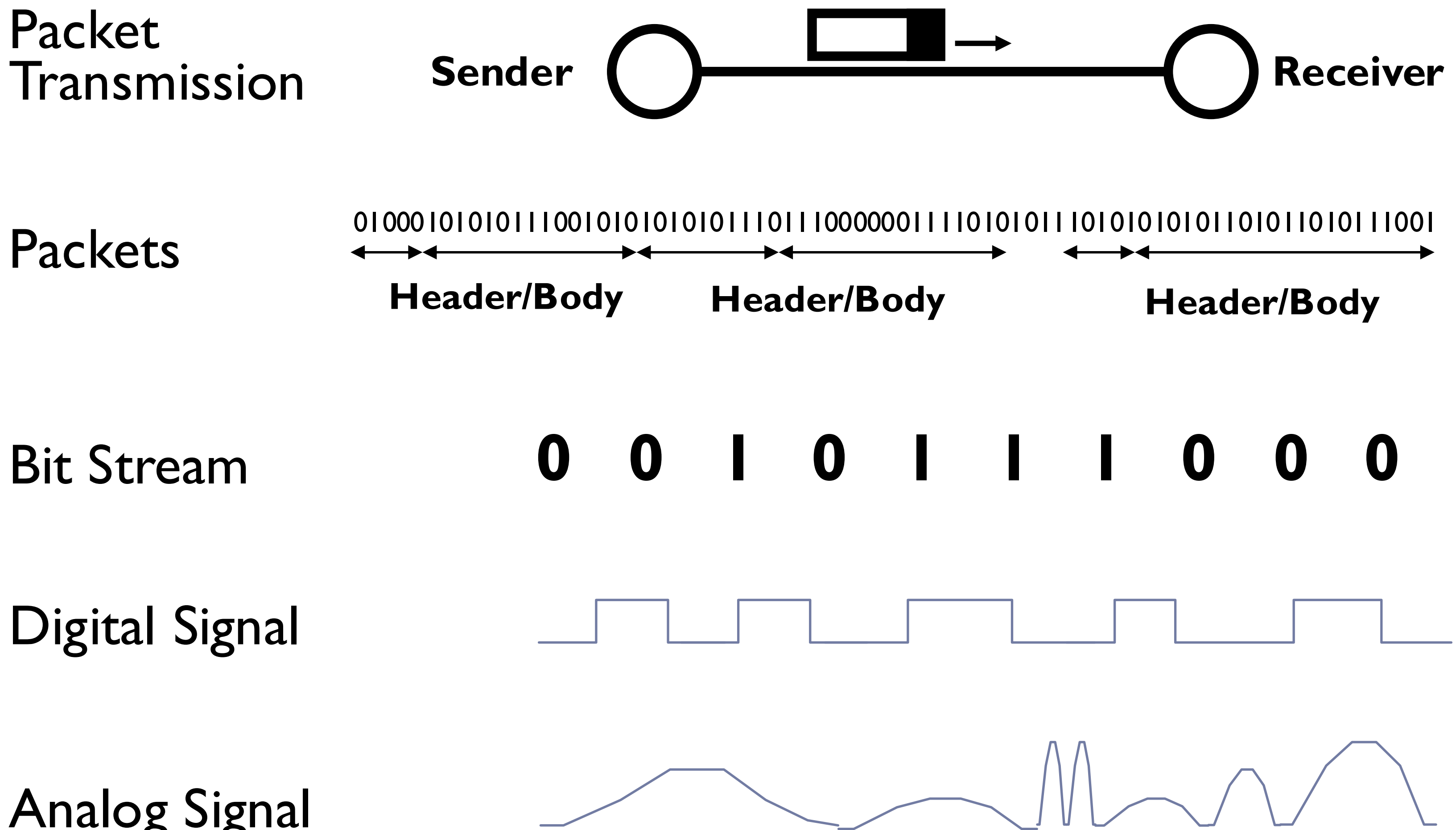
CS/ECE 439: Wireless Networking

Physical Layer – Coding and Modulation

 Fall 2026

From Signals to Packets

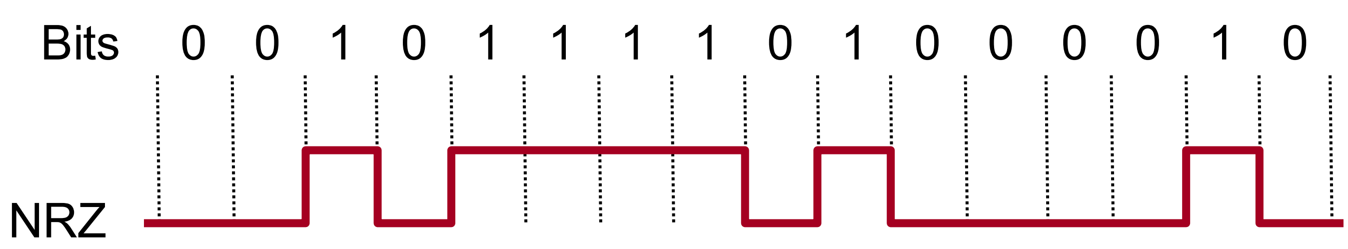


Binary Voltage Encoding

- Common binary voltage encodings
  - Non-return to zero (NRZ)
  - NRZ inverted (NRZI)
  - Manchester (used by IEEE 802.3—10 Mbps Ethernet)
  - 4B/5B

