Quantum error correction
Lecture 2: the stabilizer formalism

a) Stabilizer codes

To go further than the 9-qubit code of Shor, it is useful to take inspiration from classical coding theory. And indeed, the class of quantum stabilizer codes will be the generalization of classical linear codes.

Classical linear codes.
A linear code C encoding k logical bits in n bits is denoted $[n, k]$ and is a subspace of $\mathbb{Z}_2^n = \{0,1\}^n$ of dimension k, i.e. of size 2^k.
There are two convenient ways of describing such a code:

(i) as the image of a parity check matrix G of size $k \times n$

$$C = \operatorname{Im} G = \{x^T G \ : \ x \in \{0,1\}^k\},$$

(ii) as the kernel of a parity check matrix H of size $(n-k) \times n$:

$$C = \ker H = \{x \in \{0,1\}^n \ : \ Hx = 0\}.$$

The generator matrix is convenient to describe the encoding circuit, the parity-check matrix is convenient to describe the error correction process.
Let $c \in C$ be a codeword. If $e \in \{0,1\}^n$ is an error (the ones in e correspond to the bits which have been flipped by the noise), then the syndrome of e is defined as

$$H(c+e) = Hc + He = He.$$

The *minimum distance* d of the code C is the minimum weight of an error $e \neq 0$ that belongs to the code, i.e. such that $He = 0$. It is the minimum number of bits that need to be flipped to map a codeword to another codeword. We say that $\mathcal{C}$ is an $[n, k, d]$ code. Such a code can detect any error of weight $\leqslant d-1$ and correct any error of weight $\lfloor \frac{d-1}{2} \rfloor$. For instance, there exist code families (C_n) with parameters $[n, k, d]$ with $k = \Theta(n), d = \Theta(n)$.

A coding scheme is as follows:

– the initial message M is a k-bit long random variable,

- the encoder is $E : \{0,1\}^k \to \{0,1\}^n, M \mapsto X$, and is described by the generator matrix,
- the encoded message X is sent through the channel $\mathcal{N}$, which is usually described as a conditional probability distribution: $p(Y = y|X = x)$,
- the output Y is fed into a decoder which reads the syndrome HY outputs a guess $\hat{M}$ for the message.

A *classical channel* $\mathcal{N} : X \to Y$ is defined by conditional probabilities: $p_{Y|X}(y|x)$. Define the capacity $\mathcal{C}(\mathcal{N})$ of the channel as

$$\mathcal{C}(\mathcal{N}) = \max_{p_X(x)} I(X;Y)$$

where $I(X;Y) = H(X)+H(Y)-H(XY)$ is the mutual information between the random variables X and Y, and the optimization is over probability distributions for variable X. A simple example is the binary symmetric channel: $X, Y \in \{0,1\}$ and $p_{Y|X}(y|x) = p$ if $y \neq x$, which has capacity $\mathcal{C}(\text{BSC}) = 1 - h(p)$.
Claude Shannon established the following surprising result.

Theorem 1 (Channel coding theorem)**.** *One can reliably send information at any rate $k/n < \mathcal{C}(\mathcal{N})$ by exploiting error correcting codes over sufficiently many uses of the channel. The maximal error probability ($\max_m Pr[\hat{m} \neq m]$) goes to 0 when the code size goes to infinity.*

The proof of this theorem is via a random coding argument. A major issue is that decoding a random (linear) code is believed to be hard, and to take exponential time. For this reason, one of the main goals of channel coding in the past 60 years has been to devise explicit coding schemes that approach the rate promised by the theorem but such that both the encoding and decoding operations can be performed efficiently.

We now move to the quantum generalization of classical linear codes. This formalism – *stabilizer codes* – was developed by Daniel Gottesman in his PhD thesis in the late 90s.

Pauli and Clifford groups
Let us recall first what the Pauli and Clifford groups are. The single-qubit Pauli group $\mathcal{P}_1$ is the group $\langle i\mathbb{1}, X, Z\rangle$ generated by the Pauli matrices. Its n-qubit generalisation is the n-fold tensor product of $\mathcal{P}_1$, that is $\mathcal{P}_n = \mathcal{P}_1^{\otimes n}$:

$$\mathcal{P}_n = \langle E_1 \otimes E_2 \otimes \ldots \otimes E_n \ : \ E_i \in \mathcal{P}_1\rangle,$$

and has cardinality 4^{n+1}. An important property of Pauli operators is that any two of them either commute or anticommute.

