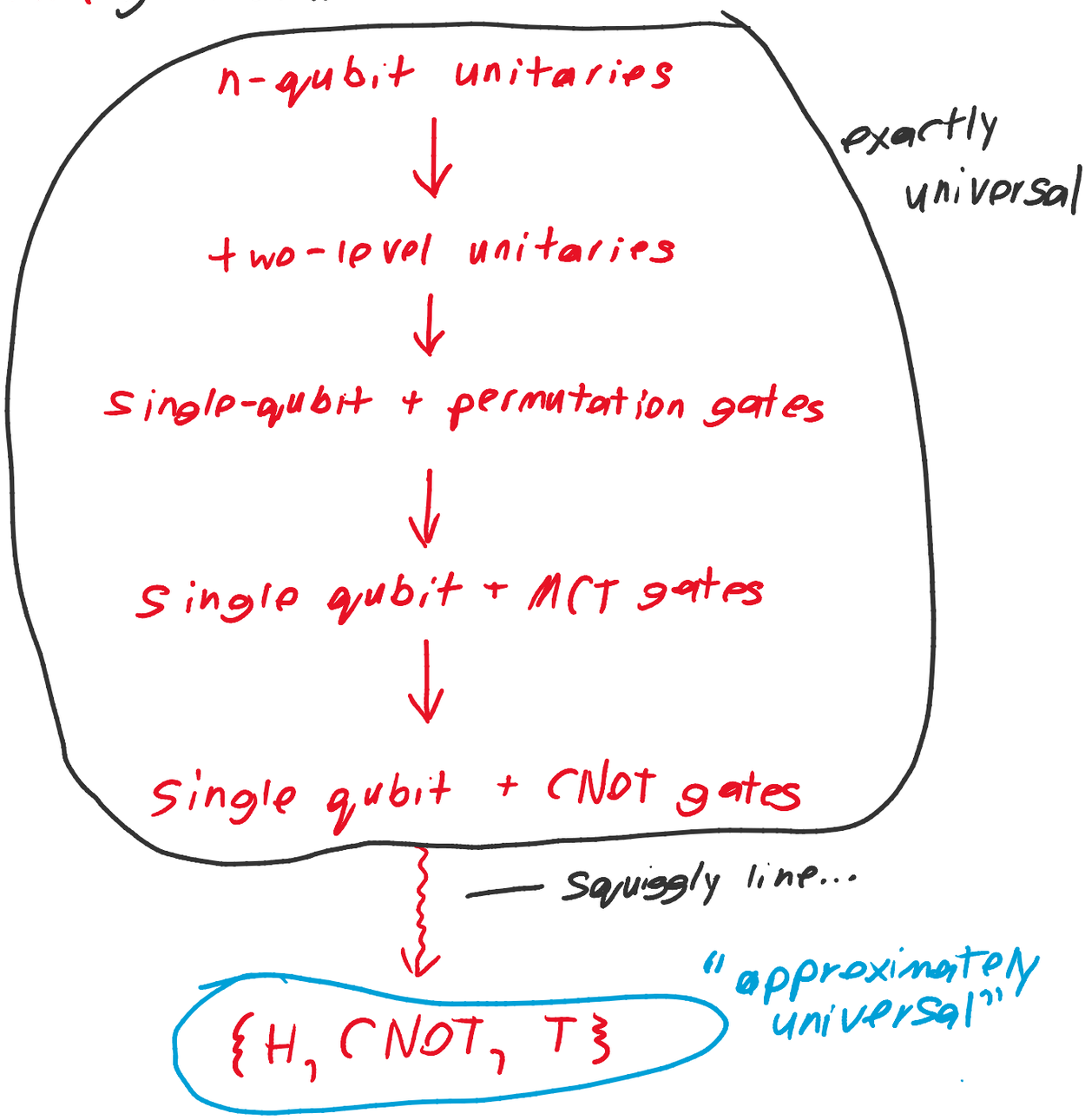
Universal construction of unitaries (Redux)

Previously we focused on the exact decomposition of unitaries over a (necessarily) infinite gate set. Motivated by practical? concerns we now look at the question of approximating unitaries over a finite gate set.



