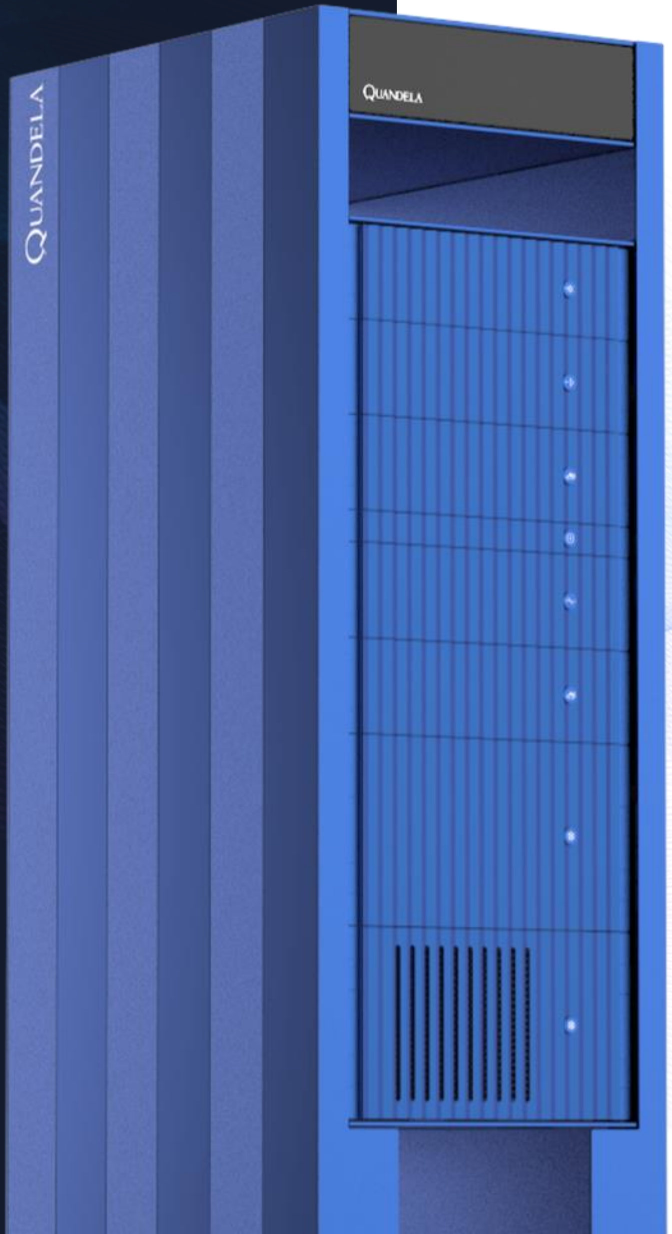
QUANDELA

Lecture on (photonic) fault-tolerant quantum computing

Paul Hilaire

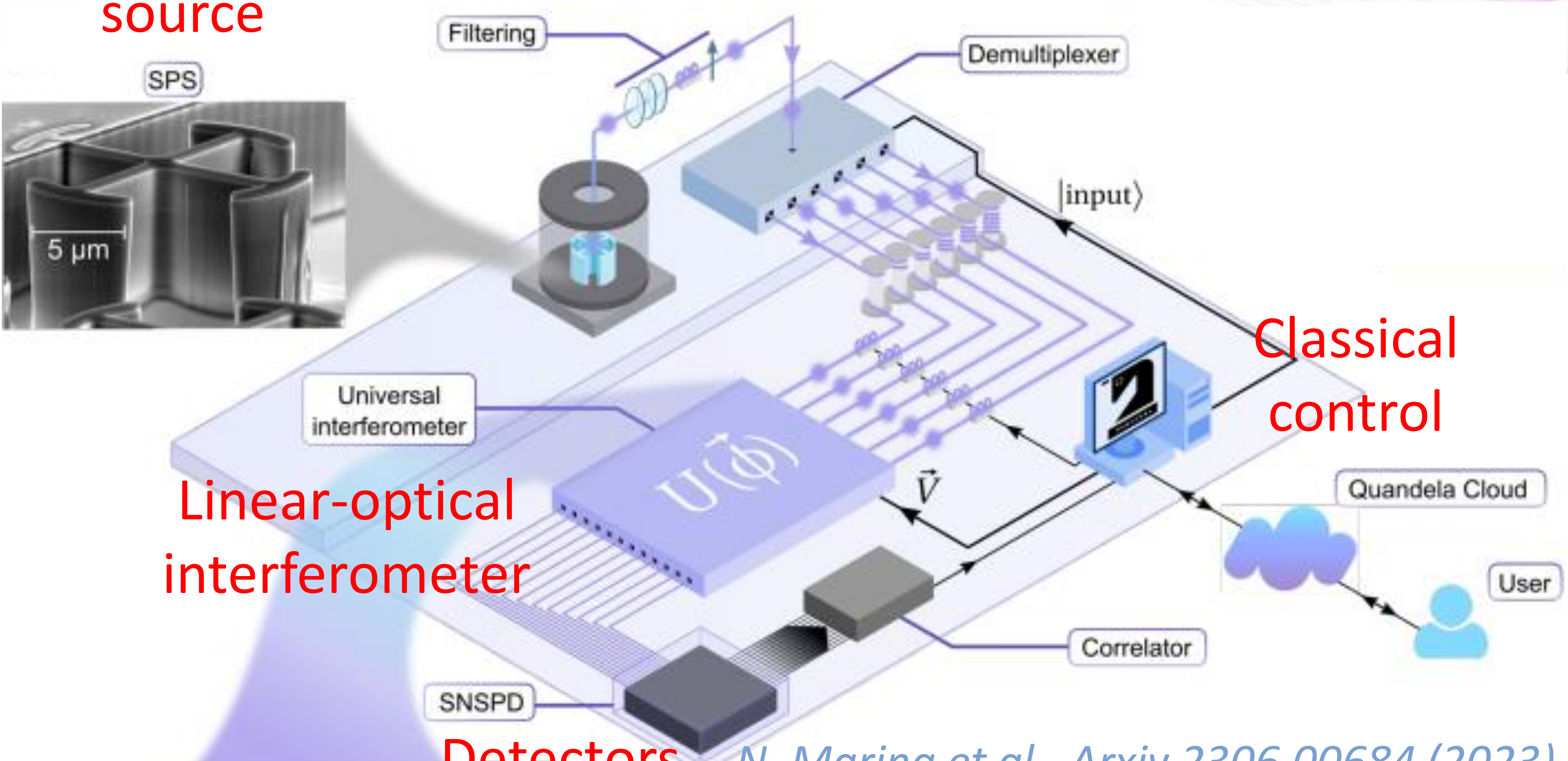


Why do we need fault-tolerant quantum computing?

The inconvenient truth about NISQ…

Current architecture at Quandela

Single-photon source



Classical control

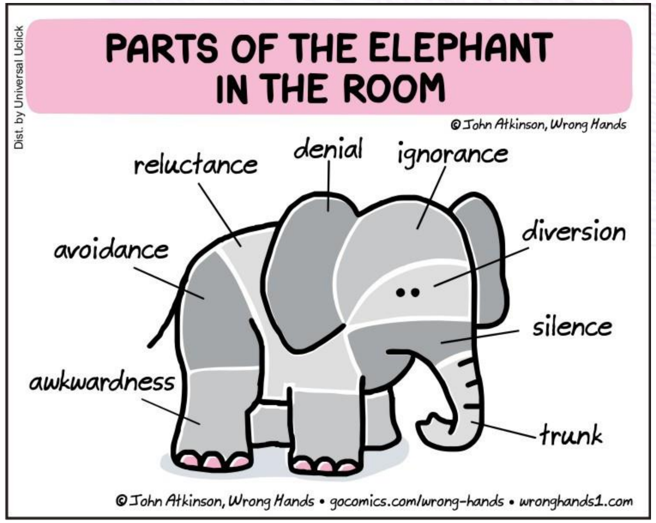
Linear-optical interferometer

Detectors

N. Maring et al., Arxiv 2306.00684 (2023)

Why is it great?

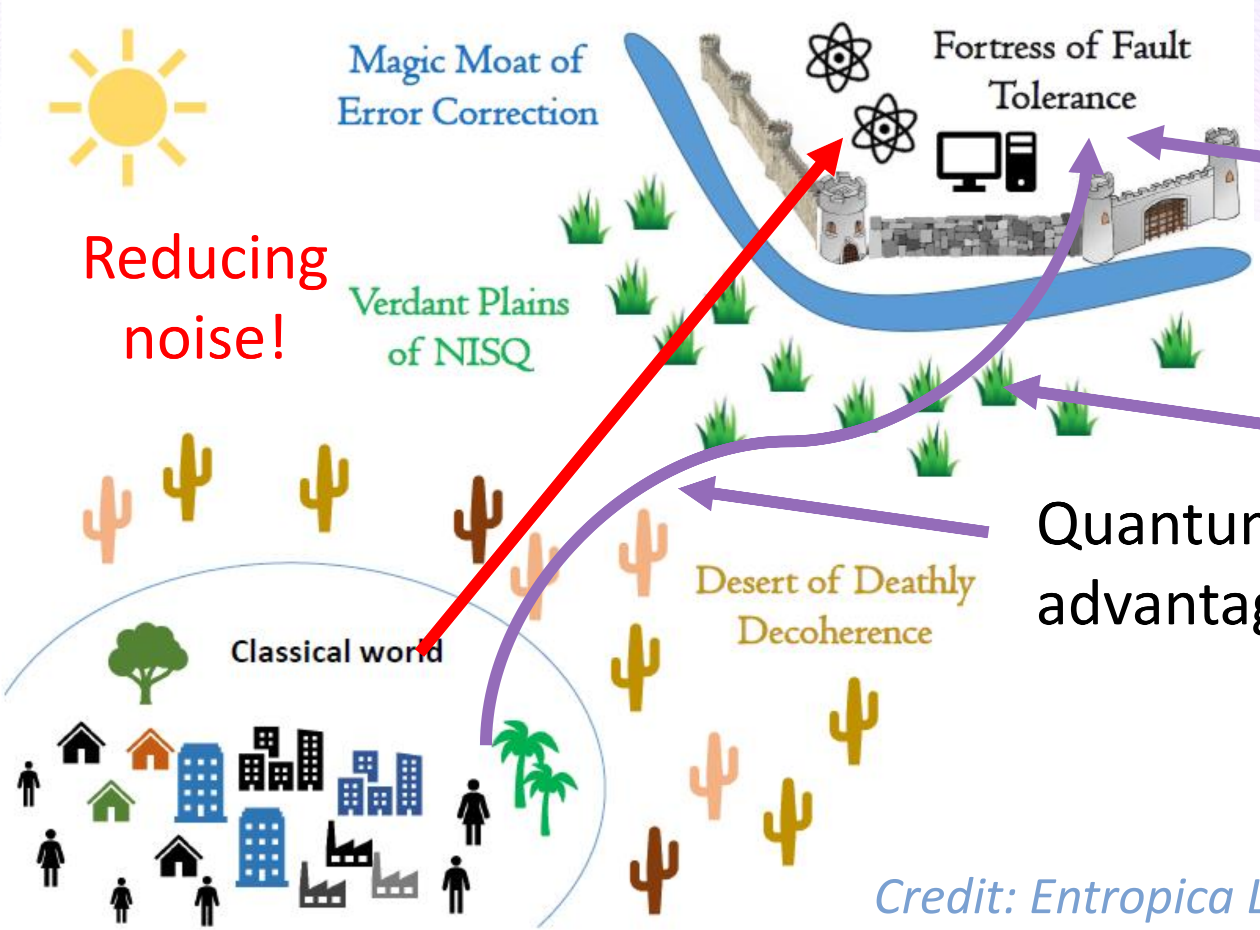
- Photon-native operations
- 1 qubit = 1 photon
- Fast repetition rate
- Good for NISQ algorithms



Errors… How bad are these?

Why do we need fault-tolerant quantum computing?

The inconvenient truth about NISQ...



Reducing noise!

QC useful Applications!

NISQ useful applications?

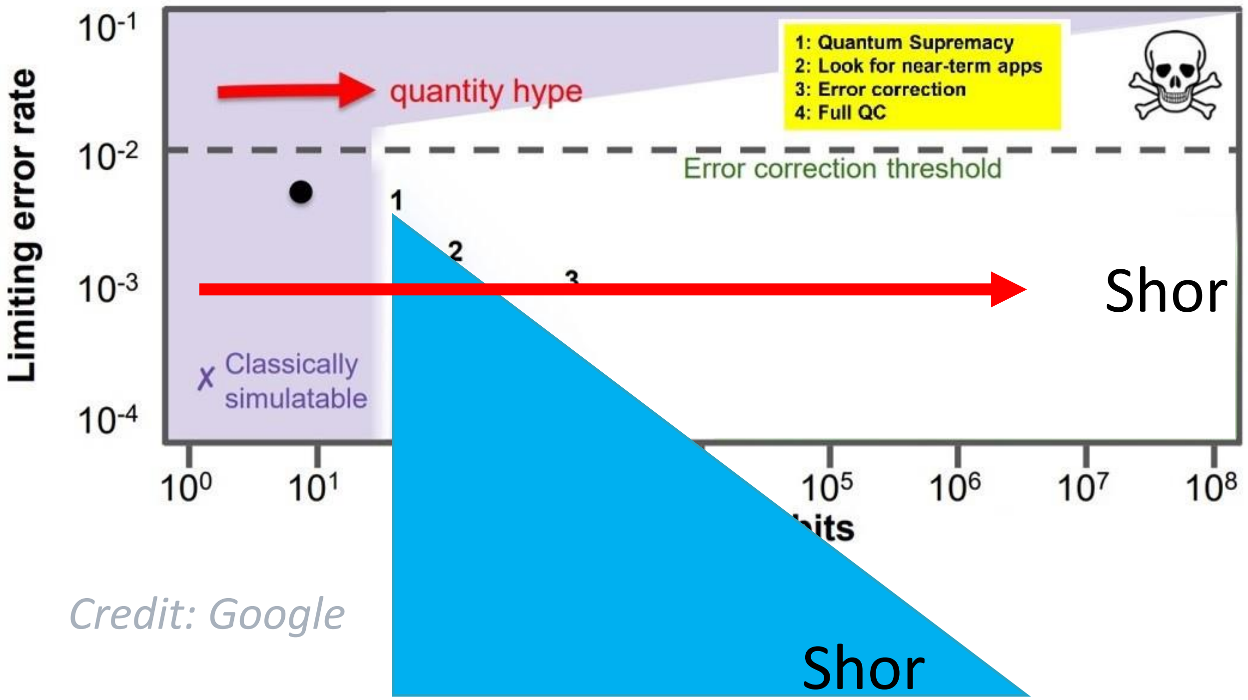
Quantum advantage

Credit: Entropica Labs

Why do we need Fault-tolerant quantum computing?

Errors are bad

How bad are these errors?



Credit: Google

Without handling errors
→ Only the tip of the Q Algo's iceberg!

Quantum error correction!

- Hardware:

Reducing physical noises

$$\varepsilon \ll 1$$

- Software:

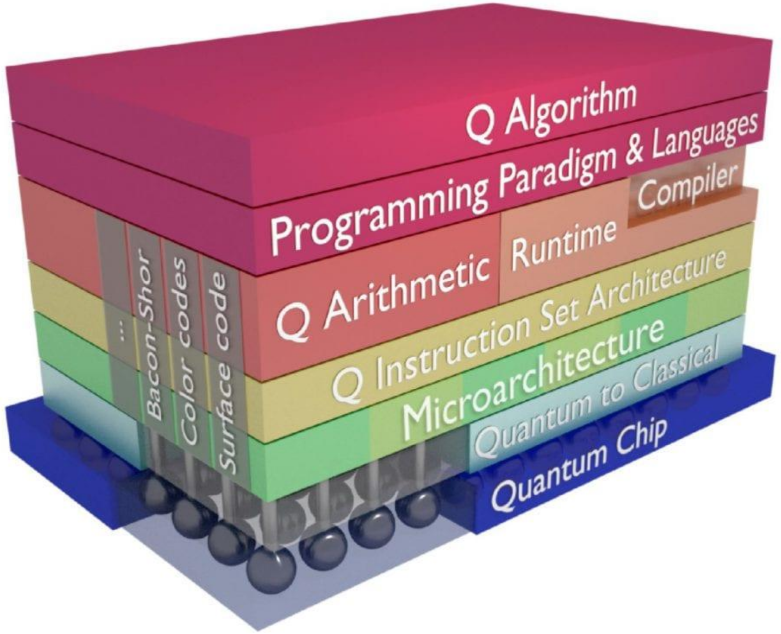
Developing a FTQC-based architecture

- **Threshold theorem**:

if $\varepsilon < \varepsilon_{th}$, we can run any algorithms!
(provided the FTQC is sufficiently big!)

Architecture for real Fault-tolerant quantum computers

Find the best FTQC architecture for a photonic platform



What is an FTQC architecture?

- A method to process quantum information
- Together with a hardware layout enabling this method
- All of this being achievable in a fault-tolerant way

What is the “best” architecture?

- An architecture with maximum fault-tolerance (high threshold)
- A relatively simple hardware layout (sufficiently simple to be implementable)
- An architecture with relatively small footprint (hardware overhead, energy consumption…)

Outline

- Classical error correction
  - Repetition code / Hamming code
- Quantum error correction
  - Challenges of quantum error correction
  - Discretization of errors
  - Stabilizer formalism
  - Simple code (Shor)
- Photonic FTQC
  - Graph state structure
  - How to build them?

Classical Error Correction

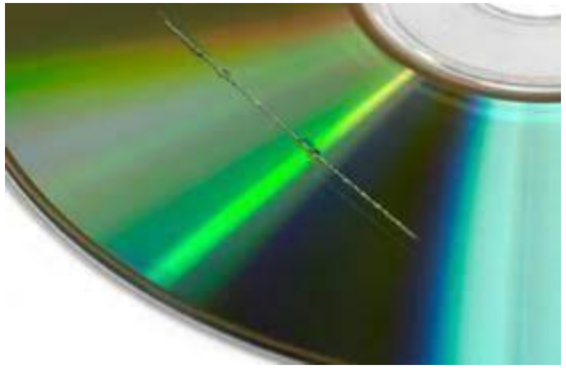
Simple examples of classical error correction

Classical computing using classical error correction

Simple examples of classical error correction:

- CD Rom

Communication protocols (e.g. 5G)



General idea:

$$[n, k, d]$$

"Encode k logical (protected) bits into n physical (noisy) bits so that it is protected against $\lfloor d-1 \rfloor /2$ bitflips"

The Repetition Code

Classical computing using classical error correction

The repetition code is a $[n, 1, n]$ code with a trivial decoder (majority vote)

The logical bit $i = 0$ or 1 is encoded as

$0_L = 0 \ldots 0$

$1_L = 1 \ldots 1$

How does it work?

