Quantum Error Correction

Lecture 2

•

Daniel Gottesman, Perimeter Institute

University of British Columbia, July 17, 2010

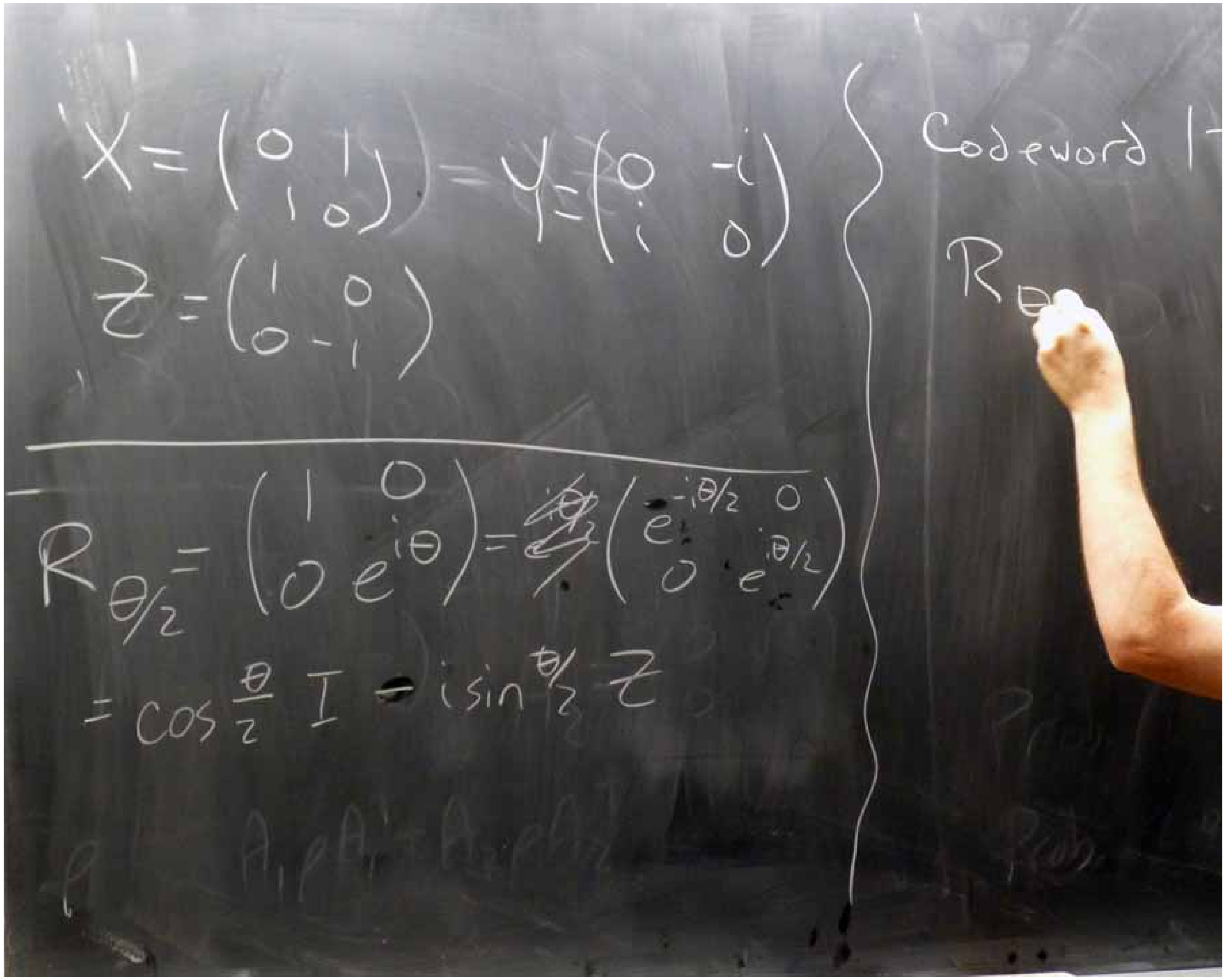
Nine-qubit code

$$|0\rangle \to (|000\rangle + |111\rangle)^{\otimes 3}$$

$$|1\rangle \to (|000\rangle - |111\rangle)^{\otimes 3}$$

Correct bit flip error by looking at each set of 3

Correct phase error by comparing 3 phases



$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
$R_{\theta/2} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}$
$= \cos\frac{\theta}{2} I - i \sin\frac{\theta}{2} Z$
Codeword
R_θ