Fault Tolerant quantum computing

Problem... Most QC's have error rates on the order of 10^{-2} per operation (including I). By contrast, classical computers have error rates on the order of 10^{-17}.

How could we hope to run algorithms?

Option 1: Use QC's to prepare states quickly, measure, + repeat

Algorithms applicable
- VQE (gate model, no-known exp speed-up)
- QAOA (ditto)
- Others (measurement-based QC)

Option 2: Correct errors as we go (called FTQEC)

Algorithms applicable
- Phase estimation (gate model, exp speed-up)
- Grover (gate model, polynomial speed-up)

Bottom line: FTQEC is our best hope for practical advantage because it works in theory and offers a known speed-up

In FTQEC, can usually only perform a finite set of encoded operations. The standard set for FTQEC is

$\{H, CNOT, T\}$

also known as the Clifford + T gate set.

Error correcting codes

Quantum fault-tolerance is built out of two parts:

- An error-correcting code, and
- Fault-tolerant encoded gates

An error-correcting code (ECC) is a way of encoding the state of n bits in the state of $m > n$ bits so that the original state can be recovered if an error occurs.

Ex.

A classic ECC is a repetition code

$0_L \equiv 000$

$1_L \equiv 111$

} 1 logical bit encoded in 3 physical bits

If a single physical bit is erroneously flipped, e.g.

$$000 \xrightarrow{\text{error}} 001$$

we can recover the correct state $0_L \equiv 000$ by taking the majority value of all 3 bits (0 in this case)

If a single bit flip has probability p, without encoding the probability of an (unrecoverable) error occuring is p. With encoding, this error rate drops to p^2 since 2 bits need to flip.

Quantum ECCs

While we can't encode a qubit redundantly as

$$|\psi_L\rangle = |\psi\rangle|\psi\rangle|\psi\rangle$$

for a multitude of reasons = no cloning theorem, can't directly observe state $|\psi\rangle$, can't determine an arbitrary error

we can instead encode basis states redundantly

Ex. (logical 0 state, logical 1 state)

Let $|0_L\rangle \equiv |000\rangle$ $|1_L\rangle \equiv |111\rangle$

Then we can encode a logical 1-qubit state as

$$|\psi_L\rangle = \alpha|0_L\rangle + \beta|1_L\rangle = \alpha|000\rangle + \beta|111\rangle$$

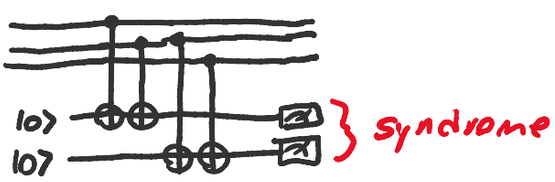
If the second bit is flipped erroneously, the result is

$$(I\otimes X\otimes I)|\psi_L\rangle = \alpha|010\rangle + \beta|101\rangle$$

Since measuring the qubits would destroy the superposition, we need some other way to detect & correct the error. This can be accomplished by measuring the Syndrome. Roughly speaking, the syndrome partitions the state space into 2-dimensional subspaces (i.e. a logical qubit state) according to which error most likely occurred. In this case, the syndrome of $|x_1x_2x_3\rangle$ is $|(x_1\oplus x_2)(x_2\oplus x_3)\rangle$:

Syndrome:	00	10	11	01
States:	$\{\|000\rangle, \|111\rangle\}$	$\{\|100\rangle, \|011\rangle\}$	$\{\|010\rangle, \|101\rangle\}$	$\{\|001\rangle, \|110\rangle\}$
Error:	no error	$X\otimes I\otimes I$	$I\otimes X\otimes I$	$I\otimes I\otimes X$

Measuring the syndrome projects $|\psi_L\rangle$ down to a 2-dimensional, so we haven't lost (if only X errors occur) any information



Fault tolerant computation

We now have Quantum error correcting codes, but we still need to figure out the computation part

Option 1:

To perform U, decode $|\psi_L\rangle \mapsto |\psi\rangle|0\cdots0\rangle$, apply U, the re-encode $|\psi'\rangle|0\cdots0\rangle \mapsto |\psi'_L\rangle$

But all these steps are error-prone!