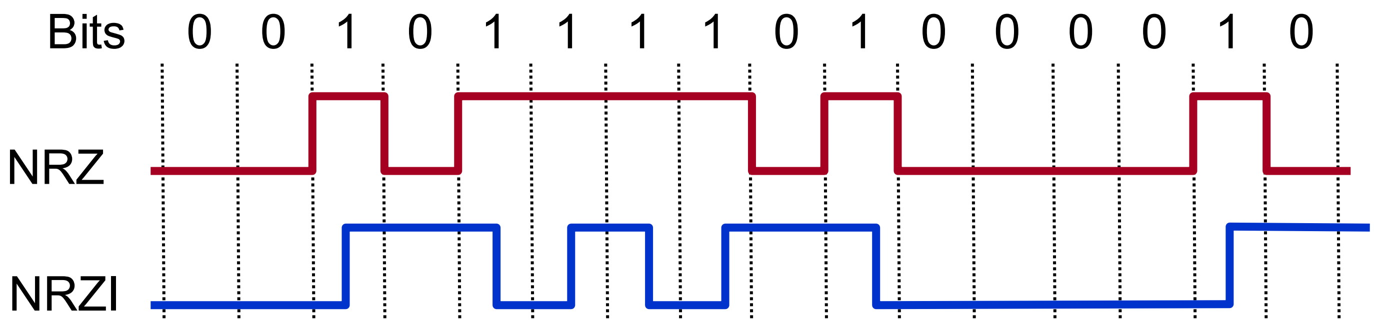
Non-Return to Zero (NRZ)

- Signal to Data
  - High ⇨ 1
  - Low ⇨ 0
- Comments
  - Transitions maintain clock synchronization
  - Long strings of 0s confused with no signal
  - Long strings of 1s causes baseline wander
  - Both inhibit clock recovery



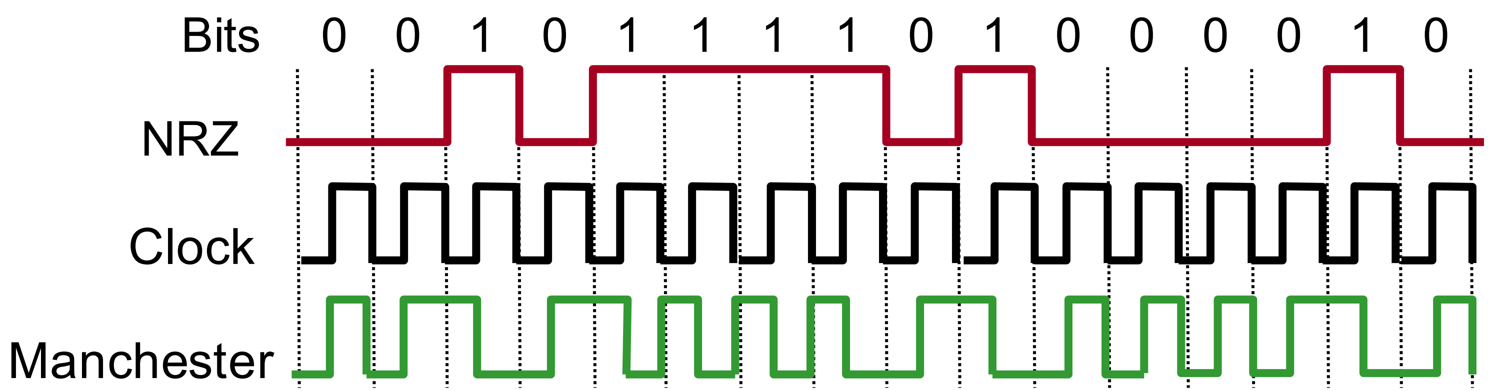
Non-Return to Zero Inverted (NRZI)

- **Signal to Data**
  - Transition ⇨ 1
  - Maintain ⇨ 0
- **Comments**
  - Solves series of 1s, but not 0s



Manchester Encoding

- Signal to Data
  - XOR NRZ data with clock
  - High to low transition ⇨ 1
  - Low to high transition ⇨ 0
- Comments
  - (used by IEEE 802.3—10 Mbps Ethernet)
  - Solves clock recovery problem
  - Only 50% efficient (½ bit per transition)



4B/5B

- Signal to Data
  - Encode every 4 consecutive bits as a 5 bit symbol
- Symbols
  - At most 1 leading 0
  - At most 2 trailing 0s
  - Never more than 3 consecutive 0s
  - Transmit with NRZI
- Comments
  - 16 of 32 possible codes used for data
  - At least two transitions for each code
  - 80% efficient