Codeword $|\psi\rangle$

$$R^{(k)}_{\theta/2}|\psi\rangle = \cos\frac{\theta}{2}\, I|\psi\rangle - i\sin\frac{\theta}{2}\, Z^{(k)}|\psi\rangle$$

Error correction: $\cos\frac{\theta}{2}\,|\psi\rangle|\text{no error}\rangle - i\sin\frac{\theta}{2}\, Z^{(k)}|\psi\rangle|Z^{(k)}\rangle$

Measure error syndrome:

Prob. $\cos^2\frac{\theta}{2}$: $|\psi\rangle|\text{no error}\rangle \rightarrow |\psi\rangle$

Prob. $\sin^2\frac{\theta}{2}$: $Z^{(k)}|\psi\rangle|Z^{(k)}\rangle \rightarrow |\psi\rangle$

Thm: If a QECC corrects A, B, then it also corrects $\alpha A + \beta B$

Cor: A QECC that corrects I, X, Y, Z on a single qubit corrects any error on a single qubit

Correcting I, X, Y, Z on t qubits $\Rightarrow$ correcting any t-qubit error.

Eigenvalue $+1$ of $Z \otimes Z \Leftrightarrow$ even parity

-1 $\Leftrightarrow$ odd parity

$Z \otimes Z$

$Z \otimes Z$

$Z \otimes Z$

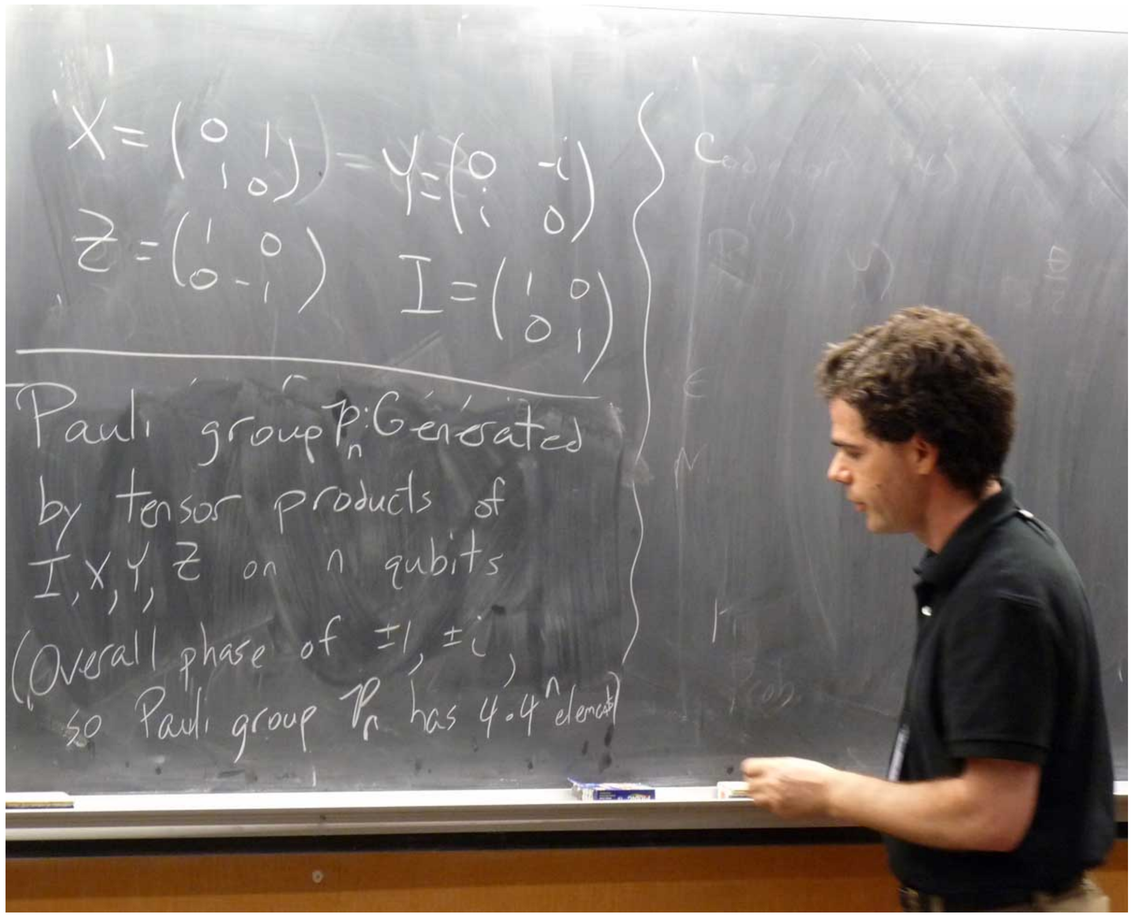
$Z \otimes Z$

$Z \otimes Z$

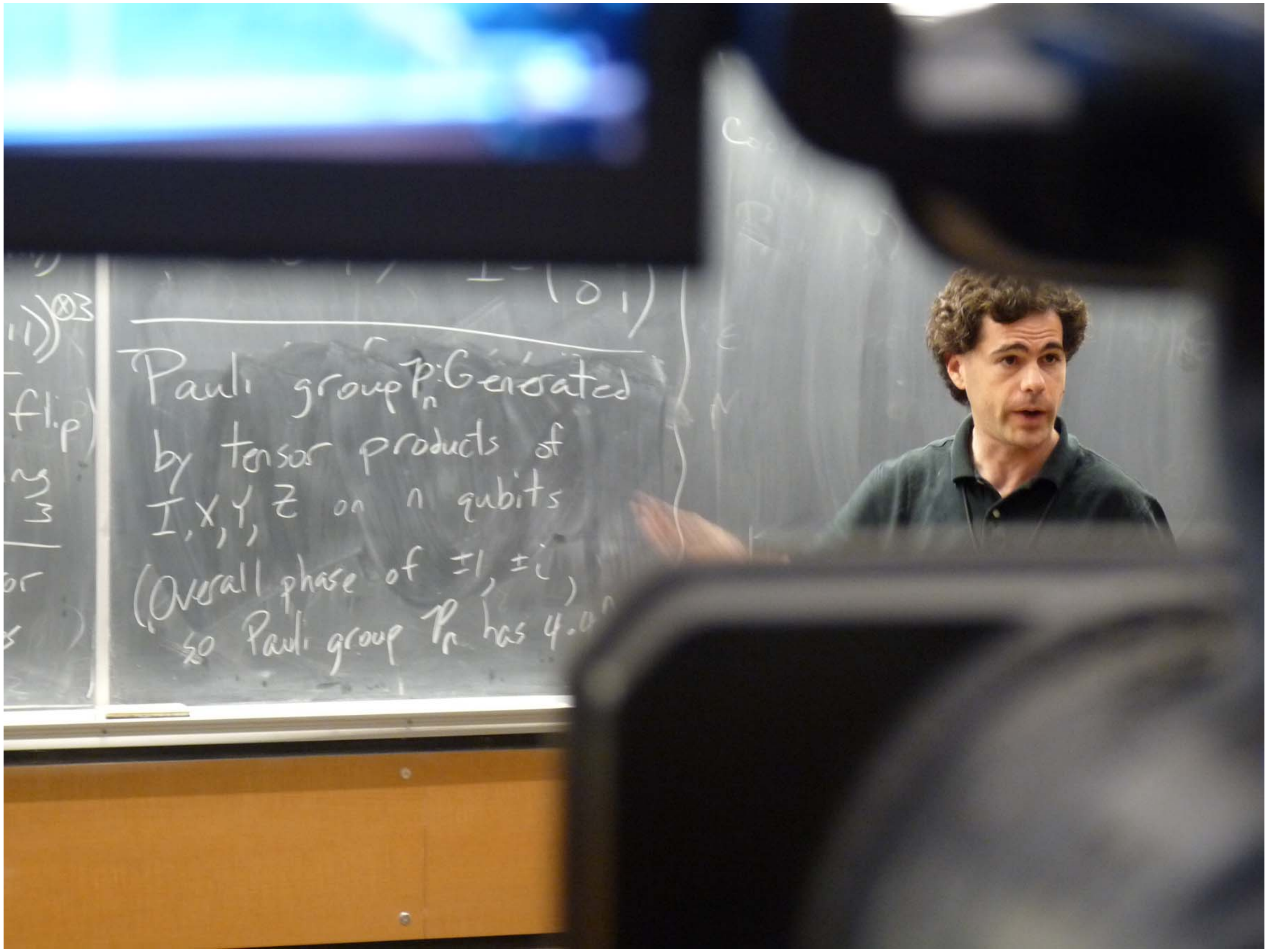
$Z \otimes Z$

$X \otimes X \otimes X \otimes X \otimes X \otimes X$

$X \otimes X \otimes X \otimes X \otimes X \otimes X$



$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
Pauli group $\mathcal{P}_n$: Generated by tensor products of I, X, Y, Z on n qubits
(Overall phase of ±1, ±i)