Option 2: (the correct one)

To perform U, do it directly on the encoded state.
I.e. find some circuit U_L s.t. $U_L|\psi_L\rangle = |\psi'_L\rangle$
where $|\psi'\rangle = U|\psi\rangle$

Ex.

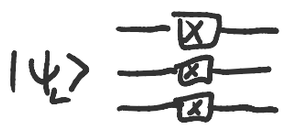
Recall our code $|0_L\rangle = |0000\rangle$, $|1_L\rangle = |1111\rangle$.
To perform a logical X gate, we need a circuit

$$X_L : |0000\rangle \leftrightarrow |1111\rangle$$

This is just an X gate on each qubit, since

$$X\otimes X\otimes X\otimes X|0000\rangle = |1111\rangle$$
$$X\otimes X\otimes X\otimes X|1111\rangle = |0000\rangle$$

As a circuit diagram,



This is an example of a Transversal encoded gate
We say a logical operation U_L in a particular QECC is transversal if it can be implemented as

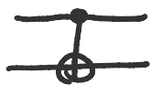
$$U_L = U_1 \otimes U_2 \otimes \cdots \otimes U_k$$

Transversality, faults and resources

Transversal gates are nice because

1. They're efficient to implement (Yay!)
2. They don't propagate errors

(error propagation)

Consider the circuit  .

Observe that 

Effectively, this means the CNOT gate copies or propagates an X error on the control. To see the effects, consider a silly 2-qubit code $|0_L\rangle = |10\rangle$, $|1_L\rangle = |11\rangle$. A logical X could be implemented as CNOT. If our initial state is $|0_L\rangle$ and we want to apply $X_L = CNOT$,

$$X_L|0_L\rangle = CNOT|10\rangle = |11\rangle = |1_L\rangle$$

If an X error occurs on the first qubit,

$$(X \otimes I)|0_L\rangle = |00\rangle$$

We can detect and correct the state to $|0_L\rangle$ by measuring the first qubit. However, if we applied Logical X to the state **before** correcting the error, we get

$$X_L|00\rangle = |00\rangle$$

which corrects, erroneously, to $|10\rangle = |0_L\rangle \neq X_L|0_L\rangle$

Requirement for FTQEC

Encoded gates must not propagate errors

(between physical qubits in the same logical block)

Universal sets of encoded gates

What we know:

- CNOT + single qubit rotations are (physically) universal
- But for FTQEC they need to be encoded
- And the encoded gates can't propagate errors

Question: Is there a useful QECC where CNOT + single qubit rotations is transversal?

Thm. (Eastin-Knill)

For any non-trivial (plus some other conditions) QECC, there is no set (even infinite) of transversal unitary gates that is universal (even under relaxed notions to come...)

Despite the Eastin-Knill theorem, not all hope is lost. It turns out that Clifford circuits are generally transversal, and when they aren't they're usually easy to implement fault-tolerantly.

Def'n (The simple one)

Clifford circuits are circuits over the gate set $\{H, CNOT, S\}$

Thm.

Clifford operations can be implemented transversally in any self-dual CSS code

(Check out Phys 523B at UBC for more info...)

Aside: the Clifford group

This isn't really needed for our purposes right now, but it's important to understand so we'll talk about it briefly

Clifford circuits and operators are an important class of operations with a close connection to the theory of Stabilizer codes which are fundamental in QECC

Def'n (Pauli group)

(unitaries w/ fixed dimension for our purpose)

The Pauli group on 1 qubit is $P_1 = \{\pm 1, \pm i\} \cdot \{I, X, Y, Z\}$

The Pauli group on n qubits is

$$P_n = \{\pm 1, \pm i\} \cdot \{g_1 \otimes \cdots \otimes g_n \mid g_i \in \{I, X, Y, Z\}\}$$

In words, the Pauli group P_n is n-fold tensor products of Pauli gates together with a phase i^x, $x \in \mathbb{Z}_4$.