4B/5B – Data Symbols

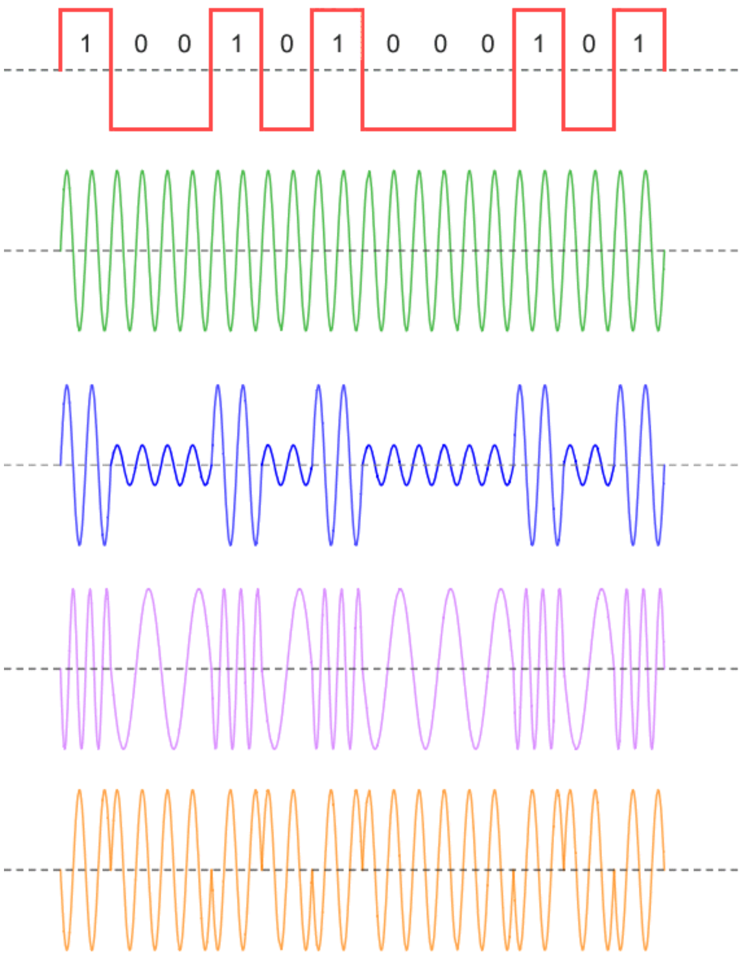
At most 1 leading 0		At most 2 trailing 0s	
0000 ⇒	11110	1000 ⇒	10010
0001 ⇒	01001	1001 ⇒	10011
0010 ⇒	10100	1010 ⇒	10110
0011 ⇒	10101	1011 ⇒	10111
0100 ⇒	01010	1100 ⇒	11010
0101 ⇒	01011	1101 ⇒	11011
0110 ⇒	01110	1110 ⇒	11100
0111 ⇒	01111	1111 ⇒	11101

4B/5B – Control Symbols

- 11111 ⇒ idle
- 11000 ⇒ start of stream 1
- 10001 ⇒ start of stream 2
- 01101 ⇒ end of stream 1
- 00111 ⇒ end of stream 2
- 00100 ⇒ transmit error
- Other ⇒ invalid

Basic Modulation Techniques

- Encode digital data in an analog signal
- Amplitude-shift keying (ASK)
  - Amplitude difference of carrier frequency
- Frequency-shift keying (FSK)
  - Frequency difference near carrier frequency
- Phase-shift keying (PSK)
  - Phase of carrier signal shifted

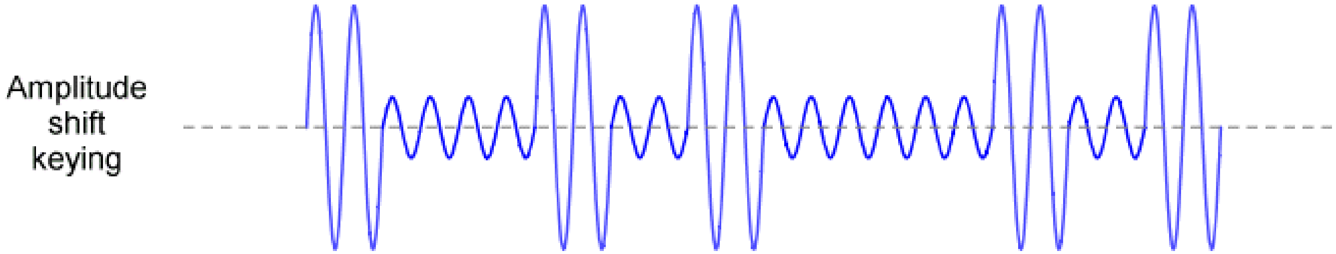


Amplitude-Shift Keying

- Binary digit (1)
  - Represented by presence of carrier, at constant amplitude
- Binary digit (0)
  - Represented by absence of carrier

$$s(t) = \begin{cases} A\cos(2\pi f_c t) & \text{binary } 1 \\ 0 & \text{binary } 0 \end{cases}$$

