Physics 430: Quantum Error Correction (Stanford University) Spring 2026

Note 4: Magic State Injection and Distillation

Instructor: Jeongwan Haah Scribe: Matthew Ding

In the previous notes, we learned about transversal implementations of logical Clifford gates in CSS codes. Clifford gates themselves can only generate circuits which can be efficiently simulated by classical computers due to the Gottesman-Knill theorem; however, Clifford+T gates generate universal quantum computation, so a transversal T gate implementation would suffice to make a universal error-corrected quantum computer. Unfortunately, we also learned in the previous notes of the Eastin-Knill theorem [EK09], which shows the impossibility of a universal transversal gate set within a single quantum code which can detect single-qubit errors.

Nevertheless, in this note we introduce magic state injection and distillation as protocols to circumvent the Eastin-Knill theorem with a fault-tolerant T gate implementation. These protocols combined with transversal Clifford gates and measurements are sufficient for fault-tolerant universal quantum computation.

4.1 Magic state injection

Recall, we define the single-qubit gate T gate as

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} = e^{i\pi/8} \exp\left(-\frac{i\pi}{8} Z\right). \tag{4.1}$$

Its action on computational basis states is $T|0\rangle = |0\rangle$ and $T|1\rangle = e^{i\pi/4}|1\rangle$.

To apply a T gate to an arbitrary state $|\psi\rangle$ using only Clifford gates and the "magic" state

$$|T\rangle \triangleq T|+\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + e^{i\pi/4}|1\rangle\big), \tag{4.2}$$

we use *magic state injection*. The framework was formalized by Bravyi and Kitaev [BK05], however similar protocols have been proposed in the literature beforehand [Sho96; GC99].

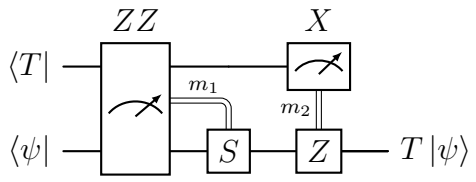

Figure 4.1: Magic state injection circuit

Magic state injection protocol:

(1) Input two qubits to the circuit, a data qubit in state $|\psi\rangle$ and an ancilla qubit in state $|T\rangle$

(2) Measure ZZ on the two qubits, obtaining outcome $m_1 \in \{+1, -1\}$.

(3) Measure X on the ancilla qubit, obtaining outcome $m_2 \in \{+1, -1\}$.

(4) Apply gate $S \in \mathcal{C}_2$ to the data qubit if $m_1 = -1$.

(5) Apply gate $Z \in \mathcal{C}_1$ to the data qubit if $m_2 = -1$.

(6) Output the state on the data qubit.

The complete action of this circuit is to apply the T gate to $|\psi\rangle$, i.e. producing state $T|\psi\rangle$. In this circuit, there are four possible measurement outcomes (m_1, m_2), each occurring with probability 1/4. For each outcome, the post-measurement state on the data qubit differs by a different Clifford gate ($\mathcal{C}_2$) correction. It is crucial that the correction step uses a gate which is in a lower level of the Clifford hierarchy than the T gate ($\mathcal{C}_3$).

Remark 4.1.1. *The ZZ measurement on $|T\rangle|\psi\rangle$ has outcomes ± 1. To see that each occurs with probability $1/2$, note that $TXT^\dagger = (X+Y)/\sqrt{2}$, which anticommutes with Z. More precisely, $TXT^\dagger$ anticommutes with ZZ on the two-qubit system:*

$$(TXT^\dagger \otimes \mathbb{I})\, ZZ = -ZZ\, (TXT^\dagger \otimes \mathbb{I}). \tag{4.3}$$

Since $|T\rangle = T|+\rangle$ is a $+1$ eigenstate of $TXT^\dagger$, the expectation value of ZZ in the state $|T\rangle|\psi\rangle$ is zero for any $|\psi\rangle$, so both outcomes ± 1 occur with probability $1/2$. Similarly, the subsequent X measurement has equal probability outcomes. Because of this, the quantum information in the system is not lost during the measurement and can be recovered using the measurement outcomes.

