Quantum Operation

- A general theory of $\rho \mapsto \mathscr{E}(\rho)$ capturing all physically possible dynamic changes to a state
  - For example, unitary evolution or measurements
  - Physically possible dynamic changes associated with maps on the set of density operators
- **System Q coupled with environment E**
  - Model 1: QE starts in $\rho \otimes \rho^E$ and undergoes U
    - $\rho \mapsto \mathrm{tr}_E\left(U(\rho \otimes \rho^E)U^\dagger\right)$
  - Analysis: without loss of generality we assume $\rho^E = |0_E\rangle\langle 0_E|$ —use purification
    - Let $\{|i_E\rangle\}$ be basis for E, define $E_i \equiv \langle i_E | U | 0_E\rangle$ (operator on Q), then $\rho \mapsto \sum E_i \rho E_i^\dagger$
      - $U|\psi\rangle|0_E\rangle = \sum \left(\langle i_E|U|0_E\rangle(|\psi\rangle)\right)|i_E\rangle = \sum \left(E_i|\psi\rangle\right)|i_E\rangle$
      - $E_i|\psi\rangle$ is the "Q-vector" component of $|i_E\rangle$ in $U|\psi\rangle|0_E\rangle$
      - Conversely, $E_i^\dagger|\psi\rangle$ is the Q-vector component of $|0_E\rangle$ in $U|\psi\rangle|i_E\rangle$
    - $\mathrm{tr}_E\left(U(\rho \otimes |0_E\rangle\langle 0_E|)U^\dagger\right) = \sum \langle i_E|U(\rho \otimes |0_E\rangle\langle 0_E|)U^\dagger|i_E\rangle = \sum \langle i_E|U|0_E\rangle\rho\langle 0_E|U^\dagger|i_E\rangle = \sum E_i\rho E_i^\dagger$
    - $\sum E_i^\dagger E_i = I \iff \rho \mapsto \mathrm{tr}_E\left(U(\rho \otimes \rho^E)U^\dagger\right)$ corresponds to (measuring Q by $\{E_i\}$) or (measuring E in computational basis) after undergoing U with result of measurement lost
    - Partial effects of joint unitary evolution $\iff$ measurement with outcome lost
  - Example: Consider single-qubit Q, E with $U = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$, then $U(\alpha|0\rangle + \beta|1\rangle)|0\rangle = \alpha|00\rangle + \beta|11\rangle$. Then $E_1(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle \implies E_0 = |0\rangle\langle 0|$, similarly $E_1 = |1\rangle\langle 1|$.
    - Lost measurement in computational basis corresponds to unitary evolution of $U|\psi\rangle|0\rangle$
  - $U \equiv \dfrac{X}{\sqrt{2}} \otimes I + \dfrac{Y}{\sqrt{2}} \otimes X$, then $U(\alpha|0\rangle + \beta|1\rangle)|0\rangle = \left(\dfrac{X}{\sqrt{2}}|\psi\rangle\right)|0\rangle + \left(\dfrac{Y}{\sqrt{2}}|\psi\rangle\right)|1\rangle$
    - $E_0 = X/\sqrt{2},\ \ E_1 = Y/\sqrt{2}$, corresponds to applying X, Y randomly with probability $1/2$
  - Model 2: QE starts in $\rho \otimes \sigma$, undergoes U and joint projective measurement $\{P_m\}$
    - Remark: General measurement = unitary evolution + projective measurement
    - Let $\mathscr{E}_m(\rho) \equiv \mathrm{tr}_E\left(P_m U(\rho \otimes \sigma)U^\dagger P_m\right),\ \sigma = \sum q_j|j\rangle\langle j|$, and $E_{jk} \equiv \sqrt{q_j} \cdot \langle k_E|P_m U|j\rangle$
    - $\mathscr{E}_m(\rho) = \sum q_j \cdot \mathrm{tr}_E\left(P_m U(\rho \otimes |j\rangle\langle j|)U^\dagger P_m\right) = \sum_{jk} E_{jk}\rho E_{jk}^\dagger$