Theorem 2. *Let $P, Q \in \mathcal{P}_n$. Then either $PQ = QP$ or $PQ = -QP$.*

Proof. For single-qubit matrices, we have

$$[X,X] = [Y,Y] = [Z,Z] = 0, \quad \{X,Y\} = \{X,Z\} = \{Y,Z\} = 0.$$

Let us write the Pauli operators as products of n single-qubit matrices: $P = P_1 \ldots P_n$ and $Q = q_1 \ldots Q_n$. Then P and Q commute if and only if they anticommute in an even number of positions. Otherwise, they anticommute. □

The *Clifford group* $\mathcal{C}_n$ is the automorphism group of the Pauli group:

$$\mathcal{C}_n = \{U \in \mathcal{U}(\mathcal{C}^{2^n}) \ : \ U\mathcal{P}_n U^\dagger = \mathcal{P}_n\}.$$

In words, any Pauli operator P is mapped to a Pauli operator via conjugation by a Clifford unitary.

Theorem 3. *The Clifford group $\mathcal{C}_n$ is generated by H, P and $CNOT$:*

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}, \quad P = \begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}, \quad CNOT = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & -1\end{bmatrix}.$$

Definition 4 (Normalizer)**.** *The normalizer of S in the Pauli group $\mathcal{P}_n$ is*

$$N(S) = \{g \in \mathcal{P}_n \ : \ gS = Sg\}.$$

A quantum code $\mathcal{Q}$ of parameters $[[n, k, d]]$ is a linear subspace of $(\mathbb{C}^2)^{\otimes n}$ of dimension 2^k. The stabilizer construction is very much inspired by the classical construction of linear codes, and there are two main ways to define a stabilizer code:

(*i*) via its *encoding circuit*: this is *Clifford unitary* $U \in \mathcal{U}(\mathbb{C}^{2^n})$ applied on $|\psi\rangle \otimes |0\rangle^{n-k}$ where $|\psi\rangle \in (\mathbb{C}^2)^{\otimes k}$ is a logical state of k qubits and $|0\rangle^{n-k}$ is an $(n-k)$-qubit ancilla. This gives

$$\mathcal{Q} = \{U|\psi\rangle \otimes |0\rangle^{n-k} \ : \ |\psi\rangle \in (\mathbb{C}^2)^{\otimes k}\}.$$

(*ii*) via its *stabilizer*, i.e. a group $\mathcal{S} = \langle g_1, \ldots, g_{n-k}\rangle$ generated by a set of $n-k$ Pauli operators that commute and that don't contain $-\mathbb{1}$. The code is then defined as the elements of the Hilbert space that are stabilized by $\mathcal{G}$:

$$\mathcal{Q} = \{|\psi\rangle \in (\mathbb{C}^2)^{\otimes n} \ : \ g_i|\psi\rangle = |\psi\rangle, \forall i \in [n-k]\}.$$

In other words, the code is defined as the $+1$ eigenspace of the generators. This space is well defined since the commutation condition ensures that the generators are all codiagonalizable. Moreover, since each generator is a Pauli operator, it has eigenvalues equal to ± 1.

In order to make reliable computations with a noisy quantum computer, the idea is to encode information with a quantum error correcting code and then perform the computation on the encoded state. We need a way to act on such states. This is done via logical operators.

Definition 5 (Logical operator)**.** *A logical operator of the stabilizer code with stabilizer $\mathcal{S}$ is a Pauli operator that leaves the code globally invariant, but that acts nontrivially on codewords. It is given by the set $N(\mathcal{S}) \setminus \mathcal{S}$, and corresponds to a Pauli operator that commutes with all the generators of $\mathcal{S}$, but that doesn't belong to $\mathcal{S}$.*

A logical operator will map a word in the quantum code to an orthogonal codeword.
The fact that the encoding circuit of a stabilizer code is a Clifford operation is particularly useful because it implies that logical Pauli errors correspond to Pauli physical errors.

