Quantum error correction

From parity checks to surface-code decoding

Eduardo Dueñez

University of Texas at San Antonio

Quantum Mathematics Seminar

13 November 2026

Slides PDF

https://utsa-quantum-math.github.io/assets/notes/qec-finale/slides.pdf

Protect information without reading it

Encode a state $\longrightarrow$ measure checks $\longrightarrow$ correct

The question for today

Can we learn how the information was disturbed without learning the information?

A rapid §1 review, followed by examples from §§2–4 of the seminar notes.

Hilbert spaces, pure states, and codes

Fix $\mathcal{H}_1 := \mathbb{C}^2$, with orthonormal basis $|0\rangle := (1,0)^{\mathsf{T}}$, $|1\rangle := (0,1)^{\mathsf{T}}$. For $n \geqslant 1$, put

$$\mathcal{H}_n := (\mathbb{C}^2)^{\otimes n}, \qquad \dim \mathcal{H}_n = 2^n.$$

Definition (Pure state)

A pure state is a complex line $[u] \in \mathbb{P}(\mathcal{H}_n)$, represented by $u \neq 0$. Thus $[u] = [\lambda u]$ for every $\lambda \in \mathbb{C}^\times$.

Definition (Code)

For a nonzero linear subspace $\mathcal{C} \subseteq \mathcal{H}_n$, its projectivization $\mathbb{P}(\mathcal{C})$ is a code. Encoding k qubits requires $\dim \mathcal{C} = 2^k$.

Global rescaling fixes a ray, but $[|0\rangle + |1\rangle] \neq [|0\rangle - |1\rangle]$.

The Pauli operators: linear, Hermitian, and unitary

Definition (Pauli operators)

The Pauli operators $X, Y, Z : \mathcal{H}_1 \to \mathcal{H}_1$ are the linear maps with the following matrices in the basis $(|0\rangle, |1\rangle)$:

$$X \coloneqq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Z \coloneqq \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad Y \coloneqq iXZ = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}.$$

$$X|0\rangle \coloneqq |1\rangle, \quad X|1\rangle \coloneqq |0\rangle; \qquad Z|0\rangle \coloneqq |0\rangle, \quad Z|1\rangle \coloneqq -|1\rangle; \qquad Y|0\rangle = i|1\rangle, \quad Y|1\rangle = -i|0\rangle.$$

They are Hermitian and unitary: $P^\dagger = P$ and $P^\dagger P = I$ for $P \in \{X, Y, Z\}$; I denotes the identity.

X_j, Y_j, Z_j act on tensor factor j and as the identity on the others.

Measuring a self-adjoint involution

Let $g : \mathcal{H}_n \to \mathcal{H}_n$ be a self-adjoint involution ($g = g^\dagger$ and $g^2 = I$).

Definition (Measurement)

The measurement of g uses its orthogonal spectral projections

$$P_\pm \coloneqq \frac{I \pm g}{2}.$$

On a pure state $[u]$, measuring g leads to two possible outcomes ± 1, with probabilities:

$$\Pr(\pm 1 \mid [u]) \coloneqq \frac{\|P_\pm u\|^2}{\|u\|^2}.$$

When this is positive, the resulting state is $[P_\pm u]$.

(Replacing g by $-g$ exchanges the outcome labels ± 1.)

Repetition: measure parity, preserve the superposition

Definition (Encoding)

An encoding is induced by a linear isometry $V : \mathcal{H}_k \to \mathcal{H}_n$.

For repetition, define $V|0\rangle := |000\rangle$ and $V|1\rangle := |111\rangle$. Then

$$u := V(\alpha|0\rangle + \beta|1\rangle) = \alpha|000\rangle + \beta|111\rangle.$$

$$g_1 := Z_1 Z_2, \qquad g_2 := Z_2 Z_3.$$

error	I	X_1	X_2	X_3
outcomes (g_1, g_2)	$(+1,+1)$	$(-1,+1)$	$(-1,-1)$	$(+1,-1)$

The outcomes are independent of α, β. The phase error Z_1 is undetected.

