Limits on Transversal and Fold-Transversal Gates

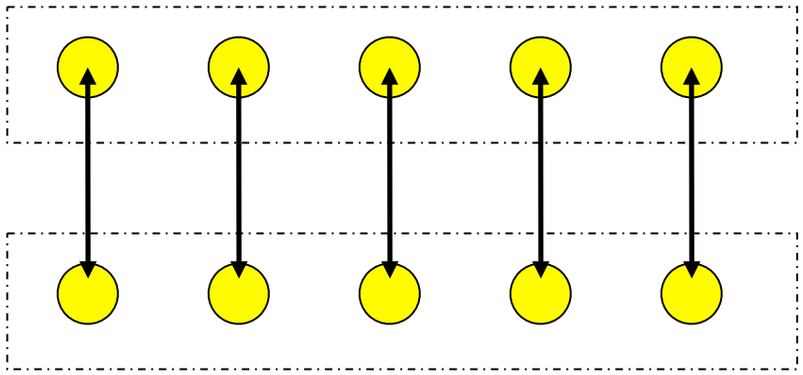
Daniel Gottesman

Work with Aranya Chakraborty
arXiv:2602.13395 [quant-ph]

Transversal Gates

A transversal gate is a gate which is a tensor product of gates only affecting corresponding qubits in different blocks of a QECC.

E.g., gates interacting the 1st qubit of 1st block with the 1st qubit of the second block; the 2nd qubit with the 2nd qubit, and so on.



For single-block gates, a transversal gate is just a tensor product of single-qubit gates:

$$U = \bigotimes U_i$$

(Note: we allow different gates on different qubits.)

Transversal gates

- Control error propagation
- Are fast
- Are easy to parallelize

Transversal Gates Are Not Universal

However, the Eastin-Knill theorem tells us that transversal gates must form a discrete group and therefore cannot be universal.

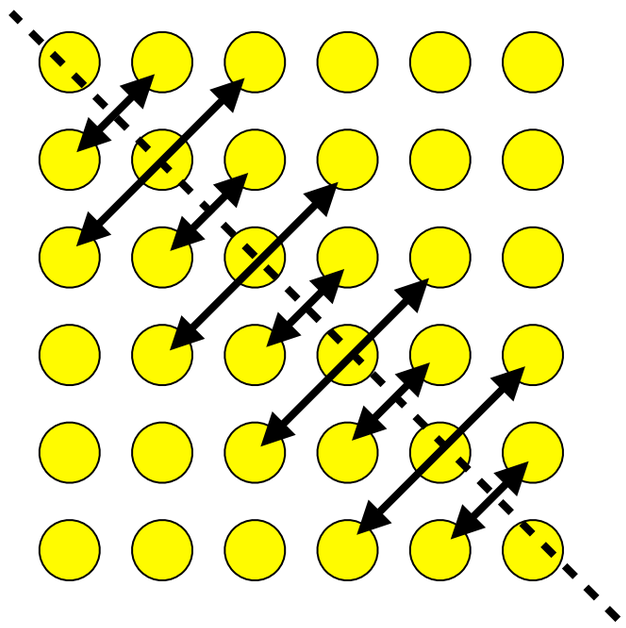
But we would like to do as much as we can with them.

For instance, we could hope to do the whole Clifford group.

Also, what if we add a little bit to transversal gates?

- Allow gates between specific pairs of qubits (fold-transversal)
- Allow permutations of qubits (automorphisms)

These modifications can increase the set of available gates.



Codes with Multiple Qubits

Even single-block transversal gates can do interesting things if the codes has multiple qubits.