- Given any $\{\mathscr{E}_m\}$ such that $\sum \mathscr{E}_m$ is trace-preserving, introduce E with basis $|m,k\rangle_E$, initial state $|0\rangle_E$, $U: U|\psi\rangle|0\rangle_E = \sum E_{mk}|\psi\rangle|m,k\rangle$, and $P_m = \sum_k |m,k\rangle\langle m,k|$, then $\mathrm{tr}_E\left(P_m U\left(\rho\otimes|0\rangle_E\langle 0|\right)U^\dagger P_m\right) = \mathscr{E}_m(\rho)/\mathrm{tr}(\mathscr{E}_m(\rho))$
- $\{\mathscr{E}_m\}$ model-able as $\mathscr{E}_m(\rho) = \mathrm{tr}_E\left(P_m U\left(\rho\otimes|0\rangle_E\langle 0|\right)U^\dagger P_m\right) \iff \mathscr{E}_m(\rho) = \sum E_{mk}\rho E_{mk}^\dagger$
  - Trace-preserving: $\mathscr{E}(\rho) = \mathrm{tr}_E\left(U\left(\rho\otimes|0\rangle\langle 0|\right)U^\dagger\right) \iff \mathscr{E}(\rho) = \sum E_k\rho E_k^\dagger,\ \sum E_k^\dagger E_k = I$
- **Axiomatic approach**: we define a dynamic change $\mathscr{E}$ to system Q in state ρ by:
  - Nonnegative probability: With initial state ρ, $\mathscr{E}$ occurs with probability $\mathrm{tr}\left(\mathscr{E}(\rho)\right)\in[0,1]$
    - Mathematically convenient definition to help cope with measurements
  - Convex-linear: $\mathscr{E}\left(\sum_i p_i\rho_i\right) = \sum_i p_i\mathscr{E}(\rho_i)$
    - We wish that $\rho\sim\{\rho_i,p_i\} \implies \dfrac{\mathscr{E}(\rho)}{\mathrm{tr}\left(\mathscr{E}(\rho)\right)} \sim \{\dfrac{\mathscr{E}(\rho_i)}{\mathrm{tr}\left(\mathscr{E}(\rho_i)\right)}, p_i\}$, then $\mathscr{E}(\rho) = \mathrm{tr}\left(\mathscr{E}(\rho)\right)\sum_i p(i\mid\mathscr{E})\dfrac{\mathscr{E}(\rho_i)}{\mathrm{tr}\left(\mathscr{E}(\rho_i)\right)}$. By $p(i\mid\mathscr{E}) = \dfrac{p_i\mathrm{tr}\left(\mathscr{E}(\rho_i)\right)}{\mathrm{tr}\left(\mathscr{E}(\rho)\right)}$ yields above
  - Completely positive: For any (including trivial) system R, $I_R\otimes\mathscr{E}$ maps to positive operators
    - If $\rho = \mathrm{tr}_Q(\rho^{RQ})$ then after $\mathscr{E}$ the joint state is still in a valid density matrix
    - Remark: positive *does not* imply completely positive: consider positive map $\rho\mapsto\rho^\dagger$ applied to the first qubit in β_{00}. Then $(\rho\mapsto\rho^\dagger\otimes I)$ transposes the 2×2 blocks $(\rho\mapsto\rho^\dagger\otimes I)\beta_{00} = \dfrac{(\rho\mapsto\rho^\dagger\otimes I)}{2}\begin{bmatrix}1&0&0&1\\0&0&0&0\\0&0&0&0\\1&0&0&1\end{bmatrix} = \dfrac{1}{2}\begin{bmatrix}1&&&\\&&1&\\&1&&\\&&&1\end{bmatrix}$ with
- Theorem: $\mathscr{E}$ satisfies axioms above $\iff$ $\mathscr{E}(\rho) = \sum_i E_i\rho E_i^\dagger$ and $\sum_i E_i^\dagger\rho E_i \le I$
  - $\sum_i E_i\rho E_i^\dagger$ obviously satisfies axioms 1 & 2, to show complete positivity: let A be any positive operator on RQ, and $|\psi\rangle$ be any state of RQ, then by A positive $\langle\psi|(I\otimes\mathscr{E})A|\psi\rangle = \langle\psi|\sum(I\otimes E_i)A(I\otimes E_i^\dagger)|\psi\rangle = \sum\langle\psi|(I\otimes E_i)A(I\otimes E_i^\dagger)|\psi\rangle \ge 0$
  - Conversely, let $\{|i_R\rangle\}, \{|i_Q\rangle\}$ span R, Q and define *maximally entangled state* $|\alpha\rangle \equiv \sum|i_R\rangle|i_Q\rangle$ and $\sigma\equiv(I_R\otimes\mathscr{E})(|\alpha\rangle\langle\alpha|) = \sum_{ij}\left(|i_R\rangle\langle j_R|\right)\otimes\mathscr{E}\left(|i_Q\rangle\langle j_Q|\right)$

