Quantum Error Correction - Notes

Ben Karsberg

2021-22

1 Week 3: Harlow Thm. 1, More Toy Model

1.1 Schmidt Decomposition and Purification

- Before going through the theorem, let's remind ourselves of the *Schmidt decomposition* and *state purification*
- These concepts are important in Harlow's proof

  Theorem 1.1 (Schmidt Decomposition). *Suppose $|\psi\rangle$ is a pure state of a composite system AB. Then, there exist orthonormal states $|i_A\rangle$ of A and $|i_B\rangle$ of B such that*

$$|\psi\rangle = \sum_i \lambda_i |i_A\rangle |i_B\rangle \tag{1.1}$$

  where the λ_i are non-negative real numbers satisfying $\sum_i \lambda_i^2 = 1$, called Schmidt coefficients.

- The proof of this is just linear algebra, invoking the *singular value decomposition*
- Why is this useful?
- Consider pure state $|\psi\rangle$ of AB as in (1.1)
- By the Schmidt decomposition, $\rho_A = \sum_i \lambda_i^2 |i_A\rangle \langle i_A|$ and $\rho_B = \sum_i \lambda_i^2 |i_B\rangle \langle i_B|$, so the eigenvalues of ρ_A and of ρ_B are identical, and both λ_i^2
- This is immediate from the decomposition, and eigenvalues are important
- The bases $|i_A\rangle$ and $|i_B\rangle$ are called *Schmidt bases* for A and B
- The number of $\lambda_i \neq 0$ is called the *Schmidt number* for $|\psi\rangle$, which in some sense quantifies the entanglement between A and B
- Note that the Schmidt number is preserved under unitaries on A or B alone
- A state $|\psi\rangle$ of AB is a product state iff it has Schmidt number 1; this allows us to easily prove that $|\psi\rangle$ is a product state iff ρ_A and ρ_B are pure
- We now come to purification

  Theorem 1.2 (Purification). *Suppose ρ_A is a state of system A. Introduce a new system R, and define a pure state $|AR\rangle$ for the joint system such that $\rho_A = Tr_R(|AR\rangle \langle AR|)$. This is called a purification, and we say $|AR\rangle$ purifies ρ_A.*

- This allows us to associate pure states with mixed states

- System R is called a *reference system*, and it has no direct physical significance
- Purification can be done to any state, and we prove this

  Proof. Suppose ρ_A has an orthonormal decomposition

  $$\rho_A = \sum_i p_i |i_A\rangle \langle i_A| \tag{1.2}$$

  Introduce a system R with the same state space as A, and orthonormal basis $|i_R\rangle$. Define a pure state for the combined system as

  $$|AR\rangle \equiv \sum_i \sqrt{p_i} |i_A\rangle |i_R\rangle \tag{1.3}$$

  We now calculate the reduced density operator for A corresponding to $|AR\rangle$:

  $$\begin{aligned} \mathrm{Tr}_R\left(|AR\rangle \langle AR|\right) &= \sum_{ij} \sqrt{p_i p_j} |i_A\rangle \langle j_A| \, \mathrm{Tr}\left(|i_R\rangle \langle j_R|\right) \\ &= \sum_{ij} \sqrt{p_i p_j} |i_A\rangle \langle j_A| \, \delta_{ij} \\ &= \sum_i p_i |i_A\rangle \langle i_A| \\ &= \rho_A \end{aligned} \tag{1.4}$$

  and so $|AR\rangle$ is a purification of ρ_A. □

- We can also think of purification in 'the other direction' - that is, if you have a mixed state ρ_A of system A, you can think of it as being a subsystem of some larger pure state ρ_{AB} of composite system AB, where the 'mixedness' of A comes from A being entangled with B and measurement of B being non-deterministic
- Note the link between Schmidt decompositions and purification: the process purifying a mixed state of A is to define a pure state who's Schmidt basis for A is just the basis in which the mixed state is diagonal, with the Schmidt coefficients being the square roots of the eigenvalues of the density operator to be purified

1.2 Theorem 1

- Let's start by stating Harlow's first theorem in the notation we've been using so far

  Theorem 1.3 (Harlow 1)**.** *Suppose $\mathcal{H}$ is a finite-dimensional Hilbert space, factorising as a tensor product $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_{\overline{A}}$. Suppose $\mathcal{H}_{code} \subseteq \mathcal{H}$ is a subspace. Then, the following 4 statements are equivalent:*

  1. *For any operator O_L with support on $\mathcal{H}_{code}$, there exists an operator O_A with support on $\mathcal{H}_A$ such that for all $|\psi_L\rangle \in \mathcal{H}_{code}$, we have*

     $$\begin{aligned} O_A |\psi_L\rangle &= O_L |\psi_L\rangle \\ O_A^\dagger |\psi_L\rangle &= O_L^\dagger |\psi_L\rangle \end{aligned} \tag{1.5}$$

  2. *For any operator $X_{\overline{A}}$ with support on $\mathcal{H}_{\overline{A}}$, we have*

     $$P_{code} X_{\overline{A}} P_{code} \propto P_{code} \tag{1.6}$$

     where P_{code} is the projector onto $\mathcal{H}_{code}$, and the constant of proportionality is a complex number.