Example: [[4,2,2]] code

$$X \otimes X \otimes X \otimes X$$
$$Z \otimes Z \otimes Z \otimes Z$$
$$\overline{X}_1 = X \otimes X \otimes I \otimes I$$
$$\overline{X}_2 = X \otimes I \otimes X \otimes I$$
$$\overline{Z}_1 = Z \otimes I \otimes Z \otimes I$$
$$\overline{Z}_2 = Z \otimes Z \otimes I \otimes I$$

Transversal S gate $S^{\otimes 4}$

$$(S : X \to Y, Z \to Z)$$

Preserves the code space

$$S^{\otimes 4} : \overline{X}_1 \to Y \otimes Y = -\overline{X}_1\overline{Z}_2$$
$$S^{\otimes 4} : \overline{X}_2 \to Y \otimes I \otimes Y = -\overline{X}_2\overline{Z}_1$$

This is (up to logical Paulis) a logical controlled-Z gate!

Physical single-qubit gates can do logical multi-qubit gates.

For codes with many logical qubits, this can be important.

2-Qubit vs. 1-Qubit Clifford Group

However, transversal Clifford gates on one block cannot do the full 2-qubit logical Clifford group.

The order of a unitary U is the minimum number r such that

$$U^r = I$$

Single-qubit Clifford group gates have order 2, 3, or 6.

Any single-block transversal gate also has order 2, 3, or 6.

But there are 2-qubit Clifford gates with order 5.

E.g., Bell gate

$$\mathrm{BELL} = \frac{e^{3\pi i/4}}{\sqrt{2}} \begin{pmatrix} 1 & i & 0 & 0 \\ 0 & 0 & i & 1 \\ 0 & 0 & i & -1 \\ 1 & -i & 0 & 0 \end{pmatrix}$$

$$X \otimes I \to Y \otimes Z$$
$$I \otimes X \to X \otimes Y$$
$$Z \otimes I \to Z \otimes Z$$
$$I \otimes Z \to X \otimes X$$

$$Z \otimes I \to Z \otimes Z \to -Y \otimes Y \to X \otimes Z \to Z \otimes Y \to Z \otimes I$$

2-Qubit vs. 1-Qubit Clifford Group

Logical gates must have an order that is a factor of the order of the physical implementation:

If the logical gate U has order r and the physical implementation V has order s, then V^r implements $U^r = I$.

V^r can be a non-trivial implementation of the identity, but $V^s = I$ must implement logical identity as well.

If s is not a multiple of r, then let $r' = s - r\lfloor s/r \rfloor$. Then $0 < r' < r$ and $V^{r'}$ implements $U^{r'}$.

But $V^{r'} = V^s (V^r)^{-\lfloor s/r \rfloor}$ implements the logical identity as well, i.e. $U^{r'} = I$. This contradicts r being the order of U.

Since single-block Clifford transversal gates have orders which are not a multiple of 5, and the Bell gate has order 5:

Single-block Clifford transversal gates cannot implement logical Bell gate!

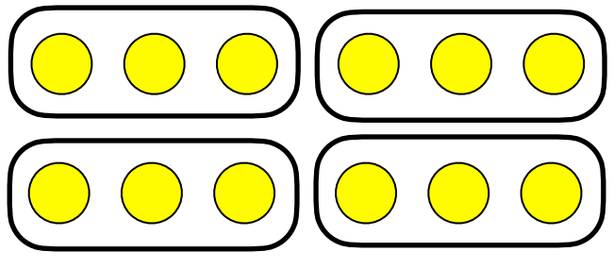
k-Fold Transversal Gates

We can extend this theorem to apply to constructions we call k-fold transversal gates.

In a k-fold transversal gate U, the qubits are divided up into sets S_i. Each set S_i has at most k qubits and U is a tensor product of gates acting within a set. That is,

$$U = \bigotimes U_i$$

where U_i acts only on S_i.