- For any $|\psi\rangle = \sum \psi_i |i_Q\rangle$ on Q, define $|\tilde{\psi}\rangle \equiv \sum \psi_i^* |i_R\rangle$ on R. Then

  $\langle\tilde{\psi}|\sigma|\tilde{\psi}\rangle = \langle\tilde{\psi}| \sum_{ij} |i_R\rangle\langle j_R| \otimes \mathscr{E}\left(|i_Q\rangle\langle j_Q|\right)|\tilde{\psi}\rangle = \sum \psi_i\psi_j^*\mathscr{E}(|i_Q\rangle\langle j_Q|) = \mathscr{E}(|\psi\rangle\langle\psi|)$

- Let $\sigma = \sum |s_i\rangle\langle s_i|$ be some decomposition of σ, then $E_i|\psi\rangle = \langle\tilde{\psi}|s_i\rangle$ satisfies

  $\sum E_i|\psi\rangle\langle\psi|E_i^\dagger = \sum \langle\tilde{\psi}|s_i\rangle\langle s_i|\tilde{\psi}\rangle = \langle\tilde{\psi}|\sigma|\tilde{\psi}\rangle$

- Remark: $I \otimes \mathscr{E}$'s action on maximally entangled state of QR uniquely determines $\mathscr{E}$

- $\mathscr{E}$ satisfies axioms $\iff$ $\mathscr{E}(\rho) = \sum E_k\rho E_k^\dagger,\ \sum E_i^\dagger E_i \leq I$ $\iff$ $\mathscr{E}(\rho) = \mathrm{tr}_E\left(PU\left(\rho\otimes\sigma\right)U^\dagger P\right)$

- Unitary freedom in operator-sum representation
  - $\{E_k\}, \{F_k\}$ equivalent if $\sum E_k\rho E_k^\dagger = \sum F_k\rho F_k^\dagger \iff \forall |j\rangle, \sum E_k|j\rangle\langle j|E_k^\dagger = \sum F_k|j\rangle\langle j|F_k^\dagger$
    - $\{E_k, F_k\}$ equivalent $\iff$ $\forall |j\rangle, \{E_k|j\rangle\}, \{F_k|j\rangle\}$ generate the same density matrix
  - Recall $\Psi\Psi^\dagger = \Phi\Phi^\dagger \iff \Psi = \Phi U$ then $\forall i, E_i|j\rangle = \sum_i u_{ki}F_k|j\rangle \implies E_i = \sum u_{ki}F_k$
  - $\{E_k\}, \{F_k\}$ equivalent $\iff$ $\mathbf{E} = U\mathbf{F}$ with $\mathbf{E}_i = E_i$ for unitary U
    - Matrix multiplication with operator as elements
    - Example: $E_1 = \frac{I}{\sqrt{2}}, E_2 = \frac{Z}{\sqrt{2}}, F_1 = |0\rangle\langle 0|, F_2 = |1\rangle\langle 1|, \begin{bmatrix} E_1 \\ E_2 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} F_1 \\ F_2 \end{bmatrix}$

