Channel

A communication channel is a system in which the output depends probabilistically on its input.

It is characterized by a probability transition matrix that determines the conditional distribution of the output given the input.

- Choose a "non-confusable" subset of input sequences so that with high probability, there is only one highly likely input that could have caused the particular output.

For a communication channel with input $X$ and output $Y$, the channel capacity $C$ is defined as

$$ C = \max_{p(x)} I(X;Y) $$

Eg 5: Binary Erasure Channel

Instead some bits are incorrectly transferred, this kind of channel loses bits – a fraction $\alpha$ of the bits are erased.

The receiver knows which bits have been erased.
Symmetric Channels

- **Symmetric channel**
  - The rows of the channel transition matrix \( p(y|x) \) are permutations of each other.
  - The columns are permutations of each other as well.

- **Weakly symmetric**
  - Every row of the transition matrix is a permutation of every other row.
  - All the column sums are equal.

\[
\begin{pmatrix}
0.3 & 0.2 & 0.5 \\
0.5 & 0.3 & 0.2 \\
0.2 & 0.5 & 0.3
\end{pmatrix}
\]

\[
\begin{pmatrix}
1/3 & 1/6 & 1/2 \\
1/3 & 1/2 & 1/6
\end{pmatrix}
\]

Channel Coding Theorem (Shannon’s Second Theorem)

- For large block lengths, every channel looks like the noisy typewriter channel.
- The channel has a subset of inputs that produce essentially disjoint sequences at the output.
- For each input \( n \)-sequence, there are approximately \( 2^{nH(Y|X)} \) possible \( Y \) sequences, all of them are equally likely.
- The total number of \( Y \) sequences is \( 2^nH(Y) \).
- The total number of disjoint sets we can send is less than or equal to \( 2^{nH(Y)}/2^{nH(Y|X)} = 2^{nH(X:Y)} \).

The Channel Coding Theorem

- All rates below capacity \( C \) are achievable. Specifically, for every rate \( R < C \), there exists a sequence of \( (2^nR, n) \) codes with maximum probability of error \( \lambda^{(n)} \to 0 \).
- Conversely, any sequence of \( (2^nR, n) \) codes with \( \lambda^{(n)} \to 0 \) must have \( R \leq C \).
The Search for Simple Good Code

- The channel coding theorem promises the existence of block codes that will allow us to transmit information at rates below capacity with an arbitrarily small probability of error if the block length is large enough.
- The search for this kind of code that is simple and easy to encode and decode.

A Communication Channel

![Diagram of a communication channel](image)

Different Coding Schemes

- The objective of coding is to introduce redundancy so that even if some of the information is lost or corrupted, it will still be possible to recover the message at the receiver.
- Options
  - Block codes
    - Map a block of information bits onto a channel codeword and there is no dependence on past information bits
    - Repetition code
      - The rate of the code goes to zero when longer repetition codes are used
  - Parity check code (error detecting code)
    - Combine the bits in some intelligent fashion so that each extra bit checks whether there is an error in some subset of the information bits
  - Convolutional codes
    - Each output block depends not only on the current input block, but also on some of the past inputs as well.
Hamming Codes (1)

- Construction of parity check matrix (H)
  - $l$ rows
  - Block length $n=2^l-1$ (non-zero binary vectors of length $l$)

\[
H = \begin{bmatrix}
0 & 0 & 0 & 1 & 1 & 1 \\
0 & 1 & 1 & 0 & 0 & 1 \\
1 & 0 & 1 & 0 & 1 & 0
\end{bmatrix}
\]

Hamming Codes (2)

- Find the codewords
  - The set of vectors of length $n$ in the null space of $H$
  - Number of codewords $2^{n-l}$
    - Rank of $H (l)$
    - Dimension of the null space ($n-l$)
  - The set of codewords is linear since
    - The sum of any two codewords is also a codeword
    - The difference between any codewords is also a codeword
  - Minimum weight of the code
    - The minimum number of 1's in any codeword
  - Minimum distance of the code
    - The minimum number of places where two codewords differ

Example – the (7,4) Hamming Code

\[
\begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & 1 & 1 & 0 & 1 & 1 & 1 \\
0 & 1 & 1 & 1 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 1 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 & 1 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 \\
1 & 0 & 1 & 0 & 1 & 0 & 1
\end{bmatrix}
\]
Hamming Codes (3)

- Decoding and error correction
  \[ r = c + \epsilon \]
  \[ Hr = Hc + He \]
- \( He_i \) is a vector corresponding to the ith column of H.
- We can find which position of the received vector was corrupted. Reversing the bit will give us a codeword
- Systematic code:
  - Use the first \( k = 2^l - l - 1 \) bits in each codeword to represent the message, and the last \( n-k \) bits are parity check bits.
- In the example, we have a (7,4,3) Hamming code

The Challenge

- No codes so far can meet the bounds suggested by Shannon’s channel capacity theorem.
- For a binary symmetric channel with crossover probability \( p \), we need a code that could correct up to \( np \) errors in a block of length \( n \) and have \( n(1-H(p)) \) information bits.