# Quantum error correction based on low-density parity check codes

Bane Vasić
Department of Electrical and Computer Engineering
Center for Quantum Networks
University of Arizona

joint work with
Nithin Raveendran, Asit Kumar Pradhan and Narayanan Rengaswamy
University of Arizona

Funded by: NSF-CIF 1855879, NSF CIF-2106189, NSF CCF-2100013, NSF CCSS-2027844, NSF CCSS-2052751, and NASA SURP

.

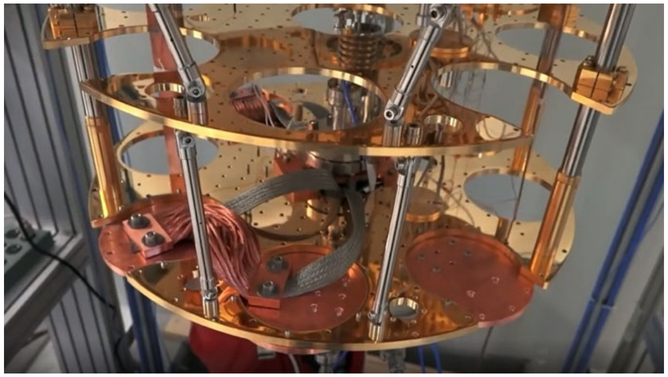
THE UNIVERSITY OF ARIZONA.
TUCSON ARIZONA

# Quantum supremacy example - classical versus quantum factoring

- To factor a 2048 bit number to break the RSA cryptosystem
- Classical algorithm:
  - 10 year runtime, server farm covering ¼ of North America,
  - $10^6$ terawatt (entire world's supply of fossil fuels in one day),
  - Cost $\$10^6$ trillion.
- Quantum algorithm on a superconducting quantum computer:
  - 16 hours runtime, 1cm spacing for wires,
  - 10 megawatt, cost <u>only</u> $100 billion.
  - 100k logical qubits, 200M physical qubits, ~$10k/qubit

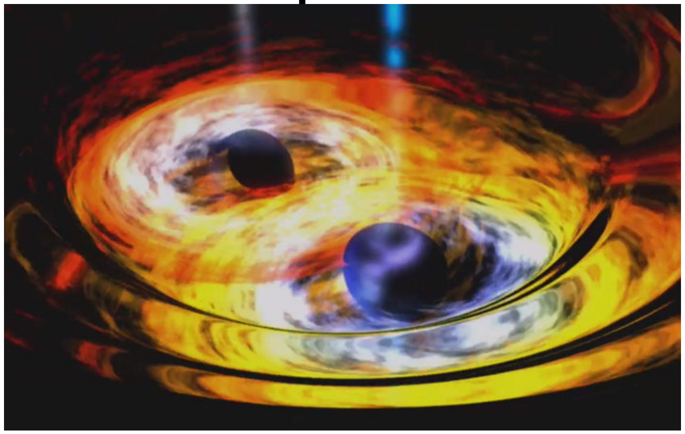
Example from: http://www.capri-school.eu/capri14/lectures/Martinis_Capri2014.pdf

# Impact of quantum technologies



computation

secure communications



sensing

simulation

sensing image credit: https://svs.gsfc.nasa.gov/cgi-bin/details.cgi?aid=10140

# Fundamental principle 1: quantum superposition

Classical

or

head = 1

tail=0

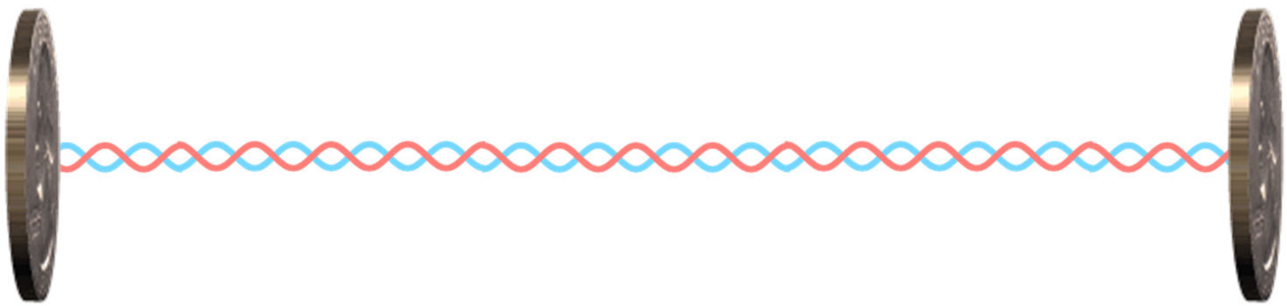
Quantum

- Analogy: flip a coin, but do not catch it (“measure” it).
- Until the coin is in the air, it is in a *superposition* of `0’ and `1’ quantum states: a “qubit”:

# Quantum superposition - Shrödinger's cat

THE UNIVERSITY OF ARIZONA.
TUCSON ARIZONA

# Fundamental principle 2: quantum entanglement



- This represents a pair of *entangled qubits*, or an *"ebit."*

Correlated

left right

Anti-correlated

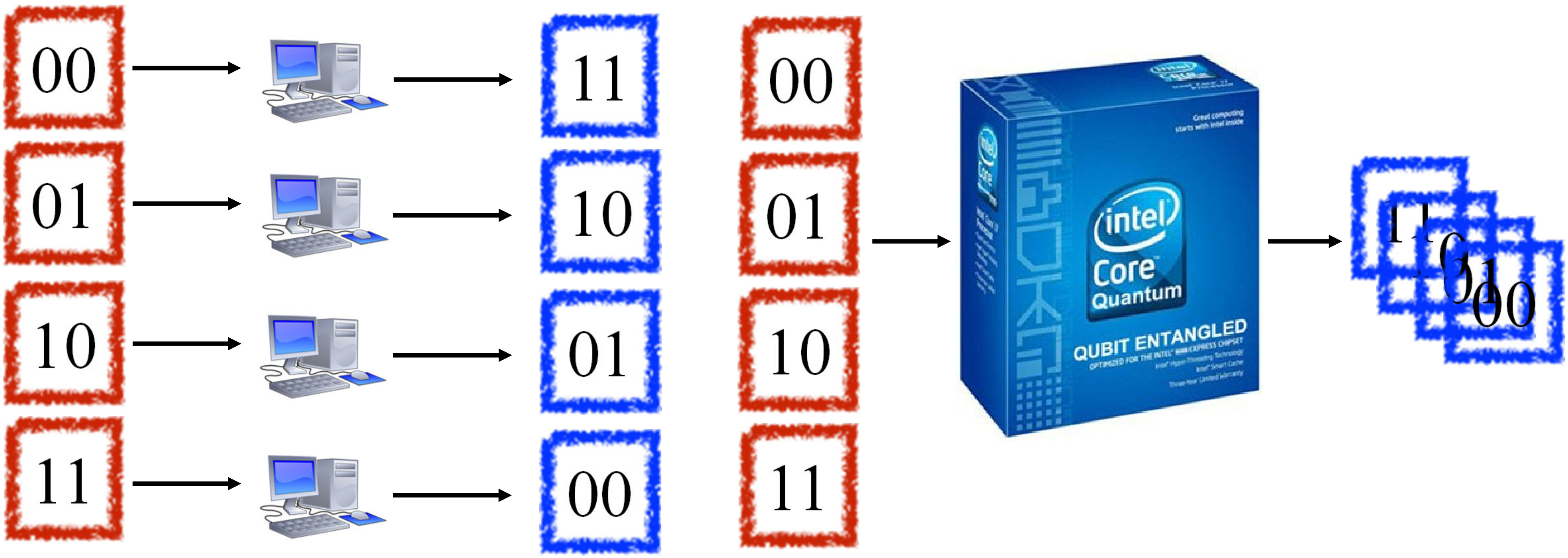
left right

THE UNIVERSITY OF ARIZONA.
TUCSON ARIZONA

# Classical and quantum computers - parallelism

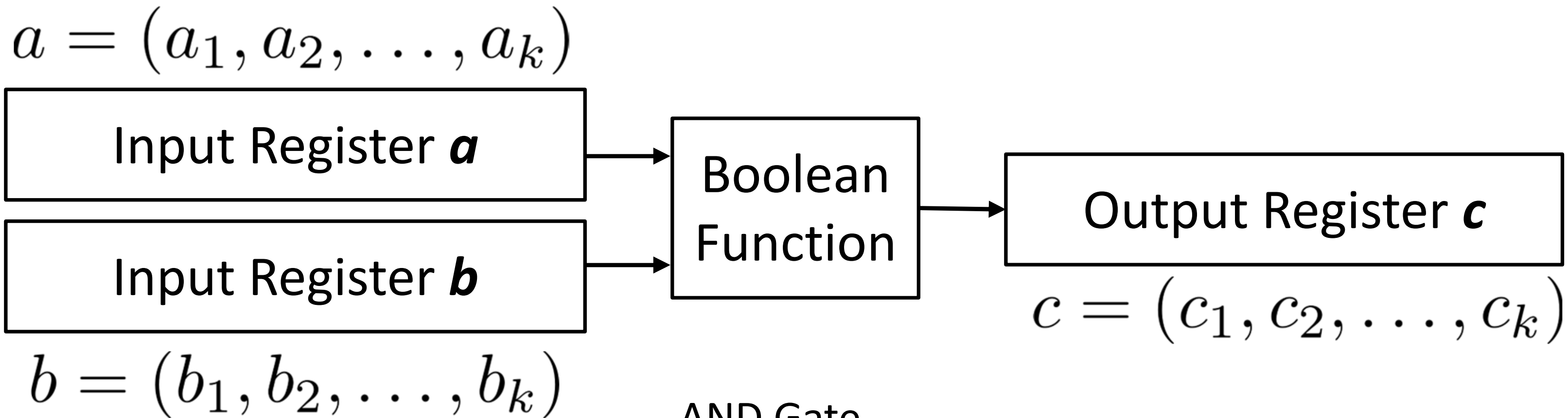
Classical

Quantum

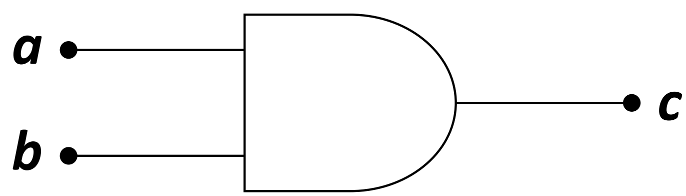


# Classical and quantum operations- logic gates

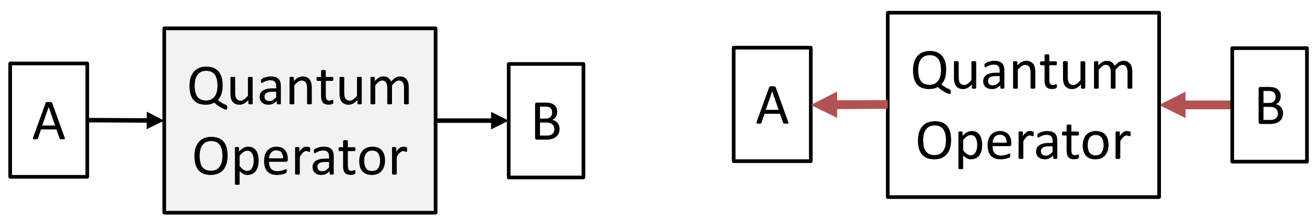
- Classical




AND Gate

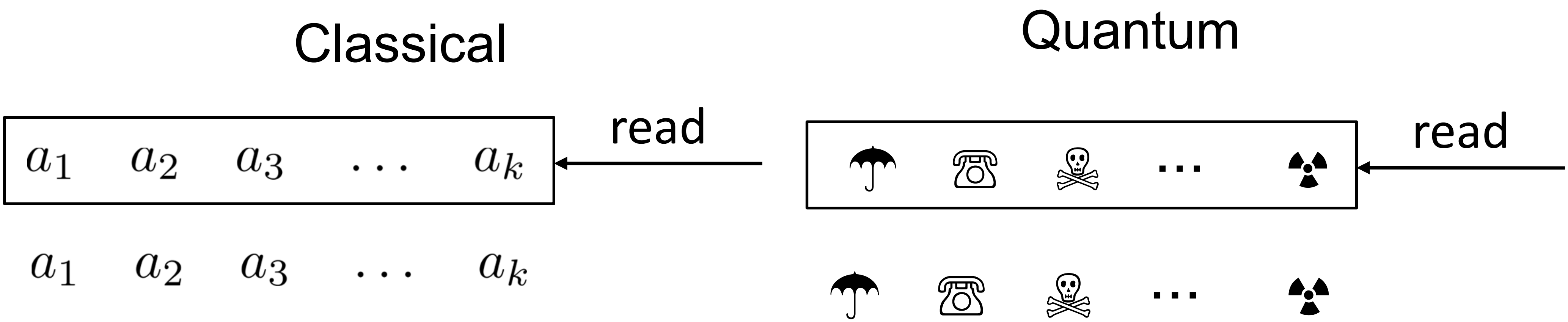



- Quantum




  – **Unitarity:** Quantum operations are time reversible

# Classical and quantum operations - read

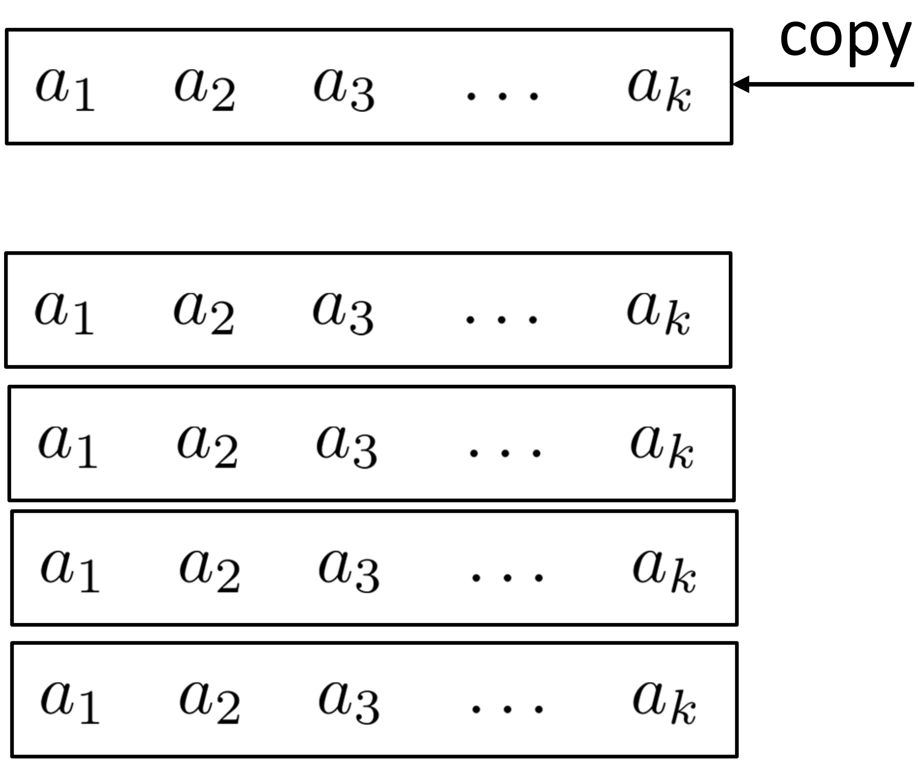



**Measurement**

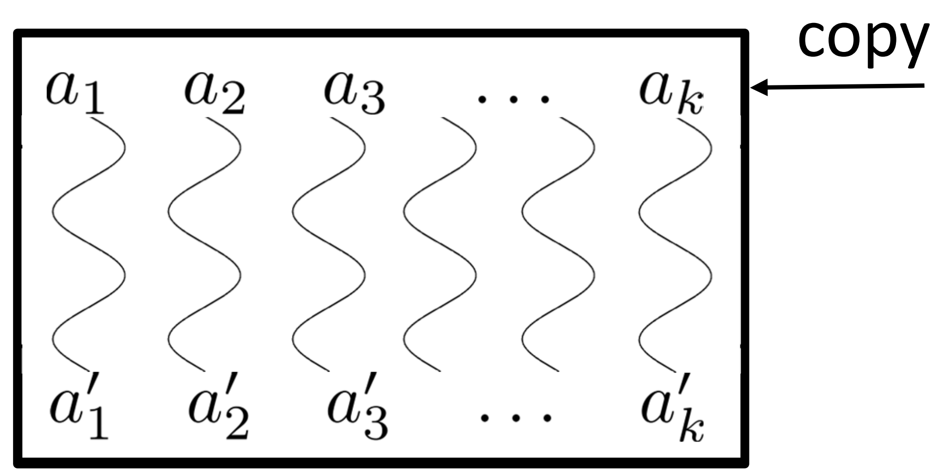
observing the quantum state results in the collapse of the system