- Any operation over E with dimension d may be described by at most d^2 operation elements
  - Assume we have more than d^2 operators $\{E_i\}$
  - Recall Hilbert-Schmidt inner product $\langle A, B\rangle = \mathrm{tr}\left(A^\dagger B\right)$
    - Let $W_{ij} = \langle E_i, E_j\rangle$. Easy to see that $W^\dagger = W$ is Hermitian
  - Lemma: W has rank at most d^2
    - At most d^2 linearly independent operators, so we have row dependence from

      $E_j = \sum_{k\neq j} \alpha_k E_k \implies E_j^\dagger E_l = \sum_{k\neq j} \alpha_k^* E_k^\dagger E_l \implies W_{jl} = \sum_{k\neq j} \alpha_k^* W_{kl}$
  - Diagonalized W has at most d^2 nonzero diagonal entries, then equivalent operator set $W\mathbf{E}$ has at most d^2effective elements

- Trace and partial trace as quantum operation
  - Trace: Let $E_i = |0\rangle\langle i|$, then $\mathscr{E}(\rho) = \sum |0\rangle\langle i|\rho|i\rangle\langle 0| = \mathrm{tr}(\rho)|0\rangle\langle 0|$
  - Partial trace: Given joint system QR with $|i_Q\rangle \otimes |j_R\rangle$ basis, then

    $E_k\left(\sum \lambda_j|j_Q\rangle|j_R\rangle\right) = \lambda_k|k_Q\rangle$ satisfies $\mathscr{E}(\rho) = \sum E_k\rho E_k^\dagger = \mathrm{tr}_R\left(\rho\right)$
  - $\sum a_{ij}\cdot E_k|i_Q\rangle|j_R\rangle\left(E_k|i_Q\rangle|j_R\rangle\right)^\dagger$

- Single-qubit quantum operations
  - Trace-preserving operations on single-qubit correspond to affine maps on the Bloch sphere
  - Recall: $\phi : |\psi\rangle\langle\psi| = \dfrac{\phi(|\psi\rangle\langle\psi|)\cdot\sigma}{2}$ is linear, and $\sigma_i|\psi\rangle\langle\psi|\sigma_i^\dagger = \dfrac{R_i\left(|\psi\rangle\langle\psi|\right)\cdot\sigma}{2}$

    where $R_I = I,\ \ R_{a\in\{x,y,z\}} = R_a(\pi/2)$

Quantum Error-correction

- Formalism of error-correction
  - An **quantum error-correcting code** is a subspace C of larger Hilbert space with projector P
  - Noise and recovery are $\mathscr{E}, \mathscr{R}$ respectively with $\mathrm{tr}\mathscr{R} = 1$ (recovery must certainly happen)
  - Error-correction condition: $\forall \rho \in C : (\mathscr{R} \circ \mathscr{E})(\rho) \propto \rho$
- Theorem: Exists ECC for $\mathscr{E}(\rho) = \sum E_i \rho E_i^\dagger \iff \exists U : PE_i^\dagger E_j P = U_{ij} P$ for Hermitian U
  - Consider diagonalization $U = SDS^\dagger$ and the equivalent operator set for $\mathscr{E}$: $\mathbf{F} = S\mathbf{E}$