Example 6. *Both the 3-qubit code and Shor's 9-qubit code are stabilizer codes: this is because their encoding circuit is a Clifford unitary. As a consequence, these codes can also be described by their stabilizer. We have see that the stabilizer of the 3-qubit code is* $\langle Z_1Z_2, Z_2Z_3\rangle$ *and that the stabilizer of Shor's 9-qubit code is*

$$\langle Z_1Z_2, Z_2Z_3, Z_4Z_5, Z_5Z_6, Z_7Z_8, Z_8Z_9, X_1X_2X_3X_4X_5X_6, X_4X_5X_6X_7X_8X_9\rangle.$$

It is straightforward to check that these groups are Abelian. As expected, these stabilizers admit respectively $2 = 3 - 1$ *(three physical qubits and one logical qubit) and* $8 = 9 - 1$ *(9 physical qubits for a single logical qubit) elements.*
The Pauli operators Z_1 *and* $X_1X_2X_3$ *are logical operators for the 3-qubit code and for Shor's 9-qubit code, respectively:*

$$\begin{aligned} \textit{3-qubit code}: & Z_1|\bar{+}\rangle = |\bar{-}\rangle \\ \textit{Shor's code}: & X_1X_2X_3|\bar{1}\rangle = -|\bar{1}\rangle. \end{aligned}$$

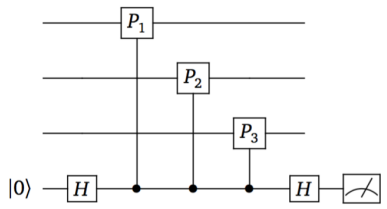
The stabilizer description is particularly useful to correct the errors. The idea is to measure the *syndrome*, that is to measure the eigenvalues of the stabilizer generators for the quantum state. The syndrome associated with error $E \in \mathcal{P}_n$ is the $(n-k)$-bitstring $\vec{s} = (s_1, \ldots, s_{n-k})$ defined by

$$s_i = \begin{cases} 0 & \text{if} \quad [E, g_i] = 0, \\ 1 & \text{if} \quad \{E, g_i\} = 0. \end{cases}$$

If $s_i = 1$, meaning that the error anticommutes with a stabilizer, then $E|\psi\rangle$ is a -1 eigenvalue of g_i (if $|\psi\rangle$ is a valid codeword):

$$g_iE|\psi\rangle = -Eg_i|\psi\rangle = -E|\psi\rangle.$$

In particular, the syndrome doesn't depend on the specific codeword, only on the Pauli error.
Note that it is easy to devise a quantum circuit to measure any Pauli operator (and in particular, any generator of the stabilizer group). The following picture for instance depicts a circuit to measure $P_1P_2P_3$ with Pauli operator P_i acting on qubit i:



The eigenvalues of any Pauli measurement P are 1 and -1, and the projector on the eigenspaces are $P_\pm = \frac{1}{2}(\mathbb{1} \pm P)$.

Definition 7 (Minimum distance)**.** *The* minimum distance *of a stabilizer code with stabilizer S is the minimum weight of a nontrivial logical operator:*

$$\begin{aligned} d_{\min}(\mathcal{Q}) &= \min\{|E| \ : \ [E, g_i] = 0 \forall i, E \notin \langle g_1, \ldots, g_{n-k} \rangle\} \\ &= \min\{|E| \ : \ E \in N(S) \setminus S\}. \end{aligned}$$

Example 8. *We have seen in the previous example that Z_1 and $X_1X_2X_3$ are logical errors for both the 3-qubit code and Shor's 9-qubit code, respectively. This implies that their respective minimum distances are upper bounded by 1 and 3. Since the 9-qubit code can correct any single-qubit error, its minimum distance is at least 3, which means that it is exactly 3.*

Coding scenario. Action of the environment

A coding scheme is as follows:

- the initial message is a k-qubit quantum state $|\psi\rangle \in (\mathbb{C}^2)^{\otimes k}$,
- it is mapped to an n-qubit state by applying an encoding operator $\mathcal{U}$ applied to $|\psi\rangle \otimes |0\rangle^{n-k}$ (i.e., state and ancilla)
- the n-qubit state goes through a noisy channel (communication channel, storage device, interaction with environment, etc) corresponding to a *completely positive trace preserving map* (cptp) $\mathcal{N}$. Alternatively, the channel is a unitary interaction between the codeword and the environment (assumed to be pure).
- a decoder with access to the output of the channel measures the syndrome of the error, outputs a guess for the error, and returns $|\hat{\psi}\rangle$ for the initial state

An important difference with classical coding is that in the quantum case, the "error" is not uniquely defined, and errors differing by an element of the stabilizer group are *equivalent*, since they act exactly in the same way on all codewords. This phenomenon is called *degeneracy*. For this reason, a quantum error correction procedure will generally not aim at recovering the "true" error that occurred, but rather the equivalence class of this error. This subtle difference with the classical scenario will lead to severe complications when devising efficient decoding algorithms.

