ECE 447 Fall 2025

Lesson 37

Error Correction: Parity, CRC, and Hamming Codes

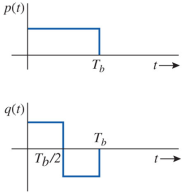
UNITED STATES AIR FORCE ACADEMY

Schedule and Admin

- Schedule.
  - Lesson 37 - Error correction
  - Lesson 38 - MATLAB Lab 7: Matched filters, multi-path, OFDM, BER (workday - no attendance for class)
  - Lesson 39 - Advanced topics: OFDM, MIMO, CDMA
  - Lesson 40 - Course review
- Admin
  - **HW8**. Due 02 Dec (Lsn 39) to Gradescope.

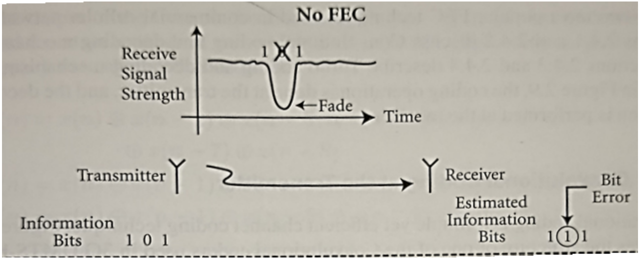
REVIEW

- Example problem: Find the BER for a system using **polar signaling** pulses $\pm 3p(t)$ with $T_b = 1\mu s$ and $N_0 = \frac{25\mu W}{Hz}$.



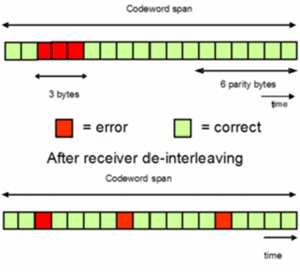
ERROR CORRECTION

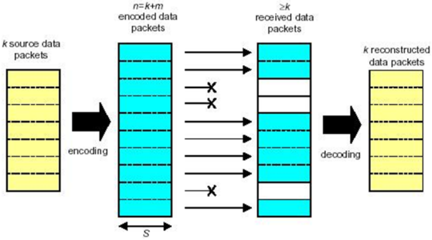
- Bit errors occur for a variety of reasons, but can correct many by pre-processing bits at the transmitter - **forward error correction (FEC)**
- "Error correction coding requires a strong mathematical background" - so true!
- Types of codes (in order of complexity): repetition, block, convolutional, Viterbi algorithm, turbo, low-density parity check (LDPC), polar



Interleaving

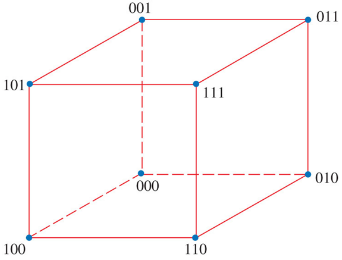
- First, though - errors often consecutive in time and/or frequency
- Interleaving spreads out code symbol errors at receiver - decoder receives few to zero consecutive errors
- Synchronization required!





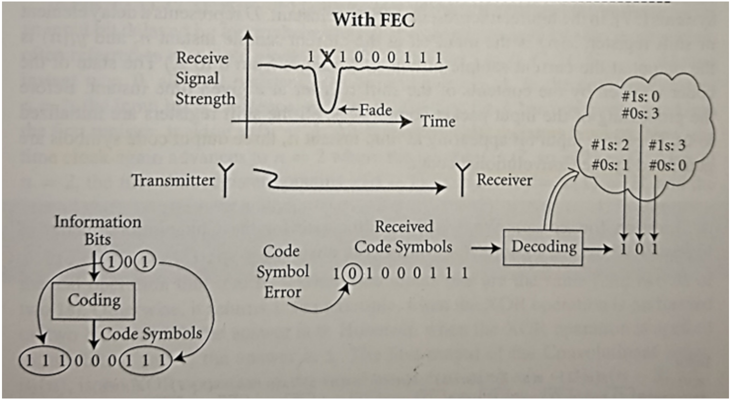
Error Correction Basics and Terminology

- **Code rate:** ratio of data bits k to total bits n - creates an (n, k) code
- $\boldsymbol{d}$ is bit vector **message** (data)
- $\boldsymbol{c}$ is bit vector **codeword**
- Number of redundant (aka check aka parity) bits is $m = n - k$
- **Hamming distance:** number of bits that are different between two bit vectors
- **Hamming space:** multi-dimensional cube; spheres drawn around possible codeword vertices - the radius spheres can have without overlapping equals the number of errors that can be corrected
- To *correct* t errors, min Hamming distance $d_{min} = 2t + 1$
- To *detect* t errors, min Hamming distance $d_{min} = t + 1$



Repetition Code

- Repeat each bit a certain number of times, then transmit
- To decode at receiver, use a simple majority rule



HAMMING CODE

- Type of linear block code
- $\boldsymbol{c} = \boldsymbol{dG}$, where $\boldsymbol{G}$ is called the **generator matrix**
- We transmit $\boldsymbol{c}$ and receive $\boldsymbol{r}$, which may have errors
- $\boldsymbol{s} = \boldsymbol{rH}^T$ is called the **syndrome**, where $\boldsymbol{H}$ is the **parity check matrix**
- The row in $\boldsymbol{H}^T$ that matches $\boldsymbol{s}$ is the bit of the codeword in error - flip that bit
- If $\boldsymbol{s} = \boldsymbol{0}$, then no errors
- **Coding gain:** reduction in req'd SNR to achieve specific BER

WHAT DO WE "GAIN"?

- **Coding gain:** reduction in req'd SNR to achieve specific BER