Stabilizers: specify the code by equations

Definition (Pauli group)

The Pauli matrix group is

$$\mathcal{P}_n \coloneqq \{\lambda P_1 \otimes \cdots \otimes P_n : P_j \in \{I, X, Y, Z\},\ \lambda \in \{\pm 1, \pm i\}\}.$$

Definition (Stabilizer code)

A stabilizer group is an abelian subgroup $S \leqslant \mathcal{P}_n$ with $-I \notin S$. Its stabilizer code is $\mathbb{P}(\mathcal{C}(S))$, where

$$\mathcal{C}(S) \coloneqq \{u \in \mathcal{H}_n : gu = u \text{ for every } g \in S\}.$$

Generators of S are the checks. Their chosen signs select the common $+1$ sector.

How much information fits?

Definition (Independent checks)

Let $g_1, \ldots, g_r$ be independent generators of S: no generator is a product of the others.

$$n \text{ physical qubits} \qquad r \text{ independent checks}$$

$$\dim \mathcal{C}(S) = 2^{n-r} = 2^k.$$

Definition (Encoded-qubit count)

The integer $k := n - r$ is the number of encoded qubits.

Repetition: $n = 3$, $r = 2$, $k = 1$.

Redundant measured checks do not reduce the dimension further.

Syndrome bits record the commutation signs

S: stabilizer group; $g_1, \ldots, g_r$: generators; any $E \in \mathcal{P}_n$ is a Pauli error on n qubits.

Definition (Syndromes)

For any check (measurement) $g \in S$, the g-bit of the **syndrome** of the error E is the bit $s_g(E) \in \{0, 1\}$ defined by

$$gE = \lambda_g(E) \cdot Eg = (-1)^{s_g(E)} \cdot Eg, \qquad \lambda_g(E) \in \{+1, -1\}.$$

$\lambda_g(E)$	$+1$	-1
$s_g(E)$	0	1

- The (full) syndrome of E is $(s_g(E))_{g \in S}$ (all 2^r-many syndrome g-bits of E);
- The abridged (succinct) syndrome of E is the r-tuple $s(E) \coloneqq (s_{g_1}(E), \ldots, s_{g_r}(E))$
  - Syndrome g_i-bits for $1 \leqslant i \leqslant r$: r-many *generator bits only*.

The full syndrome is determined by the much shorter succinct syndrome. (In the literature, "*syndrome of E*" means *succinct*.)

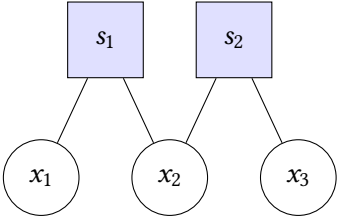
- For $u \in \mathcal{C}(S)$ & $g \in S$: $g(Eu) = (-1)^{s_g(E)} Egu = (-1)^{s_g(E)} \cdot Eu$, since $gu = u$.

Repetition: two checks and the corresponding syndrome

The space $\mathcal{C} = \mathrm{span}(|000\rangle, |111\rangle)$ is called the repetition code; it corresponds to the repetition-code stabilizer S:

$$g_1 \coloneqq Z_1Z_2, \quad g_2 \coloneqq Z_2Z_3, \quad S = \langle g_1, g_2\rangle = \{I, g_1, g_2, g_1g_2\} = \{I, Z_1Z_2, Z_2Z_3, Z_1Z_3\}.$$

$\mathbb{F}_2 \coloneqq \mathbb{Z}/2 = \{0, 1\}$: the 2-element ("1-bit") field.
$E = X_1^{x_1}X_2^{x_2}X_3^{x_3}$: Any combination of X-errors on 3-qubits.
E is specified by the exponent triple $x_E \coloneqq (x_1, x_2, x_3) \in \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2$.



Here $s_j \coloneqq s_{g_j}(E)$.

$$x_1 + x_2 = s_1, \qquad x_2 + x_3 = s_2.$$

For $x_E = (0, 1, 0)$, both checks give -1: $s = (1, 1)$.

The full syndrome, ordered by (I, g_1, g_2, g_1g_2), is $(0, s_1, s_2, s_1 + s_2)$. Additions are in $\mathbb{F}_2$.