If you receive the bitstring (encoded using a 3-bit repetition code) 010*, what is the most likely error?*

Assuming independent symmetric errors (below ½), the most likely error is e=010 and the codeword is $0_L = 000$

Simpler example with classical error correction

Classical computing using classical error correction

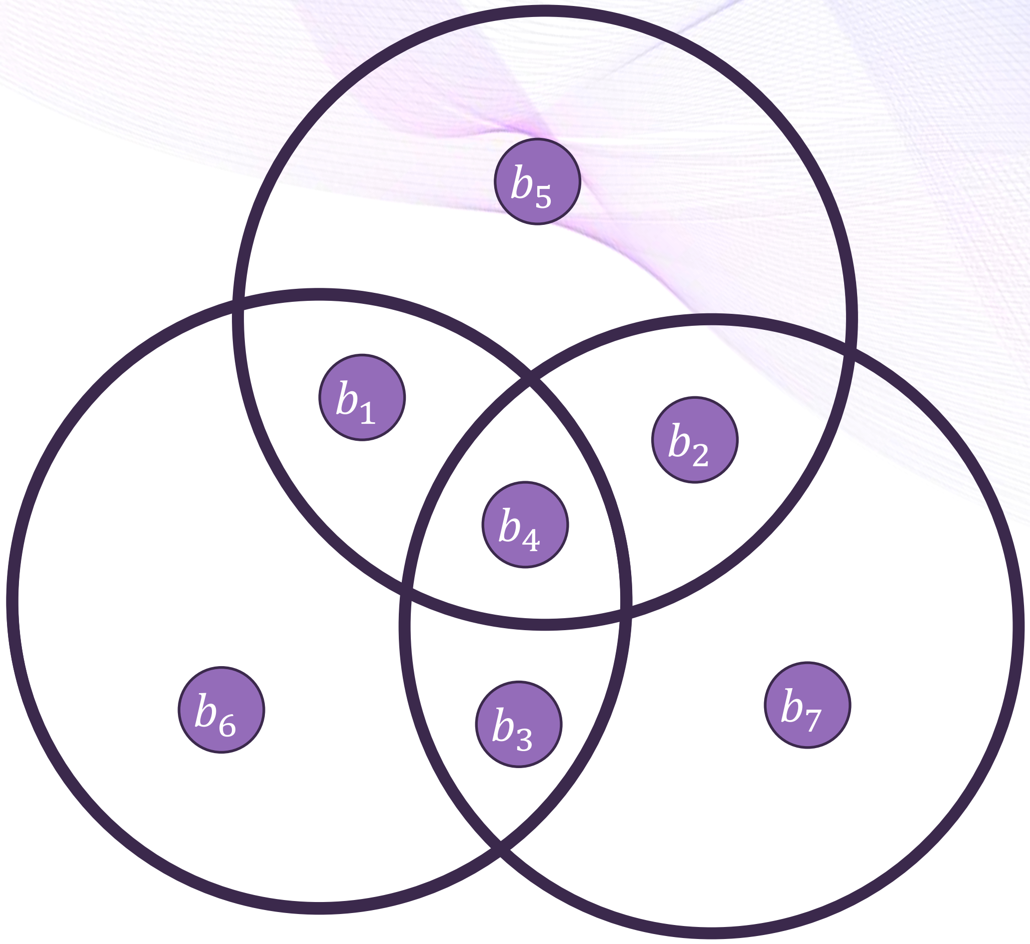
Hamming code:

- Encode 4 logical bits $l_1 l_2 l_3 l_4$
- Into 7 physical bits $b_1 b_2 b_3 b_4 b_5 b_6 b_7$

Circle constraints

$\bigoplus_i b_i = 0$

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$



Simpler example with classical error correction

Classical computing using classical error correction

Hamming code:

- Encode 4 logical bits $l_1 l_2 l_3 l_4$
- Into 7 physical bits $b_1 b_2 b_3 b_4 b_5 b_6 b_7$

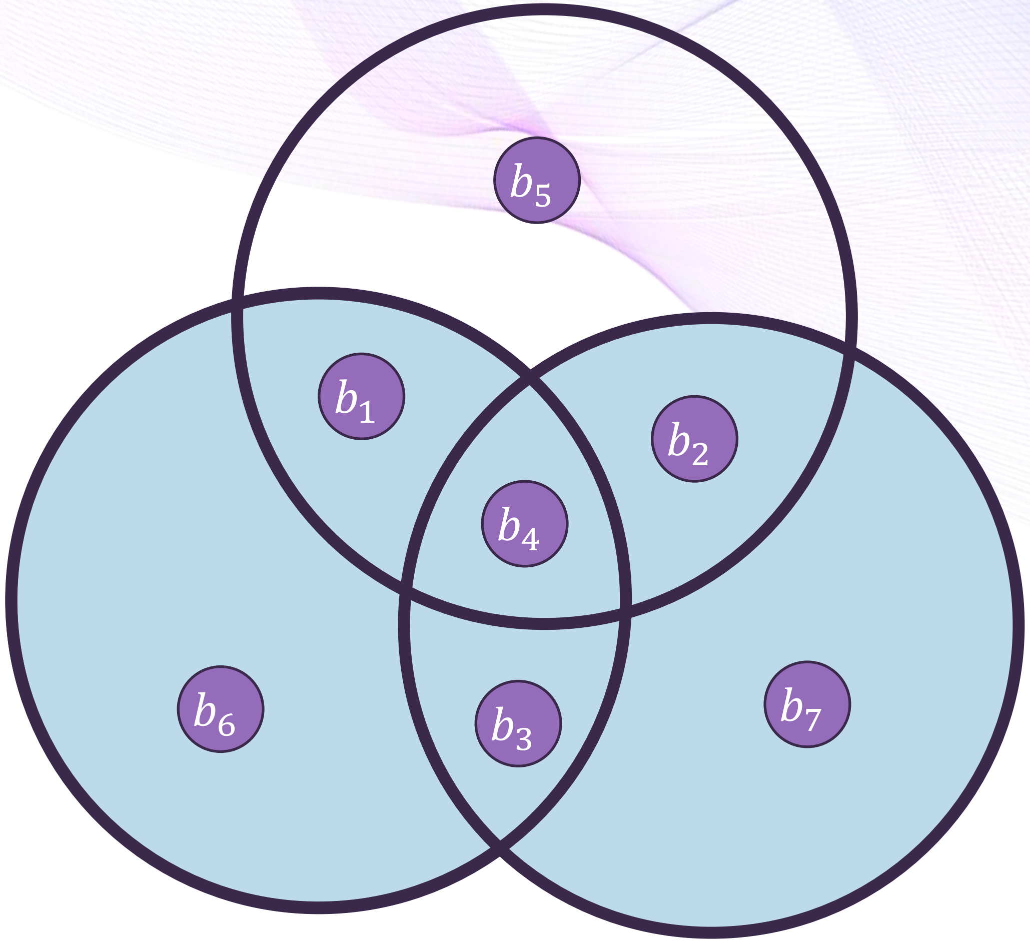
Circle constraints

$\bigoplus_i b_i = 0$

Invalid codeword $c = c_1 c_2 c_3 c_4 c_5 c_6 c_7$

Syndrome $\mathrm{s} = H\, c^T \neq 0$

Example: $H\, c^T \neq (0,1,1)^T$



Simpler example with classical error correction

Classical computing using classical error correction

General problem of error correction:

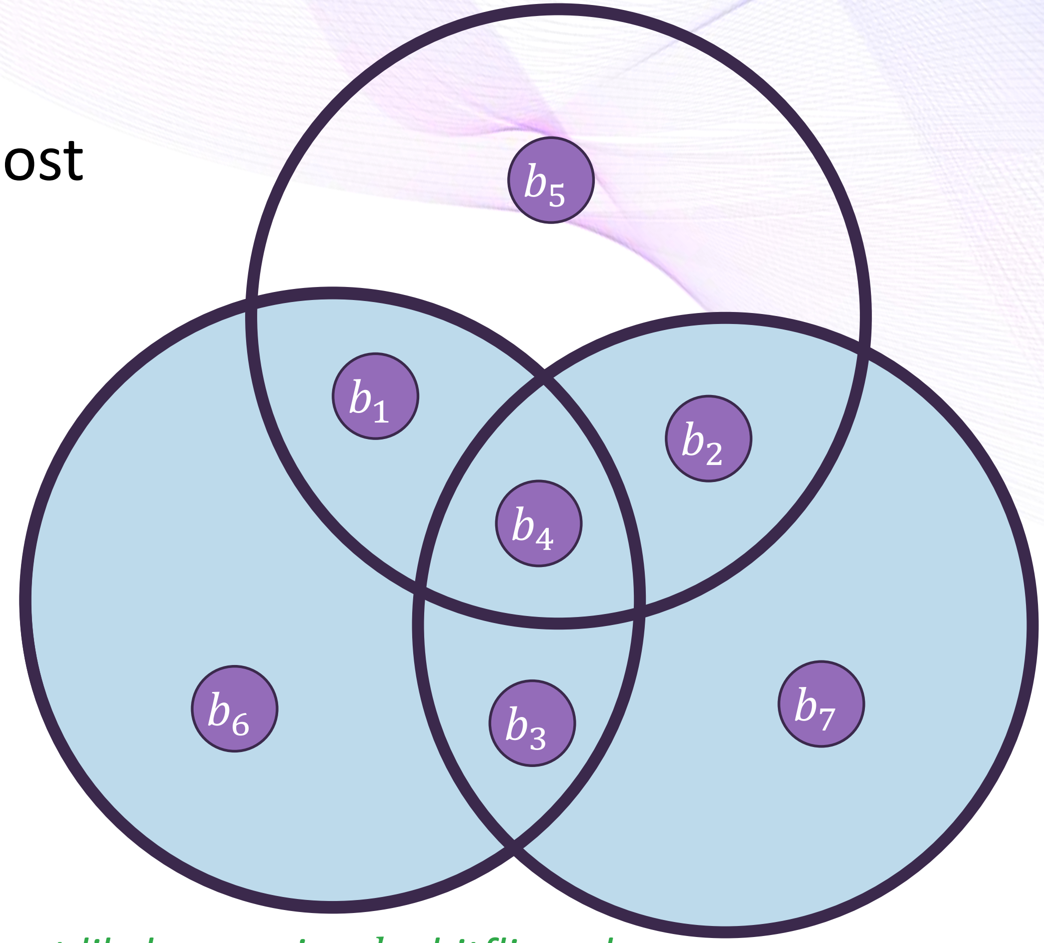
"Given a syndrome s, recover ideally the most likely error that outputs a syndrome s"

$$"c^T = H^{-1}s"$$

Given an error sampling probability $p\ (e_i)$,

We want (ideally):

$$MLDec(\mathrm{p}(\mathrm{e_i}), \mathrm{s})$$
$$= \ \mathrm{argmin}_{\mathrm{e_i}}\ [\mathrm{p}(\mathrm{e_i})|\mathrm{H\ e_i} = \mathrm{s}]$$

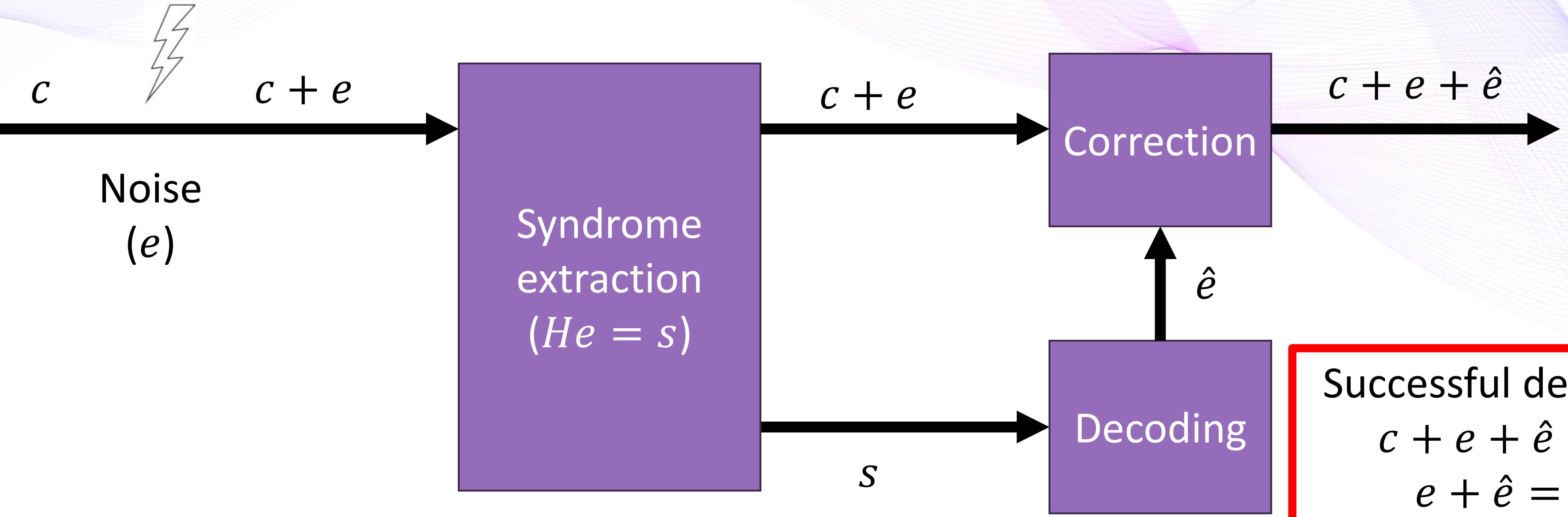


What is the most likely error, having this syndrome?

Assuming independent symmetric errors (below ½), the most likely error is a b_3 bitflip only

General summary of classical error correction

Classical computing using classical error correction



Successful decoding

$$c+e+\hat{e}=c$$

$$e+\hat{e}=0$$

That’s all for
Classical Error Correction.
Questions?

Quantum Error Correction
(intuition)

Challenges of Quantum error correction

Why isn't it conceptually easy?

Challenge 1:
Errors in classical computing are discrete.
Errors in quantum computing are continuous…

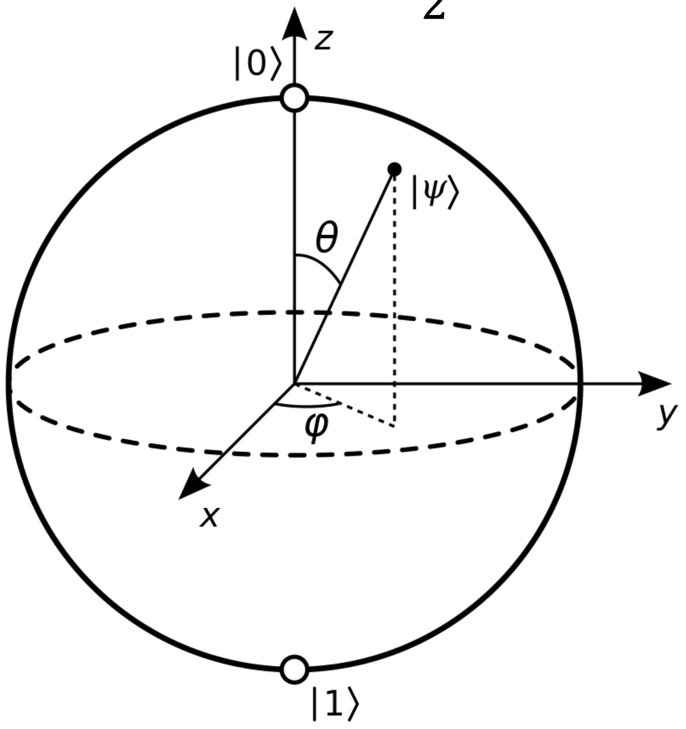
Challenge 2:
Measuring a classical bit is trivial.
Measuring a quantum state destroy this state (Born's rule / Wave function collapse…)

Challenge 3:
Classical error correction needs to protect against bitflips
In quantum computing, the phase is also important!

Errors are continuous…

Why isn't it conceptually easy?

Qubit: $|\psi(\theta,\varphi)\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$



Target state: $|0\rangle$

Noisy state: $\sqrt{1-\varepsilon}|0\rangle + \sqrt{\varepsilon}\,|1\rangle$

Measurement in the computational basis ($|0\rangle$ / $|1\rangle$)

→ $|0\rangle$ with probability $1-\varepsilon$

→ $|1\rangle$ with probability ε

Intuition 1:
Errors are continuous but measurements discretize these errors

Measurements destroy quantum states and entanglement

Why isn't it conceptually easy?

Entangled qubits:

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Measurement of the two qubits in the computational basis ($Z\ basis$)
($|0\rangle$ / $|1\rangle$)

$\rightarrow |0\rangle, |0\rangle$ with probability $\frac{1}{2}$

$\rightarrow |1\rangle, |1\rangle$ with probability $\frac{1}{2}$

No entanglement anymore…

Is it true for all measurements???

Measurement of the operator ZZ

$Z|i\rangle = (-1)^i|i\rangle$ for $i = 0,1$

What are the measurement outcomes and the resulting states?

Same question for $\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$?

+1 for both and the state remains the same

Intuition 2:
Some multi-qubit operator measurements preserve entanglement and some states.

Repetition codes for quantum states

Why isn't it conceptually easy?

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

With $|0\rangle_L = |000\rangle, |1\rangle_L = |111\rangle$

Noise:

Some small unwanted X rotations on the physical qubits…

$$|\widetilde{\psi_L}\rangle = \sqrt{1-\varepsilon}\ |\psi\rangle_L$$
$$+\sqrt{\varepsilon/3}(\alpha|100\rangle + \beta|011\rangle)$$
$$+\sqrt{\varepsilon/3}(\alpha|010\rangle + \beta|101\rangle)$$
$$+\sqrt{\varepsilon/3}(\alpha|001\rangle + \beta|110\rangle) + o(\varepsilon)$$

Measure Z_1Z_2 (+1 outcome and nothing happens)

Measure Z_2Z_3

- either +1 outcome and projection in the $|\psi\rangle_L$ state.
- either -1 outcome and error detection

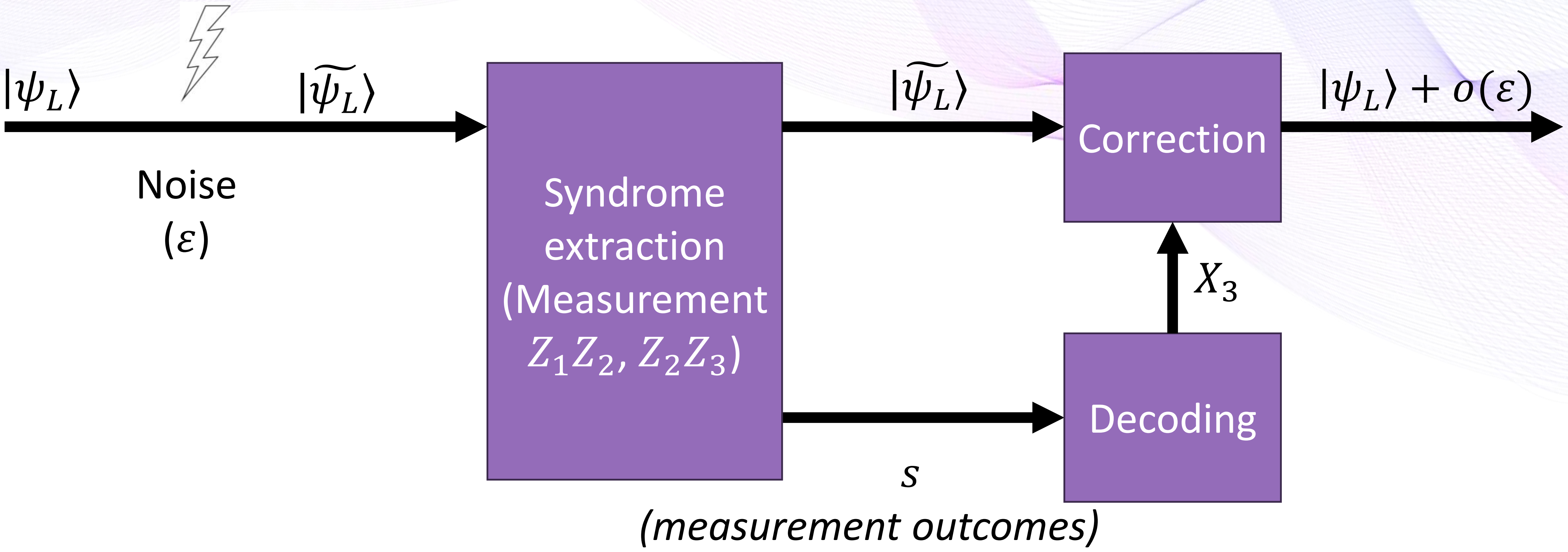
$$\alpha|001\rangle + \beta|110\rangle$$

We have obtained the syndrome measurement s=(0, 1)

Link with the parity check matrix?

Repetition codes for quantum states

Why isn't it conceptually easy?



What about phase flips?

The Shor code

Why isn't it conceptually easy?

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

With $|0\rangle_L = |000\rangle, |1\rangle_L = |111\rangle$

Noise:

Some small unwanted Z rotations on the physical qubits…

$$|\widetilde{\psi_L}\rangle = \sqrt{1-\varepsilon}\ |\psi\rangle_L + \sqrt{\varepsilon}\ \underbrace{(\alpha|000\rangle - \beta|111\rangle)}$$

Still a valid logical state!

→Impossible to correct a phase flip…

Alternative code

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

With $|0\rangle_L = |+++\rangle, |1\rangle_L = |---\rangle$

$$|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle))$$

Show that it is resistant against phase flips (Z).

What is the operator measurements?

$$X\,|\pm\rangle = \pm|\pm\rangle$$

Same discussion as in the usual repetition code, but with X_1X_2 operator measurements

The Shor code

Why isn't it conceptually easy?

Concatenating two repetition codes!

$|0\rangle_{L_Z} = |000\rangle, |1\rangle_{L_Z} = |111\rangle$ $\qquad |\pm\rangle_{L_Z} = |000\rangle \pm |111\rangle$

$|0\rangle_{L_X} = |{+}{+}{+}\rangle, |1\rangle_{L_X} = |{-}{-}{-}\rangle$

Concatenation: Replace physical qubits from the first code L_1 by logical qubits from the second code.

Shor code:

$|0\rangle_{Shor} = |+_{L_Z} +_{L_Z} +_{L_Z}\rangle, |1\rangle_{Shor} = |-_{L_Z} -_{L_Z} -_{L_Z}\rangle$

At the L_X levels, correct one phase flip, at the L_Z level, correct one bit flip.

What about $Y = -iZX$ rotation errors?

The Shor code

Why isn't it conceptually easy?

$$\alpha|0\rangle_{Shor} + \beta|1\rangle_{Shor} = \alpha(|000\rangle + |111\rangle)^{\otimes 3} + \beta(|000\rangle - |111\rangle)^{\otimes 3}$$

If an X error occur on one qubit, one block will look like $|001\rangle \pm |110\rangle$, (modulo where the bit flip occurs) which can be corrected by Z_1Z_2/Z_2Z_3 in that block.

If a Z error occurs on one qubit, one qubit block will be flipped:

$$\alpha(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle - |111\rangle)$$
$$+\beta(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle + |111\rangle)$$

Which can be detected by measuring logical $X_{L_1}X_{L_2}/X_{L_2}X_{L_3}$ operator on each block $X_{L_1} = X_1X_2X_3, X_{L_2} = X_4X_5X_6, X_{L_3} = X_7X_8X_9$

The Shor code

Why isn't it conceptually easy?

$$\alpha|0\rangle_{Shor} + \beta|1\rangle_{Shor} = \alpha(|000\rangle + |111\rangle)^{\otimes 3} + \beta(|000\rangle - |111\rangle)^{\otimes 3}$$

If a Y error occurs on a given qubit, it'll flip both a qubit on a given block and the total block sign which can be signaled by having the X and Z errors at the same time

$$Y_1(|000\rangle \pm |111\rangle) = -iZX(|000\rangle \pm |111\rangle) = -i|100\rangle \mp |011\rangle$$

(The global phase i is irrelevant)

So a Y error can be corrected as a combination of X and Z error.

Summary of the intuitions

Why isn't it conceptually easy?

- Measurements discretize errors
- Measurements of multi-qubit operators can sometimes preserve entanglement
- Some multi-qubit operators allows the detection of a bit flip or a phase flip.
- The multi-qubit operators should preserve the logical states

Can we generalize these ideas?
How does it work in practice?

Quantum Error Correction
(beyond intuition)

The stabilizer formalism

Why isn't it conceptually easy?

Some definitions

- Pauli operators:

$$I = \sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad X = \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$Y = \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Z = \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- $P_1 = \langle iI, X, Z \rangle = \{\pm 1, \pm i\} \times \{I, X, Y, Z\}$ has a group structure and is called the single-qubit Pauli group.

- $P_n = P_1^{\otimes n}$ is the n-qubit Pauli group, and we call its elements "Pauli strings".

The stabilizer formalism

The theoretical framework of QEC

We are interested in Pauli string operators that "stabilizes" a quantum state and we call these operators "stabilizers".