This method allows us to apply T gates on physical qubits, however it is insufficient by itself since none of the operations are fault-tolerant. The next step is to implement this protocol on a logical code space; this requires us to determine a method to construct high-fidelity T-states in the logical space of a quantum code with transversal Clifford gates.

4.2 Transversal T gates from level-3 orthogonal subspaces

We start by finding quantum codes that do admit transversal T gate implementations. This may seem counter-intuitive, as the Eastin-Knill theorem tells us that this code cannot have complete transversal Clifford operations. However, we shall see later how we can combine *two separate quantum codes* with a transversal Clifford and T gate implementation respectively in order to bypass the Eastin-Knill theorem.

A (classical) linear code $C \subseteq \mathbb{F}_2^n$ is called *even* if every codeword has even Hamming weight. Moreover, C is *doubly-even* if every weight is divisible by 4, and *triply-even* if every weight is divisible by 8. We generalize this notion by allowing a "sign vector" t.

Definition 4.2.1 (Level-ν orthogonal subspace)**.** *Let $t = (t_1, \ldots, t_n) \in (2\mathbb{Z}+1)^n$. A subspace $\mathcal{T} \subseteq \mathbb{F}_2^n$ is level-ν orthogonal with respect to t if*

$$\sum_{i=1}^{n} t_i \, v_i \;\equiv\; 0 \pmod{2^\nu} \quad \textit{for all } v \in \mathcal{T}. \tag{4.4}$$

Note that v is promoted to a vector in $\mathbb{Z}^n$ in this condition, even though $\mathcal{T}$ remains a subspace of $\mathbb{F}_2^n$.

The entries $t_i \in (2\mathbb{Z}+1)$ are all odd; they record a choice of phase for each physical qubit. When $t = (1, 1, \ldots, 1)$ and $\nu = 3$, the condition reduces to $\mathrm{wt}(v) \equiv 0 \pmod 8$, so $\mathcal{T}$ is triply-even in the classical sense.

Remark 4.2.2. *The definition of level-3 orthogonal is similar to triorthogonal subspaces, which are also used to construct quantum codes [BH12]. We note that all level-3 orthogonal subspaces are triorthogonal subspaces, but there exist triorthogonal subspaces that are not level-3 orthogonal with respect to any coefficient vector t [NH22, Section V].*

To verify that a given subspace $\mathcal{T}$ is level-3 orthogonal, we need to check $\sum_i t_i v_i \equiv 0 \pmod 8$ for all $v \in T$. We can apply the Parity-integer lemma from the previous notes:

Lemma 4.2.3 (Parity-integer lemma (mod 8 version))**.** *For $x_1, x_2, \ldots, x_m \in \{0, 1\} \subset \mathbb{Z}$,*

$$\frac{1 - (-1)^{\sum_i x_i}}{2} \equiv \sum_i x_i - 2\sum_{i<j} x_i x_j + 4 \sum_{i<j<k} x_i x_j x_k \pmod 8 \tag{4.5}$$

As a corollary, we can show the following condition for level-3 orthogonal subspaces:

Corollary 4.2.4. *A subspace $T \subseteq F_2^n$ is level-3 orthogonal with respect to t if and only if there exists a basis $v^{(1)}, v^{(2)}, \ldots, v^{(s)} \in \mathbb{F}_2^n$ of $\mathcal{T}$ such that the following conditions hold:*

1. *For all $a \in [s]$, $\sum_i t_i v_i^{(a)} \equiv 0 \pmod 8$.*
2. *For all $a, b \in [s]$, $\sum_i t_i v_i^{(a)} v_i^{(b)} \equiv 0 \pmod 4$.*
3. *For all $a, b, c \in [s]$, $\sum_i t_i v_i^{(a)} v_i^{(b)} v_i^{(c)} \equiv 0 \pmod 2$.*

Thus, level-3 orthogonality is checkable by row-reducing the generator matrix of T and testing the 1-, 2-, and 3-row parity conditions for all basis vectors.