# Classical and quantum operations - copy

## Classical




## Quantum

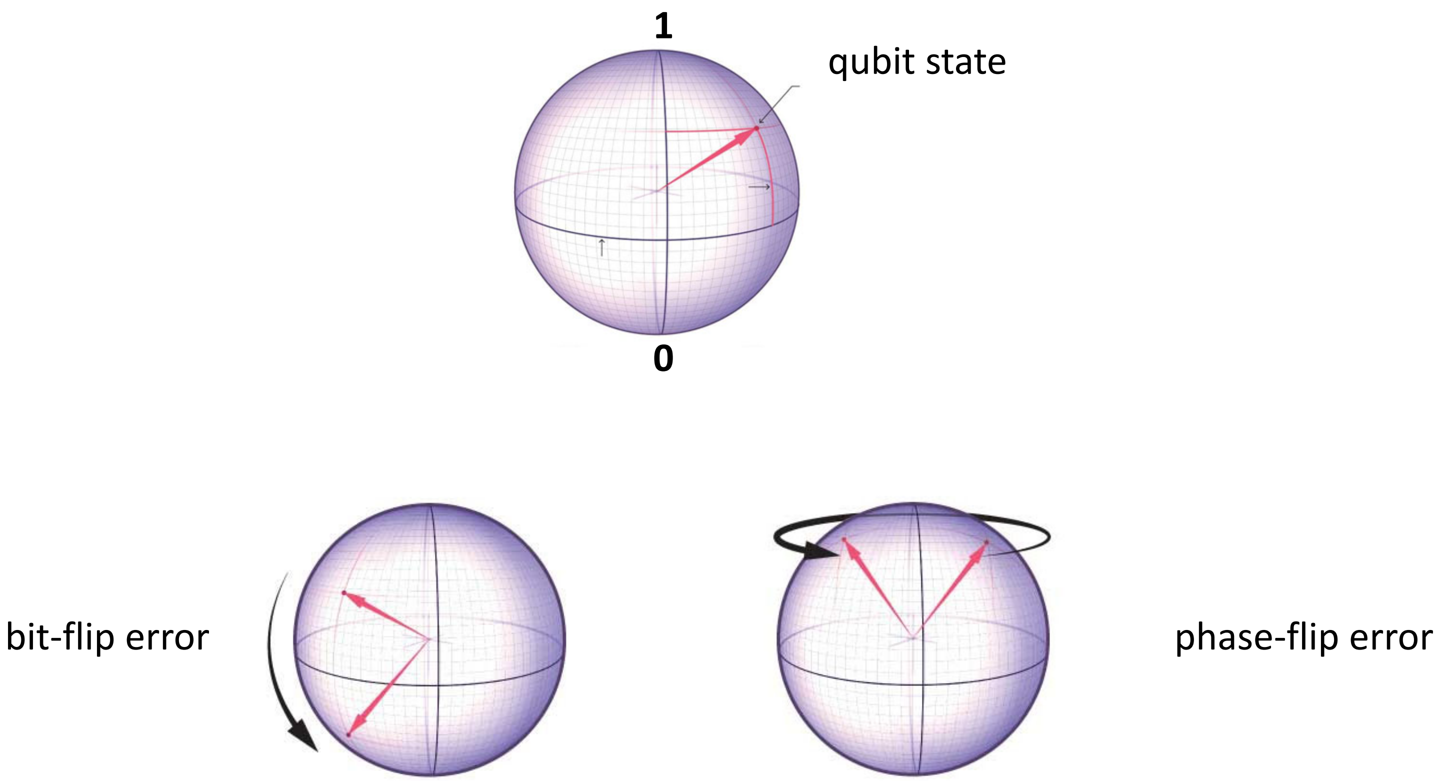



**No cloning**

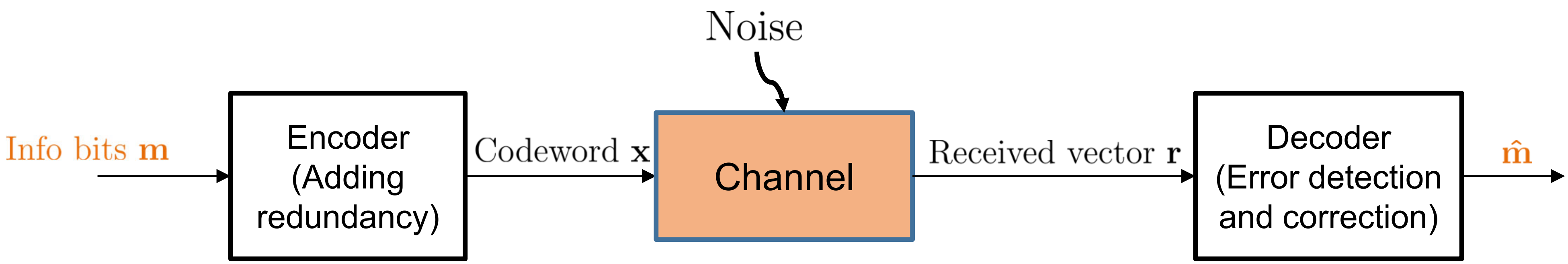
impossible to create an independent and identical copy of an arbitrary unknown quantum state

# Qubits and quantum errors

- Qubits can take on the logical values zero and one simultaneously, and thus carry out calculations faster, but are extremely susceptible to perturbations caused by the noisy environment.



# Classical error correction: linear block codes



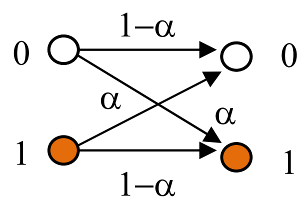

$\mathbf{m} = (m_1, \ldots, m_K) \longrightarrow \mathbf{x} = (x_1, \ldots, x_N)$

$\mathbf{r} = \mathbf{x}+\text{Noise} \longrightarrow$ Decoded word $\hat{\mathbf{x}}$ or $\hat{\mathbf{m}}$

$(1,0,0,0) \xrightarrow{\text{Encode}} (1,1,0,1,0,0,0)$

$K=4$ $N=7$

Generator Matrix




Binary Symmetric Channel (BSC(α))

$(1,1,0,0,0,0,0) \xrightarrow{\text{Decode}} (1,0,0,0)$

Parity Check Matrix

[1] S. Lin and D. J. Costello. Error control coding

# Linear Block Codes

- $[N, K, d]$ binary linear block code $\mathcal{C}$ can be defined as the null space of its parity-check matrix $H$ of size $M \times N$, $M = N - K$ such that any codeword $\mathbf{x} \in \mathcal{C}, \mathbf{x}H^{\mathrm{T}} = \mathbf{0}$ .

- For a $[7, 4, 3]$ Hamming code,

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \longleftrightarrow \begin{aligned} c_1 &: x_1 + x_4 + x_6 + x_7 = 0 \\ c_2 &: x_2 + x_4 + x_5 + x_6 = 0 \\ c_3 &: x_3 + x_5 + x_6 + x_7 = 0 \end{aligned} \quad \text{modulo-2 addition}$$

$$M \text{ rows} \rightarrow M \text{ parity-check equations}$$

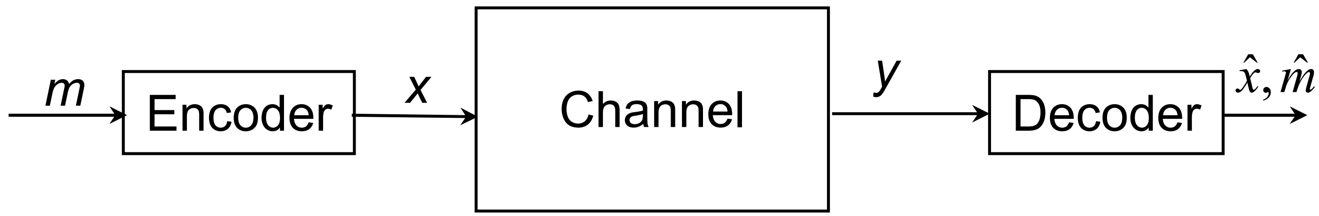
Codelength $N$, Dimension $K$, Minimum distance $d$

- Syndrome: A received vector that is not a codeword results in a nonzero syndrome vector $\sigma = \mathbf{r}H^T \neq \mathbf{0}$
  - Example: For $\mathbf{r} = (1, 1, 0, 0, 0, 0, 0)$, $\sigma = \mathbf{r}H^T = (1, 1, 0)$

    Checks $c_1$ and $c_2$ are not satisfied.

[1] S. Lin and D. J. Costello. Error control coding, volume 2. Prentice hall, 2001.