3. *Introduce an auxiliary/reference system R with dimensionality $|R| = |\mathcal{H}_{code}|$. Choose orthonormal bases $\{|i_L\rangle_{A\overline{A}}\}$ and $\{|i_L\rangle_R\}$ of $\mathcal{H}_{code}$ and R respectively. Then, the state*

$$|\phi\rangle \equiv \frac{1}{\sqrt{|R|}} \sum_{i_L} |i_L\rangle_R \, |i_L\rangle_{A\overline{A}} \tag{1.7}$$

satisfies

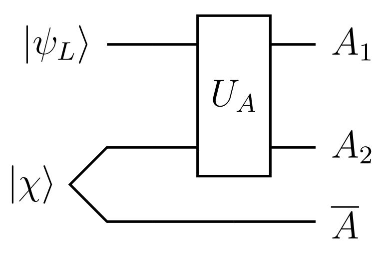
$$\rho_{R\overline{A}}(\phi) = \rho_R(\phi) \otimes \rho_{\overline{A}}(\phi) \tag{1.8}$$

4. *$|R| \leq |A|$, and decomposing $\mathcal{H}_A = (\mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2}) \oplus \mathcal{H}_{A_3}$ (by long division), where $|A_1| = |R|$ and $|A_3| < |R|$, then there exists a unitary transformation U_A on $\mathcal{H}_A$ and a state $|\chi\rangle_{A_2\overline{A}} \in \mathcal{H}_{A_2\overline{A}}$ such that*

$$|i_L\rangle_{A\overline{A}} = U_A \left(|i\rangle_{A_1} \otimes |\chi\rangle_{A_2\overline{A}} \right) \tag{1.9}$$

where $\{|i\rangle_{A_1}\}$ is an orthonormal basis of $\mathcal{H}_{A_1}$.

- Before going through the proof, what do all these mean?
- We think of A as the subsystem preserved by erasure, and $\overline{A}$ as the erased subsystem
- We also think of A_1 as the system in which erasure correction should recover our initial state on
- Point 1 states that any logical operator on $\mathcal{H}_{\text{code}}$ can be equivalently represented by an operator on A only; an operator on the code space can be represented by one acting on the system A acting equivalently
- Point 2 states that performing a projective measurement on *any* operator on the erased subsystem $\overline{A}$ cannot itself disturb the encoded information; no measurement on $\overline{A}$ can tell us anything about the encoded information
- Point 3 states that operators on the reference system R and operators on the erased subsystem $\overline{A}$ are not correlated
- Point 4 simply states that a unitary operator exists that can transform between the A_1 and the full $A\overline{A}$ systems, as in the toy model; this is essentially the statement that recoverability is possible
- We can visualise point 4 by a circuit diagram:



- The proof is basic linear algebra

Proof. (1) $\implies$ (2): This is by contradiction. Suppose there was an $X_{\overline{A}}$ such that $P_{\text{code}} X_{\overline{A}} P_{\text{code}}$ was not proportional to P_{code}. Schur's lemma in this context states that the only non-trivial operators commuting with all other operators on $\mathcal{H}_{\text{code}}$ are scalar multiples of the identity. Therefore, there must be an operator O_L on $\mathcal{H}_{\text{code}}$ which doesn't commute with $X_{\overline{A}}$ and a state $|\psi_L\rangle \in \mathcal{H}_{\text{code}}$ such that $\langle\psi_L|[P_{\text{code}} X_{\overline{A}} P_{\text{code}}, O_L]|\psi_L\rangle =$