4.2.1 CSS code and transversal T gate construction

We will show how this CSS code constructed using a level-3 orthogonal subspace gives a transversal T gate implementation which is analogous to the transversal Clifford gate constructions introduced in Note 3. More generally, it was shown by Haah that a level-ν

orthogonal code allows for a transversal implementation of a gate in level-ν of the Clifford hierarchy [Haa18].

Our high-level construction is, given a level-3 orthogonal subspace $\mathcal{T} \subseteq \mathbb{F}_2^{n+k}$, we can use its generator matrix to identify a set of k "pivot" columns (a set of k distinguished coordinates) and n "non-pivot" columns. Our code will be constructed by *puncturing* the code at the k pivots, i.e., deleting the k pivot columns from the generator matrix. The key insight is to interpret any stabilizer state on the code space of $\mathcal{T}$ as a Bell pair between (i) the system k qubits associated with the pivot columns, and (ii) logical code states of the new punctured code. This interpretation allows us to construct transversal logical gates on the punctured code.

For simplicity, assume $k = 1$ and that we choose our distinguished pivot coordinate to be the leftmost column of the generator matrix (assumed to be nonzero). More formally, we let $\mathcal{D}_X \subseteq \mathbb{F}_2^{n+1}$ be a level-3 orthogonal subspace with respect to t. We construct a CSS code with n physical qubits and 1 logical qubit as follows. We set $\mathcal{D}_Z \triangleq \mathcal{D}_X^\perp \subseteq \mathbb{F}_2^{n+1}$. The stabilizers will be the vectors in $\mathcal{D}_X$ and $\mathcal{D}_Z$ containing 0 as their first coordinate, excluding the first 0 (also known as the *shortened code* at coordinate 1):

$$\mathcal{S}_X \triangleq \{v \in \mathbb{F}_2^n : (0|v) \in \mathcal{D}_\mathcal{X}\} \qquad \mathcal{S}_Z \triangleq \{v \in \mathbb{F}_2^n : (0|v) \in \mathcal{D}_\mathcal{Z}\}$$

The logical operators (including the stabilizers) will be all codewords excluding the first coordinate (also known as the *punctured code* at coordinate 1):

$$\mathcal{S}_Z^\perp = \{v \in \mathbb{F}_2^n : (a|v) \in \mathcal{D}_X, a \in \{0,1\}\} \qquad \mathcal{S}_X^\perp = \{v \in \mathbb{F}_2^n : (a|v) \in \mathcal{D}_Z, a \in \{0,1\}\}$$

The non-trivial X and Z logical operators are given by the coset representatives of $\mathcal{L}_X \triangleq \mathcal{S}_Z^\perp/\mathcal{S}_X$ and $\mathcal{L}_Z \triangleq \mathcal{S}_X^\perp/\mathcal{S}_Z$ respectively. This yields a CSS code with n physical qubits and 1 logical qubit (see Figure 4.2 for diagram). Any CSS code stabilizer state on n qubits can be written, in a suitable computational basis, as a uniform superposition over a coset of a subspace. In particular, the code states of the CSS code constructed from the punctured code are of the form

$$|\bar{x}\rangle = \frac{1}{\sqrt{|\mathcal{S}_X|}} \sum_{s \in \mathcal{S}_X} |s + \ell_x\rangle\,, \qquad \ell_x \in \mathcal{S}_Z^\perp, \tag{4.6}$$

where ℓ_x is a logical X-coset representative of $x \in \mathcal{L}_X = \mathcal{S}_Z^\perp/\mathcal{S}_X$.

We can also consider the stabilizer states of the original, unpunctured code:

Proposition 4.2.5. *Let $\mathcal{D}_X \subseteq \mathbb{F}_2^{n+1}$ be a level-3 orthogonal subspace with respect to t. The uniform superposition state*

$$|\mathcal{D}_X\rangle = \frac{1}{\sqrt{|\mathcal{D}_X|}} \sum_{v \in \mathcal{D}_X} |v\rangle \tag{4.7}$$

satisfies

$$\bigotimes_{i=1}^{n+1} T_i^{t_i} |\mathcal{D}_X\rangle = |\mathcal{D}_X\rangle\,. \tag{4.8}$$

(we use the notation $T^{-1} \triangleq T^\dagger$, $T^{-3} \triangleq (T^\dagger)^3$.)