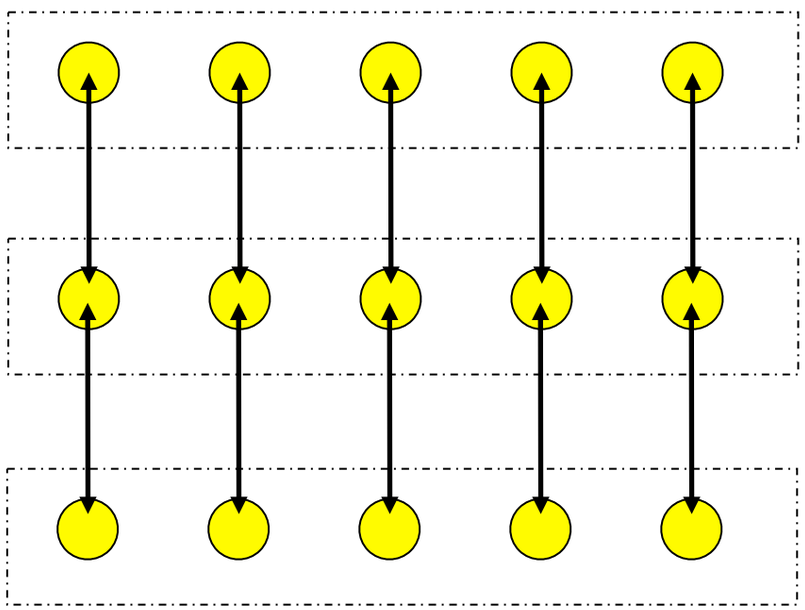
Examples of 2-fold transversal gates:

- Fold transversal gates
- Transversal gates between 2 blocks of a code, where we instead consider the 2 blocks together as a single bigger code.

Limit on k-Fold Transversal Gates

Theorem: No code supports Clifford (k-1)-fold transversal implementations (using a fixed decomposition of the qubits) of the full k qubit logical Clifford group.

In particular, there is no fold-transversal implementation of the full 3-qubit logical Clifford group. And if we have 2 blocks of a code with transversal gates, we also cannot implement the 3-qubit logical Clifford group.



More generally, if we stick to transversal gates, we cannot support the full Clifford group, even with many blocks, if the blocks encode more than 1 logical qubit each.

Limit on k-Fold Transversal Gates

The proof uses the same basic idea as the case for 2 logical qubits.

Zsigmondy's Theorem: (special case) There exists a prime p which divides $2^{2k} - 1$ but doesn't divide $2^{2i} - 1$ for all $i < k$.

Lemma: There exist elements of the k-qubit Clifford group of order $2^k - 1$ and order $2^k + 1$.

Lemma: The order of any element of the j-qubit Clifford group must divide $2^{j^2} \prod_{i=0}^{j} (2^{2i} - 1)$.

Given these lemmas, the proof works as follows:

- The p from Zsigmondy's theorem either divides $2^k - 1$ or $2^k + 1$. Let N be the one that is a multiple of p.
- Let U be an element of order N (which we know exists). Then $U' = U^{N/p}$ has order p.
- But the physical implementation is a tensor product of elements from the j-qubit Clifford group, and so can't have order p.

Proof Ideas of Lemmas

Proof Ideas of Lemmas

Zsigmondy's Theorem: (special case) There exists a prime p which divides $2^{2k} - 1$ but doesn't divide $2^{2i} - 1$ for all $i < k$.

This is a known result from number theory.

Proof Ideas of Lemmas

Zsigmondy's Theorem: (special case) There exists a prime p which divides $2^{2k} - 1$ but doesn't divide $2^{2i} - 1$ for all $i < k$.

This is a known result from number theory.

Lemma: There exist elements of the k-qubit Clifford group of order $2^k - 1$ and order $2^k + 1$.

This can be shown by viewing k qubits as indexed by the field $GF(2^k)$ and by mapping k-qubit Paulis to $GF(2^{2k})$, and then taking Cliffords which correspond to multiplying by a primitive element of the appropriate field.

Proof Ideas of Lemmas

Zsigmondy's Theorem: (special case) There exists a prime p which divides $2^{2k} - 1$ but doesn't divide $2^{2i} - 1$ for all $i < k$.

This is a known result from number theory.

Lemma: There exist elements of the k-qubit Clifford group of order $2^k - 1$ and order $2^k + 1$.