The picture has a name: Tanner graph

Definition (Tanner graph)

For a binary matrix $H \in \mathbb{F}_2^{m \times n}$, its Tanner graph has one variable vertex for each column and one check vertex for each row. Join check a to variable j exactly when $H_{aj} = 1$.

$$H = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \qquad x \in \mathbb{F}_2^3, \qquad s = Hx \in \mathbb{F}_2^2.$$

The matrix and graph encode the same parity equations.

For a specified variable vector, a check evaluates the sum of its neighboring variables.

Calderbank–Shor–Steane CSS codes: separate X checks and Z checks

For $x, z \in \mathbb{F}_2^n$, put

$$X(x) \coloneqq \prod_{j=1}^{n} X_j^{x_j}, \qquad Z(z) \coloneqq \prod_{j=1}^{n} Z_j^{z_j}.$$

Definition (Calderbank–Shor–Steane (CSS) code)

Let H_X and H_Z be binary matrices with n columns and $H_X H_Z^{\mathsf{T}} = 0$. Rows a of H_X specify checks $X(a)$; rows b of H_Z specify checks $Z(b)$. Their common $+1$ sector defines a CSS code.

A Pauli error $E = \lambda X(x) Z(z)$ has

$$s_X(E) = H_X z, \qquad s_Z(E) = H_Z x.$$

Subscripts name the check type: X checks detect Z components and conversely.

Why the two check types can coexist

X checks and Z checks commute exactly when their supports overlap evenly. For example, define

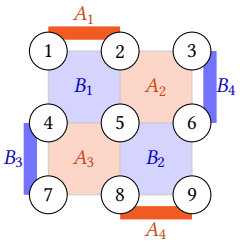
$$A_2 \coloneqq X_2X_3X_5X_6, \qquad B_1 \coloneqq Z_1Z_2Z_4Z_5.$$

Their supports intersect in qubits 2 and 5. Using $XZ = -ZX$ in each common tensor factor gives

$$A_2B_1 = (-1)^2B_1A_2 = B_1A_2.$$

$H_XH_Z^{\mathsf{T}} = 0$ expresses this even-overlap condition for every opposite-type pair.

A complete quantum code on nine qubits



Orange: X checks $A_1, \ldots, A_4$.

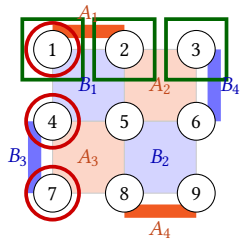
Blue: Z checks $B_1, \ldots, B_4$.

A square acts on its four corners; a boundary bar on its endpoints. There are eight independent checks:

$$n = 9, \qquad r = 8, \qquad k = 1.$$

Circles are the data qubits, numbered in row order; face centers are not extra qubits.

Invisible does not mean harmless



$$\overline{X} \coloneqq X_1X_4X_7, \qquad \overline{Z} \coloneqq Z_1Z_2Z_3.$$

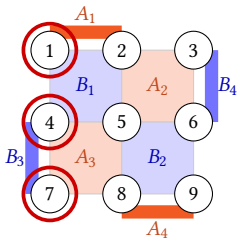
They commute with every check and anticommute with each other.

Definition (Logical operator)

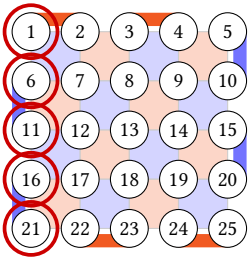
A Pauli L is a logical operator if it commutes with S and $L|_{\mathcal{C}(S)}$ is not a scalar multiple of the identity.

Red rings: X support. Green boxes: Z support. A logical operator can fix some code rays.

Distance: make harmful invisible operators large



$[[9, 1, 3]]$



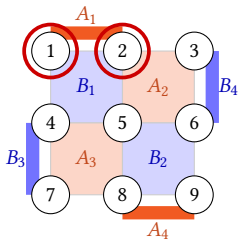
$[[25, 1, 5]]$

Definition (Weight and distance)

The weight of a Pauli string is its number of nonidentity tensor factors. For $k \geqslant 1$, the distance d is the least weight of a logical operator. The parameters are written $[[n, k, d]]$.

Odd rotated patches have parameters $[[d^2, 1, d]]$ and correct all Pauli errors of weight t if $2t < d$.

Two different errors can have the same effect



The check $A_1 \coloneqq X_1X_2$ satisfies $A_1 u = u$ for every code vector u. Consequently $X_1 u = X_2 u$.