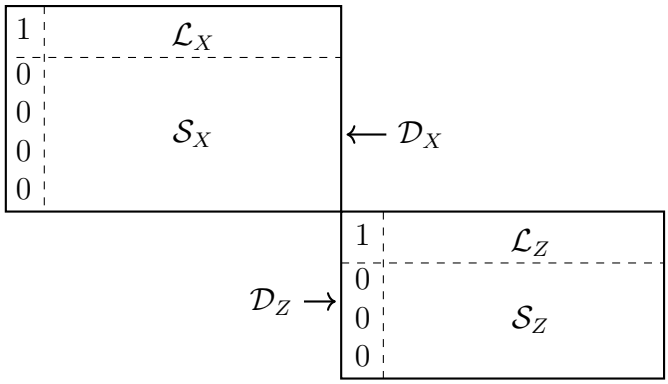

Figure 4.2: Stabilizer matrix for a level-3 orthogonal CSS code.

Proof. Apply $\bigotimes_{i=1}^{n+1} T_i^{t_i}$ term-by-term in the computational basis:

$$\bigotimes_{i=1}^{n+1} T_i^{t_i} |v\rangle = \bigotimes_{i=1}^{n+1} T^{t_i} |v_i\rangle = \prod_{i=1}^{n+1} e^{i(\pi/4)t_i v_i} |v\rangle = e^{i(\pi/4)\sum_i t_i v_i} |v\rangle . \tag{4.9}$$

Since $\mathcal{D}_X$ is level-3 orthogonal, $\sum_i t_i v_i \equiv 0 \pmod 8$ for every $v \in \mathcal{D}_X$, so $e^{i(\pi/4)\sum_i t_i v_i} = 1$. Therefore each term is unchanged, and $\bigotimes T_i^{t_i} |\mathcal{D}_X\rangle = |\mathcal{D}_X\rangle$. □

The state $|\mathcal{D}_X\rangle$ is the $+1$ eigenstate of all X-stabilizers in the original, unpunctured code, so the proposition says $\bigotimes T_i^{t_i}$ acts as the identity on this particular stabilizer state. Partitioning this stabilizer state between its "pivot" in the leftmost column and the remaining columns,

$$\frac{1}{\sqrt{|\mathcal{D}_X|}} \sum_{v \in \mathcal{D}_X} |v\rangle = \frac{1}{\sqrt{2|\mathcal{S}_X|}} \sum_{s \in \mathcal{S}_X} \left(|0\rangle |s\rangle + |1\rangle |s + \ell_1\rangle \right) = \frac{1}{\sqrt{2}} \left(|0\rangle |\bar{0}\rangle + |1\rangle |\bar{1}\rangle \right), \tag{4.10}$$

where we have defined the logical code states

$$|\bar{0}\rangle \triangleq \frac{1}{\sqrt{|\mathcal{S}_X|}} \sum_{s \in \mathcal{S}_X} |s\rangle , \qquad |\bar{1}\rangle \triangleq \frac{1}{\sqrt{|\mathcal{S}_X|}} \sum_{s \in \mathcal{S}_X} |s + \ell_1\rangle . \tag{4.11}$$

Note that $|\bar{0}\rangle$ and $|\bar{1}\rangle$ are not the logical states of the $n+1$ qubit code space defined by the level-3 orthogonal subspace; instead, they are the logical code states of the *punctured code* at coordinate 1 over n qubits.

This now gives the interpretation of $|\mathcal{D}_X\rangle$ as a Bell pair between the punctured logical code states and the pivot qubit, which will allow us to analyze the logical action of the transversal T gate on the punctured CSS code. First, we begin by describing the action of unitary operations on Bell pairs.