K stabilizes $|\psi\rangle$ if $\quad K\,|\psi\rangle = +1|\psi\rangle$

What are the stabilizers of $|0\rangle$ *?* $\{I, Z\}$

What are the stabilizers of $|1\rangle$ *?* $\{I, -Z\}$

What are the stabilizers of $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ *?* $\{II, ZZ, XX, -YY\}$

What are the stabilizers of $\alpha|00\rangle + \beta|11\rangle\ \forall \alpha, \beta$ *?* $\{I, ZZ\}$

The stabilizer formalism

The theoretical framework of QEC

A n-qubit quantum state is stabilized by 2^n operators.

- Its stabilizer operators have an **abelian** group structure.

ex. $|00\rangle + |11\rangle$ *stabilized by* $\{II, XX, ZZ, -YY\}$

- The stabilizer group of $\mathbf{2^n}$ **elements** have $\boldsymbol{n}$ **linearly independent generators**

ex. $\{II, XX, ZZ, -YY\}$ *is generated by* $\langle XX, ZZ\rangle$

$(XX\ ZZ = -YY, XX\ XX = II)$

- A stabilizer group of $\boldsymbol{n-k}$ (n-qubit) **Pauli strings generators**, stabilizes a **k-qubit Hilbert subspace** (in a n-qubit Hilbert space)

ex. $\{II, ZZ\}$ *stabilizes* $\alpha|00\rangle + \beta|11\rangle = \alpha|0\rangle_L + \beta|1\rangle_L$ *(with* $|ii\rangle = |i\rangle_L$*)*

Link with quantum error correction

The theoretical framework of QEC

A $[[n, k, d]]$ Quantum Error Correcting code encode k logical qubits into n physical qubits to protect quantum information against $\lfloor (d-1)/2 \rfloor$ errors.

Syndrome through parity check measurement

$$\mathrm{H}_X e_X = s_X, \quad \mathrm{H}_Z e_Z = s_Z$$

The stabilizer formalism gives you a way to encode a k-qubit Hilbert subspace into a n-qubit Hilbert space with constraints given by stabilizer operators. Stabilizer group generated by:

$$\langle K_1, \dots K_{n-k} \rangle$$

$$K_i \left|\tilde{\psi}\right\rangle_L = (-1)^{s_i} \left|\tilde{\psi}\right\rangle_L$$

$$\frac{1 - \langle\tilde{\psi}|_L K_i |\tilde{\psi}\rangle_L}{2} = s_i$$

If $\exists i, s_i = 1$, an error is detected

Link / challenges: classical and quantum error correction

Calderbank-Steane-Shor codes

Classical codes protects against bitflips: $He = s$

- We can create quantum codes that protects against blitflips using $H \rightarrow K_{Zi}$s, Z-type stabilizers

$$H = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \rightarrow \begin{matrix} Z_1 Z_2 I_3 \\ I_1 Z_2 Z_3 \end{matrix}, H_Z$$

- We can create quantum codes that protects against phaseflips using $H \rightarrow K_{Xi}$s, X-type stabilizers

$$H = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \rightarrow \begin{matrix} X_1 X_2 I_3 \\ I_1 X_2 X_3 \end{matrix}, H_X$$

Link / challenges: classical and quantum error correction

Calderbank-Steane-Shor codes

How to make codes that protects against phaseflips and bitflips?

Use two classical codes H_X, H_Z! $\langle K_{X1}, \dots K_{Xn,} K_{Z1}, \dots K_{Zm} \rangle$

Can we do always that?

- The stabilizer groups protect a qubit subspace
- The stabilizer group should be **abelian** $\left[K_{Xi}, K_{Zj}\right] = 0$

Show that this constraint requires $H_X . H_Z^T = 0$?

Not so easy to find such conditions!

Link / challenges: classical and quantum error correction

Calderbank-Steane-Shor codes

Relate stabilizers to H_X and H_Z matrices:

The i^{th} *row of* H_X *corresponds to* K_{Xi}*:*

Notations: $(H_X)_{ij} = h_{ij}^X$, $(H_Z)_{ij} = h_{ij}^Z$

$X^0 = I, X^1 = X,$

$X_j^{h_{ij}^X} = I_i$ if $h_{ij}^X = 0,$

$X_j^{h_{ij}^X} = X_i$ if $h_{ij}^X = 1$

So: $K_{Xi} = \prod_j X_j^{h_{ij}^X}$

Same for H_Z: $K_{Zi} = \prod_j Z_j^{h_{ij}^Z}$

Link / challenges: classical and quantum error correction

Calderbank-Steane-Shor codes

Commutation relations: $[K_{Xi}, K_{Zi'}] = 0$

if $\prod_j \left(X_j^{h_{ij}^X} Z_j^{h_{i'j}^Z} \right) = \prod_j \left(Z_j^{h_{i'j}^Z} X_j^{h_{ij}^X} \right)$

$X^{h_{ij}^X} Z^{h_{i'j}^Z} = Z^{h_{i'j}^Z} X^{h_{ij}^X}$ *if* $h_{ij}^X = 0$, *or* $h_{i'j}^Z = 0$ *(at least one is I)*

$X^{h_{ij}^X} Z^{h_{i'j}^Z} = -Z^{h_{i'j}^Z} X^{h_{ij}^X}$ *if* $h_{ij}^X = h_{i'j}^Z = 1$

So $X^{h_{ij}^X} Z^{h_{i'j}^Z} = (-1)^{h_{ij}^X \times h_{ij}^Z} \; Z^{h_{i'j}^Z} X^{h_{ij}^X}$

So $\prod_j (X^{h_{ij}^X} Z^{h_{i'j}^Z}) = (-1)^{\sum_j h_{ij}^X \times h_{i'j}^Z} \prod_j Z^{h_{i'j}^Z} X^{h_{ij}^X}$

And the operators commute if the two rows have value 1 on an even number of elements.

We can see this is true for all rows if $H_X . H_Z^T = 0$

Simple example with quantum error correction

Calderbank-Steane-Shor codes

Steane quantum code:

Circle constraints

$\bigotimes_i X_i|\psi\rangle = |\psi\rangle$

Second constraints

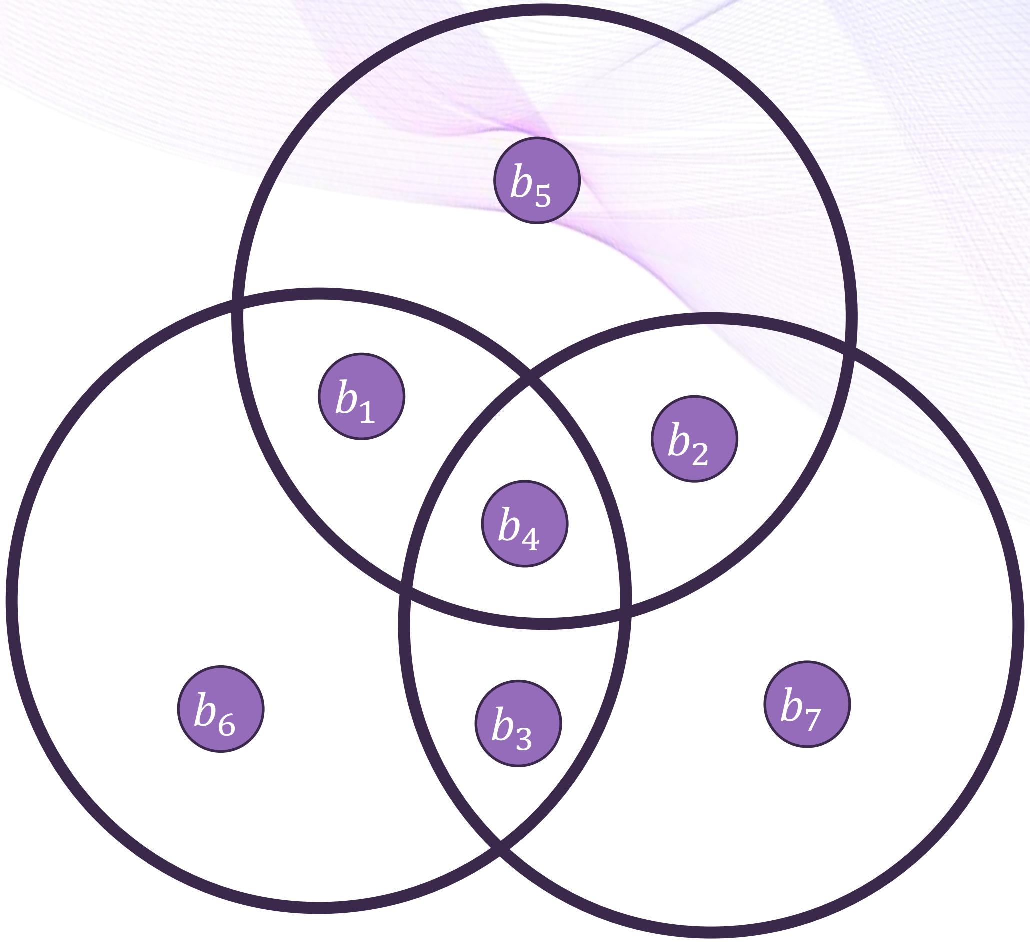
$\bigotimes_i Z_i|\psi\rangle = |\psi\rangle$

Define two parity check matrices

$$H_X\, c_X^T = 0$$
$$H_Z\, c_Z^T = 0$$

CSS codes:

$$H_X H_Z^T = 0$$



The Steane Code

Calderbank-Steane-Shor codes

Steane quantum code:

Circle constraints

$\bigotimes_i X_i|\psi\rangle = |\psi\rangle \quad (H = H_X)$

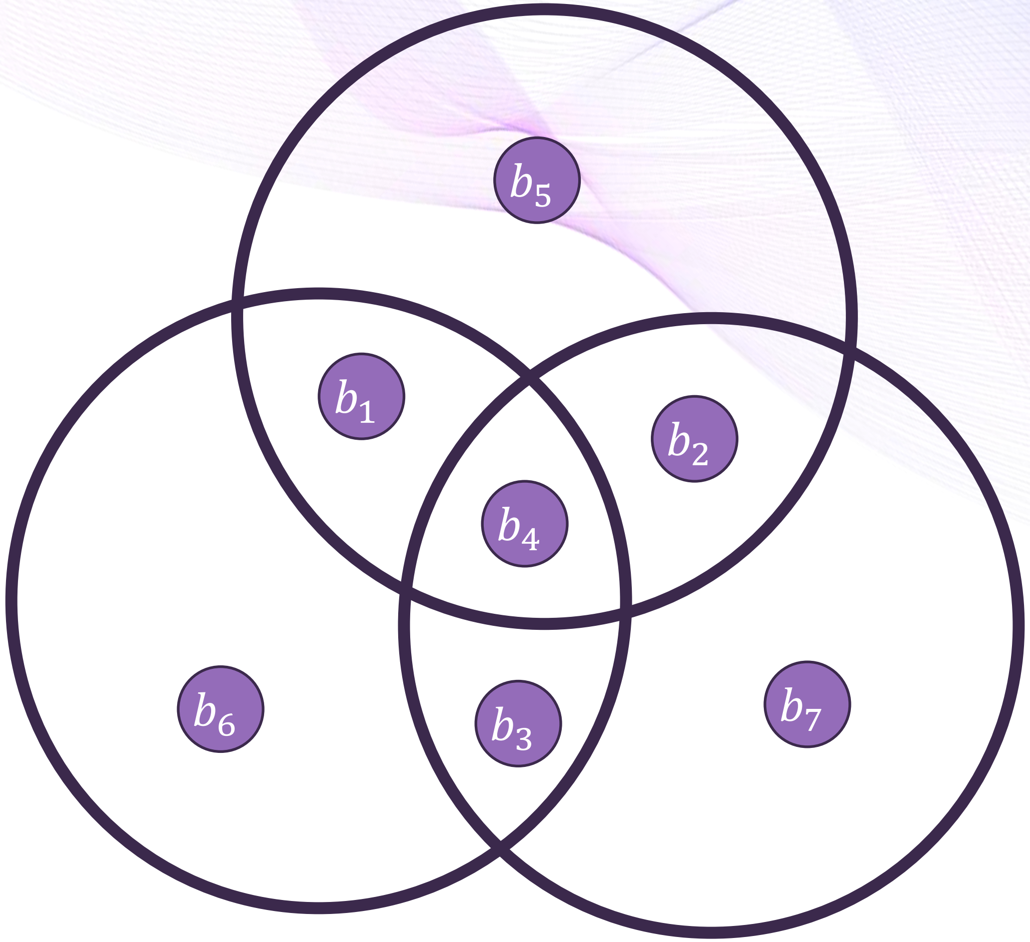
Second constraints

$\bigotimes_i Z_i|\psi\rangle = |\psi\rangle \quad (H = H_Z)$

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

This works since:

$$H\,H^T = 0$$



How to measure stabilizer operators?
Ancilla-assisted stabilizer measurements

Rule of thumb:

Multi-qubit operators are hard to measure.

Single-qubit operators are easy to measure.

Strategy: Convert a multi-qubit operator measurement into a single-qubit measurement.

Always this outcome

How to measure stabilizer operators?

Ancilla-assisted stabilizer measurements

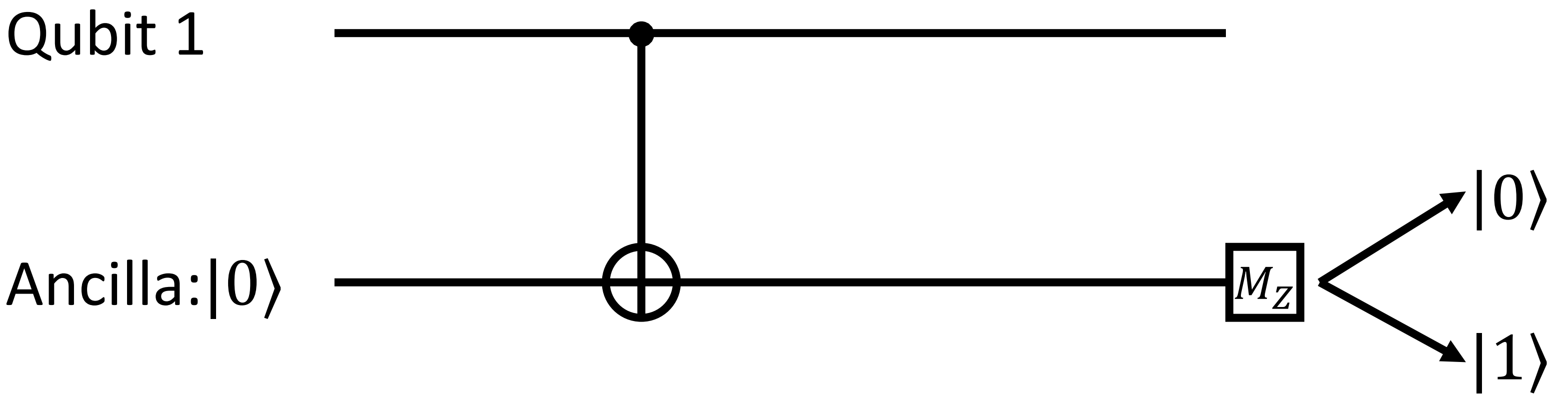
Rule of thumb:

Multi-qubit operators are hard to measure.

Single-qubit operators are easy to measure.

Strategy: Convert a multi-qubit operator measurement into a single-qubit measurement.

CNOT flip the ancilla qubit if qb 1 in state $|1\rangle$



How to measure stabilizer operators?

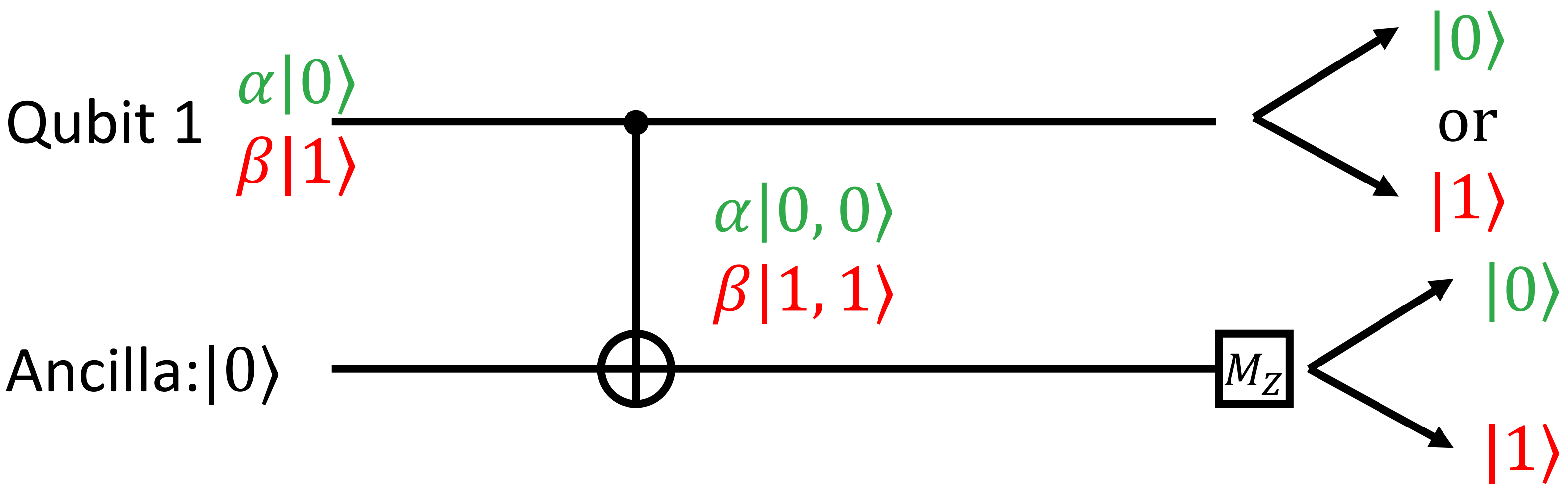
Ancilla-assisted stabilizer measurements

Rule of thumb:

Multi-qubit operators are hard to measure.

Single-qubit operators are easy to measure.

Strategy: Convert a multi-qubit operator measurement into a single-qubit measurement.



CNOT flip the ancilla qubit if qb 1 in state $|1\rangle$

Indirect measurement of qubit 1 (using ancilla) in the Z basis

How to measure stabilizer operators?

Ancilla-assisted stabilizer measurements

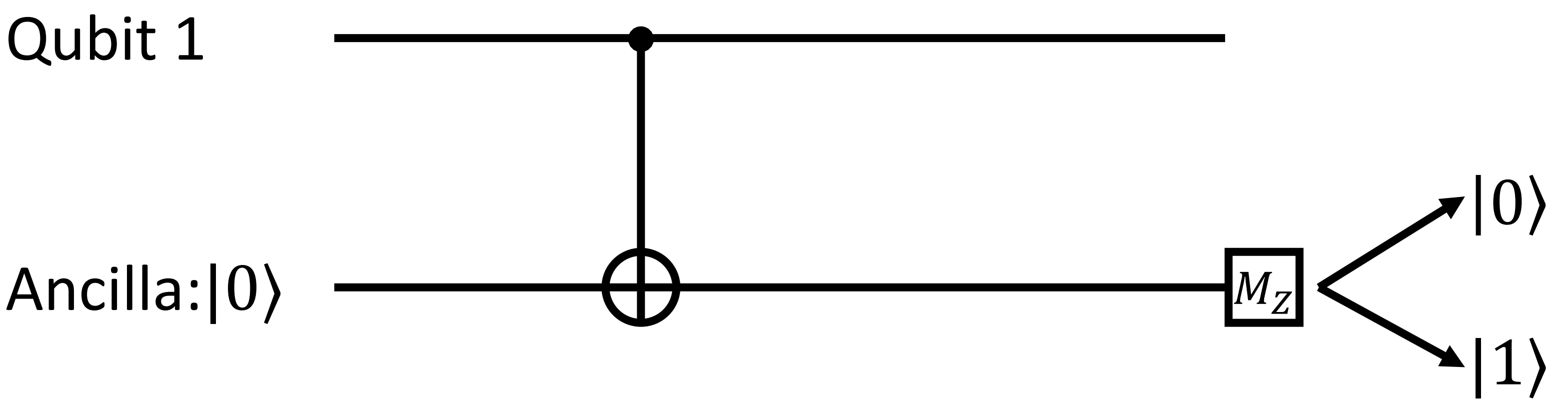
Rule of thumb:

Multi-qubit operators are hard to measure.

Single-qubit operators are easy to measure.

Strategy: Convert a multi-qubit operator measurement into a single-qubit measurement.

CNOT flip the ancilla qubit if qb 1 in state $|1\rangle$



Indirect measurement of qubit 1 (using ancilla) in the Z basis

How to measure stabilizer operators?