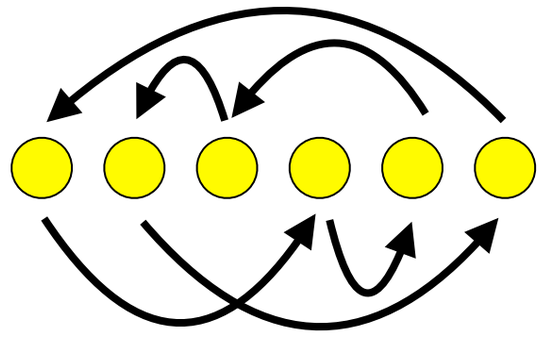
This can be shown by viewing k qubits as indexed by the field $GF(2^k)$ and by mapping k-qubit Paulis to $GF(2^{2k})$, and then taking Cliffords which correspond to multiplying by a primitive element of the appropriate field.

Lemma: The order of any element of the j-qubit Clifford group must divide $M = 2^{j^2} \prod_{i=0}^{j} (2^{2i} - 1)$.

M is the order of the j-qubit Clifford group (up to Paulis and by Lagrange's theorem, each element has order that is a factor of the size of the group.

Limit on Gates Via Permutations

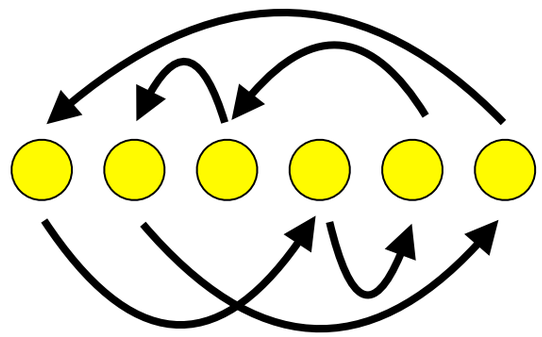
What if we want to implement logical gates by permuting the physical qubits?



The previous arguments don't apply here, because permutations can have any order.

Limit on Gates Via Permutations

What if we want to implement logical gates by permuting the physical qubits?



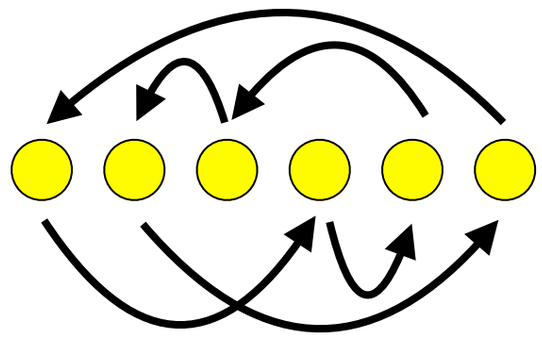
The previous arguments don't apply here, because permutations can have any order.

But instead we can note that it is always possible to choose logical Z operators for a stabilizer code so that they are all tensor products of physical Zs: Choose them to be in the dual code of the X part of the stabilizer.

(Note: If we do this, the logical Xs may be products of X and Z.)

Limit on Gates Via Permutations

What if we want to implement logical gates by permuting the physical qubits?



The previous arguments don't apply here, because permutations can have any order.

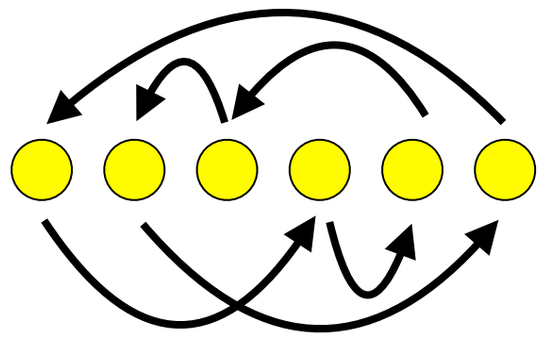
But instead we can note that it is always possible to choose logical Z operators for a stabilizer code so that they are all tensor products of physical Zs: Choose them to be in the dual code of the X part of the stabilizer.

(Note: If we do this, the logical Xs may be products of X and Z.)

But then permutation can only take logical Zs to products of logical Zs. The Bell gate does not have this property.

