Fault-tolerant non-Clifford gates

Fault-tolerant memory and Clifford gates (summary)

1) Fault-tolerant error correction is possible for any stabilizer code. It involves Clifford unitary gates (the Clifford group is generated by H, K, CNOT) , $|0\rangle$ ancillas and $\{|0\rangle, |1\rangle\}$ measurements.

   Errors in a CSS code can be corrected using a less powerful set of gates: X, Z, CNOT, $|0\rangle$ and $|+\rangle$ ancillas, and measurements in the $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ bases.

2) Logical Clifford operations can be implemented transversally (and hence, fault-tolerantly) on any self-dual CSS code of type *[[2l+1, 1]]*.

$p \to O(p^2)$

3) Logical errors can be further reduced by concatenating self-dual CSS codes.

   This works because all gates required for the error correction on a higher layer are implemented fault-tolerantly on the layer beneath it.

$p \to \left(\frac{p}{\varepsilon}\right)^{2^k}$

4) Fault-tolerant quantum memory can also be realized using surface codes.

   Since surface codes are not self-dual, the implementation of H and K is more complex.

How to achieve computational universality?

Good news: some *stabilizer* codes allow for transversal realization of *some* non-Clifford gates

Bad news: a *universal* set of gates cannot be implemented transversally on *any* code

Eastin-Knill theorem

> The logical unitary gates (considered up to an overall phase) that can be implemented $\underbrace{\text{transversally}}_{\tilde{U} = U_1 \otimes \cdots U_n}$ on a given code $\mathcal{M}$ s.t. $d(\mathcal{M}) > 1$ form a finite group $G \subseteq U(m)/\underbrace{U(1)}$

phase factors

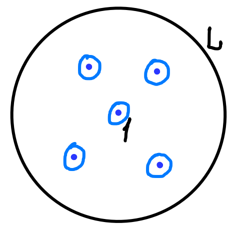
dimensionality of the code subspace

single-qubit gates

Preliminaries: Subgroups of a Lie group L

Discrete subgroups

Any discrete subgroup of a compact group is finite



$\widetilde{\mathcal{C}\ell}_1 \subseteq U(2)$ generated by H, K

$\mathcal{C}\ell_1 \subseteq \underbrace{U(2)/U(1)}_{\cong SO(3)}$ (the group of rotational symmetries of the cube)

Closed subgroups (more general)

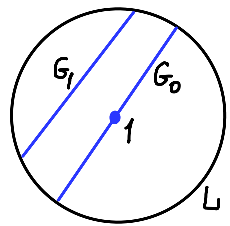
Any closed subgroup of a Lie group is a Lie subgroup

$(G_0 \subseteq L_0, \quad \mathcal{G} \subseteq \mathcal{L})$

connected components containing 1

Lie algebras

(if $G_0 = \{1\}$, then G is discrete)

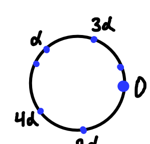


The subgroup $G \subseteq SO(3)$ preserving the *z* axis

$G_0 =$ rotations about the *z* axis (the connected component containing 1)

$G_1 =$ 180° rotations about perpendicular axes

Non-closed subgroups:



$G = \{ e^{in\alpha} : n \in \mathbb{Z} \} \subseteq U(1)$

$\frac{\alpha}{2\pi}$ is irrational

Proof of the Eastin-Knill theorem

Physical Hilbert space: $\mathcal{N} = (\mathbb{C}^d)^{\otimes n}$

Code: $\mathcal{M} \subseteq \mathcal{N}$

Lemma

The set of physical transversal gates, $\widetilde{U} = U_1 \otimes \cdots \otimes U_n$, forms a <u>closed</u> subgroup $\widetilde{G} \subseteq U(d) \times \cdots \times U(d)$

Proof

$\widetilde{U}$ preserves the code if and only if $\widetilde{U} P_{\mathcal{M}} \widetilde{U}^{-1} = P_{\mathcal{M}}$ ($P_{\mathcal{M}}$ is a projector onto $\mathcal{M}$)

It is clear that this set is a subgroup, i.e. it is closed under the multiplication and inversion:

$$(\widetilde{U}_1 \widetilde{U}_2) P_{\mathcal{M}} (\widetilde{U}_1 \widetilde{U}_2)^{-1} = \widetilde{U}_1 (\widetilde{U}_2 P_{\mathcal{M}} \widetilde{U}_2^{-1}) U_1^{-1} = P_{\mathcal{M}}$$

This set is also topologically closed: The condition $\widetilde{U} P_{\mathcal{M}} = P_{\mathcal{M}} \widetilde{U}$ is just a set of linear equations

Corollary: $\widetilde{G} \subseteq U(d) \times \cdots \times U(d)$ is a Lie subgroup.