so Pauli group $\mathcal{P}_n$ has $4 \cdot 4^n$ elements


Pauli group P_n: Generated
by tensor products of
I, X, Y, Z on n qubits
(Overall phase of ±1, ±i)
so Pauli group P_n has

Any $M \in \mathcal{P}_n$ either has $M^2 = I$ or $M^2 = -I$

Any $M, N \in \mathcal{P}_n$ either

commute $[M, N] = MN - NM = 0$

or anti-commute

$\{M, N\} = MN + NM = 0$

$XY = -YX$, $XZ = -ZX$

$YZ = -ZY$ $\qquad [X \otimes X, Z \otimes Z] = 0$

Stabilizer of a QECC T:

$$S(T) = \{ M \in \mathcal{P}_n \mid M|\psi\rangle = |\psi\rangle \ \forall |\psi\rangle \in T \}$$

Stabilizer is a group

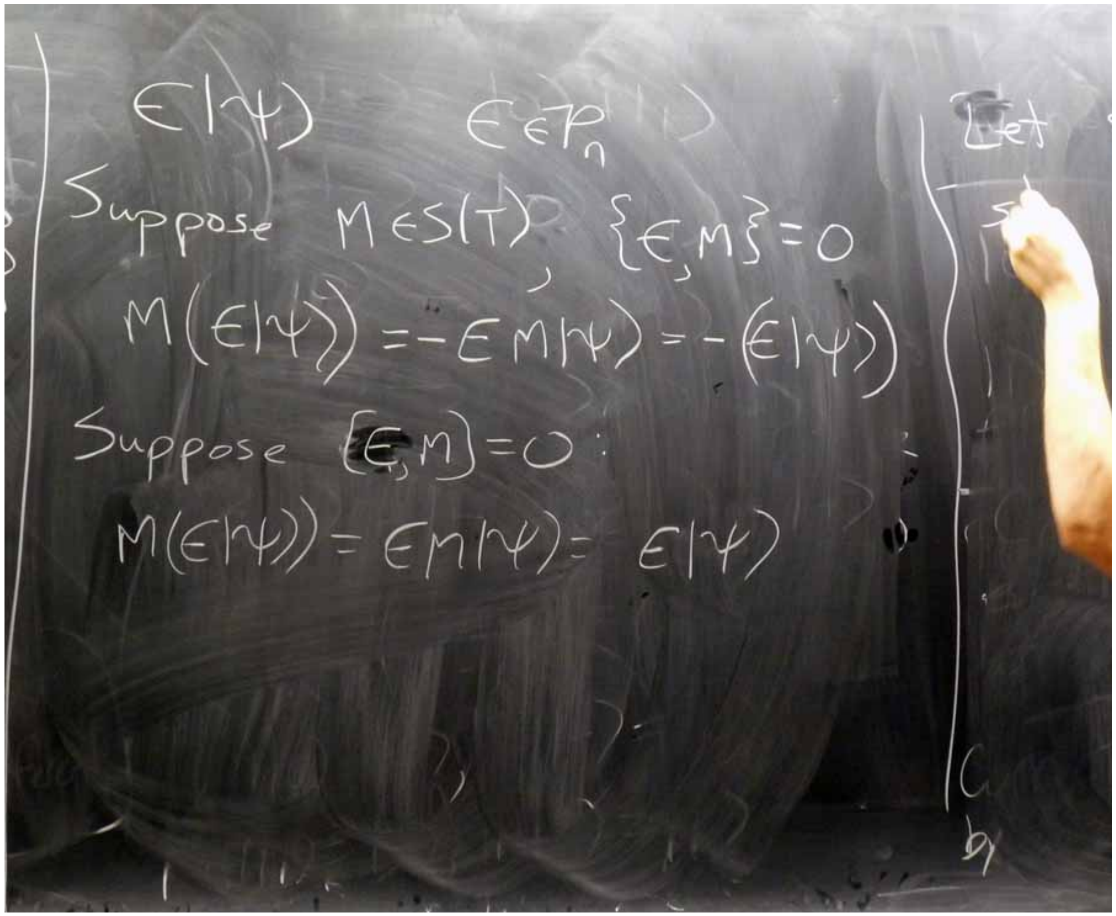
$$M, N \in S(T) \Rightarrow MN \in S(T)$$

