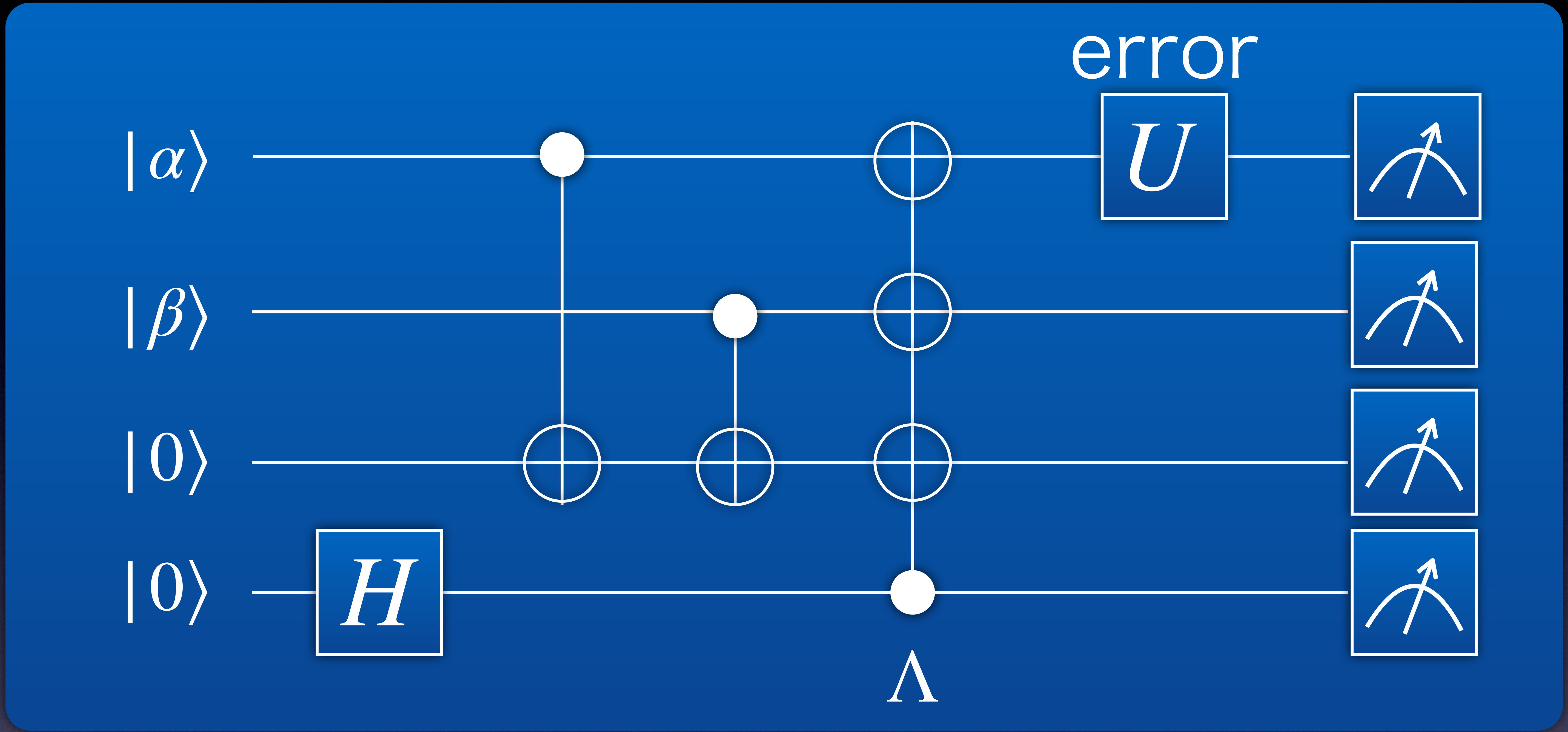


$$|\psi\rangle \to a|\psi\rangle + bX_1|\psi\rangle + cY_1|\psi\rangle + dZ_1|\psi\rangle$$

outcome of $XXXX$	+1	+1	-1	-1
outcome of $ZZZZ$	+1	-1	+1	-1
state after measurement	$\|\psi\rangle$	$X_1\|\psi\rangle$	$Z_1\|\psi\rangle$	$Y_1\|\psi\rangle$

measurement collapses the general error into a Pauli error

Quantum Error-Correcting codes



$$|\psi\rangle \rightarrow a|\psi\rangle + bX_1|\psi\rangle + cY_1|\psi\rangle + dZ_1|\psi\rangle$$

outcome of $XXXX$	+1	+1	-1	-1
outcome of $ZZZZ$	+1	-1	+1	-1
state after measurement	$\|\psi\rangle$	$X_1\|\psi\rangle$	$Z_1\|\psi\rangle$	$Y_1\|\psi\rangle$

general error can be corrected by operating the detected Pauli error!