Proposition 4.2.6. *For any unitary $U \in U(d)$,*

$$(U \otimes U^*) \sum_{i=1}^{d} |i\rangle_A |i\rangle_B = \sum_{i=1}^{d} |i\rangle_A |i\rangle_B . \tag{4.12}$$

Proof.

$$(U \otimes U^*) \sum_{i=1}^{d} |i\rangle_A |i\rangle_B = \sum_{i}^{d} (U|i\rangle)_A \otimes (U^*|i\rangle)_B = \sum_{i}^{d} \left(\sum_{j}^{d} U_{ji} |j\rangle_A \right) \otimes \left(\sum_{k}^{d} U^*_{ki} |k\rangle_B \right)$$

Since U is unitary, a direct computation gives $\sum_i U_{ji} U^*_{ki} = (UU^\dagger)_{jk} = \delta_{jk}$, so only the $|i\rangle \otimes |i\rangle$ terms remain and have amplitude 1 in the final sum. □

This means that the maximally entangled state $\sum_i |i\rangle |i\rangle$ is invariant under the operator $U \otimes U^*$. Finally, we track the logical action of $\bigotimes T_i^{t_i}$ on the code space. The global unitary $\bigotimes_{i=1}^{n+1} T_i^{t_i}$ on $|\mathcal{D}_X\rangle$ can be decomposed as:

$$\bigotimes_{i=1}^{n+1} T_i^{t_i} |\mathcal{D}_X\rangle = \frac{1}{\sqrt{2}} \left(T_1^{t_1} \otimes \bigotimes_{i=2}^{n+1} T_i^{t_i} \right) (|0\rangle \otimes |\bar{0}\rangle + |1\rangle \otimes |\bar{1}\rangle) = \frac{1}{\sqrt{2}} (|0\rangle |\bar{0}\rangle + |1\rangle |\bar{1}\rangle), \quad (4.13)$$

where the final equality is from Proposition 4.2.5. Projecting onto $\langle 0|$ and $\langle 1|$ in the first qubit shows that $\bigotimes_{i=2}^{n+1} T_i^{t_i}$ gives a phase of 1 on $|\bar{0}\rangle$ and a phase of $e^{-i\pi t_1/4}$ on $|\bar{1}\rangle$. From Proposition 4.2.6, acting by T^{t_1} on the pivot qubit and $\bar{T}^{-t_1}$ on its "dual" partner consisting of the punctured code qubits leaves the maximally entangled state invariant in the logical code space. Thus the net logical effect of $\bigotimes_{i=2}^{n+1} T_i^{t_i}$ on the code space is $\bar{T}^{-t_1}$.

Remark 4.2.7. *When $t = (+1, \ldots, +1)$, the induced logical action is $\bar{T}^\dagger$. However, we can swap the sign convention for logical $\bar{Z}$ to make the induced logical action $\bar{T}$ instead, implementing the T gate on the logical qubit transversally.*

4.2.2 Example: Quantum Reed-Muller codes

The quantum Reed-Muller code [Ste96] is a level-3 orthogonal CSS code family based on the classical Reed-Muller code.

Classical Reed-Muller codes. Take m binary variables $x_1, \ldots, x_m$ and consider polynomial functions $f(x_1, \ldots, x_m)$, e.g. $f = x_1x_3 + x_5$. Formally these are elements of quotient ring $\mathbb{F}_2[x_1, \ldots, x_m]/(x_1^2 - x_1, \ldots, x_m^2 - x_m)$. For a monomial, the number of variables appearing in it is called its *degree*: $\deg(x_1) = 1$, $\deg(x_1x_3) = 2$, $\deg(x_1x_2x_3) = 3$.

Identify $\mathbb{F}_2^m$ with $\{0, 1, \ldots, 2^m - 1\}$ via binary representation, and represent f by its evaluation vector $(f(v))_{v \in \mathbb{F}_2^m} \in \mathbb{F}_2^{2^m}$. For example, if $f = 1$ then $f = (1, 1, \ldots, 1)$, and if $f = x_1x_2x_3$ (with $m = 3$) then $f = (0, 0, 0, 0, 0, 0, 0, 1)$ (the only input where $x_1 = x_2 = x_3 = 1$ is $(1, 1, 1)$).