# Linear block codes




$$x = m_1 g_1 + m_2 g_2 + \ldots m_k g_k$$

$$x = mG$$

$$G = \begin{bmatrix} 10101 \\ 00110 \end{bmatrix}$$

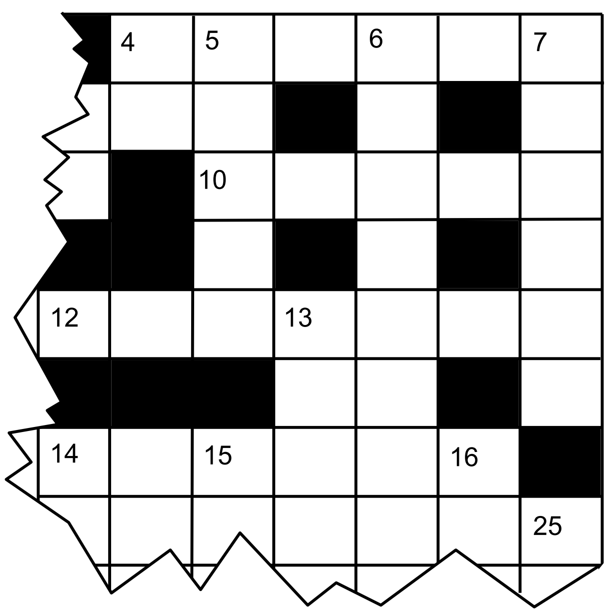
$$\begin{array}{lcl}
m = (0,0) & & x = (0,0,0,0,0) \\
m = (0,1) & & x = (1,0,1,0,1) \\
m = (1,0) & \rightarrow & x = (0,0,1,1,0) \\
m = (1,1) & & x = (1,0,0,1,1)
\end{array}$$

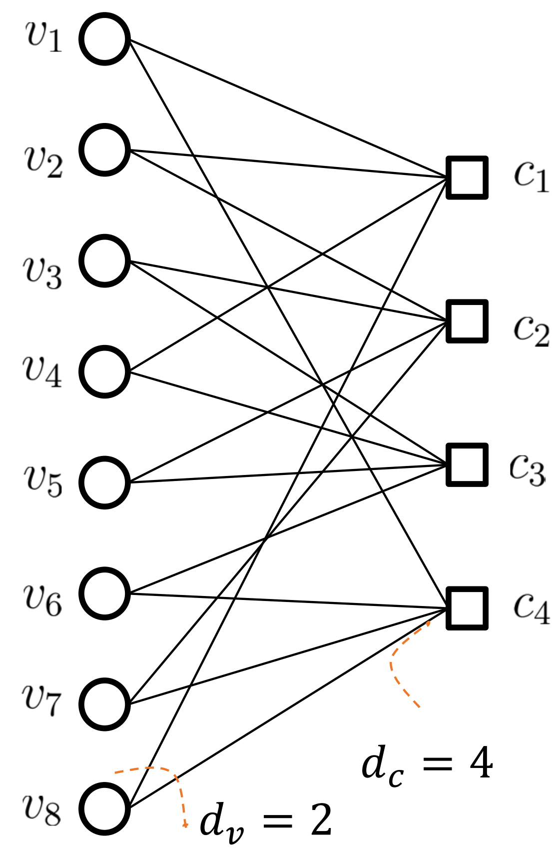
# Low density parity check (LDPC) code

- A class of linear block codes with parity check matrices having low density of nonzero entries (i.e., sparse).

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

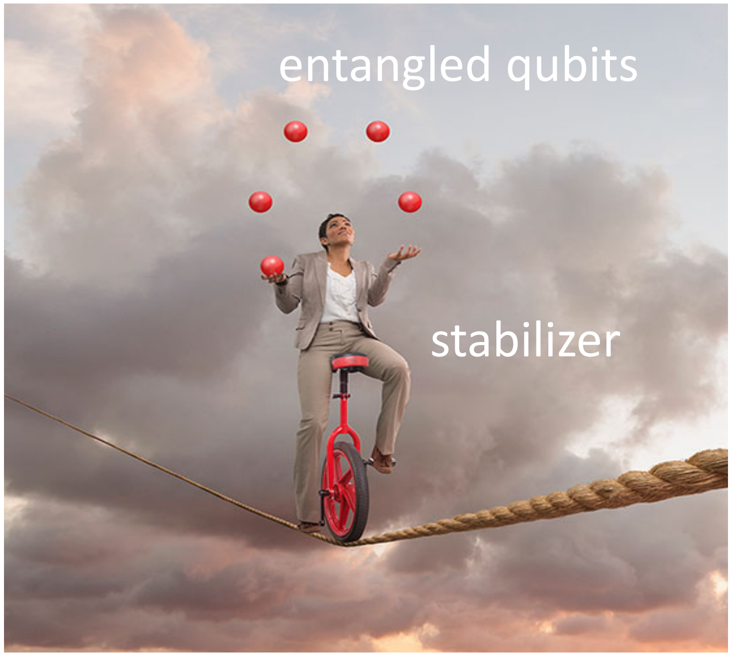
- Modern decoders – Belief Propagation



# Quantum error correction (QEC)

- Fundamental challenges:
  - Cannot copy a quantum state
  - Cannot read from a quantum memory (uncertainty principle)
  - Quantum gates are time-reversible
  - Quantum gates are noisy
- How do we correct a quantum state without learning anything about it?!
- How errors can be corrected when the gates that are used to correct them are also noisy?

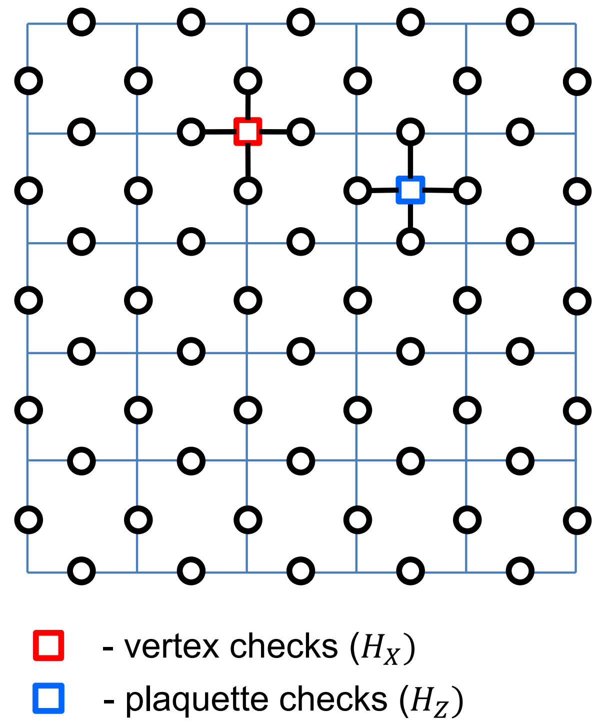


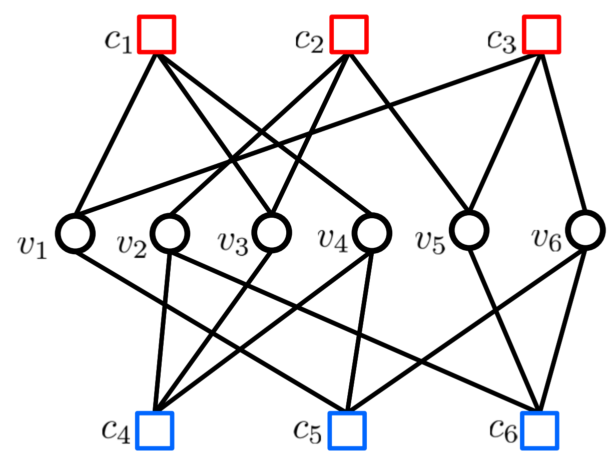

https://www.johnlund.com/page/8216/woman-juggling-riding-unicycle-on-tightrope.asp

Our approach:
quantum LDPC stabilizer codes

# Why quantum LDPC codes?

- Promise fault tolerant computation with <u>constant overhead</u>
- Decoded efficiently (in linear time) using low-complexity iterative decoding
- Involve stabilizer (parity) checks of bounded and low weight
- Finite (nonzero) asymptotic rate
- Minimum distance scaling better than square root of the code length. Better than surface codes.
- QLDPC decoding problem is still open!



# Our current projects

- Quantum projects:
  - **NASA SURP** Robust Neural Network Decoders for Quantum Error Correction Systems
  - **NSF-CIF 1855879** Medium: Quantum Decoders
  - **NSF-CIF-2106189** Collaborative Research: CIF: Medium: QODED: Quantum codes Optimized for the Dynamics between Encoded Computation and Decoding using Classical Coding Techniques
  - **NSF-ERC-1941583** Engineering Research Center for Quantum Networks (CQN)
  - **Fermi National Accelerator Laboratory** (sub-DOE) Superconducting Quantum Materials and Systems Center

# Our current projects

- Classical projects:
  - **NSF CCF-2100013** Small: Learning To Correct Errors
  - **NSF CCSS-2027844** Neural Network Nonlinear Iterative LDPC Decoders with Guaranteed Error Performance and Fast Convergence
  - **NSF-CCSS-2052751** Collaborative Research: Secure and Efficient Post-quantum Cryptography: from Coding Theory to Hardware Architecture

# Outline

- Quantum state, measurement, Pauli channel
- Stabilizer codes
- Quantum LDPC codes and their decoders

# State of a quantum system

- Pure State $|\psi\rangle$
  - $|\psi\rangle$ - a unit norm *column* vector (ket) in a complex vector space
  - $\langle\psi|$ - a unit norm *row* vector (bra) : complex conjugate of $|\psi\rangle$
  - Unit norm: $\langle\psi|\psi\rangle = 1$

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle$$

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

  - $$a, b \in \mathbb{C}, \quad \langle\psi|\psi\rangle = |a|^2 + |b|^2 = 1$$

- $|0\rangle$ and $|1\rangle$ are orthogonal, $\langle 0|1\rangle = \langle 1|0\rangle = 0,$
- $|0\rangle$ and $|1\rangle$ form the computational basis

# Quantum bit, quantum state

- Unlike classical bit having 'state' either 0 or 1, a qubit can be in a linear superposition of states.