Definition (Degenerate code)

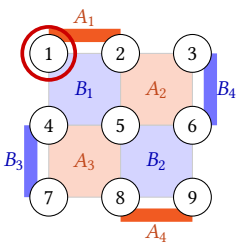
A stabilizer code of distance d is degenerate if some $g \in S \setminus \{I\}$ has weight less than d.

Here A_1 has weight $2 < 3$.

Errors X_1 and X_2 have the same syndrome and agree on the code; either corrects the other.

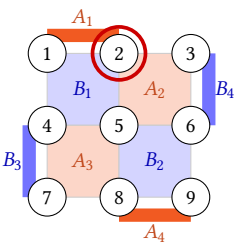
Three corrections: ask the audience

Actual error: X_1. Its Z-check syndrome is $(1, 0, 0, 0)$. For a correction C, the residual operator is $R \coloneqq CX_1$.



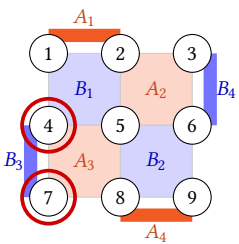
$C = X_1$

$R = I$



$C = X_2$

$R = X_1X_2 = A_1$



$C = X_4X_7$

$R = \overline{X}$

All three corrections return the state to the common $+1$ sector. Which restore every encoded state?

The decoder must choose the right equivalence class

From here on, consider only X errors: $E = X(x)$ with $x \in \mathbb{F}_2^n$.

Definition (Decoder)

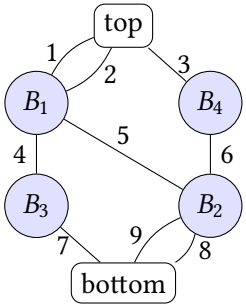
A decoder assigns to each attainable syndrome s a correction vector $\widehat{x}(s) \in \mathbb{F}_2^n$ satisfying $H_Z \widehat{x}(s) = s$. Write $\widehat{x} := \widehat{x}(H_Z x)$.

$$H_Z(x + \widehat{x}) = 0 \quad \text{means all checks are restored;}$$
$$x + \widehat{x} \in \operatorname{row}(H_X) \quad \text{means every code ray is restored.}$$

Errors with the same syndrome are equivalent when they differ by an element of $\operatorname{row}(H_X)$.

The residual logical classes form $\ker H_Z / \operatorname{row}(H_X)$.

Redraw the same patch as a decoding graph



Definition (Decoding graph for X errors)

Vertices: Z checks and two boundary vertices.

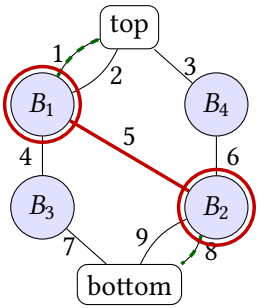
Edges: data qubits; qubit j joins the Z checks containing it, or its single Z check to the corresponding boundary.

An error support is an edge set. Its syndrome lists the check vertices of odd degree.

Unlike the Tanner graph, this graph has qubits as edges. Boundary vertices have no parity constraint.

Decoding becomes pairing endpoints

A check vertex with syndrome bit 1 is called a defect.



Defects at B_1, B_2 admit the error supports

$$\{5\} \qquad \text{and} \qquad \{1, 8\}.$$

Solid: edge 5.
Dashed: edges 1 and 8.

Connect defects in pairs or to boundaries. Minimum-weight matching minimizes the total path cost.

Under independent X noise with a common probability $0 < p < 1/2$, unit weights find a most likely error.

A noise model changes the geometry

Let $e = (e_1, \ldots, e_n)$ be a random binary error vector, with independent coordinates and $p_j := \Pr(e_j = 1) \in (0, 1/2)$.

$$\Pr(e = x) = \prod_{j=1}^{n} p_j^{x_j} (1 - p_j)^{1 - x_j}.$$

Definition (Likelihood weights)

Put $w_j := \log \dfrac{1 - p_j}{p_j}$. A most likely error with syndrome s minimizes $\sum_j w_j x_j$ subject to $H_Z x = s$.