$\widetilde{G}_0 \subseteq \widetilde{G}$ -- the connected component containing 1.

$\widetilde{G}_0$ is normal in $\widetilde{G}$, $\widetilde{G}/G_0$ is finite

Key argument: $\tilde{G}_0$ acts trivially (i.e. by overall phase factors) on the code

Proof

Let $\tilde{U} \in \tilde{G}_0$. $\quad \tilde{U} = e^{-iHt}$ for some H in the Lie algebra of $\tilde{G}_0$

$\Rightarrow$ H preserves the code

$$\tilde{U} = U_1 \otimes \cdots \otimes U_n \iff H = H_1 + \cdots + H_n$$

H_j acts on the *j*-th qudit

$$\boxed{H \in \mathcal{E}(n,1)}$$

The code treats H as a detectable error:

$$d(\mathcal{M}) > 1 \Rightarrow \forall\ |\xi\rangle, |\eta\rangle \in \mathcal{M} \quad \left.\begin{array}{l} \langle \xi | H | \eta \rangle = c \langle \xi | \eta \rangle \\ H|\eta\rangle \in \mathcal{M} \end{array}\right\} \Rightarrow H|\eta\rangle = c|\eta\rangle$$

Looking for a transversal realization of some non-Clifford gate

$$\boxed{T = K^{1/2} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}}$$

Let us try $T^{\otimes n}$ on a CSS code

$$\mathcal{M} = CSS(D_z, D_x) \qquad (D_z, D_x \subseteq \mathbb{F}_2^n, \quad D_z \perp D_x)$$

Basis vectors: $|0\rangle_L = \frac{1}{\sqrt{|D_x|}} \sum_{f \in D_x} |f\rangle$,

$|h\rangle_L = \sigma^x(\tilde{h})\,|0\rangle_L$, where $\tilde{h} \in D_z^{\perp}$ is a representative of the coset $h \in D_z^{\perp}/D_x$

$T^{\otimes n}|0\rangle_L = \frac{1}{\sqrt{|D_x|}} \sum_{f \in D_x} e^{i\frac{\pi}{4}|f|}\,|f\rangle \in \mathcal{M}$ if and only if $\boxed{\forall f \in D_x, \quad |f| \equiv 0 \pmod 8}$

We will see that the linear subspaces $D_x \subseteq \mathbb{F}_2^n$ satisfying the last condition are characterized as follows:

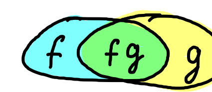
$D_x =$ linear span of $f_1, \ldots, f_q$ modulo 2

$|f_j| \equiv 0 \pmod 8$ for all j,

$|f_j f_k| \equiv 0 \pmod 4$ for all j,k,

$|f_j f_k f_l| \equiv 0 \pmod 2$ for all j,k,l.

$$|f+g| = |f| + |g| - 2|fg|$$



e.g. $f = (1\,1\,0)$, $g = (0\,1\,1)$,

$f + g = (1\,0\,1)$ (mod 2 sum of vectors)

$fg = (0\,1\,0)$ (bitwise product)

Lemma. Let $f_1,\dots,f_q$ be basis vectors of classical linear code $C \subseteq \mathbb{F}_2^n$. These conditions are equivalent:

$A_s(C)$: All vectors $g \in C$ have Hamming weight divisible by 2^s;

$B_s(f_1,\dots,f_q)$: $\begin{cases} |f_j| \equiv 0 \pmod{2^s} \text{ for all } j, \quad \text{and } |f_{j_1} f_{j_2}| \equiv 0 \pmod{2^{s-1}} \text{ for all } j_1, j_2, \\ \cdots \text{ and } |f_{j_1} \cdots f_{j_s}| \equiv 0 \pmod{2} \text{ for all } j_1,\dots,j_s. \end{cases}$

Proof of the implication $B_s(f_1,\dots,f_q) \Rightarrow A_s(C)$

<u>Induction base</u>: $B_1(f_1,\dots,f_q) \Rightarrow A_1(C)$ -- obvious

<u>Induction step</u>: Suppose $B_{s-1} \Rightarrow A_{s-1}$ is already proven, and let us assume $B_s(f_1,\dots,f_q)$. We now prove $A_s(C)$.