- For $n$–qubit state

$$|\psi\rangle = a_0 |00\ldots0\rangle + a_1 |00\ldots1\rangle + \ldots + a_{2^N-1} |11\ldots1\rangle$$

$$a_i \in \mathbb{C}, \quad \sum_i |a_i|^2 = 1$$

$$|x_1 x_2 \ldots x_N\rangle \triangleq |x_1\rangle \otimes |x_2\rangle \ldots \otimes |x_N\rangle, |x_i\rangle \in \{|0\rangle, |1\rangle\}$$

- Example, $n = 3$

$$|000\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, |001\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, |010\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, |011\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \ldots |111\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \begin{array}{c} 0 \\ 1 \\ 2 \\ 3 \\ \vdots \\ 7 \end{array}$$

# Pauli group and its properties

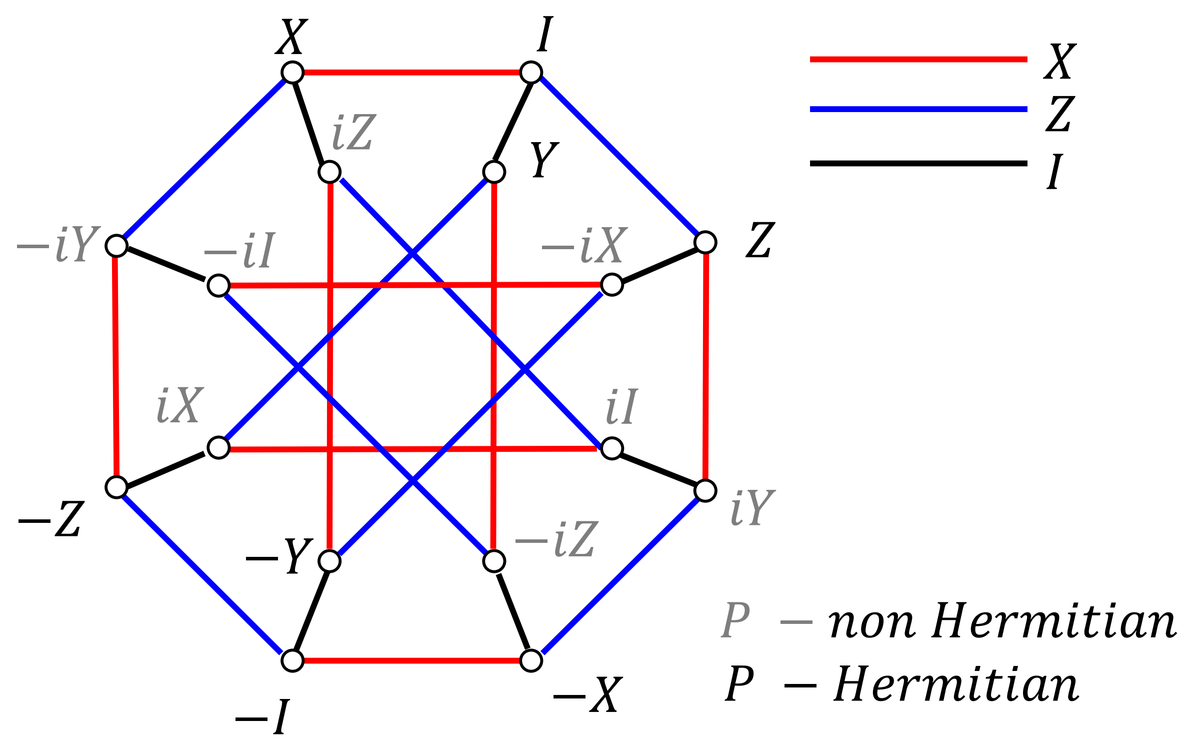
- Pauli group on a single qubit $\mathcal{P}_1$
  - Pauli matrices and multiplicative factors $\pm 1, \pm i$, closed under matrix multiplication.
  - *Pauli operators* - the Hermitian elements of this group

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

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

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

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




Cayley diagram

# Pauli group and its properties

- Pauli matrices *P* are:
  - Unitary $(PP^\dagger = I)$ $\Rightarrow$ eigenvalues have unit magnitude $e^{j\theta}$
  - Hermitian $(P = P^\dagger)$ $\Rightarrow$ eigenvalues are real
  - $\Rightarrow$ only possible eigenvalues: $\pm 1$
  - Pauli matrices either *commute* or *anticommute*, e.g., $XZ = -ZX$
  - And have self inverse, e.g., $X^2 = I$

# Pauli matrix properties

- Action of Paulis on qubits:
  - Example $$X|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

bit-flip $$X|0\rangle = |1\rangle, X|1\rangle = |0\rangle, X(a|0\rangle + b|1\rangle) = a|1\rangle + b|0\rangle$$

phase-flip $$Z|0\rangle = |0\rangle, Z|1\rangle = -|1\rangle, Z(a|0\rangle + b|1\rangle) = a|0\rangle - b|1\rangle$$

$$Y|0\rangle = -i(XZ)|0\rangle = -iX|0\rangle = -i|1\rangle$$
$$Y|1\rangle = -i(XZ)|1\rangle = -iX(-|1\rangle) = i|0\rangle$$

# *n*-qubit Pauli group

- Pauli group on *n* qubits
  - $\mathcal{P}_n$ is an *n*-fold tensor product of $\mathcal{P}_1$ -on *n*qubits.

$$\mathcal{P}_n = \{\pm I, \pm X, \pm Y, \pm Z\}^{\otimes n}$$

$$A = (X \otimes Z \otimes I \otimes I \otimes Y \otimes Z)$$

$$(X \otimes Z \otimes I \otimes I \otimes Y \otimes Z)\,|000000\rangle = i\,|100010\rangle$$

$$(X \otimes Z \otimes I \otimes I \otimes Y \otimes Z)\,|111111\rangle = -i\,|010001\rangle$$

# Commuting operators

$$\begin{array}{rcccccc}
 & 1 & 2 & 3 & 4 & 5 & 6 \\
 & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
A = & (X \otimes & Z \otimes & I \otimes & I \otimes & Y \otimes & Z) \\
| & | & \vdots_{1} & | & | & \vdots_{2} & | \\
B = & (X \otimes & X \otimes & X \otimes & Y \otimes & Z \otimes & Z)
\end{array}$$

$$\begin{array}{rcccccccccccc}
 & 1_X & 2_X & 3_X & 4_X & 5_X & 6_X & 1_Z & 2_Z & 3_Z & 4_Z & 5_Z & 6_Z \\
 & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
\mathbf{a} = & (1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1) \\
| & & & 1 & & & & & & 2 & & & \\
\mathbf{b} = & (1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1)
\end{array}$$

$$AB = BA$$

# Simplectic product

- Simplectic product

$$\mathbf{a} = (\mathbf{a}_\mathrm{X}, \mathbf{a}_\mathrm{Z})$$

$$\mathbf{b} = (\mathbf{b}_\mathrm{X}, \mathbf{b}_\mathrm{Z})$$

$$\mathbf{a}_\mathrm{X}\mathbf{b}_\mathrm{Z}^\mathrm{T} + \mathbf{a}_\mathrm{Z}\mathbf{b}_\mathrm{X}^\mathrm{T}$$

$$(\mathbf{a}_X, \mathbf{a}_Z) \odot (\mathbf{b}_X, \mathbf{b}_Z)^\mathrm{T} = \mathbf{a}_X\mathbf{b}_Z^\mathrm{T} + \mathbf{a}_Z\mathbf{b}_X^\mathrm{T}$$

# Stabilizer formalism for quantum codes

- Stabilizer Group $\mathcal{S}$ : Subgroup of *n*-qubit Pauli group $\mathcal{P}_n$ that leaves a non-trivial code state invariant.
  - Let $|\psi\rangle$ be any codeword state, then $\forall\ S \in \mathcal{S},\ S\,|\psi\rangle = |\psi\rangle$.
  - All codewords have eigenvalue $+1$ for stabilizers $S$ in $\mathcal{S}$.
  - All elements of $\mathcal{S}$ commute.
  - $-I \notin \mathcal{S}$.
- An [[*n*,*k*]] stabilizer code (in terms of stabilizers)
  - Vector space $V_{\mathcal{S}}$ stabilized by subgroup $\mathcal{S}$ of $\mathcal{P}_n$ such that $-I \notin \mathcal{S}$
  - $V_S$ is the intersection of the subspaces fixed by each operator in $\mathcal{S}$
  - $\mathcal{S}$ has *n-k* independent and commuting generators
  - Codeword is a simultaneous eigenstate of all generators of $\mathcal{S}$ with eigenvalue +1.

$$|\psi\rangle \xrightarrow{S} S\,|\psi\rangle = |\psi\rangle$$

# Quantum three-qubit repetition code

- Similar to classical repetition code.
- One quantum bit using the same three-bit repetition encoding.

$$|0\rangle_L = |0\rangle \otimes |0\rangle \otimes |0\rangle \equiv |000\rangle \quad |1\rangle_L = |1\rangle \otimes |1\rangle \otimes |1\rangle \equiv |111\rangle$$

- A general quantum state

$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ is encoded as $|\psi\rangle_L = \alpha\,|000\rangle + \beta\,|111\rangle$

- Code space is the space spanned by the codeword basis states: $|0\rangle_L$ and $|1\rangle_L$.