E.g. $-i(I \otimes X \otimes Z) \in P_3$

$-(Z \otimes Z) \in P_2$

Stabilizer codes correspond to abelian (commuting) subgroups of P_n. In particular, given $S \triangleleft P_n$, the code space is the simultaneous $+1$-eigenspace of S

$|\psi\rangle$ s.t. $U|\psi\rangle = |\psi\rangle \ \forall U \in S$

(This makes S the Stabilizer subgroup of the code)

Fact

The subgroup $S \triangleleft P_n$ generated by $k \leq n$ linearly independent and commuting Paulis $g_1, \ldots, g_k \in P_n$ has code space of dim. 2^{n-k}

Clifford group cont.

The Clifford group arises as operations which map Paulis to Paulis under conjugation.

Def'n (Clifford group)

The Clifford group on n-qubits is the normalizer of the Pauli group P_n. Explicitly,

$$C_n = \{U \mid U P_n U^\dagger = P_n\}$$

Ex.

We can verify that H, $CNOT$, S each satisfy the above:

$HXH = Z$

$HZH = X$

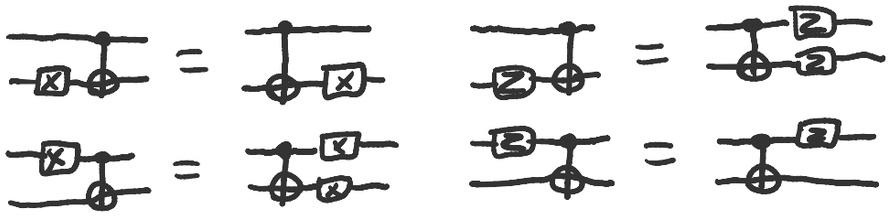
$HYH = HiXZH = iZX$

$SXS^\dagger = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -i \end{bmatrix} = Y$

$SZS^\dagger = SSZ = Z$ (S & Z are diagonal)

$SYS = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -i \end{bmatrix} = -X$

For CNOT it helps to know the following rules...



Prop.

The Clifford group C_n is exactly the n-qubit circuits over the gate set $\{H, CNOT, S\}$

The Gottesman-Knill theorem

Thm. (Gottesman-Knill)

Any circuit consisting of $\{H, CNOT, S\}$ gates and Pauli-basis measurements is classically simulable in Polynomial time on the initial state $|00\cdots0\rangle$

Pf sketch

The basic idea is to keep track of a set of generators for the Stabilizer of the current state.

We only need n such generators, since the code space of n independent commuting Paulis has dimension 1.

In particular,

$$Stab_{|00\cdots0\rangle} = \langle Z\otimes I\otimes\cdots\otimes I,\ I\otimes Z\otimes\cdots\otimes I,\ I\otimes I\otimes\cdots\otimes Z\rangle$$

If we apply $U\in C_n$, then

$$\begin{aligned} Stab_{U|00\cdots0\rangle} &= \{P U|00\cdots0\rangle = U|00\cdots0\rangle \mid P\in P_n\} \\ &= \{UP'U^\dagger U|00\cdots0\rangle = U|00\cdots0\rangle \mid P = UP'U^\dagger, P'\in P_n\} \\ &= \{UP'|00\cdots0\rangle = U|00\cdots0\rangle \mid \cdots\} \\ &= U\, Stab_{|00\cdots0\rangle}\, U^\dagger \end{aligned}$$

Ex.

$$\begin{aligned} Stab_{(H\otimes I)|00\rangle} &= \{P|+\rangle|0\rangle = |+\rangle|0\rangle \mid P\in P_n\} \\ &= \langle X\otimes I,\ I\otimes Z\rangle \\ &= (H\otimes I)\langle Z\otimes I,\ I\otimes Z\rangle(H\otimes I) \\ &= H\, Stab_{|00\rangle}\, H \end{aligned}$$