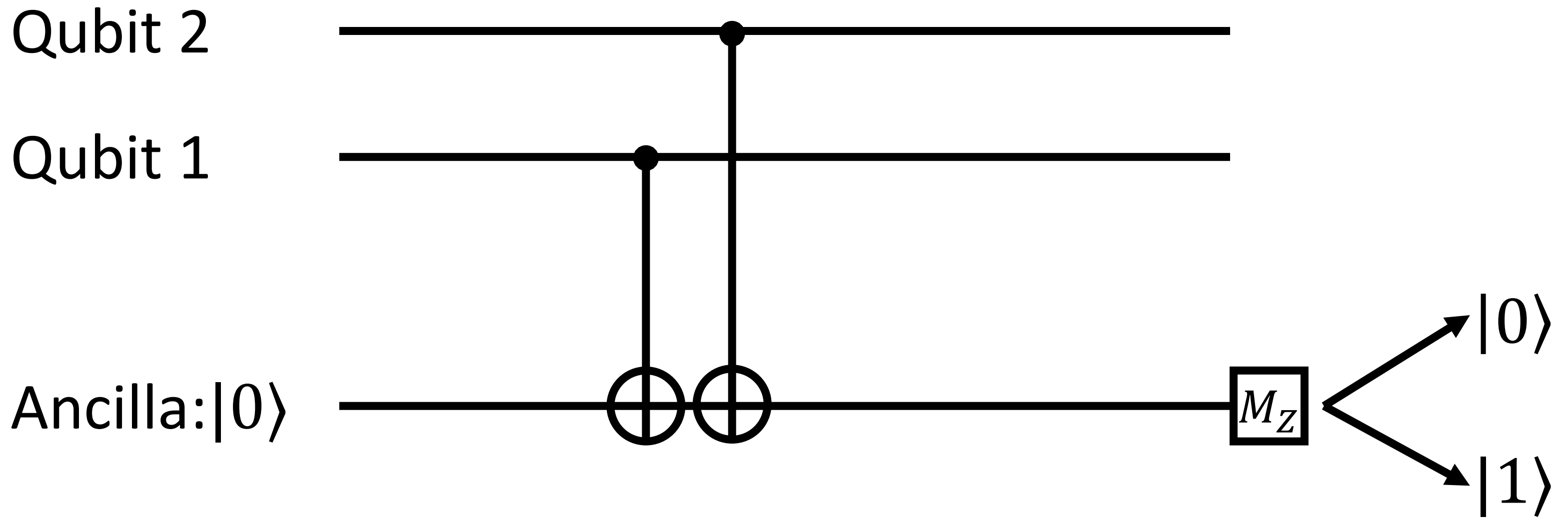
Ancilla-assisted stabilizer measurements

Rule of thumb:

Multi-qubit operators are hard to measure.

Single-qubit operators are easy to measure.

Strategy: Convert a multi-qubit operator measurement into a single-qubit measurement.



How to measure stabilizer operators?

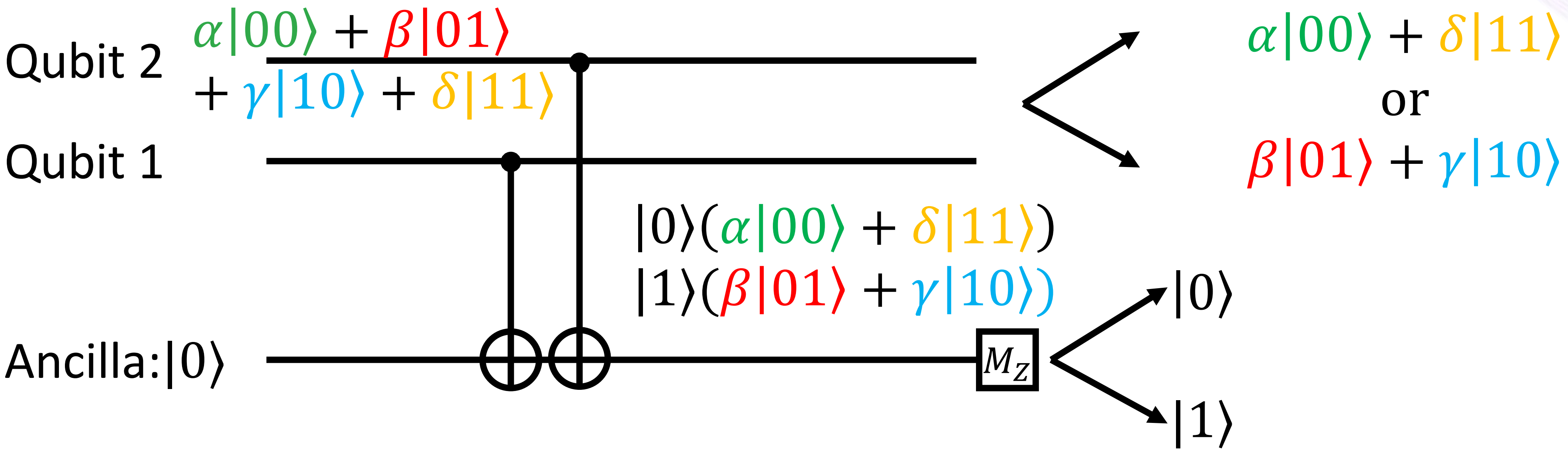
Ancilla-assisted stabilizer measurements

Rule of thumb:

Multi-qubit operators are hard to measure.

Single-qubit operators are easy to measure.

Strategy: Convert a multi-qubit operator measurement into a single-qubit measurement.



How to measure stabilizer operators?

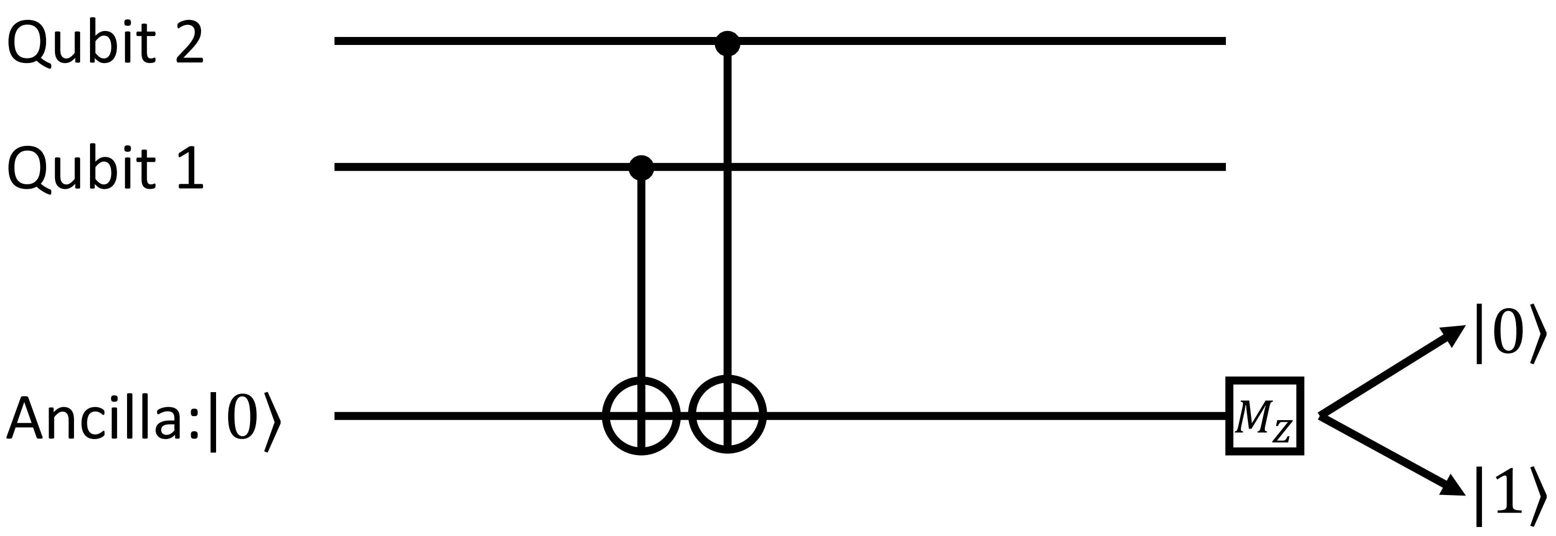
Ancilla-assisted stabilizer measurements

Rule of thumb:

Multi-qubit operators are hard to measure.

Single-qubit operators are easy to measure.

Strategy: Convert a multi-qubit operator measurement into a single-qubit measurement.



Indirect measurement of qubit 1 and 2 (using ancilla) in the ZZ basis

How to measure stabilizer operators?

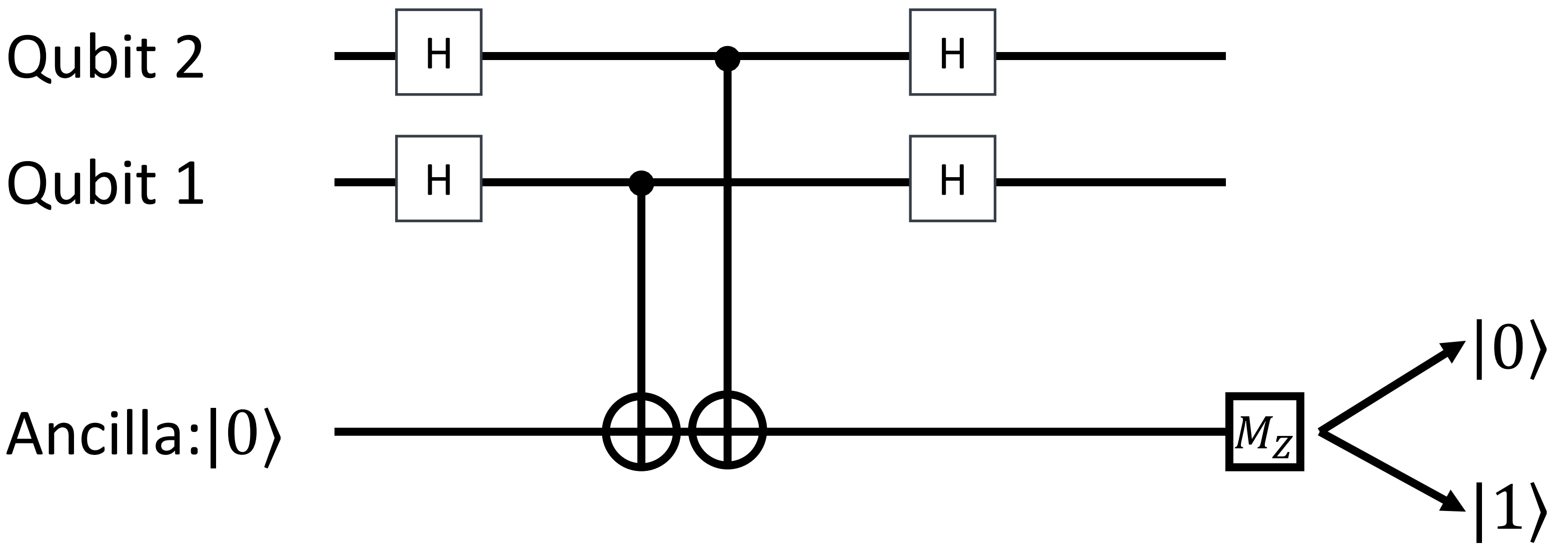
Ancilla-assisted stabilizer measurements

Rule of thumb:

Multi-qubit operators are hard to measure.

Single-qubit operators are easy to measure.

Strategy: Convert a multi-qubit operator measurement into a single-qubit measurement.



$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$HXH = Z$$

$$HZH = X$$

Indirect measurement of qubit 1 and 2 (using ancilla) in the XX basis

How to measure stabilizer operators?

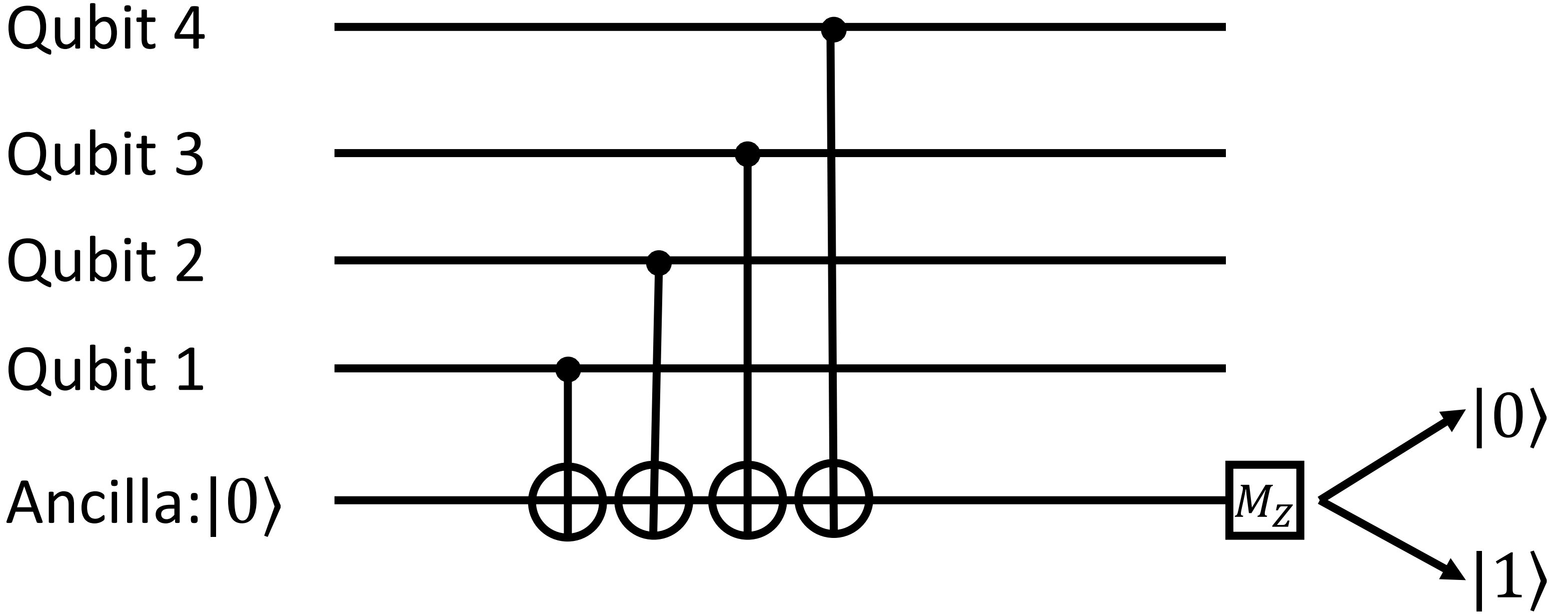
Ancilla-assisted stabilizer measurements

Rule of thumb:

Multi-qubit operators are hard to measure.

Single-qubit operators are easy to measure.

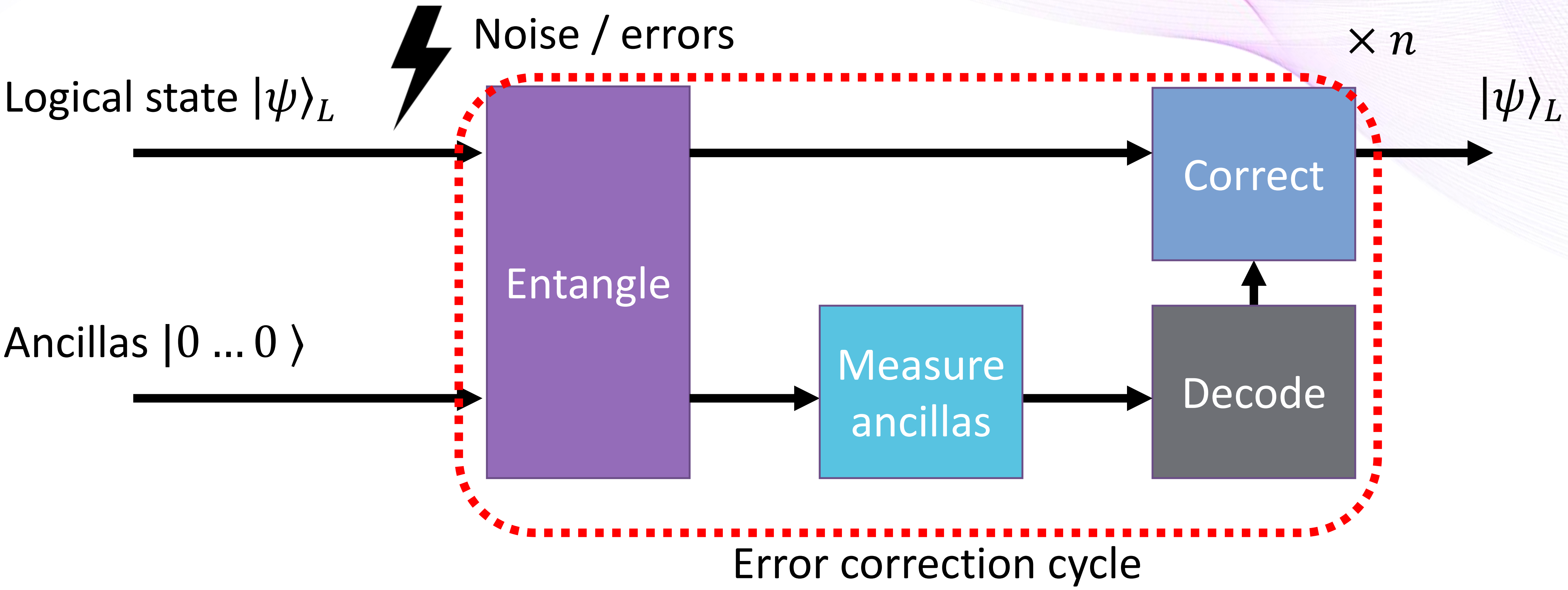
Strategy: Convert a multi-qubit operator measurement into a single-qubit measurement.



Indirect
$ZZZZ$ measurement

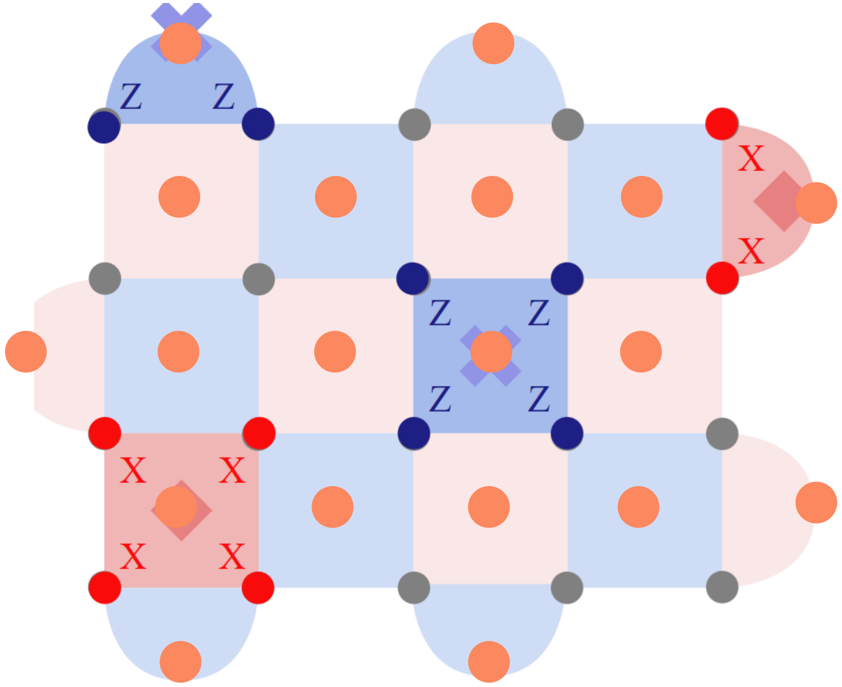
What is quantum error correction?

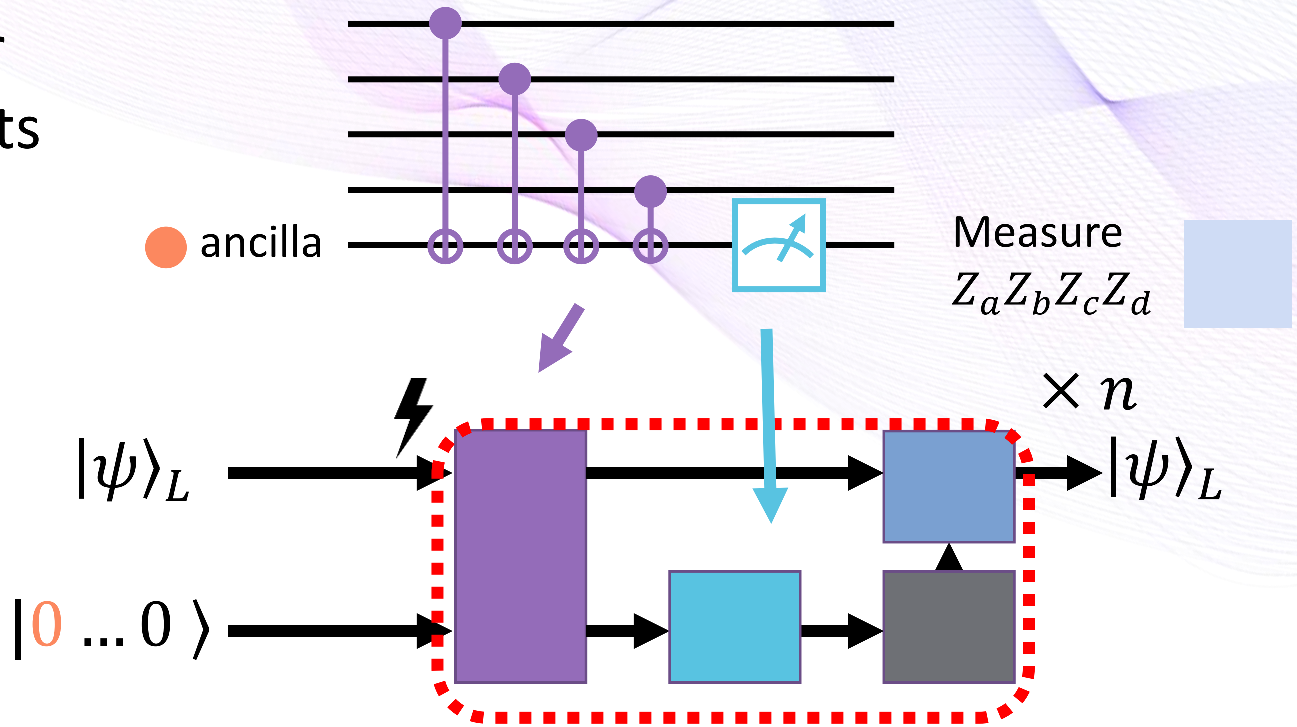
A fault-tolerant quantum computer use a QEC code and QEC detection cycles to actively detect and correct errors, using ancilla qubits.