# Stabilizers of the Quantum repetition code

$$|0\rangle_L = |0\rangle \otimes |0\rangle \otimes |0\rangle \equiv |000\rangle \quad |1\rangle_L = |1\rangle \otimes |1\rangle \otimes |1\rangle \equiv |111\rangle$$

- Observe that these four operators leave the basis states invariant: $\mathcal{S} = \{ZZI,\ ZIZ,\ IZZ,\ III\}$
- Stabilizer generators:

$$g = \langle ZZI, ZIZ \rangle$$

- Consider set of errors: $\mathcal{E} = \{XII,\ IXI,\ IIX\}$
  - All of these errors anti commute with either $ZZI$ or $ZIZ$.
  - Example: $(XXI)(ZIZ) = -(ZIZ)(XXI)$.

# Effect of errors on the code subspace

- What happens to our subspace basis elements, $|000\rangle$ and $|111\rangle$ under the (correctable) errors

$$\begin{matrix}|000\rangle\\|111\rangle\end{matrix}\ \overbrace{\longrightarrow}^{I\otimes I\otimes I}\ \begin{matrix}|000\rangle\\|111\rangle\end{matrix}$$

$$\begin{matrix}|000\rangle\\|111\rangle\end{matrix}\ \overbrace{\longrightarrow}^{X\otimes I\otimes I}\ \begin{matrix}|100\rangle\\|011\rangle\end{matrix}$$

$$\begin{matrix}|000\rangle\\|111\rangle\end{matrix}\ \overbrace{\longrightarrow}^{I\otimes X\otimes I}\ \begin{matrix}|010\rangle\\|101\rangle\end{matrix}$$

$$\begin{matrix}|000\rangle\\|111\rangle\end{matrix}\ \overbrace{\longrightarrow}^{I\otimes I\otimes X}\ \begin{matrix}|001\rangle\\|110\rangle\end{matrix}$$

- These errors map the subspace where the information is encoded into different <u>orthogonal</u> subspaces.

# Centralizer and logical operators

- For 3 bit Quantum repetition code
- Centralizer is

$$\{III,\ ZZI,\ ZIZ,\ IZZ\} \quad \text{Logical } I$$

$$\{XXX,\ -YYX,\ -YXY,\ XYY\} \text{ Logical X}$$

$$\{YXX,\ XYX,\ XXY,\ -YYY\} \text{ Logical Y}$$

$$\{ZII,\ IZI,\ IIZ,\ ZZZ\} \text{ Logical Z}$$

- The code is therefore defined by stabilizer generators

$ZZI,\ ZIZ$ plus the logical operators

$$\overline{X} = XXX \text{ and } \overline{Z} = ZII.$$

- Min distance: Minimum weight (minimum number of nontrivial (nonidentity) Paulis) of an encoded logical operator: In this case 1 (Z in ZZI).

# Error correction

- Evolution of a *closed* quantum system is described by a *unitary* transformation $E$
- Error correction must be done without learning the state

$$\begin{tikzcd} |\psi\rangle \arrow[r, "E"] & E|\psi\rangle \arrow[r, "\hat{E}^\dagger"] \arrow[d] & \hat{E}^\dagger E|\psi\rangle \\ & \hat{E} \arrow[u, phantom, ""] & \end{tikzcd}$$

channel

correction

error estimation

- Pauli channel - error operators are Pauli matrices: $\{\mathrm{I},\ \mathrm{X},\ \mathrm{Y},\ \mathrm{Z}\}$
  - Depolarizing channel – Pauli errors are independent and happen with the same probability

# Syndrome measurement

- Nature prevents us from learning anything about the probability amplitudes $\alpha$ and $\beta$ and
- Nature only allows us to measure *observables*.
  - Observable is a Hermitian operator
  - Measurement outcome is one of the eigenvalues of the operator (real number)
  - Quantum state after measurement is eigenvector corresponding to that eigenvalue
- Examples of qubit observables: the Pauli operators X, Y, and Z.
- Measurement – projection to an eigenvector.
- Idea: choose measurements so that encoded state is an eigenvector corresponding to eigenvalue +1.

# Quantum syndrome decoding

- Let $\mathbf{e}$ be a non-zero error vector, resulting in a syndrome $\mathbf{s}$

$$\mathbf{s} = \mathbf{e} \odot H^{\mathrm{T}} \neq \mathbf{0}$$

$\odot$ symplectic product

- As opposed to a *classical syndrome decoder* that tries to find $\mathbf{e}$ for a given observed syndrome, a valid output of a *quantum* decoder is any one of the vectors

$$\widetilde{\mathbf{e}} = \mathbf{e} + \mathbf{h}, \mathbf{h} \in \mathrm{rowspace(H)}$$

- When $\mathbf{e} + \widetilde{\mathbf{e}} \neq \mathbf{0}$, but

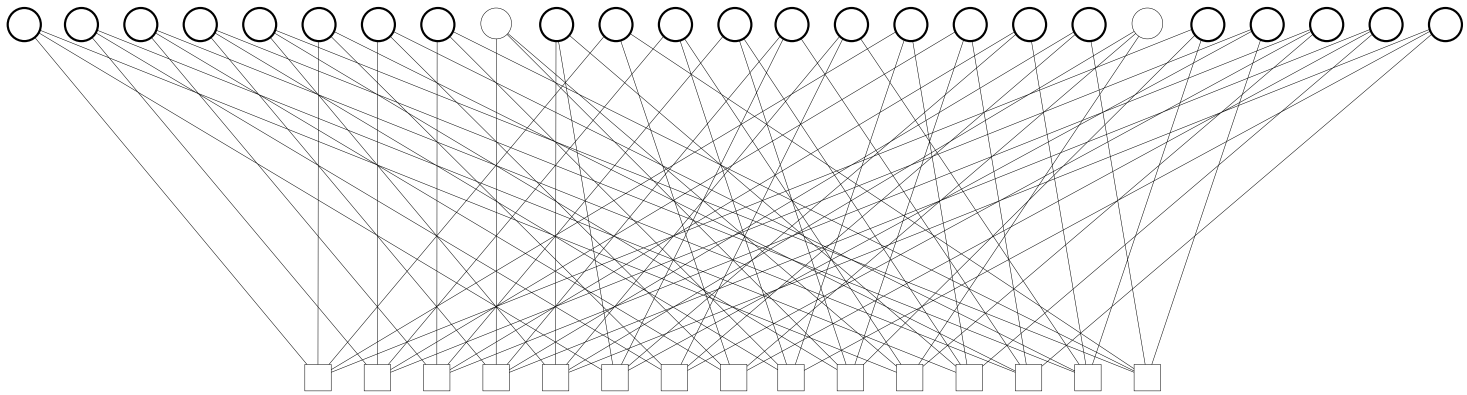
$$(\mathbf{e} + \widetilde{\mathbf{e}}) \odot H^{\mathrm{T}} = \mathbf{0}$$

