- codes — concatenation
- action — initialization, encoded operations
- analysis — error recovery

Stabilizer algebra (continued)

So far

* If $|\psi\rangle = P|\psi\rangle$ then $U|\psi\rangle = (UPU^\dagger)U|\psi\rangle$
* Clifford gates = all U s.t. $UPU^\dagger$ is Pauli when P is
  - generated by CNOT: $XI \to XX$, $IX \to IX$, $ZI \to ZI$, $IZ \to ZZ$
  H: $X \to Z$, $Z \to X$ T: $X \to Y$, $Z \to X$

⇒ Can track stabilizers under Clifford gates

Necessary extensions:

* Preparing new stabilizer states
* Measuring in the computational basis
* Tracking the evolution of stabilizer code codewords

Applications:

* Monte Carlo simulation of a circuit of Clifford operations with Pauli errors
* Preparation of ancilla states
  * Time-space tradeoff for Clifford operations
* Error correction

① Preparing new qubits in stabilizer states.

Easy! $|0\rangle \to$ add Z $|1\rangle \to -Z$

$|+\rangle \to X$ $|-\rangle \to -X$

eg. $|+\rangle$, $|0\rangle$ — CNOT: $XI \to XX$, $IZ \to ZZ$

② Measuring in the computational basis

What happens to the state/stabilizer when we measure qubit j in the $|0\rangle, |1\rangle$ basis, i.e., we measure Z_j?

- Case 1: Z_j commutes with all the stabilizers (easy to check)
  $\Leftrightarrow Z_j \in N(S)$ either $Z_j \in S$, $-Z_j \in S$, or Z_j is a measurement of the encoded state.
  If $Z_j \in S$, measurement outcome is $+1$, state unchanged
  If $-Z_j \in S$, " " -1 "
  Otherwise, it depends on the codeword

deciding btwn these cases is $O(n^3)$ naively [Gottesman], Tarasov improves it

- Case 2: Z_j anticommutes with some stabilizers
  eg. $\{Z_j, P\} \equiv Z_jP + PZ_j = 0$ and $\{Z_j, Q\} = 0$
  then $[Z_j, PQ] = 0$ $(Z_jPQ = -PZ_jQ = +PQZ_j)$
  by changing basis — replacing P and Q by P and PQ —

we may assume Z_j anticommutes with exactly one of the generators

$$\mathbb{P}[\text{measure } +1] = \mathrm{Tr}\left(\frac{1+Z_j}{2}\cdot\rho\right)$$

$$= \mathrm{Tr}\left(\frac{1+Z_j}{2}\cdot P\rho P\right) \qquad \text{since } P|\psi\rangle = |\psi\rangle$$

$$= \mathrm{Tr}\left(P\frac{1+Z_j}{2}P\,\rho\right) \qquad \text{trace is cyclic}$$

$$= \mathrm{Tr}\left(\frac{1-Z_j}{2}\rho\right) \qquad PZ_jP = -Z_j$$

$$= \mathbb{P}[\text{measure } -1]$$

$$= \frac{1}{2}$$

Resulting state is thus either $\frac{1}{2}(1+Z_j)\rho(1+Z_j) = \sigma_+$

or $\frac{1}{2}(1-Z_j)\rho(1-Z_j) = \sigma_-$

Consider a stabilizer Q with $[Z_j, Q] = 0$. Then

$$Q\,\sigma_+\,Q = \frac{1}{2}(1+Z_j)Q\rho Q(1+Z_j) = \sigma_+$$

$\Rightarrow Q$ remains a stabilizer

but if $PZ_j = -Z_jP$, $P\,\sigma_+P = \sigma_-$ $\Rightarrow P$ no longer a stabilizer

but $\pm Z_j$ is! So add this back to replace P.

(3) Tracking the evolution of stabilizer code codewords

ie. track both code stabilizers & effect within the code

recall: $N(S) = \{$Paulis that commute with all stabilizers$\}$

$N(S)$'s in Paulis/phases = logical operations

Theorem: For a 2^k-dim. stab. code, ie. $n-k$ independent stabilizers, $N(S)$'s is generated by $2k$ independent Paulis $P_1, Q_1, \ldots, P_k, Q_k$, such that $P_iP_j = P_jP_i$, $Q_iQ_j = Q_jQ_i$,

$$P_iQ_j = (-1)^{\delta_{ij}}Q_jP_i$$

Proof: As before, use Cliffords to change the stabilizers to $Z_{k+1}, Z_{k+2}, \ldots, Z_n$. Let $P_i = X_i$, $Q_i = Z_i$. □

(This description is not unique.)