    $\iff F_k = \sum S_{ki} E_i$, then $PF_i^\dagger F_j P = \sum_{kl} S_{ik}^* S_{jl} \cdot PE_i^\dagger E_j P = \sum_{kl} S_{ik}^* S_{jl} U_{ij} P = d_{kl} P$
  - $F_k P = U_k \sqrt{PF_k^\dagger F_k P} = \sqrt{d_{kk}} U_k P$. F_k rotates C onto $\mathrm{Im} U_k P = \mathrm{Im}\left(P_k \equiv U_k P U_k^\dagger = \dfrac{F_k P U_k^\dagger}{\sqrt{d_{kk}}}\right)$
    - Recall: projector P must satisfy $\langle Px, x - Px \rangle = 0 \iff P^\dagger = P^\dagger P$ and $\mathrm{Im} P = \mathrm{Im} A$
  - Now $P_l P_k = P_l^\dagger P_k = \dfrac{U_l P F_l^\dagger F_k P U_k^\dagger}{\sqrt{d_{ll} d_{kk}}} = \dfrac{U_l d_{lk} U_k^\dagger}{\cdot\cdot} = 0$ implies $k \neq l \implies \mathrm{Im}(U_k P) \perp \mathrm{Im}(U_l P)$
    - Syndrome measurement corresponds to $P_k \equiv U_k P U_k^\dagger$ and correction $U_k^\dagger$
- Theorem: $\mathscr{R}$ constructed above for $\mathscr{E} = \{E_i\}$ also corrects any error $\mathscr{F} = \{\sum m_{ji} E_i\}$
  - Corollary: we can instead talk about a set of error operators which are correctable

Quantum Error-Correcting Codes

- (All arithmetic operations taken over $\mathbb{Z}_2$ in this section)
- A $[n,k]$ **classical linear code** is a subspace $C \subset \mathbb{Z}_2^n$ with dim k. It encodes k bits into n bits
  - Codes are specified as a subspace so may be uniquely determined as kernel or image
  - Remark: linear codes are *closed under addition*
  - **Generating matrix** $G \in \mathbb{Z}_2^{n\times k}$, $C = \mathrm{Im}(G)$ specifies encoding $E(x) = Gx \in \mathbb{Z}_2^{n\times 1}$
    - Decoding $D(y') = \mathrm{argmin}_x \left[d(Gx, y')\right]$
  - **Parity check matrix** $H \in \mathbb{Z}_2^{(n-k)\times n}$, $C = \ker(H)$ facilitates
    - Let $y' = y + e = Gx + e$, then $Hy' = He$ characterizes the **error syndrome**.
    - If error syndromes distinct $H(\{e_i\} \cong \{He_i\})$ then we can identify and correct e_i from Hy'
  - To ensure $\dim C = k$ both H, G must have full rank
  - $C = \mathrm{Im}(G) = \ker(H) \implies HG \in \mathbb{Z}_2^{(n-k)\times 1} = 0$
  - $H = [A \in \mathbb{Z}_2^{(n-k)\times k} \,|\, I_{n-k}] \iff G = \begin{bmatrix} I_k \\ -A \end{bmatrix}$. These are called the **standard form**
- Define **Hamming distance** $d(x,y)$ as the number of indices in which x, y differ
  - The **Hamming weight** $\mathrm{wt}(x) \equiv d(x,0)$. $x + y = x - y \implies d(x,y) = \mathrm{wt}(x+y)$
- Define the **distance of code** $d(C) \equiv \min\limits_{x,y\in C, x\neq y} d(x,y) = \min\limits_{x\in C-\{0\}} \mathrm{wt}(x)$
  - Let $d \equiv d(C)$, we say that C is an $[n,k,d]$ code
- Theorem: a $[n,k,d]$ code with $d \geq 2t+1$ corrects error on up to t bits
  - $y = Gx, y' = y + e$. Now $d(y', y) \leq t$ while $\min_{y_1\neq y_2} d(y_1, y_2) \geq 2t+1$. Decoding is unique
- If *any* $d-1$ columns of H are linearly independent but some subset of d columns are linearly dependent $\iff$ $C = \ker H$ has distance d
  - Recall $x \in C \iff Hx = 0$. If $x \neq 0$ and $Hx = 0$, condition above implies that x cannot have $\leq d-1$ nonzero entries. The converse is also true
- Singleton bound: an $[n,k,d]$ code satisfies $n - k \geq d - 1$
  - An $[n,k,d]$ code has $H \in \mathbb{Z}_2^{(n-k)\times n}$ of full rank. Some subset of $n-k+1$ columns must be linearly dependent so $d \leq n-k+1$
  - Remark: H full rank $\implies$ some (generally not all) $n-k$ columns are independent, so the last result does not imply $d - 1 = n - k$