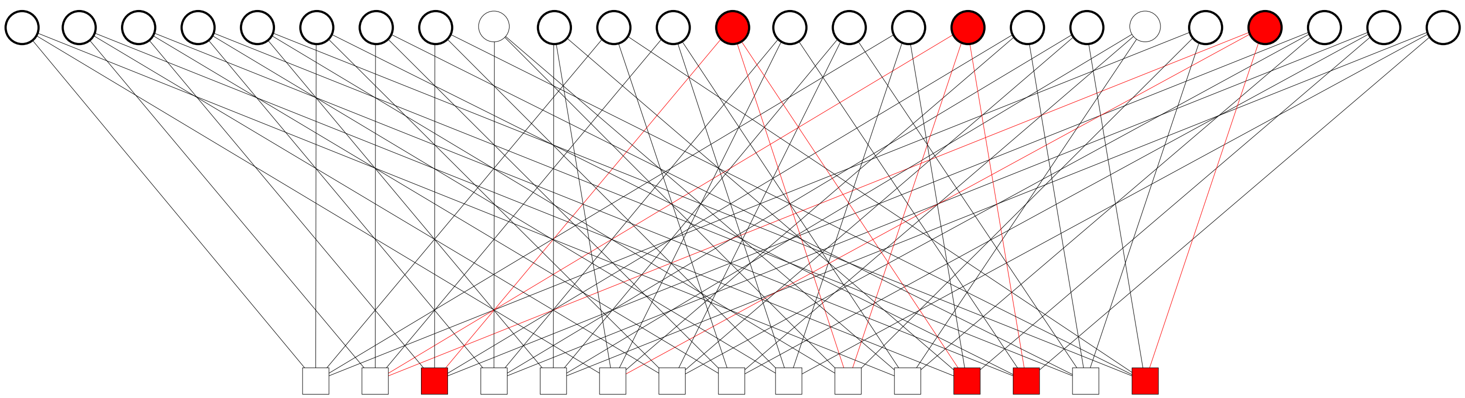
then the correction vector $\mathbf{e} + \widetilde{\mathbf{e}}$ is applied to flip bits in the (unobservable) quantum codeword is also a codeword, and a logical, undetectable, error occurs.

# Flaws of existing decoders of LDPC codes

- Why the existing decoders of QLDPC codes fail?
- Because of degenerate errors and because of trapping sets (they are related)
- To design better decoders we need to understand trapping sets in syndrome decoding
- Two types of trapping sets in QLDPC codes
  - classical-like trapping sets
  - trapping sets imbedded in symmetric stabilizers

# Tanner graph of $H$ and syndrome matching



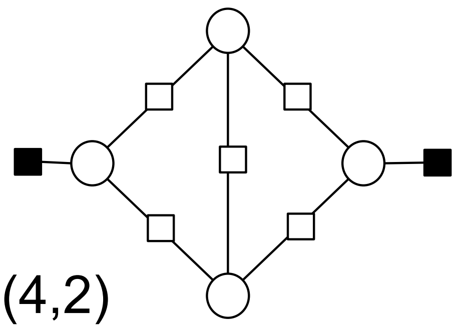


THE UNIVERSITY OF ARIZONA. TUCSON ARIZONA

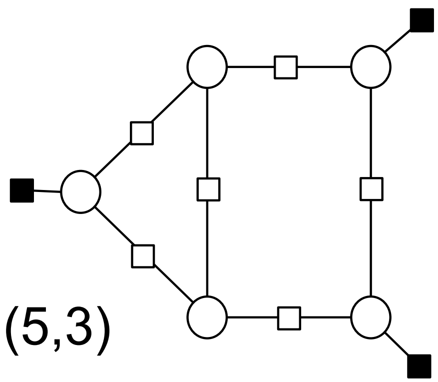
# Summary of our findings

- QLDPC codes have two classes of trapping sets:
- Classical-looking trapping set due to dense subgraphs

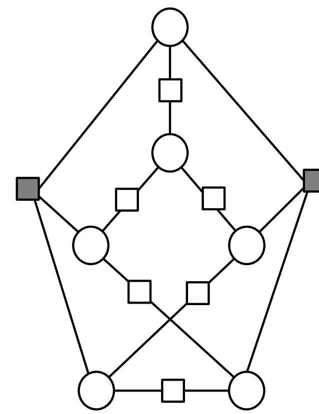
in [[900,36,10]] code



(4,2)



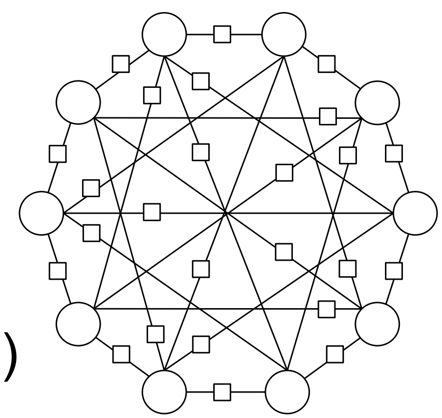
(5,3)



(6,2)

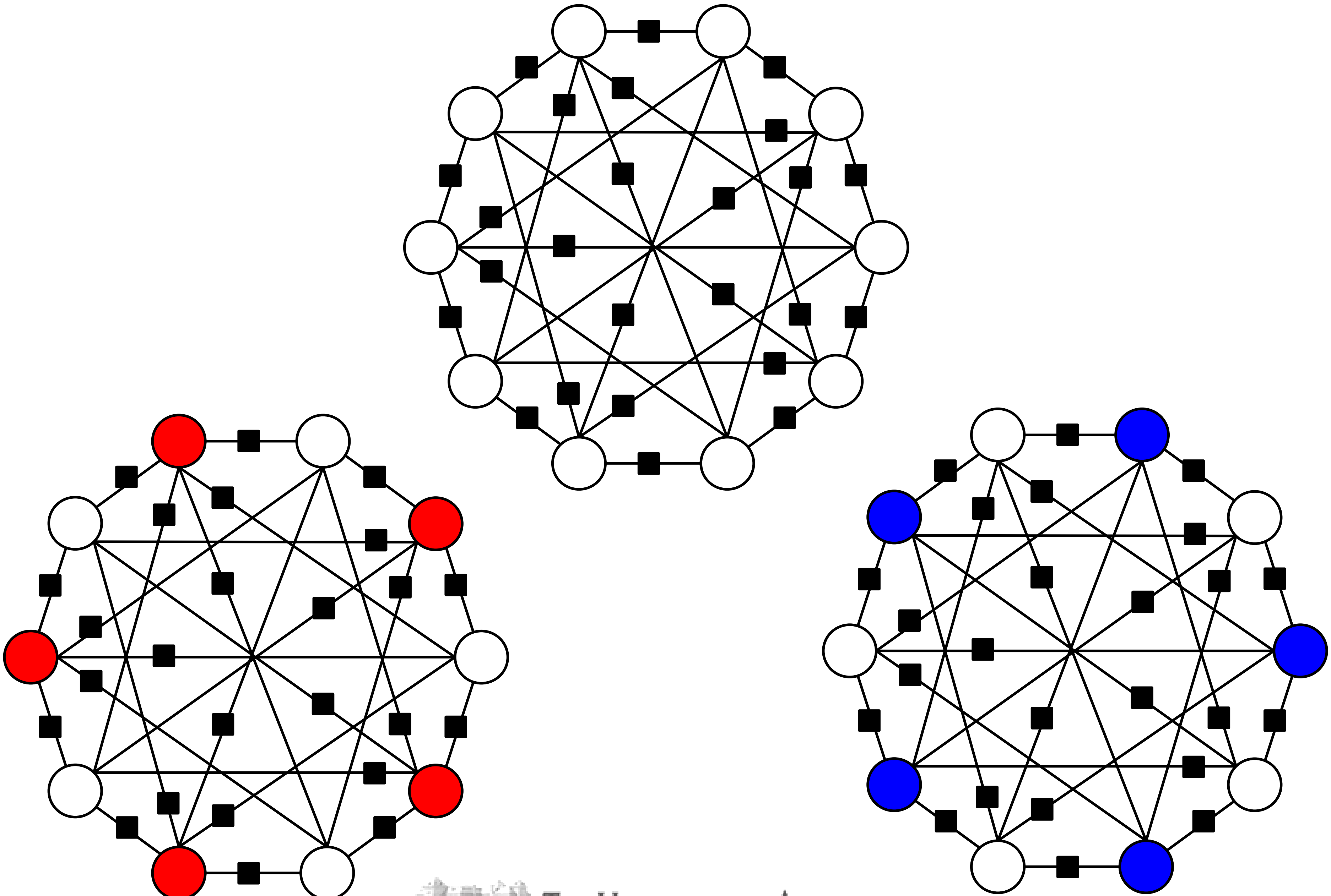
- Inherently-quantum trapping sets due to the symmetry of stabilizers

in [[254,28]] code,
“A1” code of Panteleev and Kalatchev



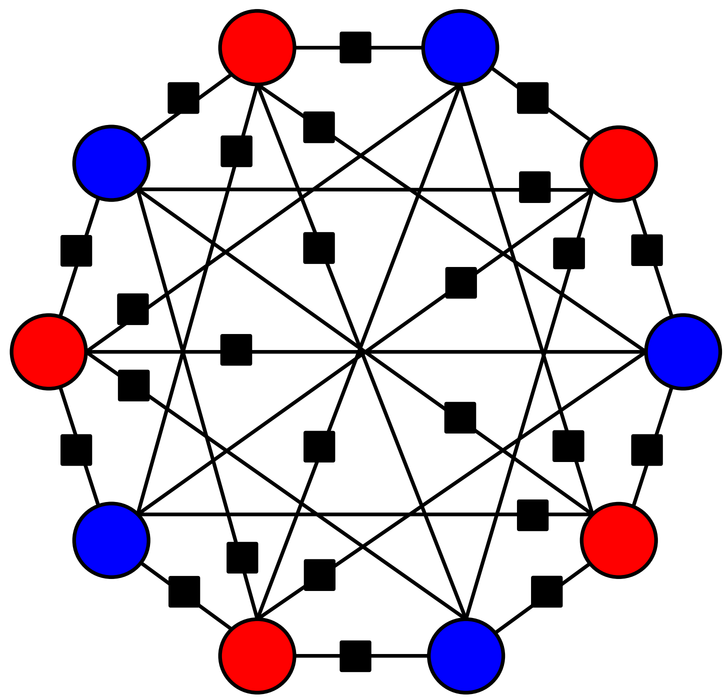
(10,0)