- where the carrier signal is $A\cos(2\pi f_c t)$



Amplitude-Shift Keying

- Binary digit (1)
  - Represented by presence of carrier, at constant amplitude
- Binary digit (0)
  - Represented by absence of carrier

$$s(t) = \begin{cases} A\cos(2\pi f_c t) & \text{binary } 1 \\ 0 & \text{binary } 0 \end{cases}$$

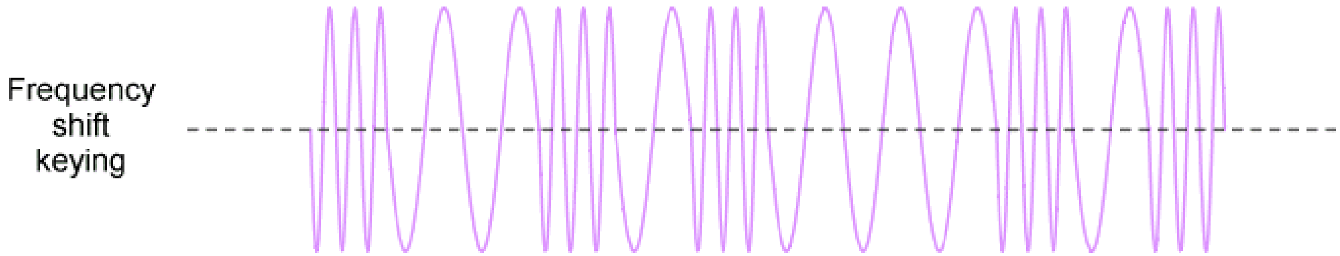
    - where the carrier signal is $A\cos(2\pi f_c t)$
- Inefficiencies
  - Sudden gain changes
  - Only used when bandwidth is not a concern, e.g. on voice lines (< 1200 bps) or on digital fiber

Binary Frequency-Shift Keying (BFSK)

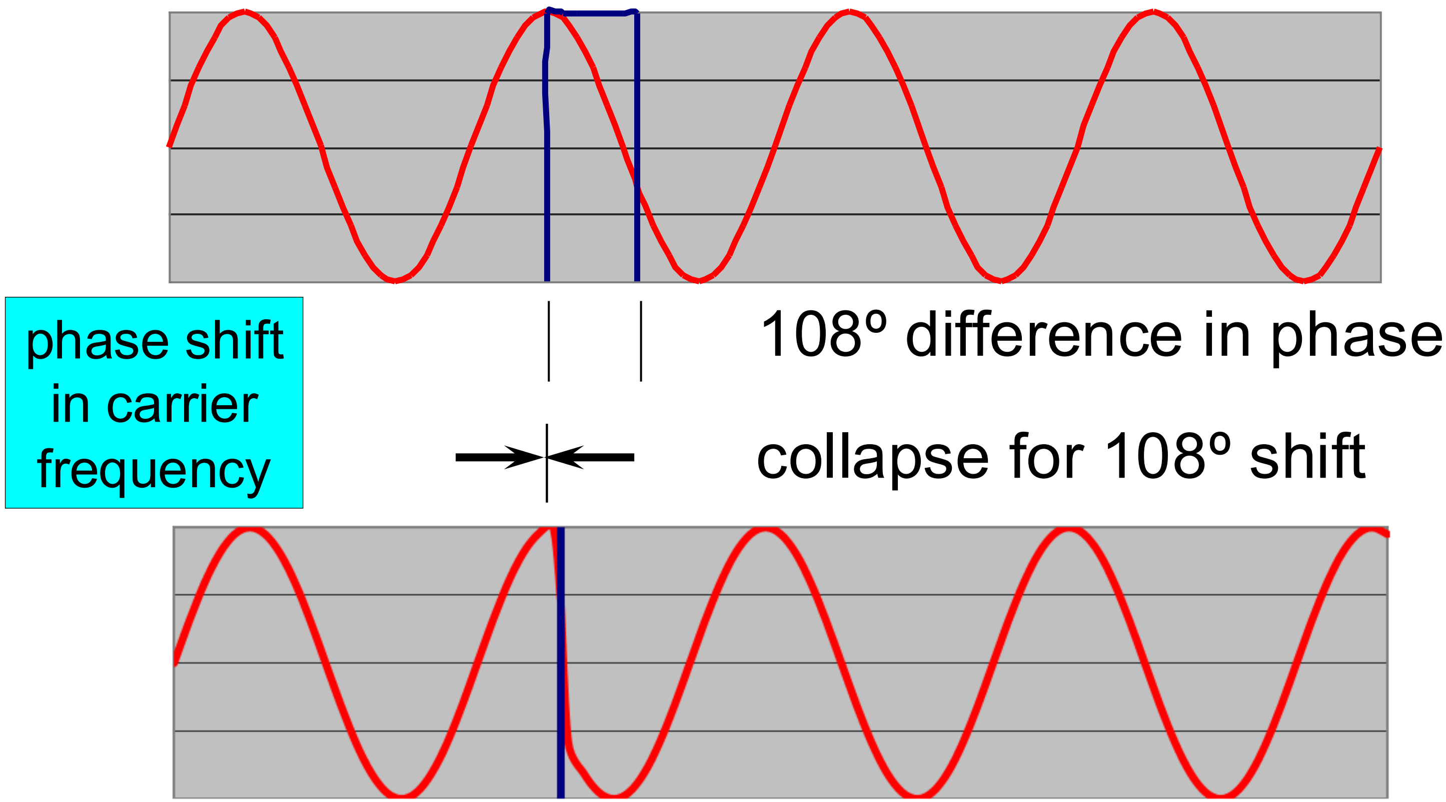
- Binary digits (0 and 1)
  - Represented by two different frequencies near the carrier frequency