For $p_1 = p_8 = 0.1$, $p_5 = 0.01$ (all other $p_j = 0.001$),

$$w_1 + w_8 = 2 \log 9 < \log 99 = w_5.$$

Thus the two-edge support $\{1, 8\}$ is more likely than the one-edge support $\{5\}$.

Most likely error versus most likely class

A three-qubit CSS example: $H_X = (1\ 1\ 0)$, $H_Z = (1\ 1\ 1)$. Let $p = (0.2, 0.2, 0.3)$ and observe syndrome 1.

Definition (Class probability)

For $H_Z x = s$, the error class $\mathcal{K} := x + \mathrm{row}(H_X)$ has posterior probability

$$\Pr(e \in \mathcal{K} \mid H_Z e = s) = \sum_{y \in \mathcal{K}} \Pr(e = y \mid H_Z e = s).$$

class	unnormalized posterior masses	total
$\{100, 010\}$	$0.112 + 0.112$	0.224
$\{001, 111\}$	$0.192 + 0.012$	0.204

The most likely error lies in the less likely class. All masses normalize by the same factor 0.428.

Gains from scaling up

Fix the odd rotated patches, independent X errors of probability p, perfect check measurements, and a minimum-weight matching decoder. Let $P_L(d,p)$ be its logical failure probability:

$$P_L(d,p) \coloneqq \Pr(e + \widehat{x}(H_Z e) \notin \operatorname{row}(H_X)) .$$

Definition (Positive threshold)

There is a positive threshold if some $0 < p_0 \leqslant 1/2$ satisfies

$$\lim_{\substack{d\to\infty \\ d\,\text{odd}}} P_L(d,p) = 0 \qquad \text{for every } 0 < p < p_0.$$

Surface-code memory has such a regime. Faulty repeated measurements require a different noise model.

What successful recovery means

1. An encoded ray $[u]$ is corrupted to $[X(x)u]$.
2. Commuting check measurements give the classical syndrome $s = H_Z x$.
3. A decoder chooses $\widehat{x}(s)$ and applies $X(\widehat{x}(s))$.

$$\text{The residual is } X(x + \widehat{x}).$$

The recovery criterion

Every encoded ray is restored precisely when

$$x + \widehat{x} \in \mathrm{row}(H_X).$$

Restoring the check outcomes alone is insufficient: a residual logical operator can remain.

Continue exploring

Seminar notes: §§1–4; later sections develop belief propagation, quantum low-density parity-check codes, and circuit noise.

Interactive patch: toggle errors and compare corrections on the talk page.

References

D. Gottesman, *An introduction to quantum error correction and fault-tolerant quantum computation*, arXiv:0904.2557, §§2–3.
E. Dennis et al., *Topological quantum memory*, J. Math. Phys. 43 (2002).
J. Roffe, *Quantum error correction: an introductory guide*, Contemp. Phys. 60 (2019).

`https://utsa-quantum-math.github.io/talks/2026-11-13-duenez/`

Optional: Shor's nine-qubit encoding

Definition (Three-qubit block states)

Put $|G_+\rangle := (|000\rangle + |111\rangle)/\sqrt{2}$ and $|G_-\rangle := (|000\rangle - |111\rangle)/\sqrt{2}$.



Definition (Shor encoding)

Define $V|0\rangle := |\overline{0}\rangle := |G_+\rangle^{\otimes 3}$ and $V|1\rangle := |\overline{1}\rangle := |G_-\rangle^{\otimes 3}$, extending V linearly. The code is $\mathbb{P}(\mathrm{span}\{|\overline{0}\rangle, |\overline{1}\rangle\})$.

Shor (1995), Phys. Rev. A 52, R2493; seminar notes §2.6.