# An example of a degenerate error

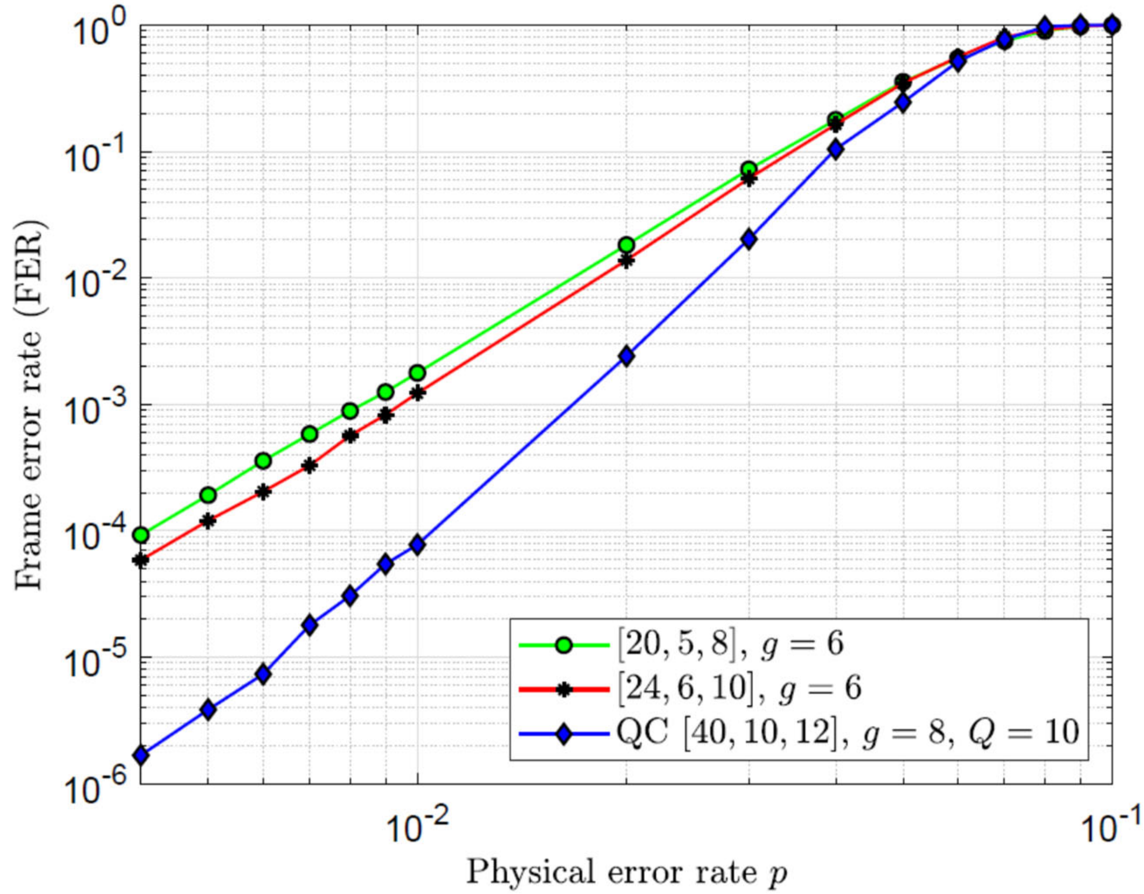


# An example of a degenerate error

- Error patterns $e$ and $f$ induce a subgraph of a codeword.
- Iterative decoder attempts to converge to both $e$ and $f$ simultaneously leading to decoder failure.



# TS-aware code construction



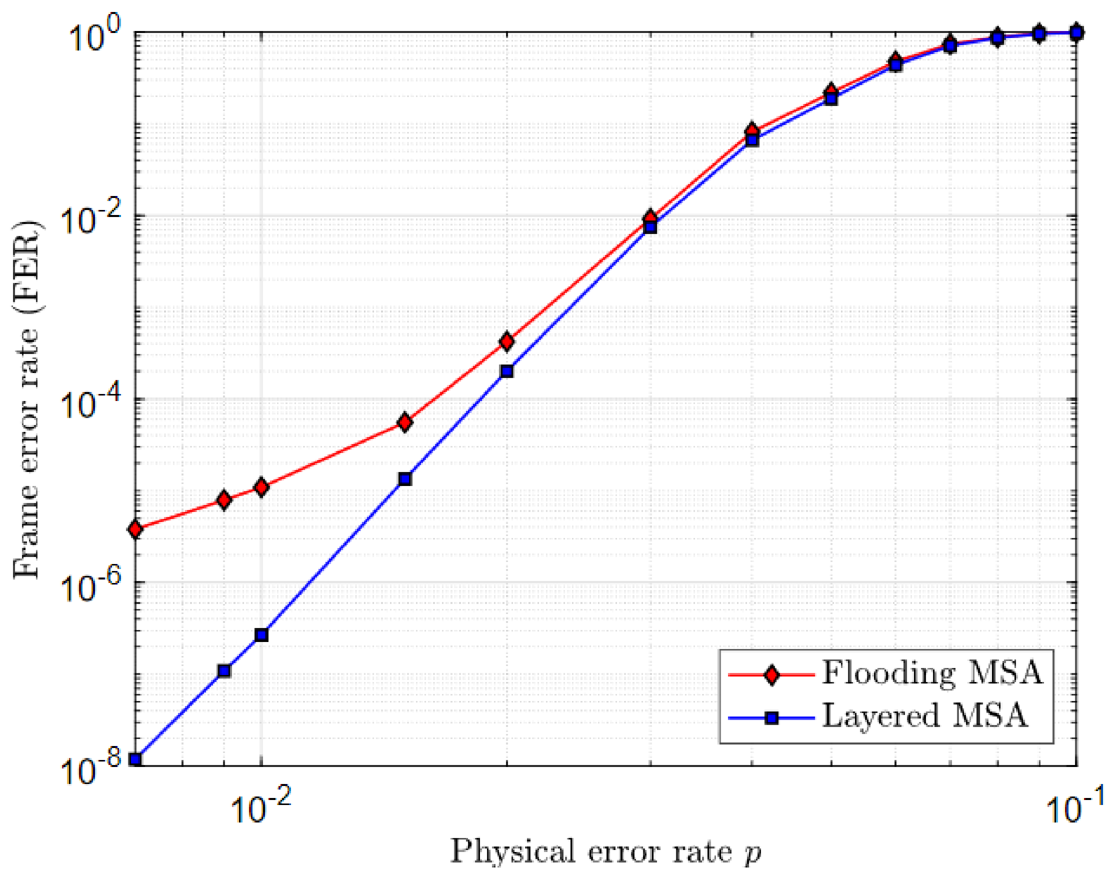

symmetric HP codes constructed using random constituent codes [20,5,8] and [24,6,10] from Roffe et al.

HP code constructed using a trapping set aware QC[40,10,12] code from Roffe

Roffe et al. May 2020. arXiv:2005.07016 [quant-ph]

# Better decoders

- A1 [[254,28]] code decoded by the min-sum algorithm (MSA) for two different schedules:
  - The layered schedule corrects **<u>all</u>** symmetric stabilizer TSs and numerous classical-type TSs.
  - Large unexplored area with potentially big impact.



# Summary

- Iterative decoders on QLDPC codes fail due to presence of trapping sets - dense subgraphs of specific structure:
  - classical looking (but quite different message dynamic)
  - symmetric stabilizers
- We present the methodology to identify and enumerate trapping sets.
- Current work – using the knowledge of trapping sets we train a neural network to learn the decoder capable of correcting errors in trapping sets.

# Thank you!

N. Raveendran and B. Vasic, “Trapping Sets of Quantum LDPC Codes,” Quantum 5, 562, Oct. 2021. also at arXiv:2012.15297 [cs.IT]

THE UNIVERSITY OF ARIZONA.
TUCSON ARIZONA