Definition 4.2.8 ((Classical) Reed-Muller code)**.** *$\mathcal{R}(r, m)$ is the classical binary linear code consisting of the set of all evaluation vectors of multivariate polynomials of degree $\leq r$ in m binary variables.*

$\mathcal{R}(r, m)$ is a linear subspace of $\mathbb{F}_2^{2^m}$. It is a $[2^m, k, 2^{m-r}]$ code, where its dimension $k = \sum_{j=0}^{r} \binom{m}{j}$ counts the independent monomials of degree $\leq r$.

Example 4.2.9. *$\mathcal{R}(1,4)$ has length $n = 2^4 = 16$ and dimension $k = 5$. Its generator matrix is given by the 5×16 matrix whose rows evaluate the five polynomials $1, x_1, x_2, x_3, x_4$ at all points of $\mathbb{F}_2^4$ (columns ordered so the jth column is the binary representation of j):*

$$\mathcal{R}(1,4) = \text{row span} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Using the Parity-integer lemma for the basis rows in Example 4.2.9:

- *Each row x_i has weight $\mathrm{wt}(x_i) = 8 \equiv 0 \pmod 8$ (and the constant row has weight $16 \equiv 0 \pmod 8$).*
- *The dot product of any two distinct non-constant rows x_i, x_j equals $\mathrm{wt}(x_i x_j) = 4 \equiv 0 \pmod 4$ (repeated rows or the constant row reduce to the first case).*
- *The triple overlap of any three distinct non-constant rows x_i, x_j, x_k equals $\mathrm{wt}(x_i x_j x_k) = 2 \equiv 0 \pmod 2$ (repeated rows or the constant row reduce to the first two cases).*

By the Parity-integer lemma, $\mathrm{wt}(v) \equiv 0 \pmod 8$ for every $v \in \mathcal{R}(1,4)$. Thus $\mathcal{R}(1,4)$ is triply even, or equivalently, a level-3 orthogonal space with $t = (+1, \ldots, +1)$.

The $[[15,1,3]]$ quantum Reed-Muller code. To construct a $k = 1$ quantum code, we use the puncturing method defined in the previous subsection on a classical Reed-Muller code. The dual of a punctured Reed-Muller code is the shortened code at coordinate 1 of the dual Reed-Muller code. Since $\mathcal{R}(1,4)^\perp = \mathcal{R}(2,4)$, we can construct a CSS code from the pair of the punctured $\mathcal{R}(1,4)$ code and shortened $\mathcal{R}(2,4)$ code at coordinate 1. This construction gives the $[[15,1,3]]$ quantum Reed-Muller code. Since $\mathcal{R}(1,4)$ is triply-even (Example 4.2.9), the X-stabilizer space is level-3 orthogonal with $t = (+1, \ldots, +1)$. By the construction of Section 4.2.1, the transversal gate $T^{\otimes n}$ implements a logical $\bar{T}$ gate on the encoded qubit under our logical sign convention.

4.3 Magic state distillation

Using magic state injection, we can apply fault-tolerant single qubit T gates in the logical code space given the ability to create high-fidelity logical T-states. But how do we create high-fidelity logical T-states?

The solution was proposed independently by Knill and Bravyi–Kitaev [Kni04; BK05] and is called *magic state distillation*. The goal of distillation is to convert many noisy copies of a resource state (in this case, $|T\rangle = T|+\rangle$) into a smaller number of high-fidelity copies using only Clifford operations and measurements. We show how this can be done by combining a

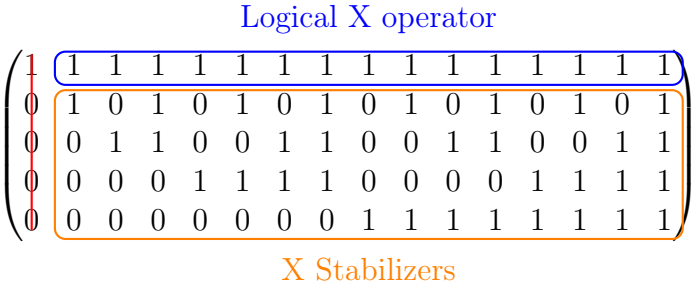

Figure 4.3: Construction of the $[[15, 1, 3]]$ quantum Reed-Muller code X stabilizers and logical operators from the punctured $\mathcal{R}(1, 4)$ Reed-Muller code. Stabilizer states of the full matrix are interpreted as Bell pairs between a qubit represented by the pivot column in the leftmost position and the remaining 15 columns denoting the physical qubits of the punctured code.