$$s(t) = \begin{cases} A\cos(2\pi f_1 t) & \text{binary } 1 \\ A\cos(2\pi f_2 t) & \text{binary } 0 \end{cases}$$

  - where f_1 and f_2 are offset from carrier frequency f_c by equal but opposite amounts



Binary Frequency-Shift Keying (BFSK)



Binary Frequency-Shift Keying (BFSK)

- Binary digits (0 and 1)
  - Represented by two different frequencies near the carrier frequency

$$s(t) = \begin{cases} A\cos(2\pi f_1 t) & \text{binary } 1 \\ A\cos(2\pi f_2 t) & \text{binary } 0 \end{cases}$$

    - where f_1 and f_2 are offset from carrier frequency f_c by equal but opposite amounts
- Less susceptible to error than ASK
- Sometimes used for radio (3 to 30 MHz) or coax
- Demodulator looks for power around f_1 and f_2

Multiple Frequency-Shift Keying (MFSK)

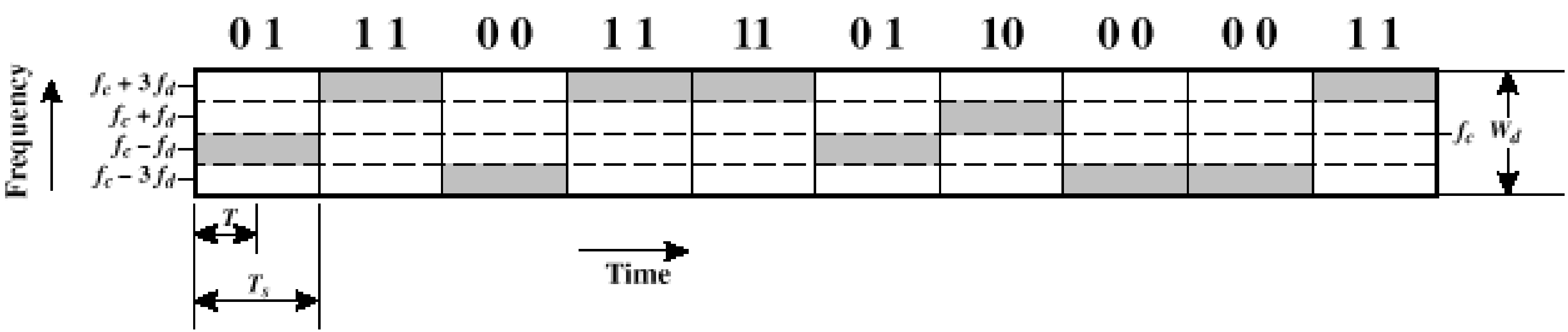
- More than two frequencies are used
  - More bandwidth efficient but more susceptible to error

$$s_i(t) = A\cos 2\pi f_i t \qquad 1 \le i \le M$$

  - $f_i = f_c + (2i - 1 - M)f_d$
  - f_c = the carrier frequency
  - f_d = the difference frequency
  - M = number of different signal elements = 2^L
  - L = number of bits per signal element

Multiple Frequency-Shift Keying (MFSK)

- More than two frequencies are used
  - More bandwidth efficient but more susceptible to error
- Each symbol represents L bits
  - Symbol length is $T_s = LT$ seconds, where T is the bit period



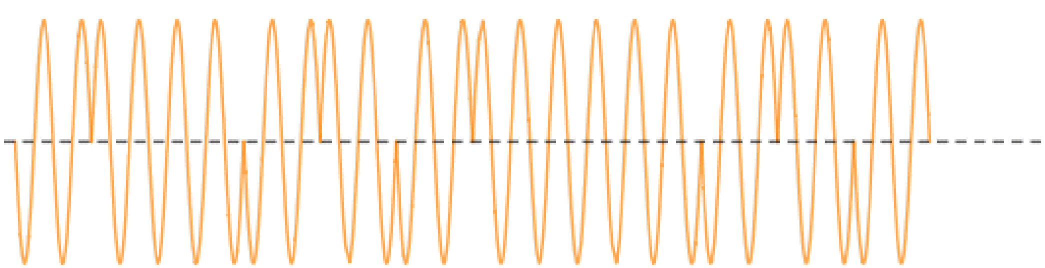
Phase-Shift Keying (PSK)

- Two-level PSK (BPSK)
  - Uses two phases to represent binary digits

$$s(t) = \begin{cases} A\cos(2\pi f_c t) & \text{binary } 1 \\ A\cos(2\pi f_c t + \pi) & \text{binary } 0 \end{cases}$$