If $g \in C$, then $g = \underbrace{\underbrace{f_{k_1}}_{h_1} + f_{k_2}}_{h_2} + \cdots + f_{k_\ell} \Rightarrow |g| = |h_1| + (|h_2| - |h_1|) + \dots + (|h_\ell| - |h_{\ell-1}|)$

All terms have the form $|h_j + f_k| - |h_j|$, $k = k_{j+1}$
We need to show that they are multiples of 2^s

Let $h \in C$ and consider $|h + f_k| = |h| + |f_k| - 2|h f_k|$

$h f_k \in C f_k = \text{lin.span}\{\underbrace{f_1 f_k, \dots, f_q f_k}\}$

satisfy B_{s-1}, e.g. $|f_1 f_k \cdot f_2 f_k| = |f_1 f_2 f_k| \equiv 0 \pmod{2^{s-2}}$

$A_{s-1}(C f_k)$ (by induction hypothesis)

$\Rightarrow |h f_k| \equiv 0 \pmod{2^{s-1}}$

$\Rightarrow \boxed{|h + f_k| - |h| \equiv 0 \pmod{2^s}}$

Reed-Muller codes (recap)

$$[x_1] = (0\ 1\ 0\ 1\ 0\ 1\ 0\ 1)$$
$$[x_2] = (0\ 0\ 1\ 1\ 0\ 0\ 1\ 1)$$
$$[x_3] = (0\ 0\ 0\ 0\ 1\ 1\ 1\ 1)$$
$$\overline{x_3 x_2 x_1}:\ 000\ \ 001\ \ 010\ \ 011\ \ 100\ \ 101\ \ 110\ \ 111$$

$n = 2^m$ bits are indexed by binary numbers: $x = \overline{x_m \dots x_1}$

Elements of $\mathbb{F}_2^n$ are associated with functions of x

Monomials: $x^A = \prod_{s \in A} x_s$, e.g. $x^{\{1,3\}} = x_1 x_3$

Convenience notation: function $f \to$ vector $[f] \in \mathbb{F}_2^n$ (the value table)

e.g. $f(\overline{x_3 x_2 x_1}) = x_1$, $[f] = (0\,1\,0\,1\,0\,1\,0\,1)$

$$\boxed{RM(m,\ell) = \text{linear span}\,\{[x^A] : |A| \le \ell\}}$$

e.g. $RM(3,1) = \text{lin. span}\{[1], [x_1], [x_2], [x_3]\}$

Familiar properties

of logical qubits: $K = \sum_{p=0}^{\ell} \binom{m}{p}$; distance: $d = 2^{m-\ell}$

$$RM(m,\ell)^{\perp} = RM(m, m-\ell-1)$$

When do all codewords of a Read-Muller code have Hamming weight divisible by 2^s ?

Checking condition B_s:

$|[x^A]| = 2^{m-|A|} \equiv 0 \pmod{2^s}$ for all A of size $\leq \ell$ iff $m-\ell \geq s$

$|[x^A]\cdot[x^B]| = |[x^{A\cup B}]| = 2^{m-|A\cup B|} \equiv 0 \pmod{2^{s-1}}$ for all A, B iff $m-2\ell \geq s-1$

. . . .

$|[x^{A_1}]\cdots[x^{A_s}]| = |[x^{A_1\cup\cdots\cup A_s}]| = 2^{m-|A_1\cup\cdots\cup A_s|} \equiv 0 \pmod{2}$ for all $A_1,\ldots,A_s$ iff $\boxed{m-s\ell \geq 1}$

the strongest inequality if $l>0$

Conclusion: All codewords of $RM(m,\ell)$ with $\ell>0$ have Hamming weight divisible by 2^s iff $\boxed{m > s\ell}$

8 $\quad m > 3\ell$

For example, $RM(4,1)$ has codewords of weight divisible by 8

The 15-qubit code (Knill, Laflamme, Zurek, quant-ph/9610011)

$$\mathcal{M} = CSS(D_z, D_x), \qquad \text{type } [[15, 1, 3]]$$

$$\boxed{D_x = RM''(4,1) = \text{lin. span}\{[x_1],[x_2],[x_3],[x_4]\}}$$

(the weights of all codevectors are divisible by 8)

Modified Reed-Muller codes:

$RM'(m,\ell)$: remove the $x=0$ bit

$RM''(m,\ell)$: remove the $x=0$ bit and the $[1]$ basis vector

$$RM''(m,\ell)^{\perp} = RM'(m, m-\ell-1)$$

$$D_z = RM''(4,2) = \text{lin. span}\{[x_1],[x_2],[x_3],[x_4],[x_1x_2],[x_1x_3],[x_1x_4],[x_2x_3],[x_2x_4],[x_3x_4]\}$$