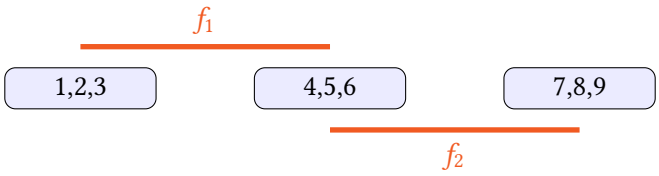
Shor's checks: within blocks and between blocks

The Z checks compare neighboring bits within each block:

$$h_1 \coloneqq Z_1Z_2, \qquad h_3 \coloneqq Z_4Z_5, \qquad h_5 \coloneqq Z_7Z_8,$$
$$h_2 \coloneqq Z_2Z_3, \qquad h_4 \coloneqq Z_5Z_6, \qquad h_6 \coloneqq Z_8Z_9.$$

The X checks compare the signs of neighboring whole blocks:

$$f_1 \coloneqq X_1X_2X_3X_4X_5X_6, \qquad f_2 \coloneqq X_4X_5X_6X_7X_8X_9.$$



$$S_{\text{Shor}} \coloneqq \langle h_1, \ldots, h_6, f_1, f_2 \rangle, \qquad k = 9 - 6 - 2 = 1.$$

Opposite types overlap in zero or two qubits. All eight generators are independent.

Read a Shor syndrome in two parts

Use the abridged syndrome in the specified order:

$$s_{\text{Shor}}(E) \coloneqq \big(s_{h_1}(E), \ldots, s_{h_6}(E) \mid s_{f_1}(E), s_{f_2}(E)\big).$$

error	Z-check bits	X-check bits
X_5	001100	00
Z_1	000000	10
Z_2	000000	10
Z_4	000000	11
Z_7	000000	01
Y_5	001100	11

Z checks locate a bit flip within its block; X checks locate a phase flip's block.

The full syndrome has one bit for each element of S_{Shor}; it is determined by these eight generator bits.

Why equal syndromes need not prevent recovery

$$s_{\text{Shor}}(Z_1) = s_{\text{Shor}}(Z_2).$$

For every code vector u, the check h_1 satisfies

$$Z_1 Z_2 u = u \qquad \text{and hence} \qquad Z_1 u = Z_2 u.$$

If the actual error was Z_2 and the correction is Z_1, then

$$\underbrace{Z_1}_{\text{correction}} \underbrace{Z_2}_{\text{error}} u = h_1 u = u.$$

The useful ambiguity

We need to identify the error's stabilizer class, not the individual qubit on which this phase error occurred.

Shor's code is degenerate: the weight-two check h_1 has weight below its distance three.

Physical Pauli type and logical action are different labels

For the displayed encoding, define

$$\overline{X}_{\text{Shor}} \coloneqq Z_1 Z_4 Z_7, \qquad \overline{Z}_{\text{Shor}} \coloneqq X_1 X_2 X_3.$$

	$\lvert\overline{0}\rangle$	$\lvert\overline{1}\rangle$
$\overline{X}_{\text{Shor}}$	$\lvert\overline{1}\rangle$	$\lvert\overline{0}\rangle$
$\overline{Z}_{\text{Shor}}$	$\lvert\overline{0}\rangle$	$-\lvert\overline{1}\rangle$

Each physical Z changes $|G_+\rangle$ into $|G_-\rangle$ and conversely. Applying one Z in each block therefore exchanges the two code basis vectors.

Logical X exchanges the chosen encoded basis vectors, even when its physical factors are Z's.

Why Shor's code corrects an arbitrary single-qubit error

A nontrivial pure-X logical must occupy at least one whole block:

$$d_X = 3, \qquad \text{attained by } X_1X_2X_3.$$

A nontrivial pure-Z logical must meet all three blocks oddly:

$$d_Z = 3, \qquad \text{attained by } Z_1Z_4Z_7.$$

Parameters and correction guarantee

$d = \min(d_X, d_Z) = 3$: Shor's code is $[[9, 1, 3]]$. It corrects every single-qubit Pauli error, including $Y_j = iX_jZ_j$.

The same recovery corrects channels whose Kraus operators are linear combinations of I and single-qubit Pauli errors.

The Pauli-span recovery theorem supplies the last step; it does not identify coherent noise with a stochastic Pauli mixture.

Two nine-qubit codes, two different check geometries

Both Shor's code and our surface patch have parameters $[[9, 1, 3]]$.

	Shor	rotated surface patch
physical qubits	9	9
independent checks	8	8
Z-check weights	2	2 or 4
X-check weights	6	2 or 4
encoded qubits	1	1
distance	3	3

Shor's construction organizes repetition in blocks; the surface patch uses local checks on a square grid.

Code parameters alone do not describe the measurement geometry or decoding problem.