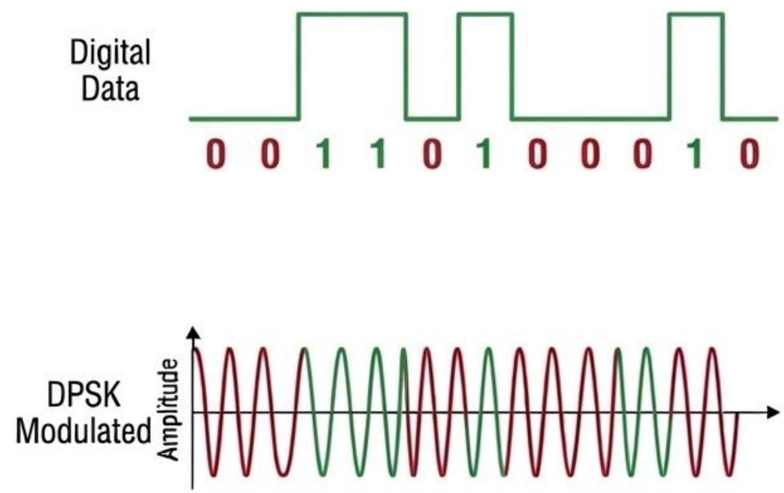
$$= \begin{cases} A\cos(2\pi f_c t) & \text{binary } 1 \\ -A\cos(2\pi f_c t) & \text{binary } 0 \end{cases}$$

Phase shift keying



Phase-Shift Keying (PSK)

- Differential PSK (DPSK)
  - Phase shift with reference to previous bit
    - Binary 0
      - Signal of same phase as previous signal burst
    - Binary 1
      - Signal of opposite phase to previous signal burst



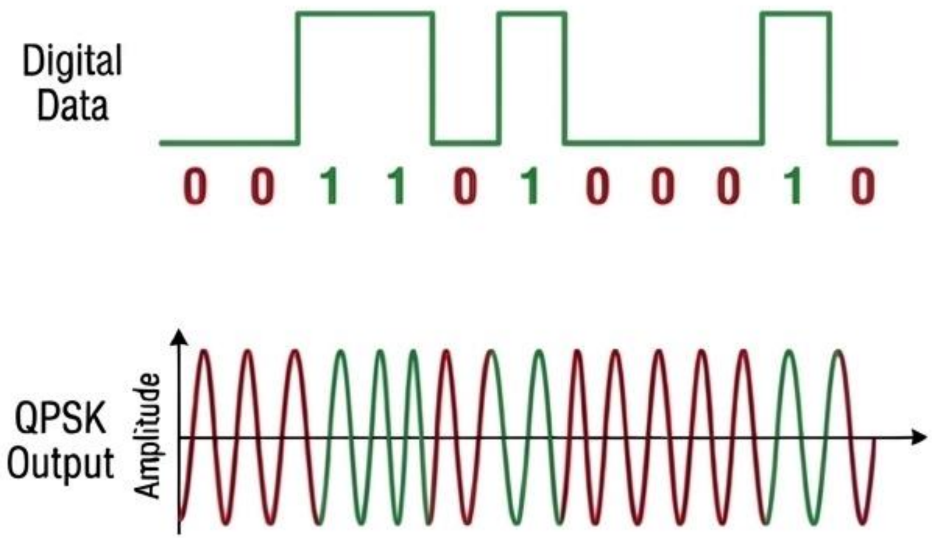
Phase-Shift Keying (PSK)

- Four-level PSK (QPSK)
  - Each element represents more than one bit
  - Ex. Phase shift of multiples of 2π (90°)

$$s(t)=\begin{cases} A\cos\left(2\pi f_c t+\dfrac{\pi}{4}\right) & 11 \\ A\cos\left(2\pi f_c t+\dfrac{3\pi}{4}\right) & 01 \\ A\cos\left(2\pi f_c t-\dfrac{3\pi}{4}\right) & 00 \\ A\cos\left(2\pi f_c t-\dfrac{\pi}{4}\right) & 10 \end{cases}$$

Phase-Shift Keying (PSK)

- Four-level PSK (QPSK)
  - Each element represents more than one bit
  - Ex. Phase shift of multiples of 2π (90°)



Phase-Shift Keying (PSK)

- Multilevel PSK
  - Each angle has more than one amplitude
  - Multiple signals elements