An alternative description of the noisy channel is as an interaction with the environment. One starts with some pure product states of 3 registers: data, ancilla, environment, modeled as a quantum space $D \otimes A \otimes E$. The initial state has the form $|\psi\rangle_D \otimes |0\rangle_A \otimes |0\rangle_E$, where $|0\rangle_E$ is unknown (but that doesn't matter). The encoding corresponds to acting on D and A via the encoding map U. The new state is

$$(U_{DA} \otimes \mathbb{1}_E)|\psi\rangle_D \otimes |0\rangle_A \otimes |0\rangle_E = |\bar{\psi}\rangle_{DA} \otimes |0\rangle_E.$$

The quantum channel is modeled as a unitary interaction V with the environment:

$$V|\bar{\psi}\rangle_{DA} \otimes |\phi\rangle_E = \sum_{P_i \in \mathcal{P}_n} P_i|\bar{\psi}\rangle_{DA} \otimes |e_{P_i}\rangle_E$$

where the states $|e_{P_i}\rangle$ are not necessarily normalized nor orthogonal. The quantum channel entangles the three registers. The decoding process acts on D and A, with the goal of returning the original state in D and an entangled state in AE. In thermodynamical terms, the data data is cooled down (returns to being pure) while ancilla is heated up.

b) CSS codes

The CSS codes (for the name of their inventors, Calderbank, Shor, Steane) form an interesting subclass of all stabilizer codes where the generators of the stabilizer group are either products of Pauli-X or products of Pauli-Z. This is an appealing restriction because the commutativity condition between the generators now needs to be checked only between X-type and Z-type generators, since both X-type generators and Z-type generators obviously commute among themselves. In that case, both types of generators are described by binary words (with 1s at the coordinates corresponding to an X or Z-type operator).

A general way of defining both classes of generators is by choosing special types of classical codes. Let $\mathcal{C}$ be an $[n,k]$ classical linear code with a $n \times k$ generator matrix G and an $(n-k) \times n$ parity-check matrix H. This means

$$\mathcal{C} = \{Gy \ : \ y \in \mathbb{F}_2^k\} = \ker H.$$

Here we consider column vectors.
The *dual code* of $\mathcal{C}$, denoted $\mathcal{C}^\perp$, is defined as

$$\mathcal{C}^\perp = \{y \in \mathbb{Z}_2^n \ : \ x \cdot y = 0, \forall x \in \mathcal{C}\}.$$

This is an $[n, n-k]$ linear code. Moreover the generator and parity-check matrices of $\mathcal{C}$ and $\mathcal{C}^\perp$ are swapped (up to transposition):

$$G^\perp = H^T, \quad H^\perp = G^T.$$

We say that a code $\mathcal{C}$ is *weakly self-dual* if $\mathcal{C} \subseteq \mathcal{C}^\perp$ and *(strictly) self-dual* if $\mathcal{C} = \mathcal{C}^\perp$. A necessary and sufficient condition for $\mathcal{C}$ to be weakly self-dual is that $G^T G = 0$.

Definition 9. *A* CSS code $\mathrm{CSS}(\mathcal{C}_1, \mathcal{C}_2)$ *is defined from two classical linear codes* $\mathcal{C}_1$, $\mathcal{C}_2$ *of parameters* $[n, k_1]$ *and* $[n, k_2]$, *such that* $\mathcal{C}_2 \subseteq \mathcal{C}_1$. *The quantum code has parameters* $[[n, k_1 - k_2]]$ *and is spanned by the vectors*

$$|x_j + \mathcal{C}_2\rangle := \frac{1}{2^{k_2/2}} \sum_{y \in \mathcal{C}_2} |x_j + y\rangle,$$

where the elements of $\{x_j\}_{j=1\ldots 2^{k_1-k_2}}$ *belong to the quotient* $\mathcal{C}_1/\mathcal{C}_2$. *In other words, they satisfy* $x_i + x_j \notin \mathcal{C}_2$, *for any pair* $x_i \neq x_j$.