"distillation" quantum code admitting a transversal T gate implementation with a "ground" quantum code with transversal Clifford operations.

We will go over two related protocols for magic state distillation utilizing the quantum Reed-Muller code as a distillation code.

4.3.1 Protocol 1: Standard 15-to-1 distillation

The first distillation protocol uses the $[[15, 1, 3]]$ quantum Reed-Muller code as the distillation code. Assume we have a ground code which allows for perfect Clifford operations, which can be done by sufficiently reducing the logical error rate of the ground code. We will treat the ground code logical qubits as "physical qubits" and apply our distillation code on top of the ground code: this process is called *code concatenation*. Thus in this section we will assume all operations are done in the logical code space of the ground code unless stated otherwise.

Protocol (15-to-1 distillation):

(1) Prepare 15 noisy copies of $|T\rangle$.

(2) Initialize 1 logical qubit (in the $|+\rangle$ state), 4 X-stabilizer ancillas (in the $|+\rangle$ state), and 10 Z-stabilizer ancillas (in the $|0\rangle$ state).

(3) Prepare the logical $|\bar{+}\rangle$ state in the $[[15, 1, 3]]$ distillation code using CNOT operations.

(4) Apply $T^{\otimes 15}$ (one T gate per physical qubit) using the magic state injection protocol and the noisy $|T\rangle$ copies.

(5) Measure stabilizer generators of the distillation code. **Accept** if all measurement outcomes are $+1$; otherwise **reject**.

(6) If accepted, apply the distillation code decoding using CNOT operations to extract the logical output qubit which is in state $|\bar{T}\rangle$ in the ground code.

The correctness of step (4) follows from the level-3 orthogonal subspace: since $T^{\otimes 15}$ implements the logical $\bar{T}$ gate on $[[15, 1, 3]]$ under our logical sign convention, applying $T^{\otimes 15}$ to $|\bar{+}\rangle$ produces $\bar{T}\,|\bar{+}\rangle = \left|\bar{T}\right\rangle$ in the ground code.

Error suppression. Suppose each physical T gate is faulty: with probability p the gate produces ZT (the ideal gate followed by a phase-flip error). The single-qubit error model (justified in Homework 3, Problem 3) is

$$\rho_{\text{noisy}} = (1-p)\,T\,|+\rangle\langle+|\,T^\dagger + p\,T\,|-\rangle\langle-|\,T^\dagger. \tag{4.14}$$

Since the $[[15, 1, 3]]$ code has distance $d = 3$, it can detect any 1- or 2-qubit error. Any error pattern of weight ≤ 2 will be detected by (some of) the stabilizer measurements and cause rejection. Errors of weight ≥ 3 can fool the code, but they occur only at order p^3. Therefore the output fidelity satisfies $F = 1 - O(p^3)$, giving a cubic improvement in the error rate when p is small.

4.3.2 Protocol 2: Space-efficient version

The second protocol utilizes the same $[[15, 1, 3]]$ quantum Reed-Muller code but modifies the preparation scheme to save the number of qubits used at the cost of more sequential operations.

In the original protocol, because the encoding circuit is composed of only CNOT gates, it is a Clifford unitary that preserves the X and Z bases. Its action on the Pauli group is block-diagonal and can be represented by a symplectic matrix over $\mathbb{F}_2$: $U = \begin{pmatrix} E & 0 \\ 0 & D \end{pmatrix}$, where $E = D^{-\top}$. The transversal T gate operation combined with the encoding/decoding procedure can be written in exponential form up to a global phase:

$$U^{-1}T^{\otimes 15}U = \prod_{i=1}^{15} \exp\left(-i\frac{\pi}{8}U^{-1}Z_iU\right) \tag{4.15}$$