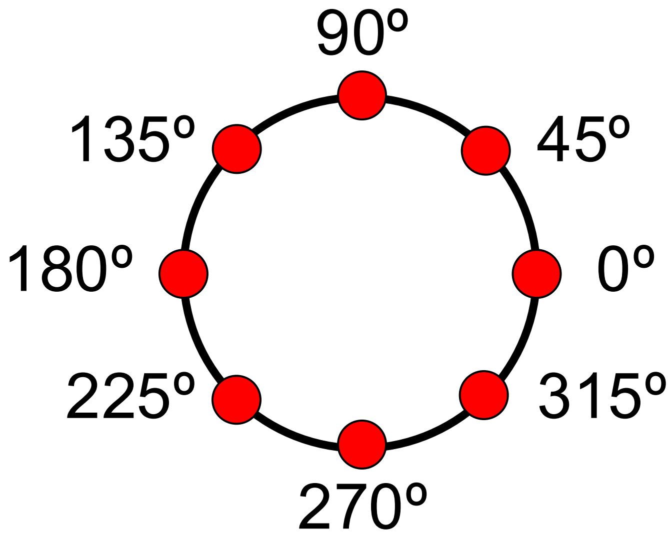
$$D = \frac{R}{L} = \frac{R}{\log_2 M}$$

- D = modulation rate, baud
- R = data rate, bps
- M = number of different signal elements = 2^L
- L = number of bits per signal element

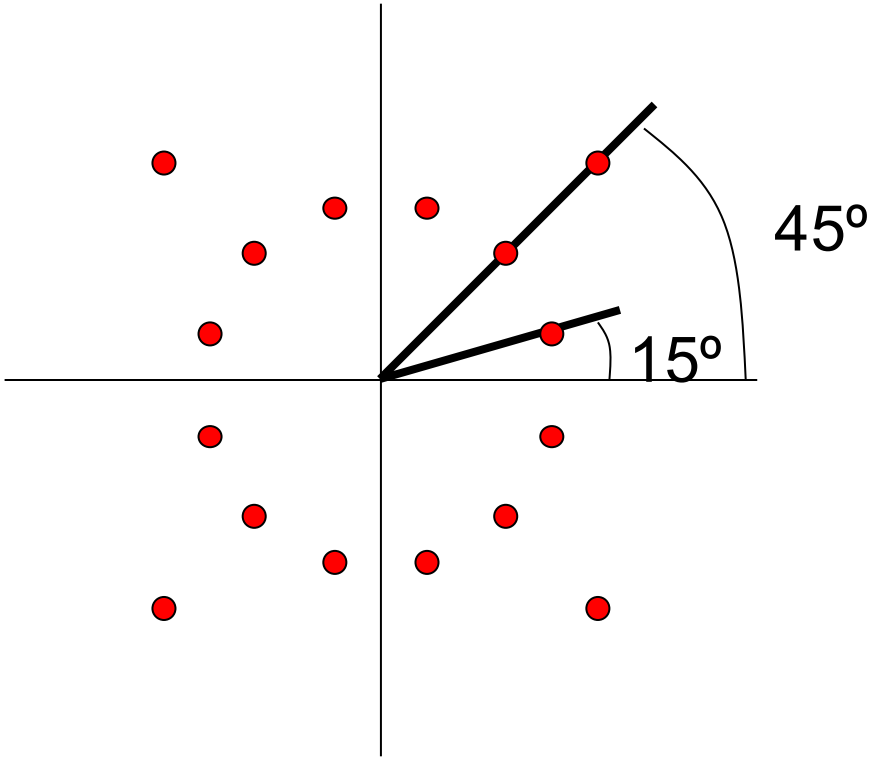
Phase-Shift Keying (PSK)

- Send carrier frequency for one period
  - Perform phase shift
  - Shift value encodes symbol
    - Value in range [0, 360º)
    - Multiple values for multiple symbols
    - Represent as circle

[8-symbol example]



Quadrature Amplitude Modulation (QAM)



16-symbol example

- Uses a combination of amplitude and phase modulation
  - Sends one of N signals each clock cycle
- Each transition represents a symbol
  - Transmission rate = symbols per second
- Each symbol contains multiple bits
  - Ex. 16 QAM: log2 16 = 4 bits
- Points in constellation diagram
  - Chosen to maximize error detection

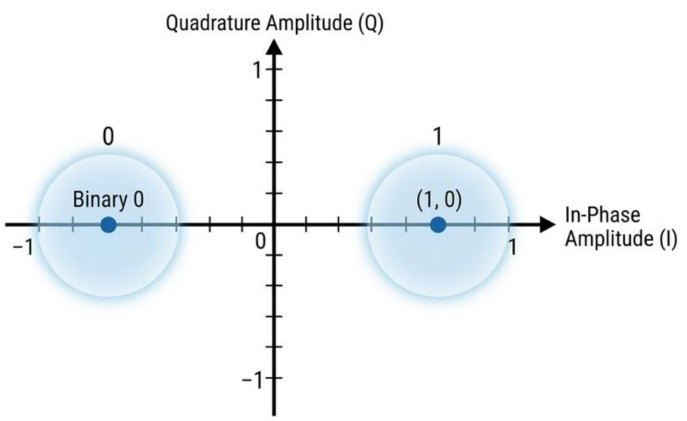
Quadrature Amplitude Modulation (QAM)