More advanced codes

Quantum circuit for stabilizer measurements



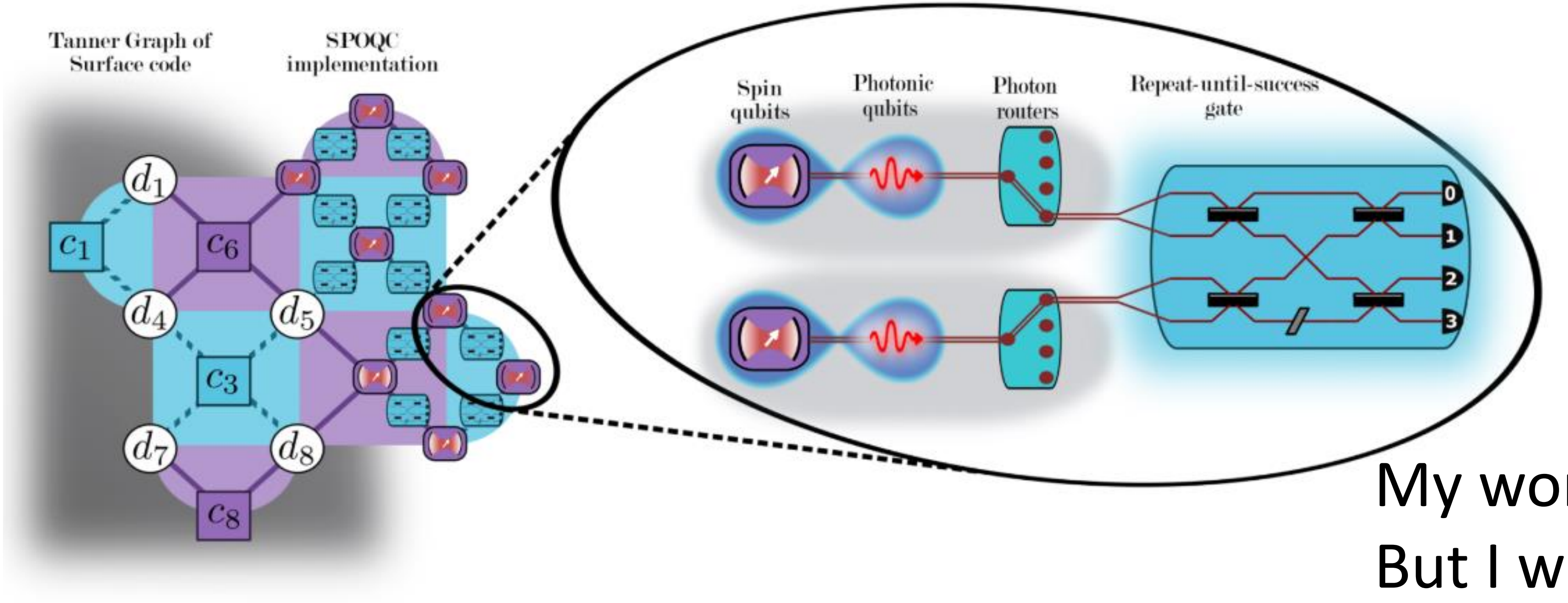


Issue: Two-qubit gates are probabilistic with photonics

Implementation on a real system?

Hybrid strategies (spin + photon) to facilitate FTQC

https://quantum-journal.org/papers/q-2024-07-24-1423/



My work at Quandela…

But I won’t talk about it

That’s all for quantum error correction! Questions?

Link with photonics?

Advantage of photonics

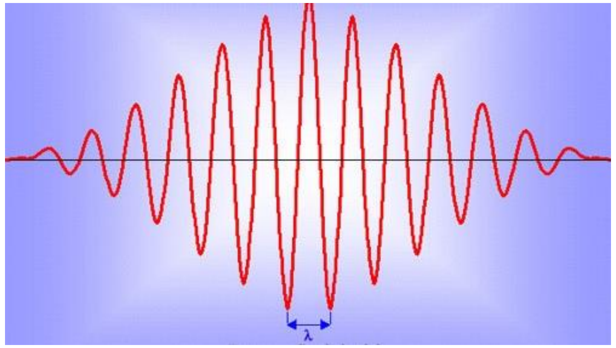
Photonic quantum computing

Photons as quantum information carriers:

- Easy, efficient, and fast single-photon operation.
- Decoherence free, can store information for arbitrary long time.
- Travel at the speed of light.
- Other paradigms of quantum computing (boson-sampling like algorithms)
- No deterministic two qubit gates / only probabilistic ones
- Photons can be lost.

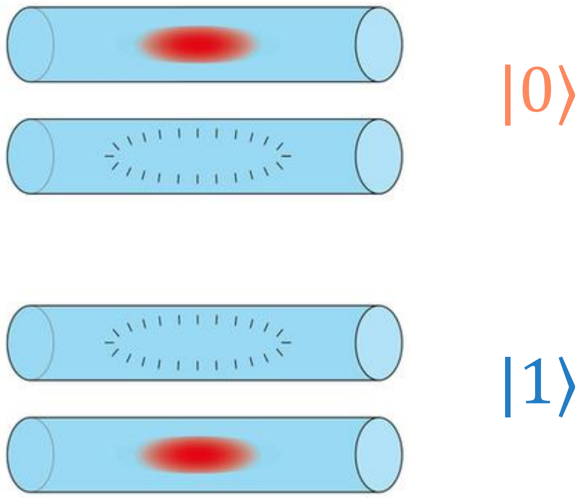
Quantum error correction with graph states:

- No two-qubit gate required only measurements on graph.
- Offline generation of photonic graph states

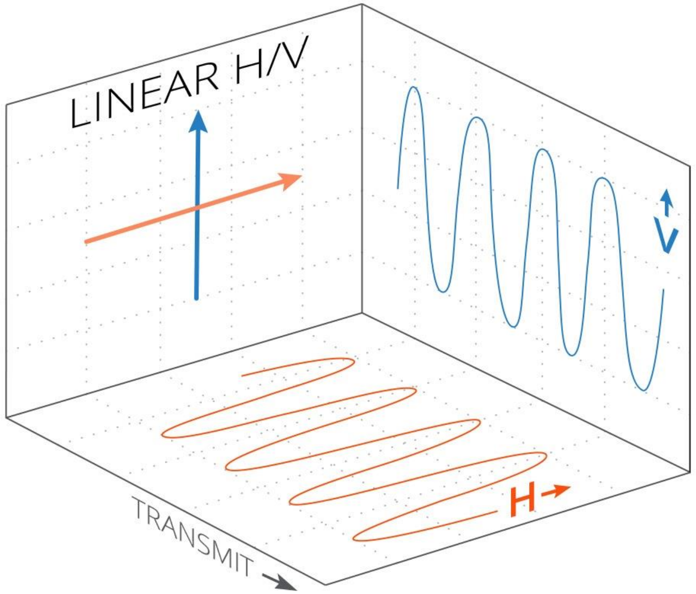


Dual-rail encoding
Photonic quantum computing

Defining a photonic qubit:
- Dual-rail encoding (2 modes for 1 photon)



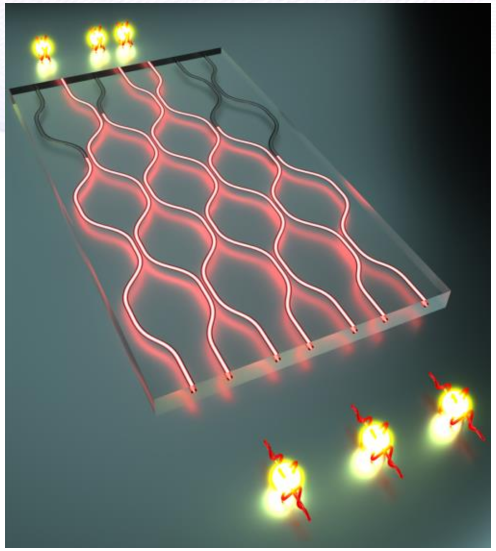
Path encoding



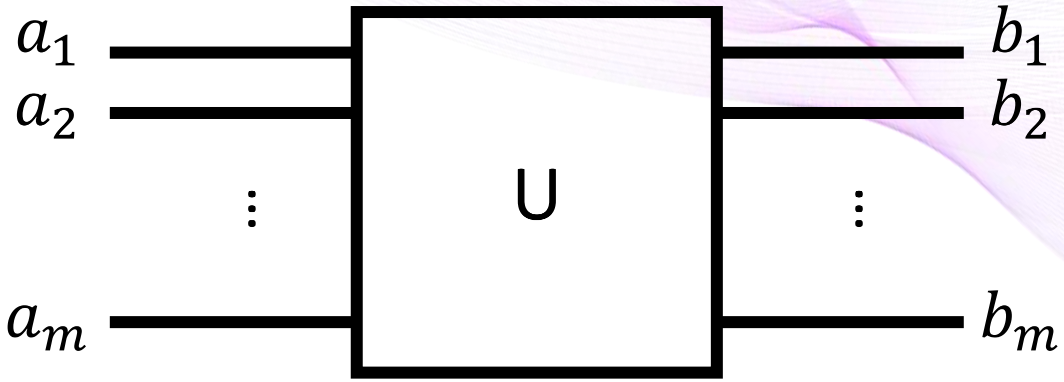
Polarization encoding

Entanglement with linear optics

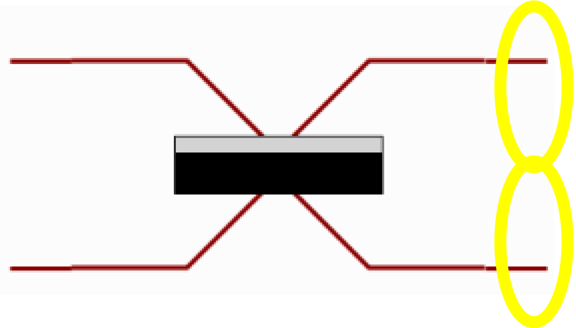
Photonic quantum computing



$$\vec{b} = (b_1, b_2, \dots, b_m)^T = U\,\vec{a} = U(a_1, a_2, \dots, a_m)^T$$



$|1\rangle$



$|1\rangle$

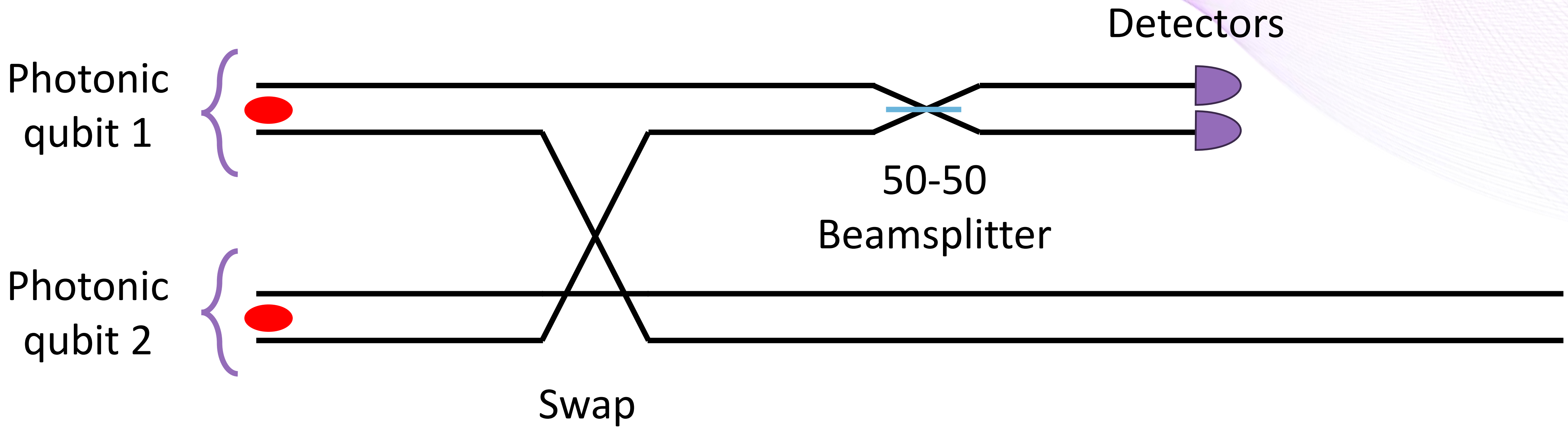
$|2,0\rangle - |0,2\rangle$

Cannot be in the qubit subspace
Intuition why no deterministic 2-qubit gates

Fusion gates

Photonic quantum computing

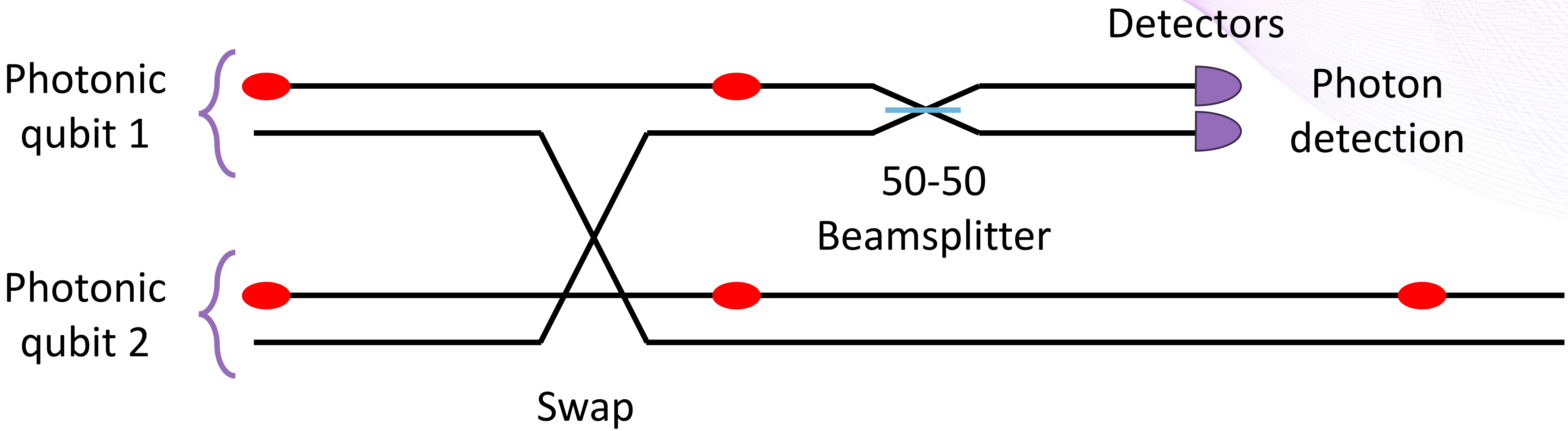
Focusing on a specific class of photonic gates: fusion gates
Type I fusion gates (take 2 photons and output one photon)



Fusion gates

Photonic quantum computing

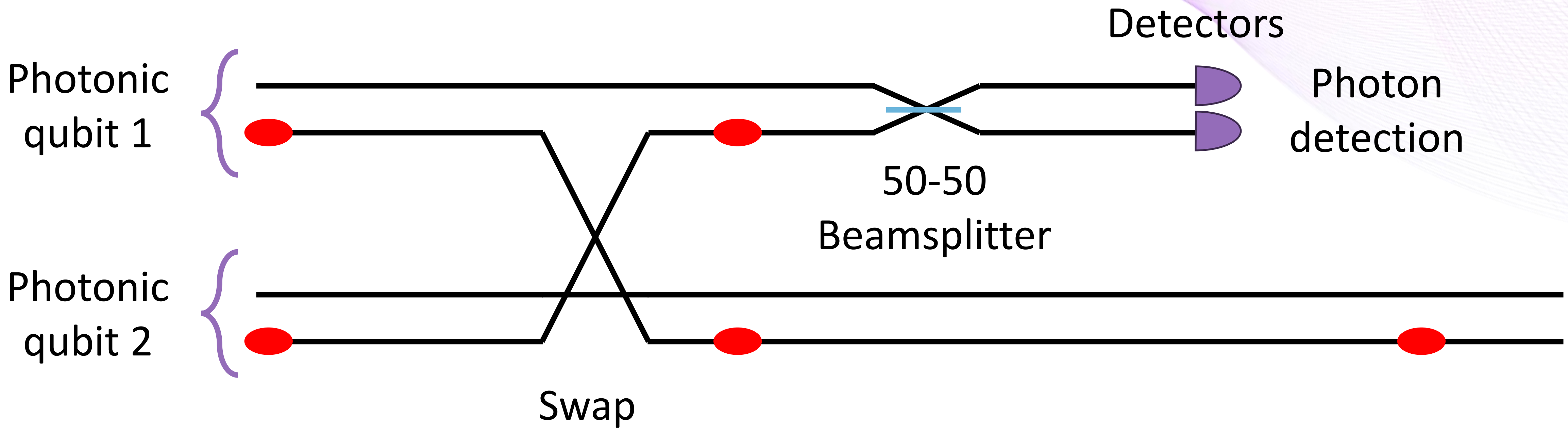
$$F_I = |0\rangle\langle 00| \ldots$$



Fusion gates

Photonic quantum computing

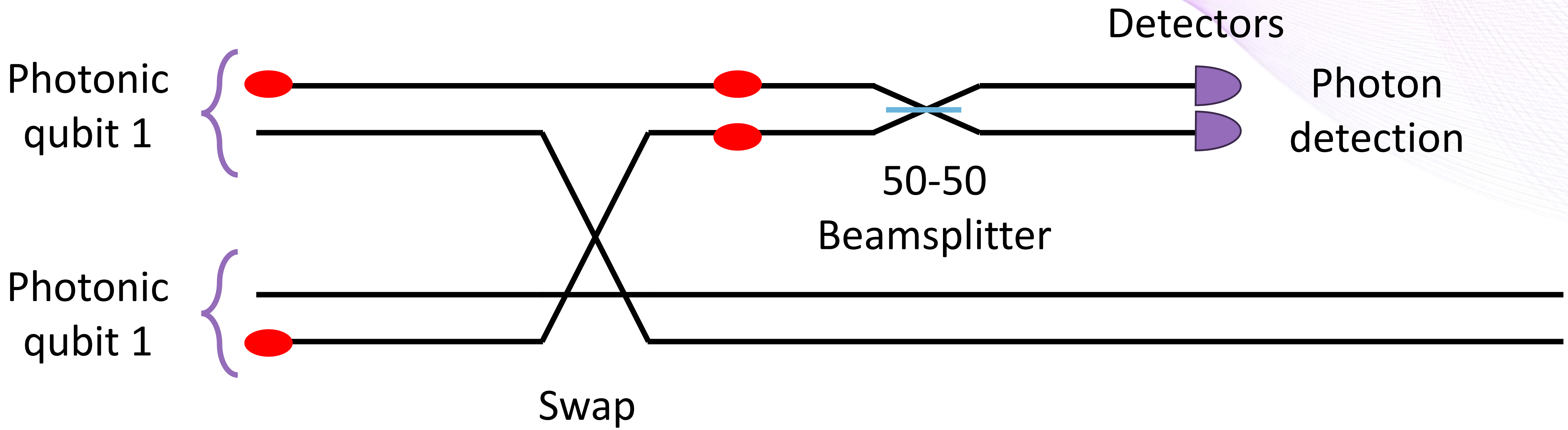
$$F_I = |0\rangle\langle 00| + e^{i\phi}|1\rangle\langle 11| \ldots$$



Fusion gates

Photonic quantum computing

$$F_I = |0\rangle\langle 00| + e^{i\phi}|1\rangle\langle 11| \ldots$$
$$Fail = |\emptyset\rangle\langle 01|$$



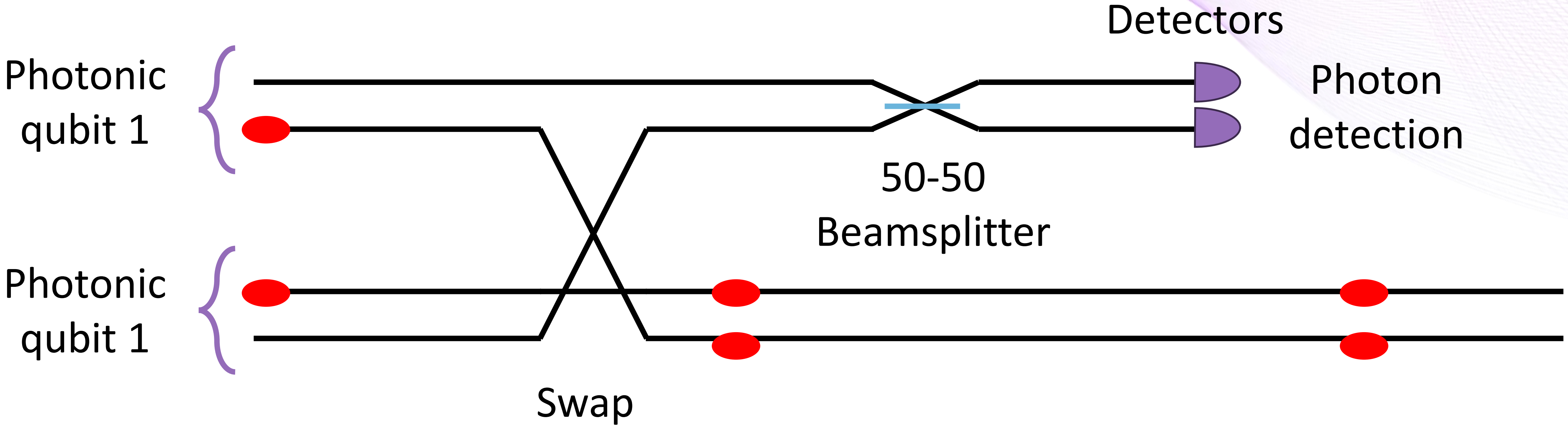
Fusion gates

Photonic quantum computing

$$F_I = |0\rangle\langle 00| + e^{i\phi}|1\rangle\langle 11| \ldots$$

$$Fail = |\emptyset\rangle\langle 01|,$$

$$Fail_2 = |2\rangle\langle 10|$$

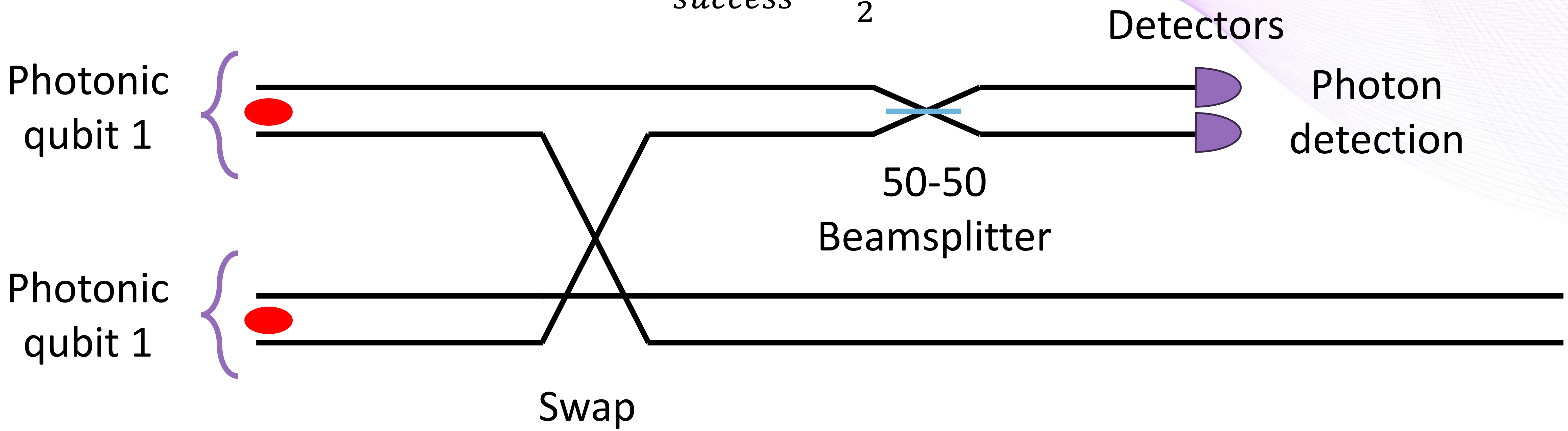


Fusion gates

Photonic quantum computing

In practice this gate takes 2 photons and output one

- $F_I = |0\rangle\langle 00| + (-1)^m|1\rangle\langle 11|$ (m detector)
- Postselect on successful outcome. $P_{success} = \frac{1}{2}$