Can be used to define a basis for the codewords.

X	X	X	X	
Z	Z	Z	Z	
X	X	1	1	} op's P_1
1	Z	1	Z	} op's Q_1 on encoded qubit 1
X	1	X	1	} op's P_2
1	1	Z	Z	} op's Q_2 on encoded qubit 2

$|00\rangle_L$ = stabilized by Z_{1L}, Z_{2L}. →

Imprecise argument for randomized coding:

Theorem: For any $\varepsilon > 0$, for large enough n, there exists a (stabilizer) QECC that with high probability corrects $\frac{1}{2} - \varepsilon$ probability erasure errors.

"Proof:" Let C be a uniformly random stabilizer code.

By large deviation bounds, we need to consider effect of erasure errors on a random subset of $pn = (\frac{1}{2} - \delta)n$ locations

First, replace all erased qubits with 0s and measure the syndrome, σ. If σ is nontrivial, then correct it.

Goal: Show that ≤ 1 Pauli acting on erased qubits could produce that syndrome

Indeed, a given nontrivial Pauli error's syndrome on a random stabilizer is equally likely $+1$ or -1.

Prob. of any ~~given~~ σ syndrome is therefore $\sim \frac{1}{2^{n-k}}$ (not rigorous)

$\mathbb{P}[\text{some Paulis give } \sigma] \leq \frac{4^{pn}}{2^{n-k}} = 2^{-\Omega(n)}$

For CSS: $\left(\frac{2^{pn}}{2^{\frac{n-k}{2}}}\right)^2$

$\therefore \mathop{\mathbb{P}}_{C, \text{error}}[\text{incorrect decoding on code } C] = 2^{-\Omega(n)}$.

$= \sum_C \mathbb{P}[C] \cdot \mathop{\mathbb{P}}_{\text{error}}[\text{incorrect decoding} \mid \text{code } C]$

so some good code exists. □

Remark: also for CSS codes

This is tight! (by no-cloning)

A similar argument works for, eg., depolarizing noise, and in that case the lower bound against random noise matches the Hamming upper bound for worst-case noise (distance) for nondegenerate codes.

$\sum_{j=0}^{(p+\varepsilon)n} \binom{n}{j} 3^j$ errors can occur

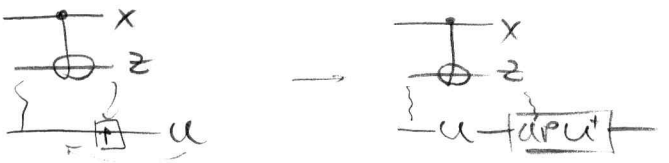
$\log_2 \# \approx \log_2 \binom{n}{\delta n} 3^{\delta n} \approx \left(h(\delta) + \delta \log_2 3\right) n$ $\quad j = p + \varepsilon$

$h(\delta) = -\delta \log_2 \delta - (1-\delta)\log_2(1-\delta)$

syndromes 2^{n-k}

$\Rightarrow$ good provided $h(\delta) + \delta \log_2 3 < 1$

Threshold ½ for erasure errors [Knill]



Say we have prepared $(I \otimes U_L)(|00\rangle_L + |11\rangle_L)$

multiqubit ((overhead

* universality (save till later)

Replace Bell measurements with transversal ones: 

X	X	X	X	1	1	1	1
Z	Z	Z	Z	1	1	1	1
1	1	Z	Z	1	1	1	1
X	X	1	1	X	X	X	X
Z	1	Z	1	Z	Z	1	1
				1	1	Z	Z
				X	X	1	1
				Z	1	Z	1

Exercise: Verify that this works for non-CSS codes, too, eg. the 5-qubit code.

Ancilla factory: massive preps of states

logical operators can be tracked in the same way as stabilizers

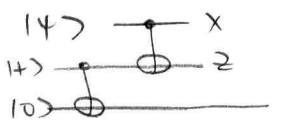
eg.

		swap $2 \leftrightarrow 3$		
	X X X X	→	X X X X	
	Z Z Z Z		Z Z Z Z	
X_{1L}	X X 1 1		X 1 X 1	$= X_{2L}$
Z_{1L}	1 Z 1 Z		1 1 Z Z	$= Z_{2L}$
X_{2L}	X 1 X 1		X X 1 1	$= X_{1L}$
Z_{2L}	1 1 Z Z		1 Z 1 Z	$= Z_{1L}$

Gottesman-Knill Theorem

implements <u>encoded</u> swap !

Teleportation



1	X	X
1	Z	Z
X	1	1
Z	1	1

(Justification: adding reference qubit)