Lemma 10. *The code* $\mathrm{CSS}(\mathcal{C}_1, \mathcal{C}_2)$ *is a stabilizer code.*

The proof will be treated in exercise.
In particular, if $\mathcal{C}$ is weakly self-dual with parameters $[n,k]$, then $\mathrm{CSS}(\mathcal{C}^\perp, \mathcal{C})$ is a stabilizer code with parameters

$$[[n, n-2k]].$$

Codewords of the CSS code have the form $|x + \mathcal{C}_2\rangle$ where $x \in \mathcal{C}_1$ and two codewords $|x + \mathcal{C}_2\rangle$ and $|x' + \mathcal{C}_2\rangle$ differ if and only if x and x' belong to different cosets of $\mathcal{C}_2$ in $\mathcal{C}_1$.

An example of CSS code is Steane's 7-qubit code, where we take $\mathcal{C}_2 = \mathcal{C}_1^\perp$ and $\mathcal{C}_1$ to be the $[7, 4]$ Hamming code with generator[1] and parity-check matrices

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}, \quad H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

One can construct general Hamming codes by taking all possible words (except the all-zero word) for the columns of the parity-check matrix. These generalized codes have parameters $[2^m - 1, 2^m - m - 1, 3]$ and can tolerate one bit-flip since they all have distance 3. One can check that the dual of the Hamming code is weakly self-dual, since $(G^\perp)^T G^\perp = HH^T = 0$, and therefore $\mathrm{CSS}(\mathcal{C}_1, \mathcal{C}_1^\perp)$ is a valid CSS code encoding $4-3 = 1$ logical qubit. Taking $x_0 = 0000000$ and $x_1 = 1111111$ as representatives of $\mathcal{C}_1/\mathcal{C}_1^\perp$, and enumerating the elements of $\mathcal{C}_1^\perp = \mathrm{Im}(H)$ as

$$\mathcal{C}_1^\perp = \{0000000, 0001111, 0110011, 0111100, 1010101, 1011010, 1100110, 1101001\},$$

we obtain the logical qubits as

$$\begin{aligned} |\bar{0}\rangle = \frac{1}{2\sqrt{2}}(&|0000000\rangle + |0001111\rangle + |0110011\rangle + |0111100\rangle + |1010101\rangle \\ &+ |1011010\rangle + |1100110\rangle + |1101001\rangle, \\ |\bar{1}\rangle = \frac{1}{2\sqrt{2}}(&|1111111\rangle + |1110000\rangle + |1001100\rangle + |1000011\rangle + |0101010\rangle \\ &+ |0100101\rangle + |0011001\rangle + |00101101\rangle. \end{aligned}$$

This illustrates one of the main strengths of the stabilizer formalism: in general, the logical qubits are given by very long expressions (a superposition over an exponential number of basis states), and the generators of the stabilizer yield a much more efficient description of the code.

The generators of the stabilizer can be chosen to be the rows of H_1 for X-type generators and the rows of $H_2^\perp = H_1$ for Z-type generators:

$$\begin{aligned} &X_4X_5X_6X_7, \\ &X_2X_3X_6X_7, \\ &X_1X_3X_5X_7, \\ &Z_4Z_5Z_6Z_7, \\ &Z_2Z_3Z_6Z_7, \\ &Z1Z_3Z_5Z_7. \end{aligned}$$

Lemma 11. *The minimum distance of a CSS code* $\mathrm{CSS}(\mathcal{C}_1, \mathcal{C}_2)$ *is* $\min(d(\mathcal{C}_1), d(\mathcal{C}_2^\perp))$.

[1]Here, we take the convention that the image of G is the right image, i.e., $\mathrm{Im}(G) = \{Gx : x \in \mathbb{Z}_2^4\}$.

This implies that Steane's 7-qubit code is a $[[7, 1, 3]]$ quantum code.
We prove the lemma by describing an explicit error correction strategy for a CSS code.

Error correction for a CSS code.

The general strategy is as usual: measure the syndrome and apply a correction. For CSS codes, the syndrome is naturally divided into two parts: X-type errors are corrected with the syndrome of the Z-type generators, and Z-type errors are corrected with the syndrome of the X-type generators. This suggests a two-part procedure:

- **X-type errors:** (i) compute the syndrome for code $\mathcal{C}_1$ (i.e. for generators of the form Z^f for f a row of H_1): this is the reversible operation

$$|y\rangle|0\dots0\rangle \mapsto |y\rangle|s_1(y)\rangle,$$

  with $s_1(y) = H_1 y$, the syndrome of y with respect to code $\mathcal{C}_1$; (ii) measure the syndrome, and (iii) correct for bit-flips by applying Pauli-X corrections;

- **swapping between codes:** apply a Hadamard transform to every qubit;

- **Z-type errors:** same procedure as before but for the code $\mathcal{C}_2^\perp$, i.e. generators of the form X^e for e a row of $H_2^\perp$;

- **returning to the initial code:** apply again a Hadamard transform to every qubit.