The columns of E contain the X-stabilizers, and the matrix dictates how the X operators map into the code space as $UX(a)U^\dagger = X(Ea)$. Correspondingly, U^{-1} maps the Z_i operators back to the unencoded space as $U^{-1}Z(b)U = Z(E^\top b)$. Since $D = E^{-\top}$, the Z_i operator pulls back to the multi-qubit Pauli Z operator $Z(v_i') = U^{-1}Z_iU$ where $v_i' = E^\top e_i$ is the ith row of E. Substituting this back yields:

$$U^{-1}T^{\otimes 15}U = \prod_{i=1}^{15} \exp\left(-i\frac{\pi}{8}Z(v_i')\right). \tag{4.16}$$

When the operator $\prod_{i=1}^{15}\exp\left(-i\frac{\pi}{8}Z(v_i')\right)$ acts on the 10 ancillas initialized to $|0\rangle$, it leaves them invariant since $|0\rangle$ is a $+1$-eigenstate of Z. Therefore, we can completely trace out or

"truncate" the last 10 bits of the vector v_i', dropping all terms acting on the $|0\rangle$ subspace. This leaves $v_i \in \mathbb{F}_2^5$, which consists only of the first 5 bits of the ith row of E. Because $T^{\otimes 15}$ acts as a valid logical $\bar{T}$ on the encoded space, pulling the operation back to the unencoded space and resolving the trivial $|0\rangle$ components must result in a standard physical T gate on the single data qubit, while leaving the 4 X-stabilizer ancillas unchanged.

Thus, applying the truncated sequence of Z-rotations to the 5 qubits initialized in the $|+\rangle$ state is mathematically identical (up to a global phase) to applying a single T gate ($\exp(-i\frac{\pi}{8}Z_1)$) to the first qubit:

$$\prod_{i=1}^{15} \exp\left(-i\frac{\pi}{8}Z(v_i)\right)|+\rangle^{\otimes 5} = \exp\left(-i\frac{\pi}{8}Z_1\right)|+\rangle^{\otimes 5} \tag{4.17}$$

This identity demonstrates that we can bypass the full 15-qubit encoding and instead prepare only 5 qubits in the $|+\rangle$ state, sequentially applying 15 correlated Z-rotations to achieve the exact same distillation logic.

References

[BH12] Sergey Bravyi and Jeongwan Haah. "Magic-state distillation with low overhead". In: *Physical Review A* 86.5 (Nov. 2012), p. 052329. DOI: 10.1103/PhysRevA.86.052329.

[BK05] Sergey Bravyi and Alexei Kitaev. "Universal quantum computation with ideal Clifford gates and noisy ancillas". In: *Physical Review A* 71.2 (Feb. 2005). ISSN: 1094-1622. DOI: 10.1103/physreva.71.022316.

[EK09] Bryan Eastin and Emanuel Knill. "Restrictions on Transversal Encoded Quantum Gate Sets". In: *Physical Review Letters* 102.11 (Mar. 2009). ISSN: 1079-7114. DOI: 10.1103/physrevlett.102.110502.

[GC99] Daniel Gottesman and Isaac L Chuang. "Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations". In: *Nature* 402.6760 (1999), pp. 390–393.

[Haa18] Jeongwan Haah. "Towers of generalized divisible quantum codes". In: *Physical Review A* 97.4 (Apr. 2018). ISSN: 2469-9934. DOI: 10.1103/physreva.97.042327.

[Kni04] E. Knill. *Fault-Tolerant Postselected Quantum Computation: Schemes*. 2004. arXiv: quant-ph/0402171 [quant-ph].

[NH22] Sepehr Nezami and Jeongwan Haah. "Classification of small triorthogonal codes". In: *Physical Review A* 106.1 (July 2022). ISSN: 2469-9934. DOI: 10.1103/physreva.106.012437.

[Sho96] Peter W Shor. "Fault-tolerant quantum computation". In: *Proceedings of 37th Conference on Foundations of Computer Science*. IEEE. 1996, pp. 56–65.

[Ste96] Andrew Steane. *Quantum Reed-Muller Codes*. 1996. arXiv: quant-ph/9608026 [quant-ph].