(the weights are even)

$$D_z^{\perp} = RM'(4,1) = \underbrace{D_x}_{\text{weights } 0,\ 8} \cup \underbrace{([1]+D_x)}_{\text{weights } 15,\ 7}$$

$$|0_L\rangle = \frac{1}{4}\sum_{f\in D_x}|f\rangle, \qquad |1_L\rangle = \frac{1}{4}\sum_{f\in D_x}|[1]+f\rangle$$

$$T^{\otimes 15}|0_L\rangle = |0_L\rangle, \qquad T^{\otimes 15}|1_L\rangle = e^{-i\frac{\pi}{4}}|1_L\rangle,$$

where $T = K^{1/2} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$

$\boxed{T^{\otimes 15} \text{ realizes the logical } T^{-1}}$

Some approaches to fault-tolerant universal quantum computation

1) Code switching, for example, between the 15-qubit code $\mathcal{M}$ and its dual $H^{\otimes 15}\mathcal{M}$

(The rest of this lecture)

2) Computational ancillas (a.k.a. "magic ancillas"), which can be checked and discarded if an error is detected

$$|H\rangle = \left(\cos\frac{\pi}{8}\right)|0\rangle + \left(\sin\frac{\pi}{8}\right)|1\rangle, \qquad |A\rangle = \frac{|0\rangle + e^{i\pi/4}|1\rangle}{\sqrt{2}}$$

(Next lecture)

3) Non-Abelian anyons

Code switching

$$\mathcal{M} = CSS(D_z, D_x), \quad D_z = RM''(4,2), \quad D_x = RM''(4,1)$$

$\mathcal{M}$ allows for the transversal implementation of CNOT, T, and $K = T^2$, but H is missing.

Trying to implement H

$H^{\otimes 15}$ acts correctly on $Z_L = Z^{\otimes 15}$, $X_L = X_L^{\otimes 15}$:

$$\boxed{\begin{aligned} H^{\otimes 15} Z_L H^{\otimes 15} &= X_L \\ H^{\otimes 15} X_L H^{\otimes 15} &= Z_L \end{aligned}}$$

But $H^{\otimes 15}\mathcal{M} = CSS(D_x, D_z) \neq \mathcal{M}$

Idea: extend both $\mathcal{M}$ and $H^{\otimes 15}\mathcal{M}$ to an $H^{\otimes 15}$-invariant code $\tilde{\mathcal{M}}$.

Let $\tilde{\mathcal{M}} = CSS\left(RM''(4,1), RM''(4,1)\right)$ (type *[[15, 7, 3]]*)

Although the encoded state includes some extra stuff, $\tilde{\mathcal{M}}$ still protects from one error

Subsystem encoding: $W : \underbrace{\mathcal{B}}_{\text{logical qubit}} \otimes \underbrace{\mathcal{B}^{\otimes 6}}_{\text{6 extra qubits. In the subcode } \mathcal{M}\text{, their state is fixed}} \longrightarrow \mathcal{B}^{\otimes 15}$, $\quad \mathrm{Image}(W) = \tilde{\mathcal{M}}$

$H^{\otimes 15}$ acts on the logical qubit and the extra qubits separately. We just need to return the extra qubits to their original state, e.g. by measuring the $\mathcal{M}$ stabilizers and correcting the detected "errors".

How are the extra qubits encoded?

The 6 extra qubits correspond to $\binom{4}{2}$ two-element subsets of $\{1,2,3,4\}$.

The extra logical operators are $\underbrace{Z_A = \sigma^z([x^A])}_{\boxed{\text{stabilizers of } \mathcal{M}}}$, $X_A = \sigma^x([x^{\bar{A}}])$ e.g $A=\{1,2\}$, $\bar{A}=\{3,4\}$

Checking the commutation relations

$$\underbrace{\sigma^z(f)}_{Z_A \text{ or } Z_L} \underbrace{\sigma^x(g)}_{X_A \text{ or } X_L} = (-1)^{(f,g)} \sigma^x(g)\,\sigma^z(f)$$

$$([x^A],[x^{\bar{B}}]) = \left\{ \begin{array}{ll} 1 & \text{if } A \cup \bar{B} = \{1,2,3,4\} \\ 0 & \text{otherwise} \end{array} \right\} = \delta_{AB}$$

$$([x^A],[1]) = 0$$

$$([1],[1]) = 1$$

Implementation of the logical H on $\mathcal{M} \subseteq \widetilde{\mathcal{M}}$

> Apply $H^{\otimes 15}$, measure (part of) the $\mathcal{M}$ syndrome using Z_A, and correct the "errors" using X_A.

Drawback of the code switching method

To achieve arbitrarily small error rate, we need to concatenate 15-qubit codes. That's too expensive...