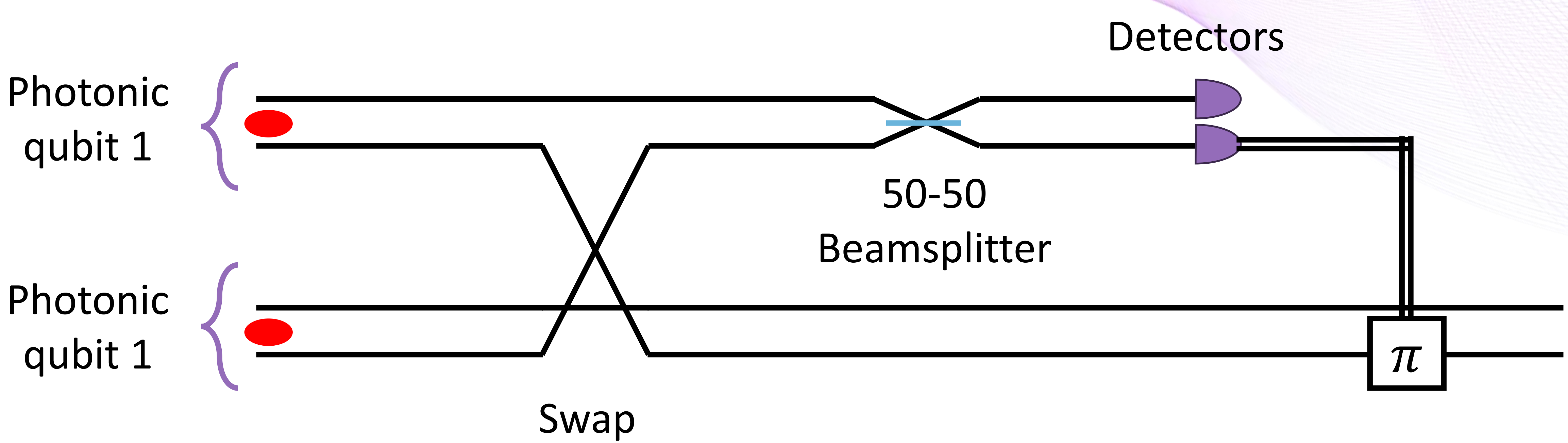


Fusion gates

Photonic quantum computing

In practice this gate takes 2 photons and output one

- $P_{success} = \frac{1}{2}$

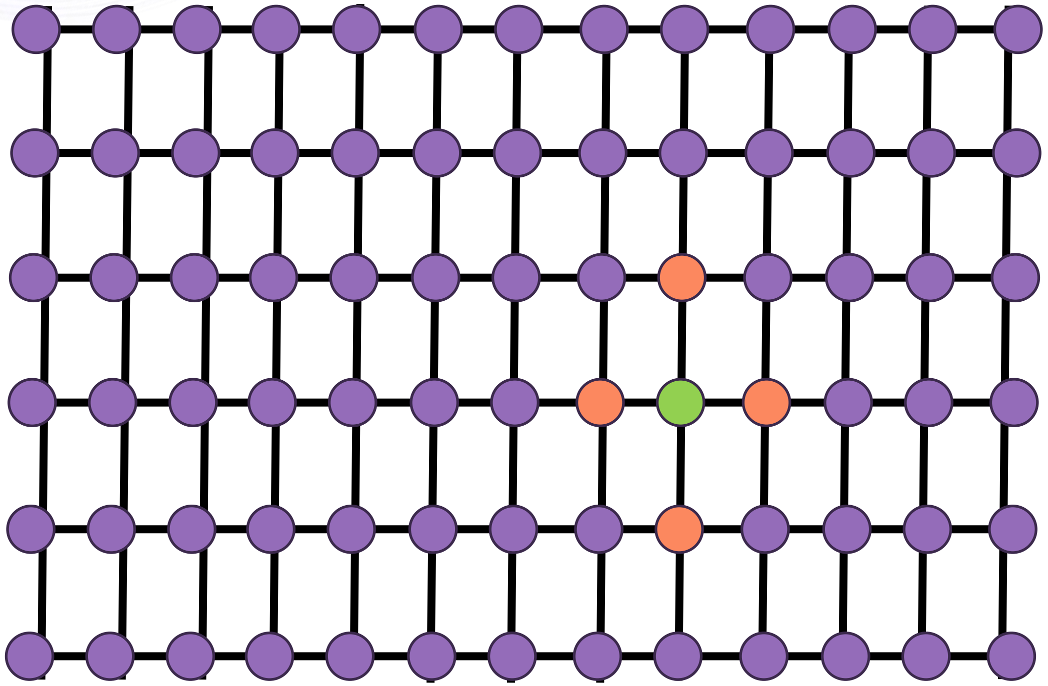


$$F_I = |0\rangle\langle 00| + |1\rangle\langle 11|$$

Stabilizer states and tree graph codes: The graph states

Partial solution: measurement-based quantum computing

A method to perform QC without the need of two-qubit gates (provided that you have a large entangled resource state…)



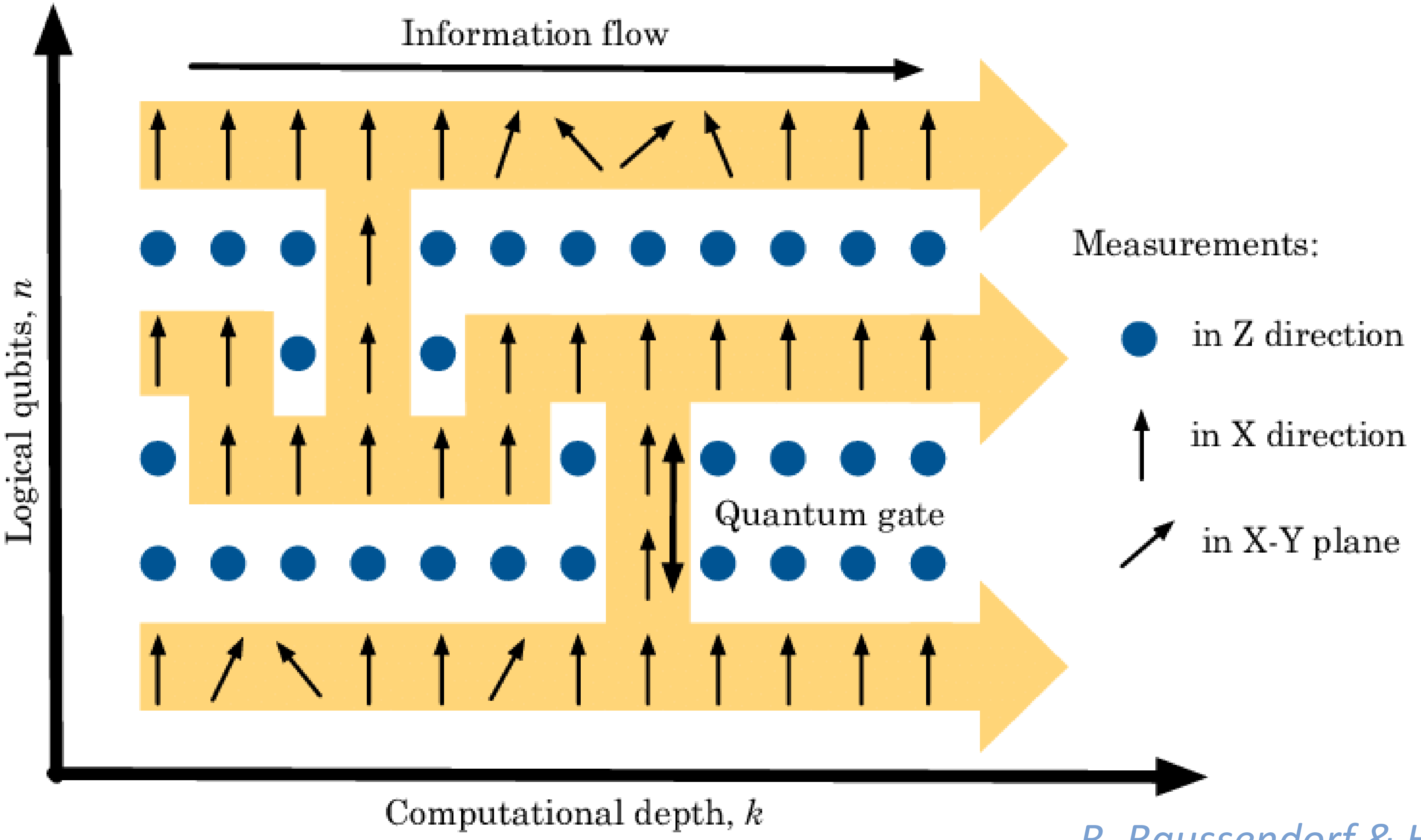
$|G = (E, V)\rangle$
E edge set
(entanglement link CZ)
V vertex set
(qubits $|+\rangle$)

$$CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

R. Raussendorf & HJ. Briegel, PRL 86, 9188 (2001)

Partial solution: measurement-based quantum computing

A method to perform QC without the need of two-qubit gates (provided that you have a large entangled resource state…)



$|G = (E, V)\rangle$

E edge set

(entanglement link CZ)

V vertex set

(qubits $|+\rangle$)

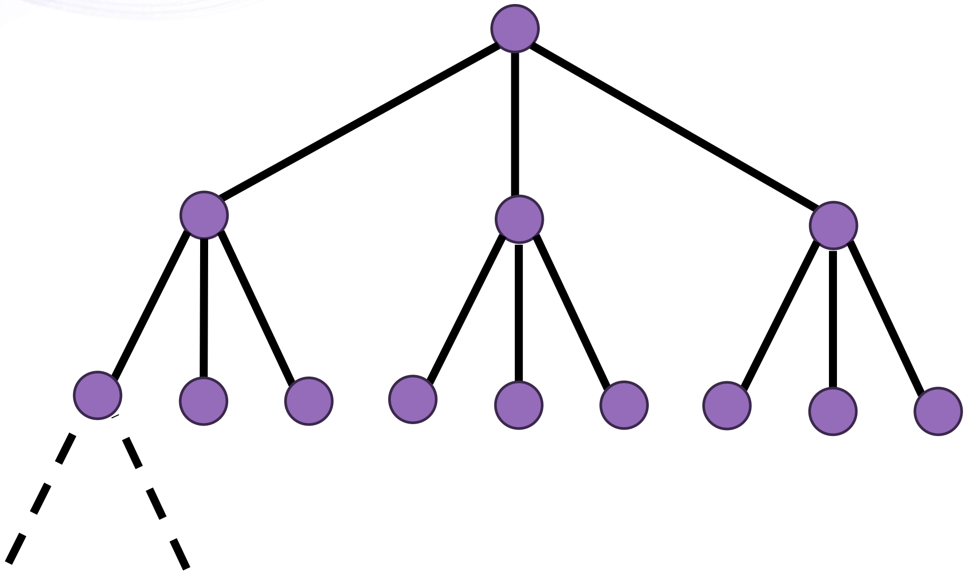
$$K_v|G\rangle = |G\rangle$$

$$K_v = X_v \prod_{(v,w)\in E} Z_w$$

R. Raussendorf & HJ. Briegel, PRL 86, 9188 (2001)

Measurement-based QEC with tree graph codes

MBQEC



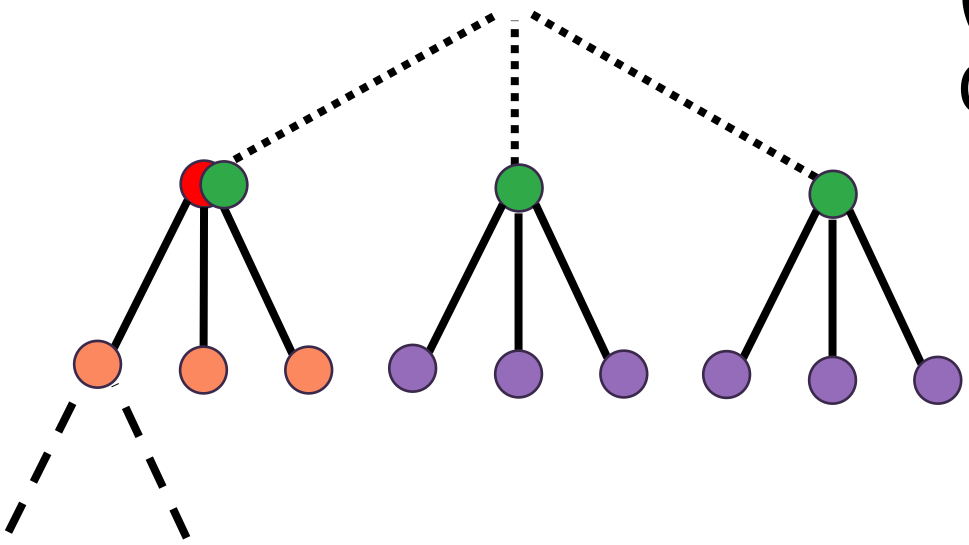
$$|G = (E,V)\rangle = \left(\prod_{(i,j)\in E} CZ_{ij}\right)|+\rangle^{\otimes v\in V}$$

Perfectly defined state.
(no qubit degree of freedom)
A lot of stabilizers

$$\forall v \in V, K_v = X_v \prod_{(v,w)\in \mathrm{E}} Z_w$$

Measurement-based QEC with tree graph codes

MBQEC



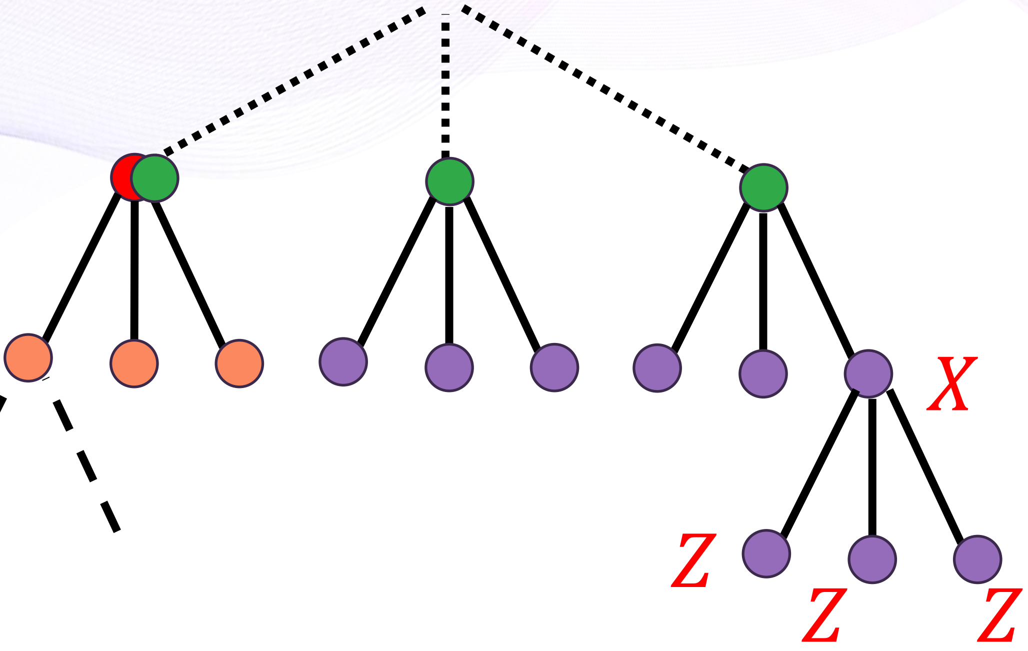
Create a tree code, remove the top qubit (and it's related stabilizers)

Create a qubit degree of freedom:

$$X_L = X\ ZZZ$$
$$Z_L = ZZZ$$

Measurement-based QEC with tree graph codes

MBQEC



How does it work. Suppose that you want to measure the logical Z_L operator. You can directly measure its qubits…
But you can also indirectly measure them using the stabilizers!

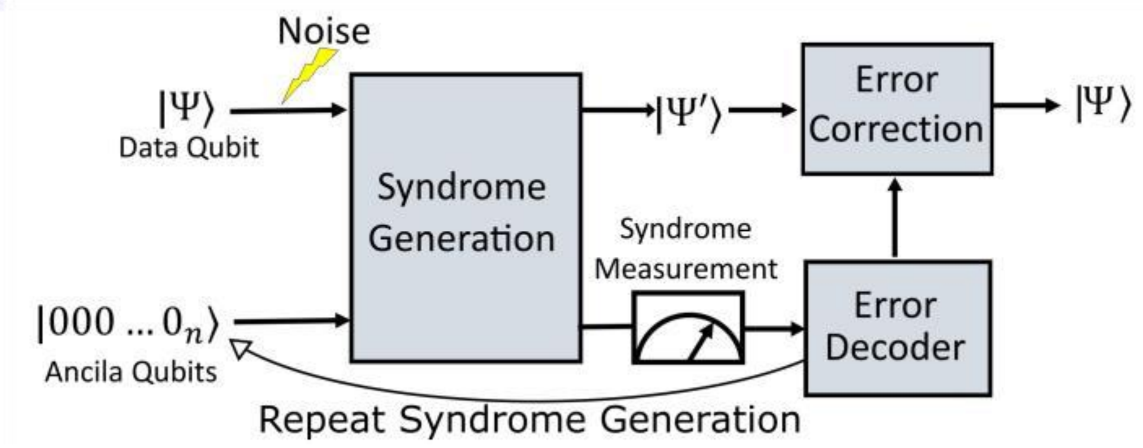
$$K_v|\psi\rangle = |\psi\rangle$$

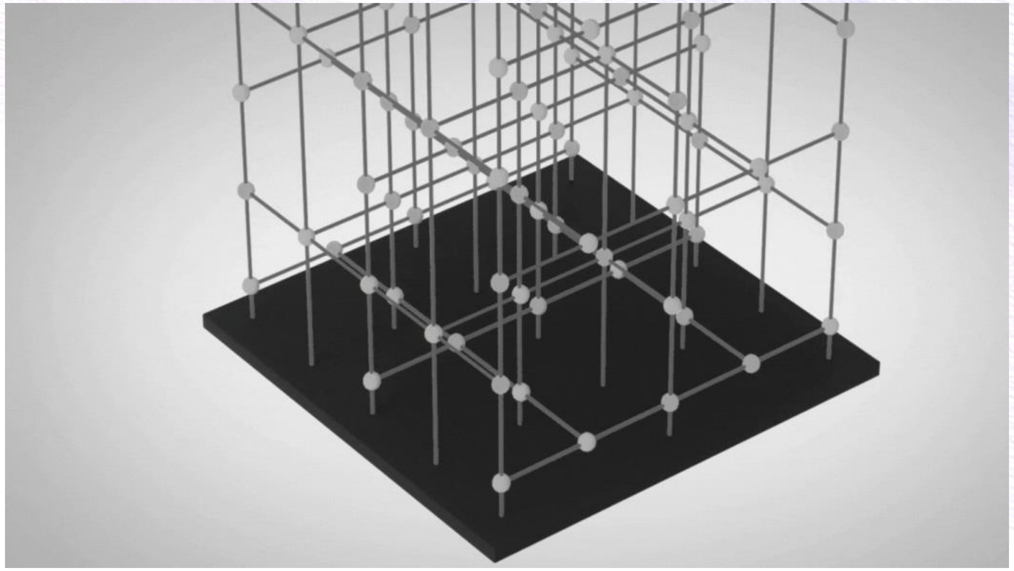
$$K_v = Z_{v_0} X_v \prod_{\substack{(v,w)\in E \\ w\neq v_0}} Z_w$$

$$Z_{v_0}|\psi\rangle = X_v \prod_{\substack{(v,w)\in E \\ w\neq v_0}} Z_w\,|\psi\rangle$$

Measurement-based QEC

MBQEC





Credit: Xanadu

In practice, tree graphs are too simplistic, 3D lattices are the real deal!