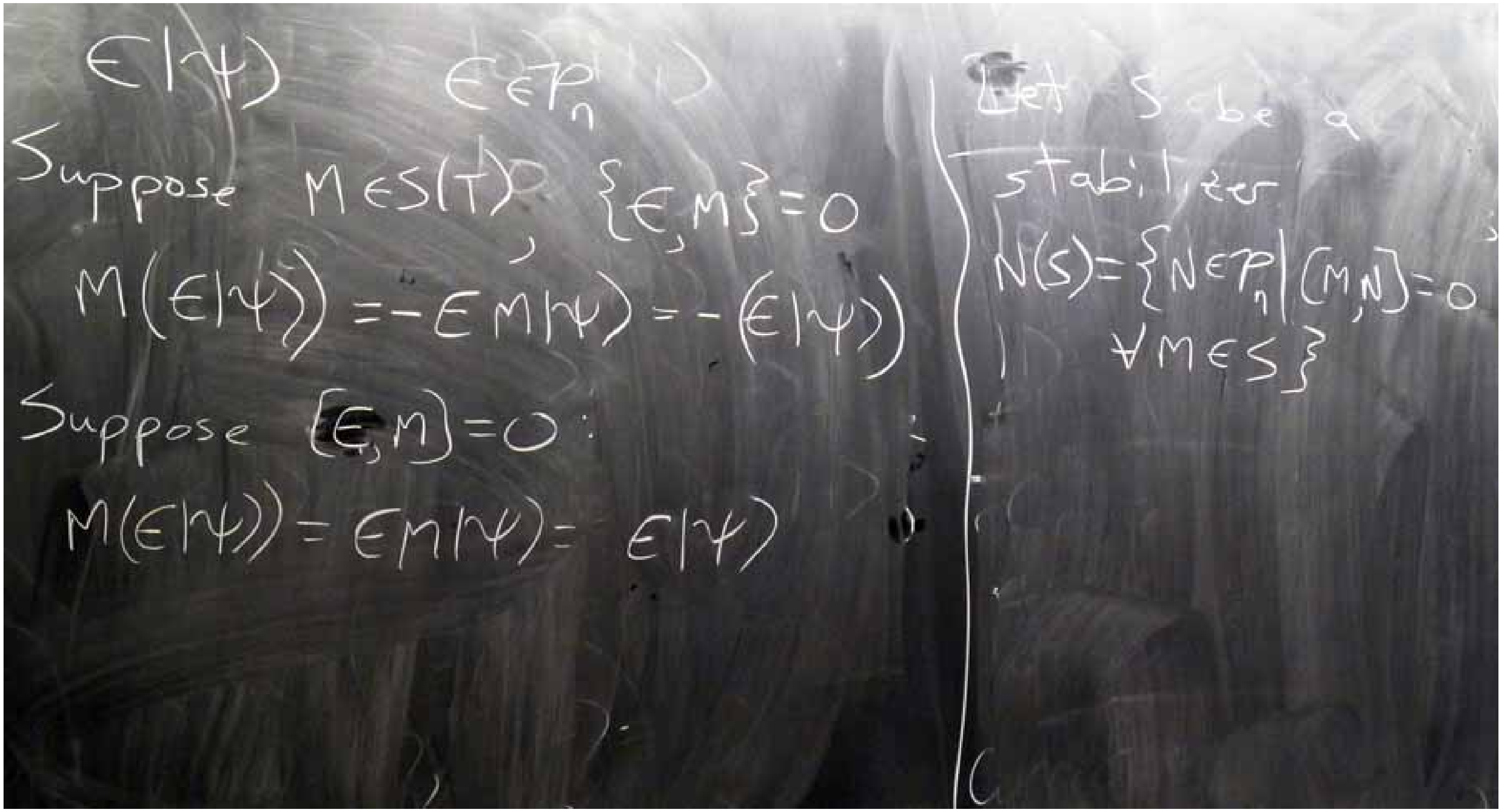
$$N|\psi\rangle = |\psi\rangle \Rightarrow M(N|\psi\rangle) = M|\psi\rangle = |\psi\rangle$$