- **Hamming codes**: Given $r \in \mathbb{N}$, let columns of parity check matrix $H_r \in \mathbb{Z}_2^{r \times (2^r - 1)}$ be all r-bit nonzero strings, then H_r defines a $[2^r - 1, 2^r - r - 1]$ linear code
  - All Hamming codes have distance 3: any two columns are different and some three columns are independent. Hamming codes are $[2^r - 1, 2^r - r - 1, 3]$ linear codes
  - Example: $H_3 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$
- **Gilbert-Varshamov bound**: for large n there exists $[n, k, d \geq 2t + 1]$ code for some k s.t. $k/n \geq 1 - H(2t/n)$ with $H \equiv -x \log x - (1 - x)\log(1 - x)$
  - Prove the Gilbert-Varshamov bound
- Given an $[n, k]$ code C, its **dual code** $C^\perp$ has generator H^T and parity check matrix G^T
  - $x \in C^\perp \iff \forall c^T x = 0 \iff x \in \ker G^T \implies G^T$ parity checks $C^\perp$
  - A code is **weakly self-dual** if $C \subseteq C^\perp$ and **strictly self-dual** if $C = C^\perp$
  - Over $\mathbb{C}, \mathbb{R}$ fields, $C^\perp \cap C = \{0\}$ but over $\mathbb{Z}_2$ field $C^\perp \cap C$ can be nontrivial
  - Remark: Hamming distance is not a valid inner product in strict sense e.g. $d(x, x)$ can be 0 for nonzero x, but it obeys triangle inequality
- Code with generator G is weakly self-dual $\iff G^T G = 0$
  - Follows from definition: $G^T G = 0 \iff \mathrm{Im} G \subseteq \ker G^T$
- Lemma: $\sum_{c \in C} (-1)^{y \cdot c} = \begin{cases} 0 & \text{if } y \notin C^\perp \\ |C| & \text{if } y \in C^\perp \end{cases}$
  - $y \in C^\perp \implies \forall c \in C, \ \ y \cdot c = 0$
  - $y \notin C^\perp \implies \exists c_0 \in C : c_0 \cdot y = 1$ then for every $c : c \cdot y = 0$ we have $(c + c_0) \cdot y = 1$
    - Bijection between $\{c \in C : c \cdot y = 0\}$ and $\{c \in C : c \cdot y = 1\}$
- **Calderbank-Shor-Steane** (CSS) codes
  - Given $[n, k_1]$ code C_1 and $[n, k_2]$ code C_2 s.t. $C_2 \subsetneq C_1$ and $C_1, C_2^\perp$ both correct t errors
    - $\dim C_1 = \dim C_2^\perp = t \implies k_1 = t, n - k_2 = t$, and $k_2 < k_1$
  - Remark: we're assuming bit then phase error, but it's without loss of generality up to e_1, e_2
  - We can construct an $[n, k_1 - k_2] = [n, 2t - n]$ quantum code $\mathrm{CSS}(C_1, C_2)$ as follows:
    - Define $x + C_2 = [x]^{C_2} \equiv \{x' \in C_1 : x' - x \in C_2\} \in C_1/C_2$
    - For each unique $[x]^{C_2}$, define $|[x]^{C_2}\rangle \equiv \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x + y\rangle$
    - Define $\mathrm{CSS}(C_1, C_2) = \mathrm{span}(\{|[x]^{C_2}\rangle\})$, then $\dim \mathrm{CSS}(C_1, C_2) = k_1 - k_2$

- $|[x]^{C_2}\rangle$ is well-defined i.e. $x - x' \in C_2 \implies |[x]^{C_2}\rangle = |[x']^{C_2}\rangle$
  - $|x + (y \in C_2)\rangle = |x + (y + x' - x \in C_2)\rangle$
- $|[x]^{C_2}\rangle$ is orthonormal: $[x]^{C_2} \neq [x']^{C_2} \implies \nexists y_1, y_2 \in C : |x + y_1\rangle = |x' + y_2\rangle$