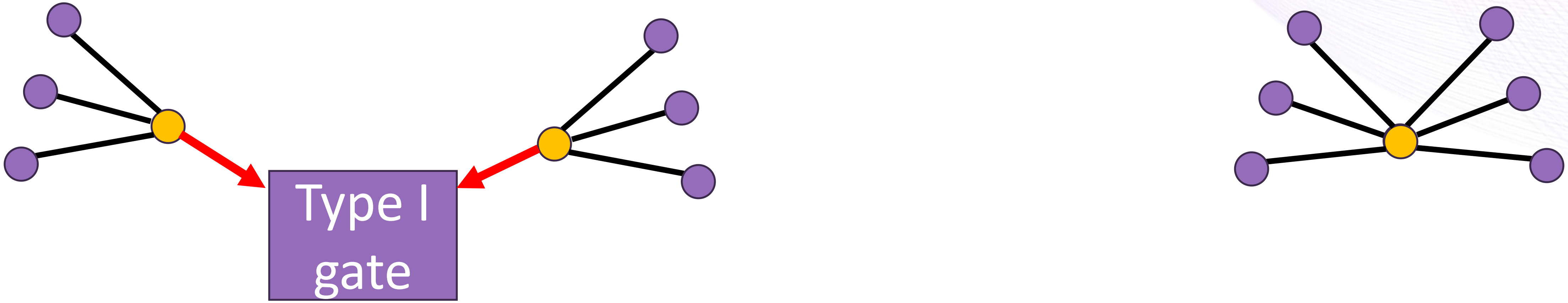
How to generate a large graph state without deterministic gates?

Fusion gates

Photonic quantum computing

Why this gate?

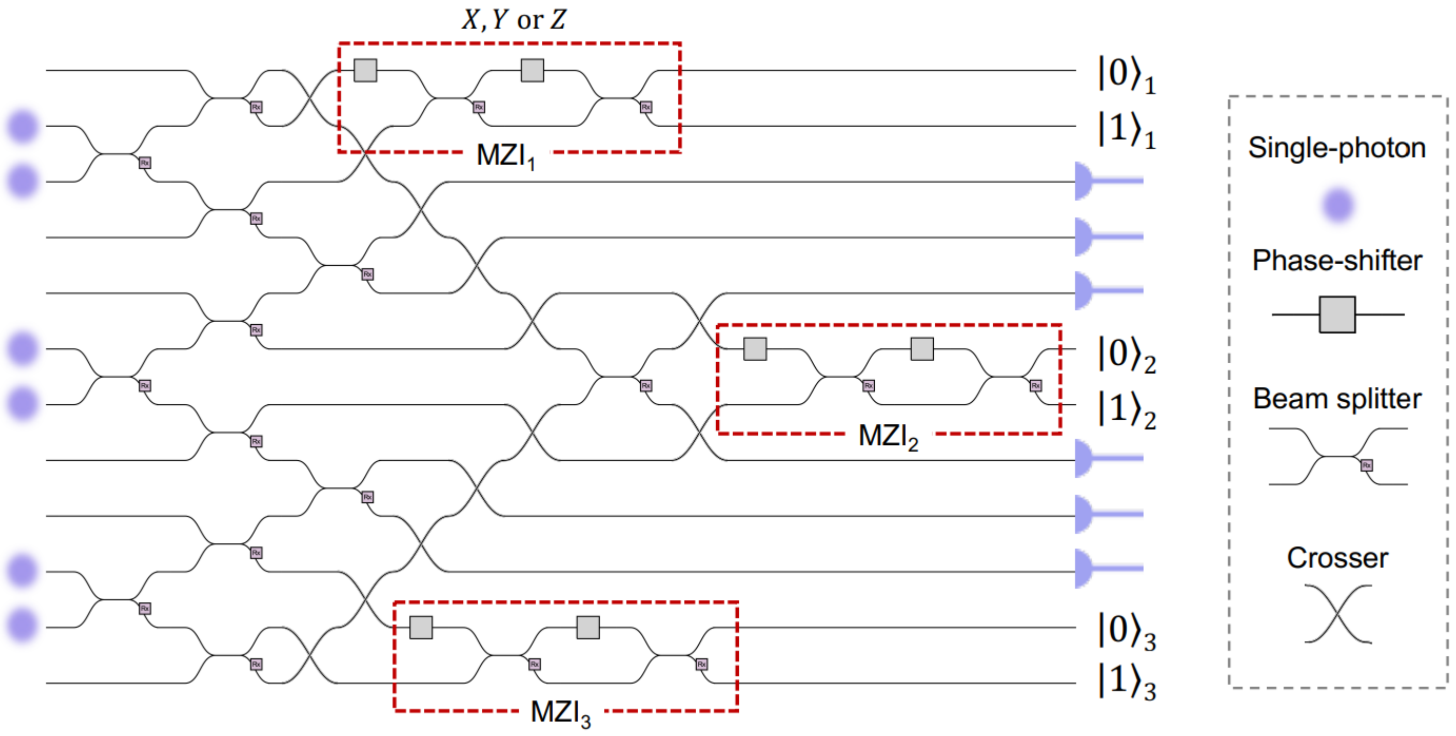
- It combines well with graph states
- It fuses the vertex of the two graphs
- You can create larger entangled state from smaller ones



Small entangled state generation
Photonic quantum computing

We also need to produce small entangled state.

Solution 1: Linear-optics.



Create a photonic GHZ state:

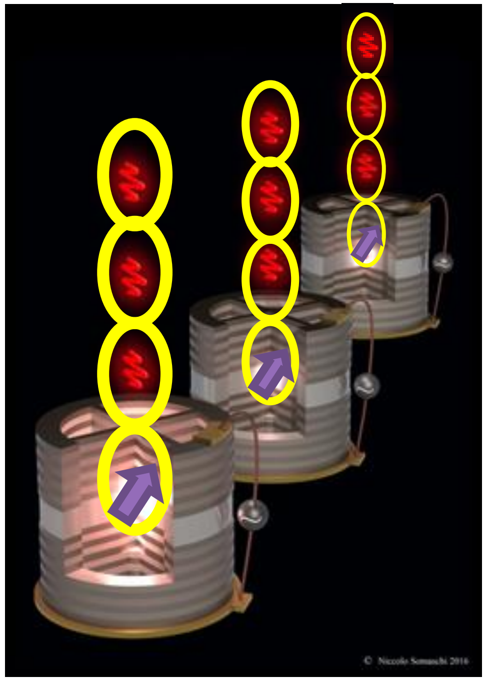
- $|000\rangle + |111\rangle$
- Requires 6 photons
- Ouputs 3 entangled photons
- Based on detection outcomes
- Success probability 1/32…

Small entangled state generation

Photonic quantum computing

We also need to produce small entangled state.

Solution 2: Deterministic generation through quantum emitters.



Entangled source of photons

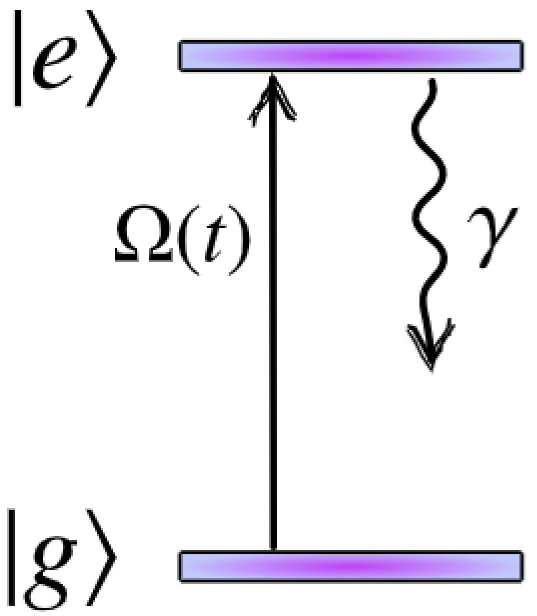
- Use a spin degree of freedom as a photon entangler
- Create photonic GHZ and linear graph states

N. Coste et al., Nat. Photon. 17, 582 (2023)

Small entangled state generation

Photonic quantum computing

Optical transitions:



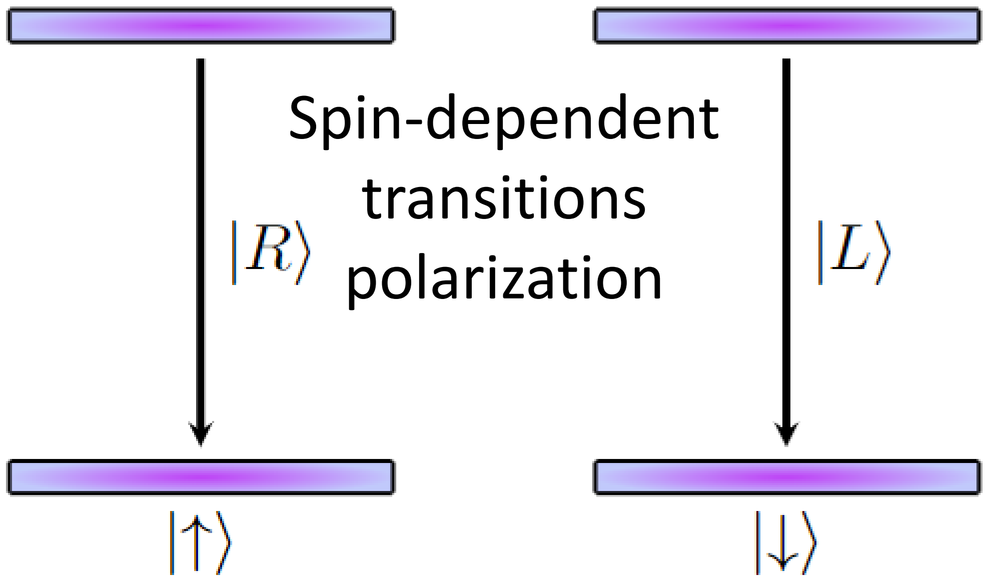
Two level system:

- Excite optically with a laser the ground state ($\Omega(t)$)
- The quantum emitter is in the excited state $|e\rangle$
- The quantum emitter relaxes its energy by emitting a single photon (in a time T_1, called the relaxation time).
- After $t \gg T_1$, the quantum emitter is in the ground state $|g\rangle$ and a single photon has been deterministically generated.

Small entangled state generation

Photonic quantum computing

Optical transitions:



Stable spin degree of freedom

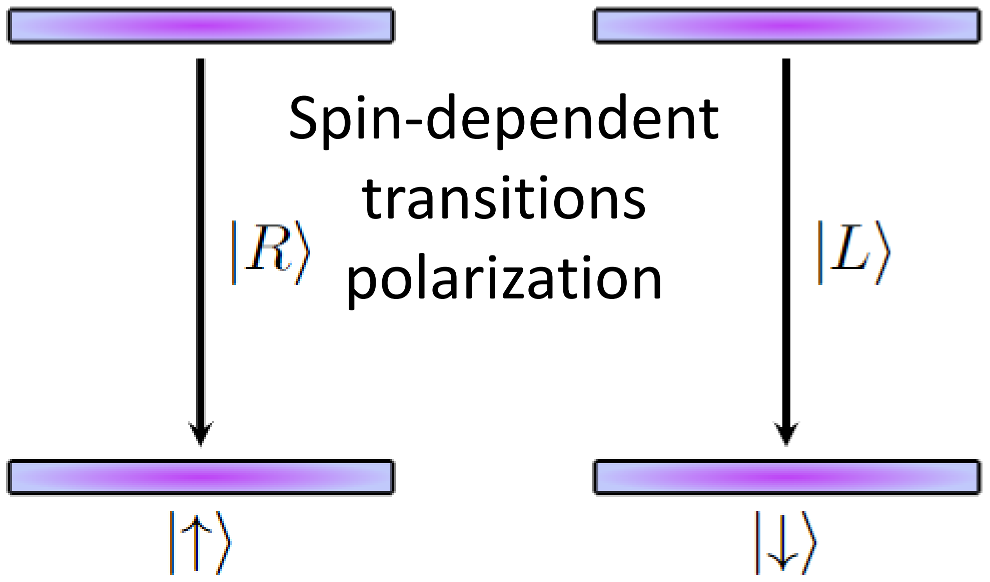
Four-level system:

- The spin is in a given initial state
$$|\psi_s\rangle = \alpha|\uparrow\rangle + \beta|\downarrow\rangle$$
- With a laser, put it in the two excited state.
- After spontaneous emission, a photon is emitted with spin-dependent polarization
$$|\psi_{s,ph}\rangle = \alpha|\uparrow, R\rangle + \beta|\downarrow, L\rangle$$

Small entangled state generation

Photonic quantum computing

Optical transitions:



Stable spin degree of freedom

$$|+\rangle = |\uparrow\rangle + |\downarrow\rangle$$

After first emission

$$|\psi_{s,ph}\rangle = \alpha|\uparrow, R\rangle + \beta|\downarrow, L\rangle$$

Second emission:

$$|\psi_s\rangle = \alpha|\uparrow, R, R\rangle + \beta|\downarrow, L, L\rangle$$

n^{th} emission:

$$|\psi_{s,ph}\rangle = |\uparrow\rangle|R\rangle^{\otimes n} + |\downarrow\rangle|L\rangle^{\otimes n}$$

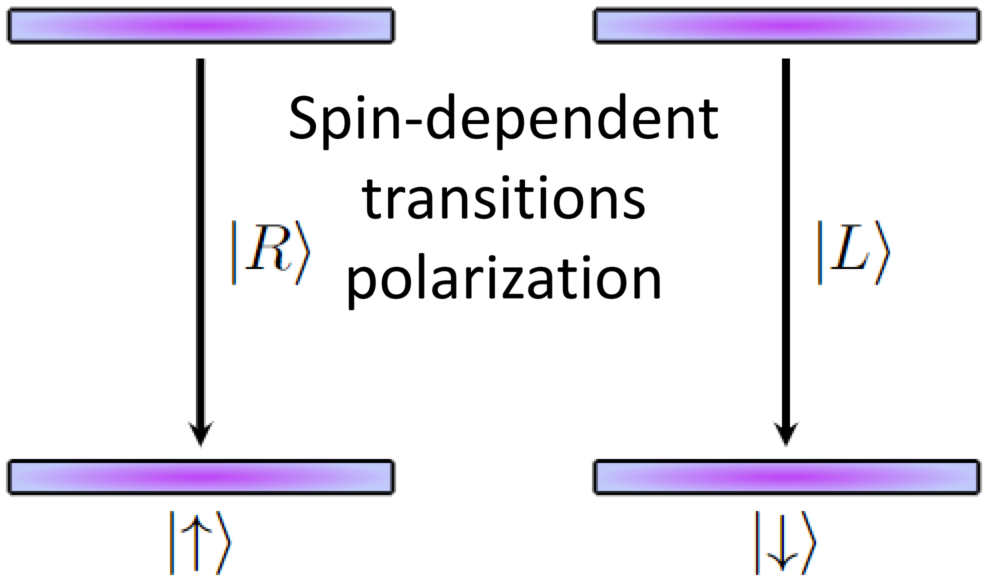
$$|\psi_{s,ph}\rangle = |0\rangle|0\rangle^{\otimes n} + |1\rangle|1\rangle^{\otimes n}$$

We can create a GHZ state deterministically

Small entangled state generation

Photonic quantum computing

Optical transitions:

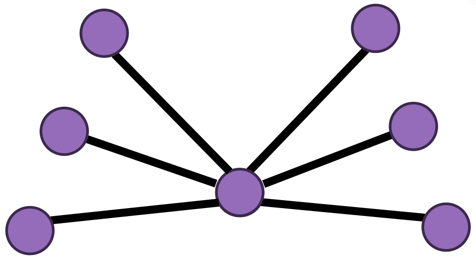


Stable spin degree of freedom

$$|\psi_{s,ph}\rangle = |0\rangle^{\otimes n} + |1\rangle^{\otimes n}$$

$$=$$

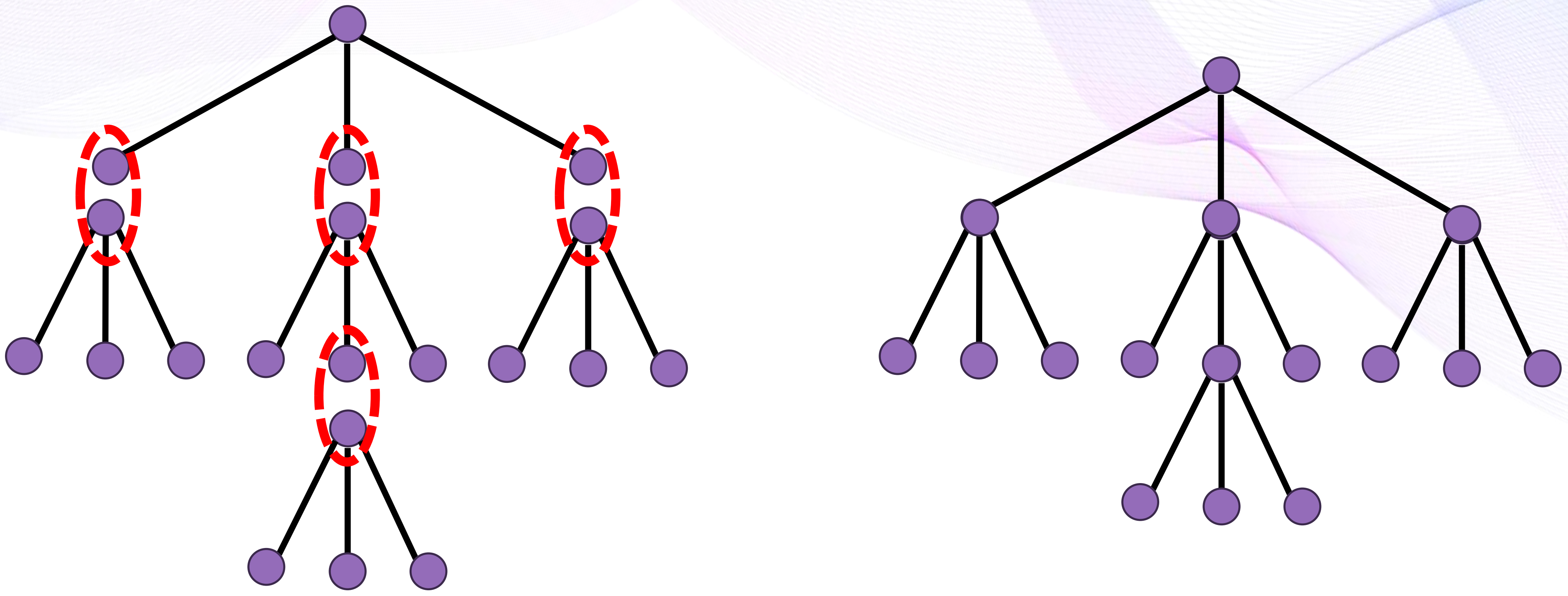
(up to single-qubit rotations)



This star graph state is in fact
$|0\rangle|+\rangle^{\otimes n-1} + |1\rangle|-\rangle^{\otimes n-1}$

Advanced graph state generation

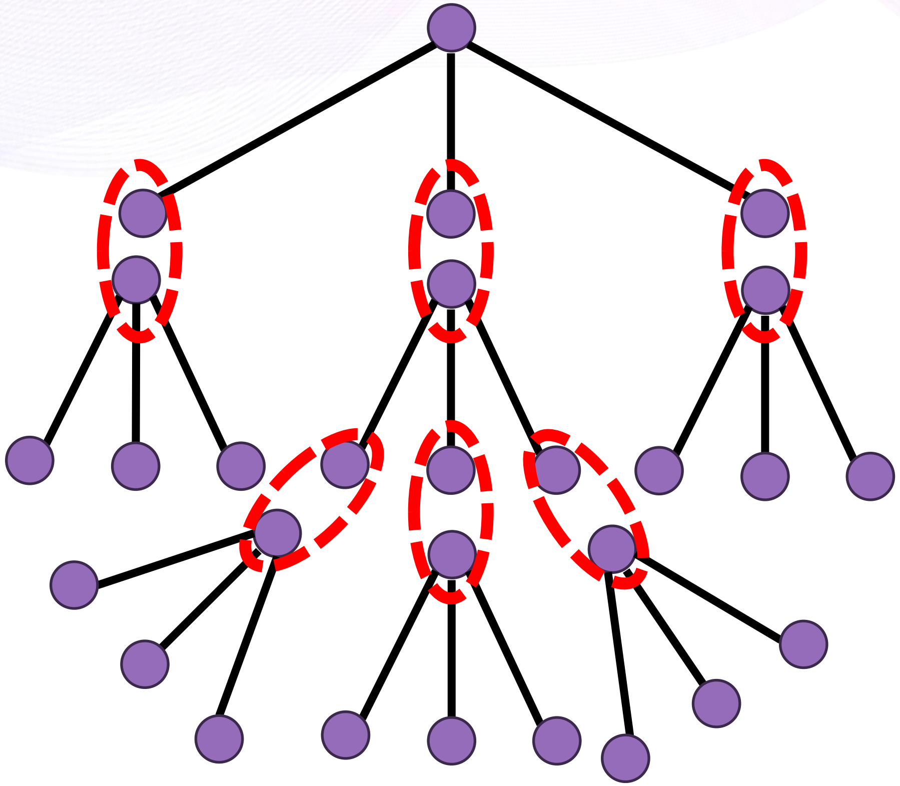
Combining fusions and small entangled state generation