$\langle\psi_L|[X_{\overline{A}}, O_L]|\psi_L\rangle \neq 0$. But such an O_L cannot have a representation O_A on $\mathcal{H}_A$ since this would automatically commute with $X_{\overline{A}}$, which contradicts (1).
(2) $\implies$ (3): Consider arbitrary operators O_R on $\mathcal{H}_R$ and $X_{\overline{A}}$ on $\mathcal{H}_{\overline{A}}$. We rewrite (2) as

$$\begin{aligned} P_{\text{code}} X_{\overline{A}} P_{\text{code}} &= \sum_{ij} |i_L\rangle \langle i_L|_{A\overline{A}} X_{\overline{A}} |j_L\rangle \langle j_L|_{A\overline{A}} \\ &= \lambda P_{\text{code}} \\ &= \lambda \sum_i |i_L\rangle \langle i_L|_{A\overline{A}} \end{aligned} \tag{1.10}$$

which implies $\langle i_L|X_{\overline{A}}|j_L\rangle_{A\overline{A}} = \lambda\delta_{ij}$. However, note that

$$\begin{aligned} \langle\phi|X_{\overline{A}}|\phi\rangle &= \frac{1}{|R|}\sum_{ij} \langle i_L|_R \langle i_L|X_{\overline{A}}|j_L\rangle_{A\overline{A}} |j_L\rangle_R \\ &= \frac{1}{|R|}\lambda \sum_i \langle i_L|i_L\rangle_R \\ &= \lambda \end{aligned} \tag{1.11}$$

Therefore, we must have $P_{\text{code}} X_{\overline{A}} P_{\text{code}} = \langle\phi|X_{\overline{A}}|\phi\rangle\, P_{\text{code}}$. But this implies

$$\begin{aligned} \langle\phi|X_{\overline{A}} O_R|\phi\rangle &= \langle\phi|O_R P_{\text{code}} X_{\overline{A}} P_{\text{code}}|\phi\rangle \\ &= \langle\phi|X_{\overline{A}}|\phi\rangle \langle\phi|O_R|\phi\rangle \end{aligned} \tag{1.12}$$

where the first equality comes from noting that $P_{\text{code}}|\phi\rangle = |\phi\rangle$, and that P_{code} commutes with O_R. Therefore, so long as $|\phi\rangle$ has no non-vanishing connected (?) correlation functions for any such O_R and $X_{\overline{A}}$, then $\rho_{R\overline{A}}[\phi] = \rho_R[\phi] \otimes \rho_{\overline{A}}[\phi]$, where $\rho_R[\phi]$ is the reduced density matrix $\mathrm{Tr}_{A\overline{A}}(|\phi\rangle\langle\phi|)$ etc.
(3) $\implies$ (4): First, note that by definition, $|\phi\rangle$ is a purification of $\rho_{R\overline{A}}[\phi] = \rho_R[\phi] \otimes \rho_{\overline{A}}[\phi]$ on A. Also, note that

$$\rho_R[\phi] = \mathrm{Tr}_{A\overline{A}}\left(\frac{1}{|R|}\sum_{ij} |i_L\rangle \langle j_L|_R |i_L\rangle \langle j_L|_{A\overline{A}}\right) = \frac{1}{|R|}\sum_i |i_L\rangle\langle i_L|_R = \frac{1}{|R|} I_R \tag{1.13}$$

so $|\phi\rangle$ maximally entangles R with A (or $\overline{A}$), and $\rho_R[\phi] = I/|R|$ is the maximally mixed state. This means that (3) becomes

$$\rho_{R\overline{A}}[\phi] = \frac{I_R}{|R|} \otimes \rho_{\overline{A}}[\phi] \tag{1.14}$$

Let's now perform long division on A. Say k is the largest integer such that $|A| = k|R| + r$. Since the R and $\overline{A}$ registers are unentangled in (1.14), we can factorise $\mathcal{H}_A = (\mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2}) \oplus \mathcal{H}_{A_3}$ such that $|A_1| = |R|$, $|A_2| = k$, and $|A_3| = r$.
We now define the following two states:

$$|\Psi\rangle_{RA_1} = \frac{1}{\sqrt{|R|}}\sum_i |i_L\rangle_R |i\rangle_{A_1}, \qquad |\chi\rangle_{A_2\overline{A}} = \sum_j \sqrt{p_j}\, |j\rangle_{A_2} |j\rangle_{\overline{A}} \tag{1.15}$$

and note that the state

$$|\phi'\rangle = |\Psi\rangle_{RA_1} \otimes |\chi\rangle_{A_2\overline{A}} \tag{1.16}$$

purifies $\rho_{R\overline{A}}[\phi]$ on A_1A_2:

$$\begin{aligned} \mathrm{Tr}_{A_1A_2}\left(|\Psi\rangle\langle\Psi|_{RA_1} \otimes |\chi\rangle\langle\chi|_{A_2\overline{A}}\right) &= \mathrm{Tr}_{A_1}\left(|\Psi\rangle\langle\Psi|_{RA_1}\right) \mathrm{Tr}_{A_2}\left(|\chi\rangle\langle\chi|_{A_2\overline{A}}\right) \\ &= \rho_R[\phi] \otimes \rho_{\overline{A}}[\phi] \end{aligned} \tag{1.17}$$