Limit on Gates Via Permutations

What if we want to implement logical gates by permuting the physical qubits?



The previous arguments don't apply here, because permutations can have any order.

But instead we can note that it is always possible to choose logical Z operators for a stabilizer code so that they are all tensor products of physical Zs: Choose them to be in the dual code of the X part of the stabilizer.

(Note: If we do this, the logical Xs may be products of X and Z.)

But then permutation can only take logical Zs to products of logical Zs. The Bell gate does not have this property.

Permutations cannot implement the Bell gate.

Limit on Automorphisms

What if we allow (single-block) transversal gates *and* permutations?

(These are the automorphisms, symmetries of the QECC.)

Theorem: There is no stabilizer code for which Clifford automorphisms can implement the full 2-qubit logical Clifford group.

The proof for this is a little more involved, but again the idea is to make use of the Bell gate.

The transversal gate part of the automorphism cannot have order 5, but the permutation part can. However, the permutations by themselves also cannot implement Bell.

The idea will be to show that if an automorphism for the Bell gate exists, then there is a pure permutation that implements a power of the Bell gate on an equivalent code.

Simplifying an Automorphism

Suppose U is an automorphism implementation of the Bell gate. Then U has an order that is a multiple of 5.

> Suppose U has order $5^m q$, where q is not a multiple of 5. Then $U' = U^q$ has order 5^m. U' implements a non-trivial power of the Bell gate.

Let us look at the cycle structure of the permutation part of U'.

$$(1,2,3,4,5)(6)(7)(8,9,10,11,12)$$

Because it has order 5^m, all the cycles must have a size that is a power of 5 as well, since $(U')^{5^m}$ must have a trivial permutation.

> Moreover, the Clifford operations on any trivial cycles must also be trivial, since the Clifford gates have order that is not a power of 5.

Equivalence to Permutation

Lemma: If U' is a product of cycles with single-qubit Cliffords only on the qubits in the non-trivial cycles, then there is a transversal Clifford gate V such that $V^\dagger U' V$ is just a product of permutations.

Proof: Looking at a single cycle within U', we can follow its action on single-qubit Paulis.

$$X_1 \to P_2 \to P_3 \to P_4 \to P_5 \to X_1$$
$$Z_1 \to Q_2 \to Q_3 \to Q_4 \to Q_5 \to Z_1$$

P_i and Q_i must anticommute, so there is a Clifford change of basis that maps them to X_i and Z_i.

If we let V apply this single-qubit Clifford on all qubits, the cycle in $V^\dagger U' V$ just takes single-qubit X to X on another qubit, and similarly for Z. That is, the cycle is a pure permutation. Do this for all cycles in U and we prove the lemma.

Finishing the Theorem

We have U' which satisfies the conditions of the lemma and implements a non-trivial power of the Bell gate.

> The lemma tells us that there is a code that is equivalent, up to local unitaries, to the original code, that has a pure permutation implementation of a non-trivial power of the Bell gate.

But non-trivial powers of the Bell gate have the same property, that they take some product of Zs into a product that is not all Zs.

> This, we know, is not possible.

Thus, no automorphism implementation of the Bell gate can exist.

Permutations and k-Fold Transversal

What if we allow a combination of permutations and k-fold transversal gates?

It is not clear what is the right definition of the allowed set of gates here.

- If we allow arbitrary products of permutations and k-fold transversal gates, you can do any physical operation in the Clifford group.
- A single k-fold transversal gate followed by a permutation might be acceptable.
- Or one could look at the group generated by k-fold transversal gates without permutations and by pure permutations.
- Or one could look at gates combining any k-fold transversal gate with any permutation that respects the decomposition into sets of size k.

Open Questions

- How do we generalize to combine k-fold transversal gates with permutations?
- Do our theorems generalize to the above case?
- What about non-Clifford k-fold transversal gates? (With or without permutations.)
- What about qudit codes?
- Are there other types of restrictions on the possible logical multi-qubit gates implemented by transversal or k-fold transversal gates?