- Error correction: denote bit and phase errors by n-bit binary strings e_1, e_2 respectively
  - $|[x]^{C_2}\rangle \mapsto \dfrac{1}{\sqrt{|C_2|}} \sum_{x \in C_2} (-1)^{(x+y)\cdot e_2} |x + y + e_1\rangle$
  - Apply $|x\rangle|0\rangle \mapsto |x\rangle|H_1 x\rangle$ obtaining $\dfrac{1}{\sqrt{|C_2|}} \sum_{x \in C_2} (-1)^{(x+y)\cdot e_2} |x + y + e_1\rangle |H_1 e_1\rangle$
    - Remark: $x + y \in C_1 \implies H_1(x + y + e_1) = H_1 e_1$
    - Measure second register, obtain e_1, and correct $\mapsto \dfrac{1}{\sqrt{|C_2|}} \sum_{x \in C_2} (-1)^{(x+y)\cdot e_2} |x + y\rangle$
  - $H^{\otimes n}$: $\dfrac{1}{\sqrt{|C_2|2^n}} \sum_{y \in C_2} (-1)^{(x+y)\cdot e_2} \sum_{z \in \mathbb{Z}_2^n} (-1)^{(x+y)\cdot z} |z\rangle = \dfrac{1}{\sqrt{|C_2|2^n}} \sum_{y \in C_2} \sum_{z \in \mathbb{Z}_2^n} (-1)^{(x+y)\cdot(z+e_2)} |z\rangle$
  - Substitute $z' = z + e_2$: $\dfrac{1}{\sqrt{|C_2|2^n}} \sum_{z \in \mathbb{Z}_2^n} (-1)^{x\cdot z'} \left(\sum_{y \in C_2} (-1)^{y\cdot z'} \right) |z' - e_2\rangle$. Recall lemma
    - Remark: $+$ and $-$ are the same in mod-2 arithmetic
  - $\sqrt{\dfrac{|C_2|}{2^n}} \sum_{z \in \mathbb{C}_2^\perp} (-1)^{x\cdot z'} |z' - e_2\rangle = \dfrac{1}{\sqrt{|C_2^\perp|}} \sum_{z \in \mathbb{C}_2^\perp} (-1)^{x\cdot z'} |z' - e_2\rangle$
    - Hadamard code takes Hadamard code to itself
    - Apply $|x\rangle|0\rangle \mapsto |x\rangle|G_2^T x\rangle$, obtaining $\dfrac{1}{\sqrt{|C_2^\perp|}} \sum_{z \in \mathbb{C}_2^\perp} (-1)^{x\cdot z'} |z' - e_2\rangle | - G_2^T e_2\rangle$
    - Measure second register and retrieve e_2 from $-G_2^T e_2$
  - Correct by applying X to obtain $\dfrac{1}{\sqrt{|C_2^\perp|}} \sum_{z \in \mathbb{C}_2^\perp} (-1)^{x\cdot z'} |z'\rangle$
    - Note how this equals $H^{\otimes n} \left(\dfrac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(x+y)\cdot e_2} |x + y\rangle \right)$ for $e_2 = \mathbf{0}$

- Apply $H^{\otimes n}$ to obtain $\frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x + y\rangle = |[x]^{C_2}\rangle$ as encoded state

- **Shifted CSS** codes: define $\mathrm{CSS}_{u,v}(C_1, C_2)$ with $|[x]^{C_2}\rangle \equiv \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{u \cdot y} |x + y + v\rangle$
- Lemma: $\forall u, v, \mathrm{CSS}_{u,v}(C_1, C_2)$ has the same coding properties as $\mathrm{CSS}(C_1, C_2)$
  - Equivalent to encoding bit / phase error e_1, e_2 with $e_1 + u, e_2 + v$