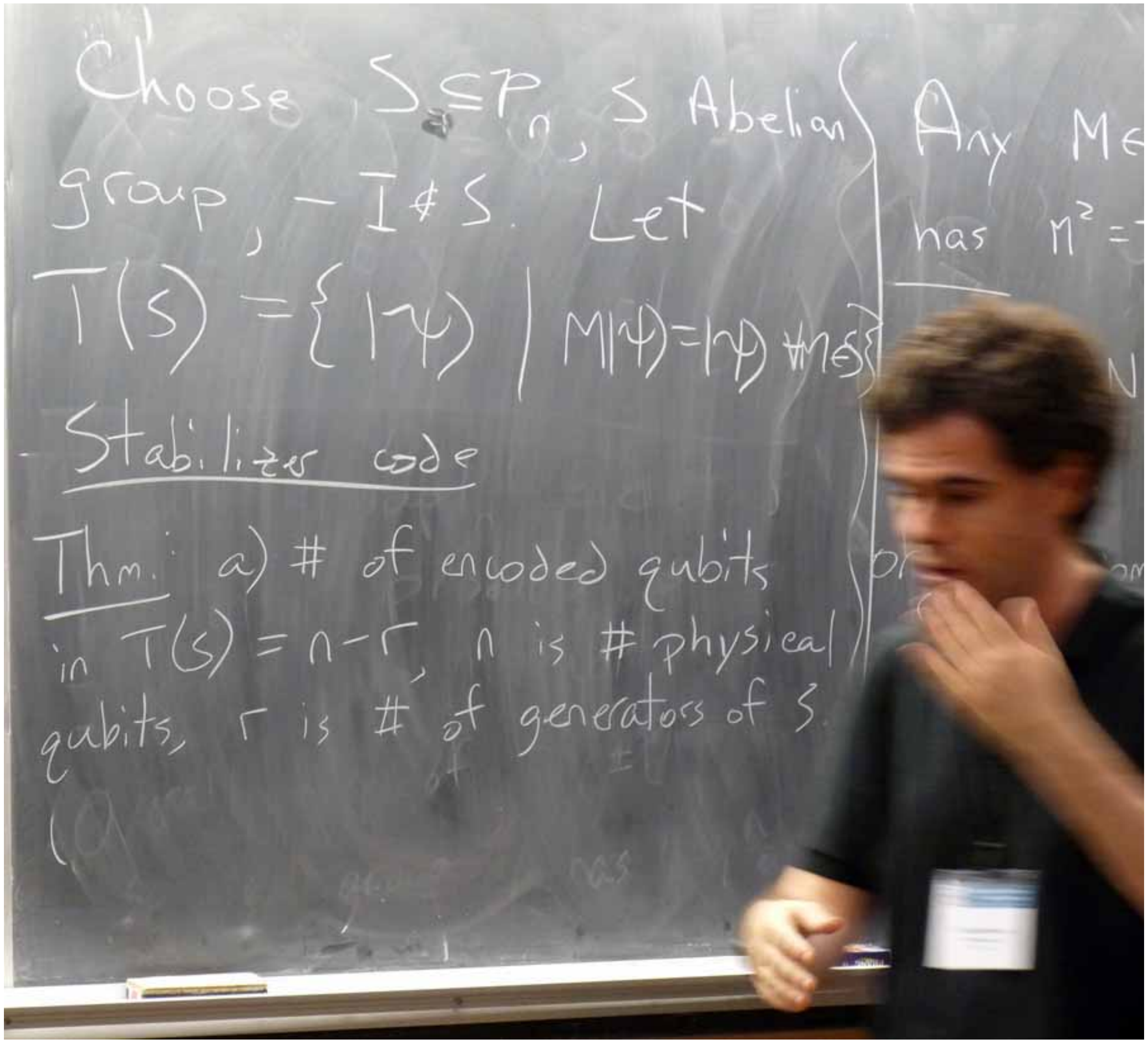
Stabilizer is Abelian:

$$[M,N]|\psi\rangle = MN|\psi\rangle - NM|\psi\rangle = |\psi\rangle - |\psi\rangle = 0$$

$M, N \in \mathcal{P}_n \Rightarrow$ commute.


$\epsilon|\psi\rangle \quad \epsilon \in \mathcal{P}_n$
Suppose $M \in S(T)$, $\{\epsilon, M\} = 0$
$M(\epsilon|\psi\rangle) = -\epsilon M|\psi\rangle = -(\epsilon|\psi\rangle)$
Suppose $[\epsilon, M] = 0$:
$M(\epsilon|\psi\rangle) = \epsilon M|\psi\rangle = \epsilon|\psi\rangle$
Let


$E|\psi\rangle$
$E \in \mathcal{P}_n$
Suppose $M \in S(T)$, $\{E, M\} = 0$
$M(E|\psi\rangle) = -EM|\psi\rangle = -(E|\psi\rangle)$
Suppose $[E, M] = 0$:
$M(E|\psi\rangle) = EM|\psi\rangle = E|\psi\rangle$
Let S be a stabilizer
$N(S) = \{N \in \mathcal{P}_n \mid [M, N] = 0 \ \forall M \in S\}$


Choose S ⊆ P_n, S Abelian
group, −I ∉ S. Let
T(S) = {|ψ⟩ | M|ψ⟩ = |ψ⟩ ∀M∈S}
Stabilizer code
Thm: a) # of encoded qubits
in T(S) = n−r, n is # physical
qubits, r is # of generators of S.

b) The code detects errors outside $N(S)\setminus S$

Errors in $N(S)\setminus S$ are undetectable.

c) $T(S)$ can correct a set $\mathcal{E}$ of errors if

$\forall E, F \in \mathcal{E}, \quad E^\dagger F \notin N(S)\setminus S$

Suppose $E^\dagger F \in N(S)$

$\{E^\dagger F, M\} = 0 \quad \forall M \in S$

$\Longleftrightarrow$ $\forall M \in S$, either $[E, M] = [F, M] = 0$

or $\{E, M\} = \{F, M\} = 0$

$\Longleftrightarrow$ E & F have same error syndrome

$E^\dagger F \notin N(S) \Longleftrightarrow E$ & F have <u>different</u> error syndromes

Def.: The *distance* of a stabilizer code is the smallest weight of $N \in N(S) \setminus S$.

The weight of $N \in \mathcal{P}_n$ is # of qubits with non-identity action

To correct all t-qubit errors, distance should be $\geq 2t+1$.

5-qubit code

$X \otimes Z \otimes Z \otimes X \otimes I$

$I \otimes X \otimes Z \otimes Z \otimes X$

$X \otimes I \otimes X \otimes Z \otimes Z$

$Z \otimes X \otimes I \otimes X \otimes Z$

$n = 5$ physical qubits

$r = 4$ generators of S

$\Rightarrow k = 1$ encoded qubit.

Code corrects any single-qubit error

$\Rightarrow$ distance 3. $\Rightarrow [[5,1,3]]$

---

n physical qubits

k logical (encoded) qubits

distance d

$[[n, k, d]]$