Let us verify that this decoding procedure correctly recovers the codeword provided that the weight of the error is less than t, where t is the maximum number such that both $\mathcal{C}_1$ and $\mathcal{C}_2^T$ can tolerate t errors[2].
Consider a Pauli error $X^v Z^w$ with bit strings $v, w \in \{0,1\}^n$ applied to a codeword $\sum_j \alpha_j |x_j + \mathcal{C}_2\rangle$. The state becomes

$$X^v Z^w \sum_j \alpha_j |x_j + \mathcal{C}_2\rangle = \sum_j \alpha_j (-1)^{v\cdot w} Z^w |x_j + v + \mathcal{C}_2\rangle$$

where we used that $X^v Z^w = (-1)^{v\cdot w} Z^w X^v$.
The first step of the correction procedure corrects X-type errors by computing the syndrome relative to $\mathcal{C}_1$. This will yield the syndrome of v for $\mathcal{C}_1$, and provided that $|v| \leqslant t$, the procedure will return v and apply the Pauli correction X^v, giving,

$$\sum_j \alpha_j (-1)^{v\cdot w} X^v Z^w |x_j + v + \mathcal{C}_2\rangle = Z^w \sum_j \alpha_j |x_j + \mathcal{C}_2\rangle.$$

[2]The parameter t is related to the minimum distance via $d = 2t + 1$.

After the Hadamard transformation, the state becomes

$$\begin{aligned} H^{\otimes n} Z^w \sum_j \alpha_j |x_j + \mathcal{C}_2\rangle &= X^w H^{\otimes n} \sum_j \alpha_j |x_j + \mathcal{C}_2\rangle && \text{(since } H^{\otimes n} Z^w = X^w H^{\otimes n}\text{)} \\ &= \sum_j \alpha_j X^w H^{\otimes n} X^{x_j} |\mathcal{C}_2\rangle \\ &= \sum_j \alpha_j X^w H^{\otimes n} X^{x_j} H^{\otimes n} |\mathcal{C}_2^\perp\rangle && \text{(proven in exercise)} \\ &= \sum_j \alpha_j X^w Z^{x_j} |\mathcal{C}_2^\perp\rangle. \end{aligned}$$

Using the same argument as before, one can compute the syndrome relative to $\mathcal{C}_2^\perp$ and correct the X-type error. This will work correctly provided that $|w| \leqslant t$, where t is a lower bound on the correction capacity of $\mathcal{C}_2^\perp$. Undoing the Hadamard transform then returns the original codeword.

Gilbert-Varshamov bound. The first bound guarantees the existence of good quantum codes, such that both the number of logical qubits and the minimum distance are linear in n.

Theorem 12 (Gilbert-Varshamov)**.** *There exist CSS codes $[[n, k, d]]$ with rate $R = k/n$ satisfying*

$$R \geqslant 1 - 2h\left(\frac{d}{n}\right),$$

where $h(x) = -x \log_2 x - (1-x)\log_2(1-x)$ is the binary entropy.

Proof. The proof strategy is a counting argument. Once we fix a code, it is always possible to apply a random linear transformation to it to get another code. In particular, this shows that any vector is equally likely to belong to a random code. Let us therefore use the union bound to bound the probability that a random code of dimension k contains a nonzero word of weight less than d:

$$\begin{aligned} \mathbb{P}(\text{code of dim } k \text{ with word of weight } \leqslant d) &\leqslant (\text{number of words}) \times (\text{word has weight } \leqslant d) \\ &\leqslant 2^k \frac{\sum_{i=0}^{d} \binom{n}{i}}{2^n} \\ &\approx 2^k 2^{nh\left(\frac{d}{n}\right)} 2^{-n} \\ &\approx 2^{n\left(\frac{k}{n} - 1 + h\left(\frac{d}{n}\right)\right)}. \end{aligned}$$

In particular, if $\frac{k}{n} \geqslant 1 - 2h\left(\frac{d}{n}\right)$, then this probability is strictly less than 1. □