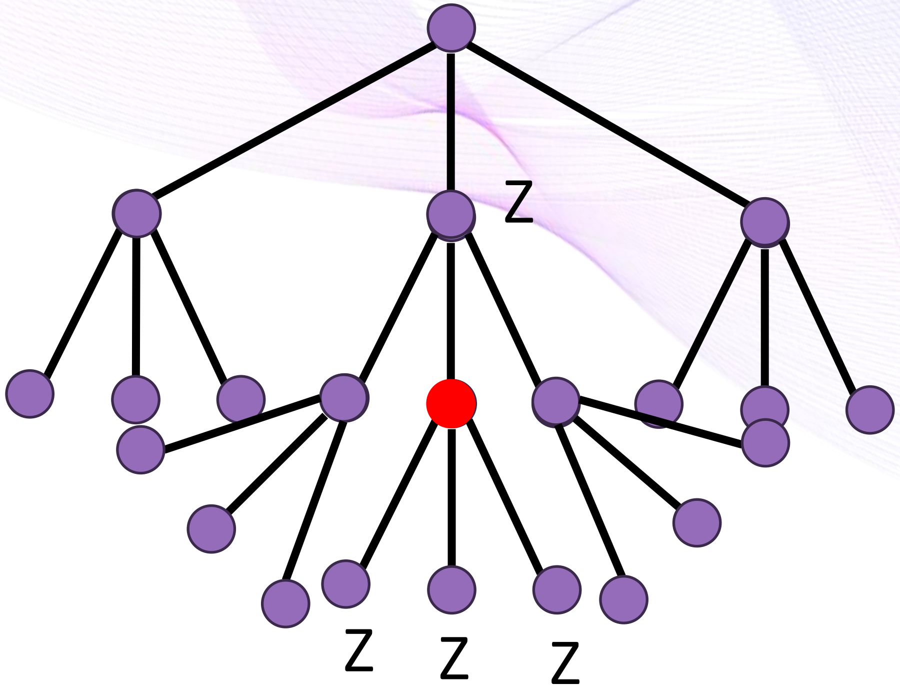
Successful

Advanced graph state generation

Combining fusions and small entangled state generation



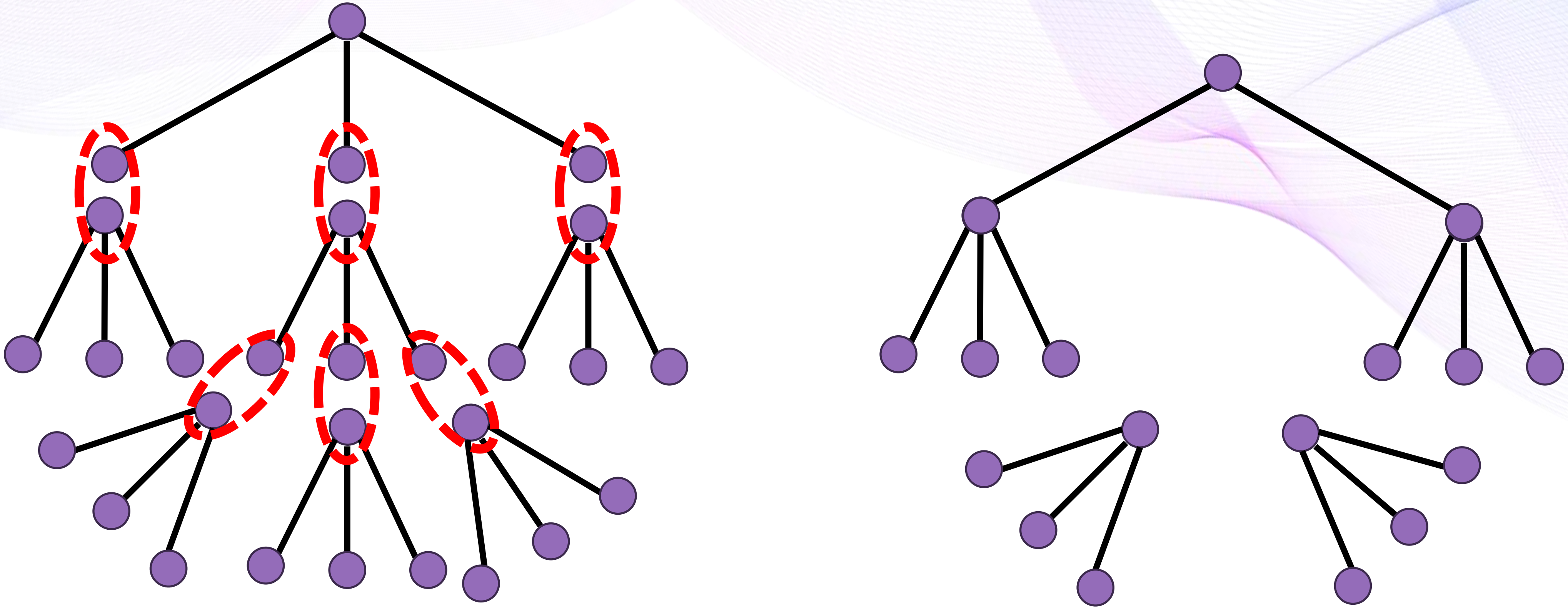
Failure



Failure

Advanced graph state generation

Combining fusions and small entangled state generation



Recycling idea

Fusion-based quantum computing

Fusion based-quantum computing

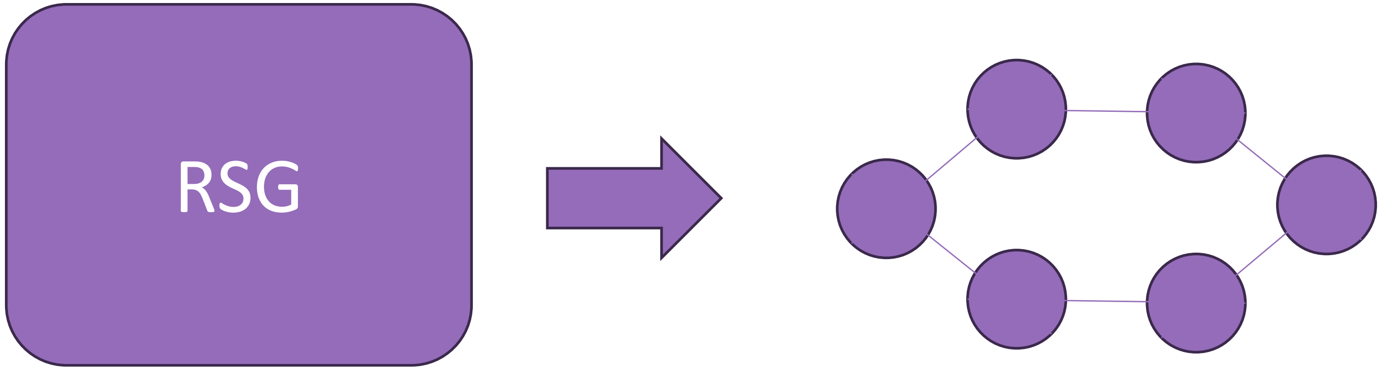
Mixing MBQC + probabilistic photonic gates

General intuition #1:

- Small entangled states are easier to produce than large ones
- If we have a system which can produce a graph with success proba p_G…
- …We can use N of these systems to produce, to produce at least 1 graph with proba

$$1 - (1 - p_G)^N \xrightarrow[N \to \infty]{} 1$$

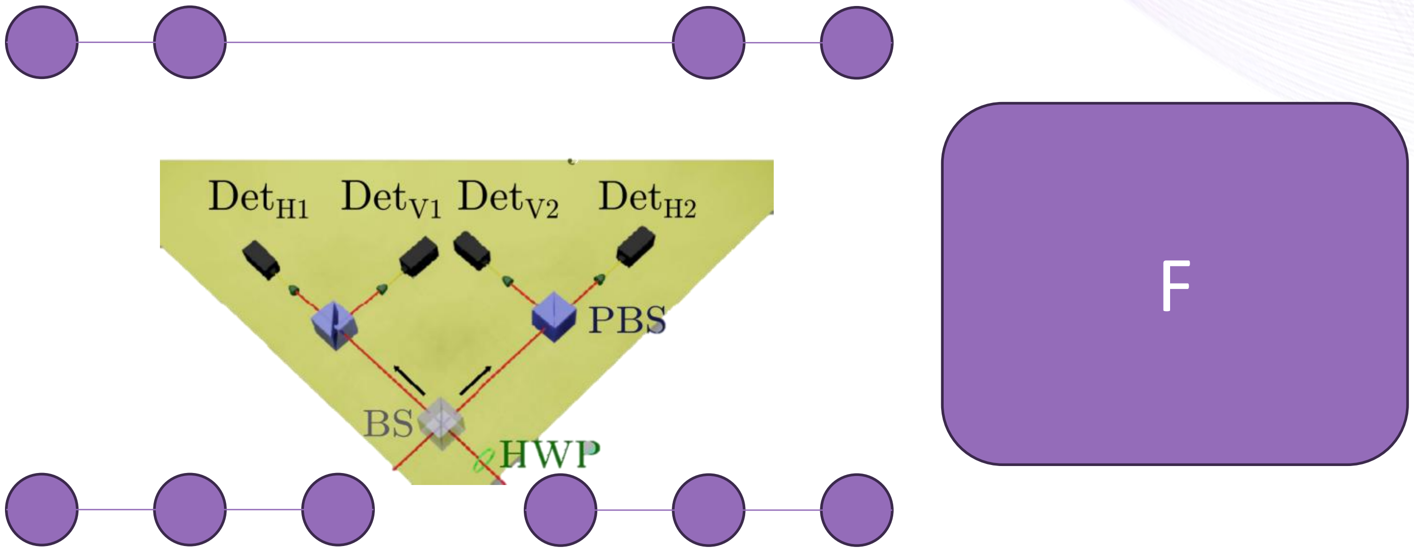
- We can build a resource state generator which produce a small graph with arbitrarily high probability



Fusion based-quantum computing
Mixing MBQC + probabilistic photonic gates

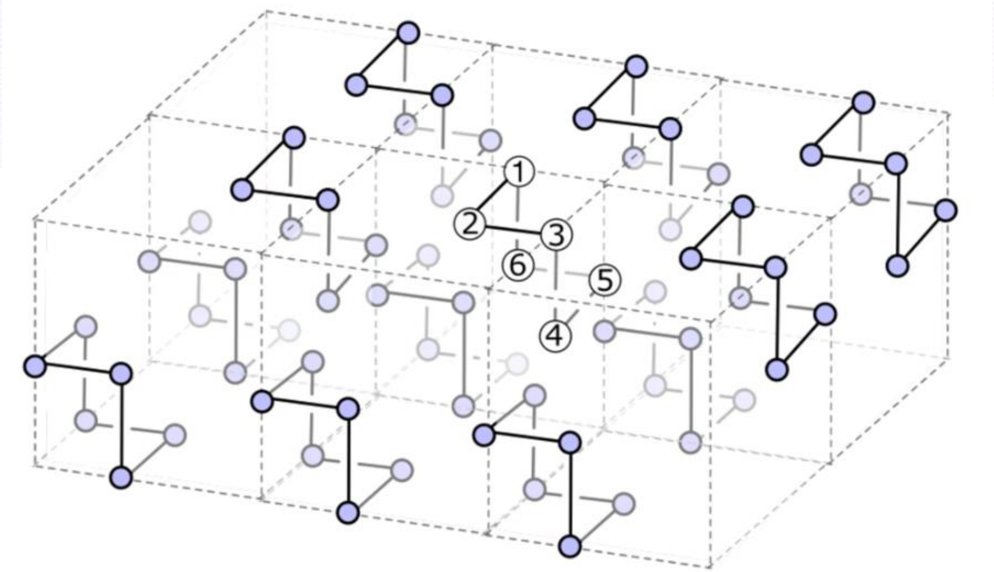
General intuition #2:

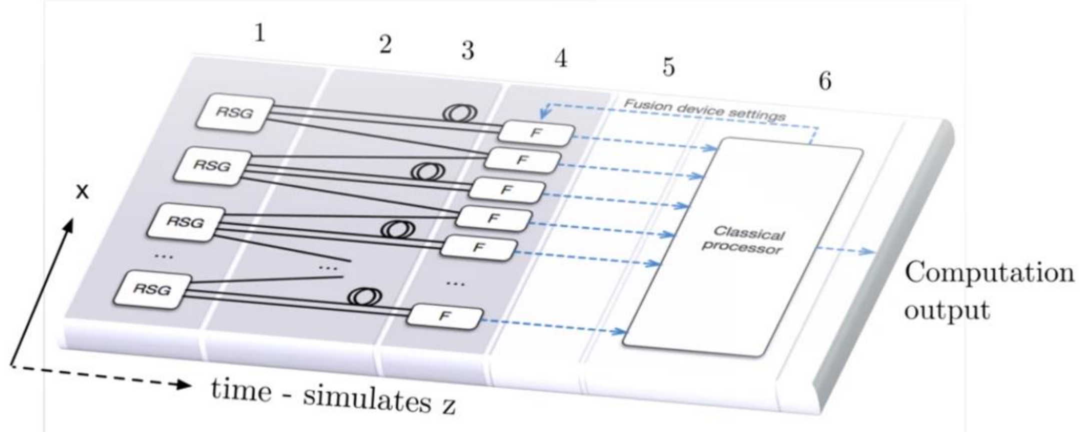
- Quantum gates have smaller success rate than fusion gates
- Fusion gates can have arbitrarily large success probability (provided ancilla use)
- Replace CNOT gates by fusion gates (BSM)

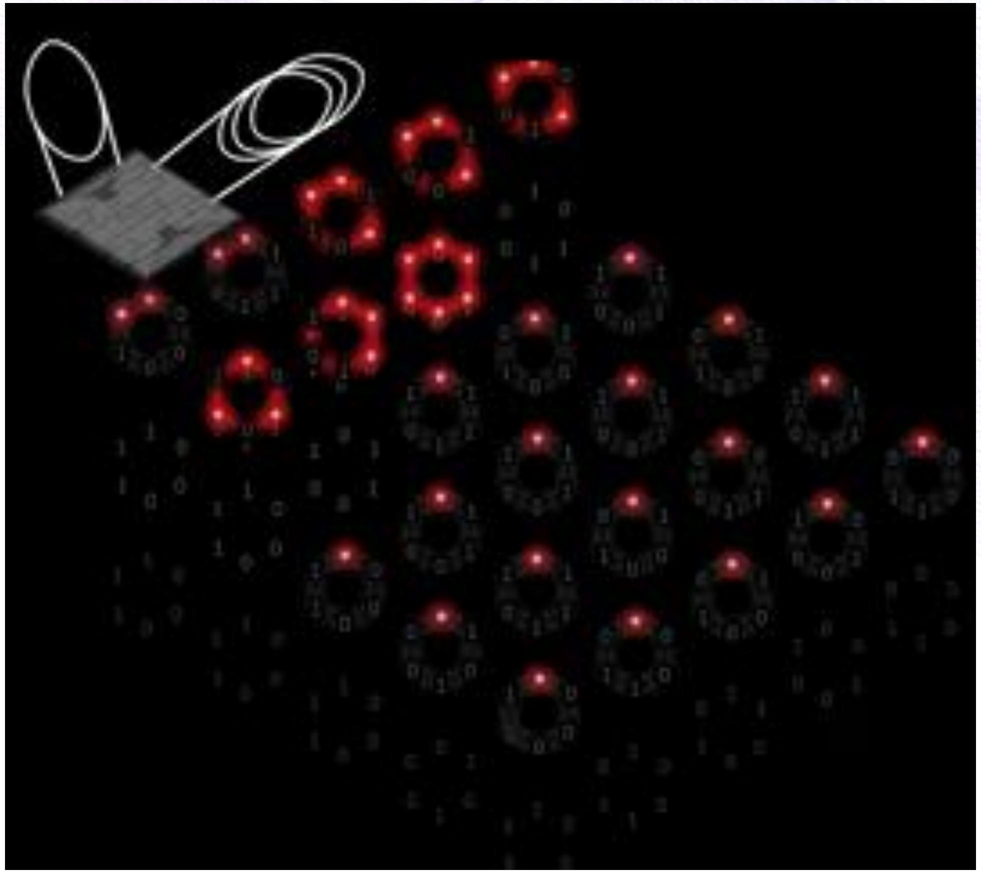


Fusion based-quantum computing

Mixing MBQC + probabilistic photonic gates



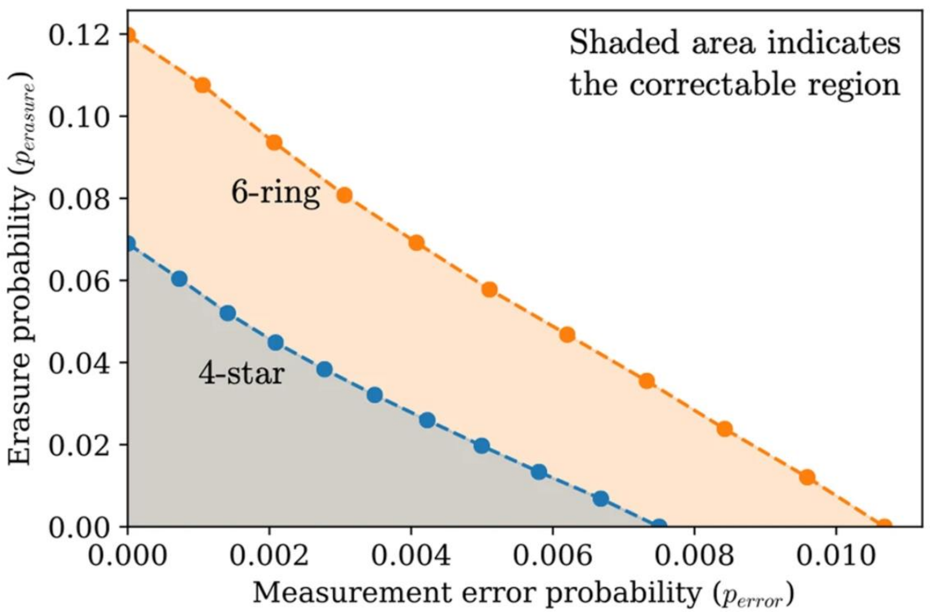




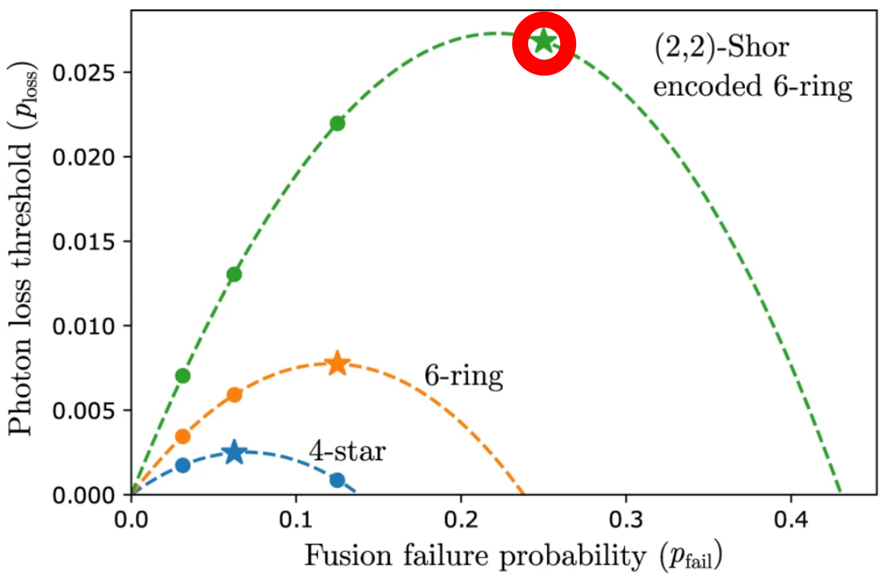
Fusion-based quantum computing

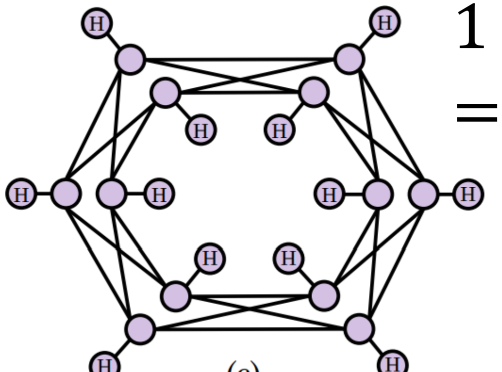
Performances

Loss probability
of a fusion gate



Computational error probability
of a fusion gate





(c)

$$1 - p_{erasure} = (1 - p_{fail})(1 - p_{loss})^n$$

(2,2)-Shor encoded 6-ring

Conclusion

What have we seen?

Introduction about quantum error correction:

- Need to correct blitflips and phaseflips
- An introduction to the stabilizer formalism (the main framework for QEC)
- Syndrome extraction in QEC (with circuit-based paradigm)

Introduction to graph state codes:

- Codes particularly well suited for measurement-based QEC (photonics friendly!)
- Basic error correction schemes with trees.

What have we seen?

Photonic ingredients to produce graph codes.

- Simple fusion gates
- Small graph state generation through linear-optics
- Small graph state generation using quantum emitters

A brief introduction about more advanced schemes

- Fusion-based quantum computing

Disclaimer

The field of fault-tolerant quantum computing is vast! This lecture is only an introduction.

What I haven't discuss here

- Quantum error correction is a very active field with recent important discoveries:
  - "Standard" codes like the surface codes
  - "Good" quantum error correcting codes (quantum Low-Density Parity Check codes)
  - Quantum error correction *circuits* *https://www.youtube.com/watch?v=tNACODva-6A*
- Decoding a code is a critical problem too, not trivial at all.
  - Minimum-Weight Perfect Matching / Union Find decoders

Disclaimer

What I haven't discuss here (follow up)

- Performing fault-tolerant gates on logically-encoded qubits
  - Eastin-Knill theorem
  - Lattice surgery / Magic state distillation
- Conversion from QEC to graph states
  - MBQC https://www.youtube.com/watch?v=zBjAoOW3xHk
  - Foliation technique https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.117.070501
  - The 3D "Raussendorf Harrington Goyal" lattice
- Advanced photonic gates for graph state generation
  - Ancilla-photon-assisted gates
- Deep connections with quantum information theory

Thank you