where $|\Psi\rangle_{RA_1}$ purifies $\rho_R[\phi]$ on A_1, and $|\chi\rangle_{A_2\overline{A}}$ purifies $\rho_{\overline{A}}[\phi]$ on A_2. In a purification, the dimension of the purifying system A needs to be at least as big as the rank of the state being purified, so we therefore have $|A_1| = |R|$ (since $\rho_R[\phi]$ is maximally mixed), and $\mathrm{Rank}\left(\rho_{\overline{A}}[\phi]\right) \leq |A_2|$.
However, purifications are unitarily equivalent on the purifying system - A in our case - so there exists unitary U_A on A taking $|\phi\rangle = U_A |\phi'\rangle$. Overall, we therefore have:

$$\begin{aligned} \frac{1}{\sqrt{|R|}} \sum_i |i_L\rangle_R |i_L\rangle_{A\overline{A}} &= U_A \left(\frac{1}{\sqrt{|R|}} \sum_i |i_L\rangle_R |i\rangle_{A_1} \otimes |\chi\rangle_{A_2\overline{A}} \right) \\ \implies |i_L\rangle_{A\overline{A}} &= U_A \left(|i\rangle_{A_1} \otimes |\chi\rangle_{A_2\overline{A}} \right) \end{aligned} \tag{1.18}$$

(4) $\implies$ (1): Just define $O_A \equiv U_A O_{A_1} U_A^\dagger$, where O_{A_1} is an operator on $\mathcal{H}_{A_1}$ with the same matrix elements as O_L does on $\mathcal{H}_{\text{code}}$. ■ □

- One thing this theorem doesn't do is tell us the full set of erasures that can be corrected by a given code subspace
- For example, the toy model could correct for *any* single qutrit erasure, but this isn't immediately obvious from a specific decomposition into A and $\overline{A}$
- In the toy model, this robustness was a consequence of $|\chi\rangle_{23}$ having non-zero entanglement; the same is true here - if $|\chi\rangle_{A_2\overline{A}}$ is a product state, then $\overline{A}$ provides no additional information and we can do away with it

1.3 A Ryu-Takayanagi Formula

- Point (4) has some immediate implications if the erasure of $\overline{A}$ is correctable
- Consider an arbitrary mixed state ρ^L on $\mathcal{H}_{\text{code}}$, and an operator ρ_{A_1} on $\mathcal{H}_{A_1}$ with the same matrix elements as ρ^L
- (4) then gives us:

$$\begin{aligned} \rho^L &= U_A \left(\rho_{A_1} \otimes |\chi\rangle \langle\chi|_{A_2\overline{A}} \right) U_A^\dagger \\ \rho^L_A \equiv \mathrm{Tr}_{\overline{A}} \rho^L &= U_A \left(\rho_{A_1} \otimes \mathrm{Tr}_{\overline{A}}(|\chi\rangle\langle\chi|) \right) U_A^\dagger \\ \rho^L_{\overline{A}} \equiv \mathrm{Tr}_A \rho^L &= \mathrm{Tr}_{A_2}(|\chi\rangle\langle\chi|) \end{aligned} \tag{1.19}$$

- If we further denote $\chi_{A_2} \equiv \mathrm{Tr}_{\overline{A}} |\chi\rangle\langle\chi|$ and $\chi_{\overline{A}} = \mathrm{Tr}_{A_2} |\chi\rangle\langle\chi|$, we can rewrite these as

$$\begin{aligned} \rho^L_A &= U_A \left(\rho_{A_1} \otimes \chi_{A_2} \right) U_A^\dagger \\ \rho^L_{\overline{A}} &= \chi_{\overline{A}} \end{aligned} \tag{1.20}$$

- So, calculating the von Neumann entropies, we find

$$\begin{aligned} S(\rho^L) &= S(\rho_{A_1}) + S(|\chi\rangle\langle\chi|) = S(\rho_{A_1}) \\ S(\rho^L_A) &= S(\rho_{A_1}) + S(\chi_{A_2}) = S(\rho^L) + S(\chi_{A_2}) \\ S(\rho^L_{\overline{A}}) &= S(\chi_{\overline{A}}) = -\mathrm{Tr}_{A_2}\left[\mathrm{Tr}_{\overline{A}}\left[|\chi\rangle\langle\chi|\right]\right] = S(\chi_{A_2}) \end{aligned} \tag{1.21}$$

- If we define an 'area operator' $\mathcal{L}_A \equiv S(\chi_{A_2}) I_{\text{code}}$, the latter two of these are reminiscent of the Ryu-Takayanagi formula

$$S(\rho_A) = \mathrm{Tr}(\rho \mathcal{L}_A) + S_{bulk}(\rho_{\mathcal{E}_A}) \tag{1.22}$$

- The 'area term' arises from the non-zero entanglement in $|\chi\rangle$