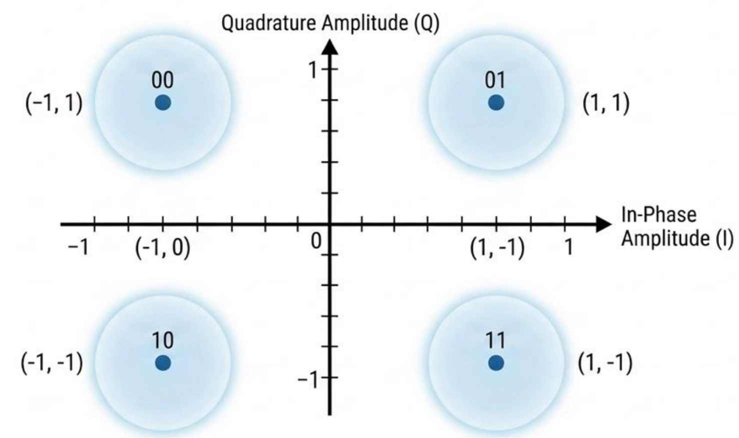
- QAM uses two-dimensional signaling
  - ASK and PSK
  - A_k modulates in-phase $\cos(2\pi f_c t)$
  - B_k modulates quadrature phase $\sin(2\pi f_c t)$

$$s(t) = A_k(t)\cos 2\pi f_c t + B_k(t)\sin 2\pi f_c t$$

Signal Constellations

- Each pair defines a point in the plane
- Signal constellation set of signaling points



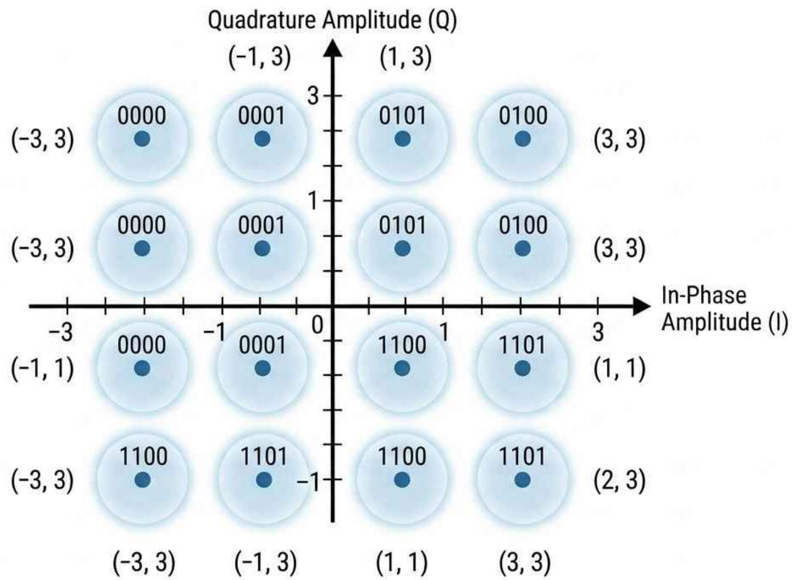


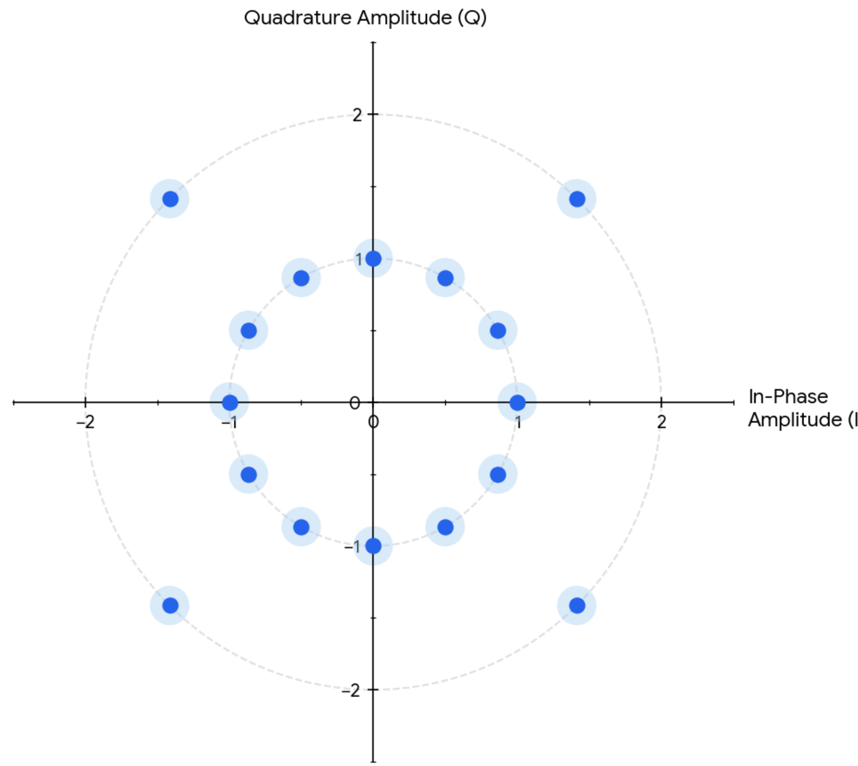
2 possible points per *T* sec.
1 bit / pulse

4 possible points per *T* sec.
2 bits / pulse

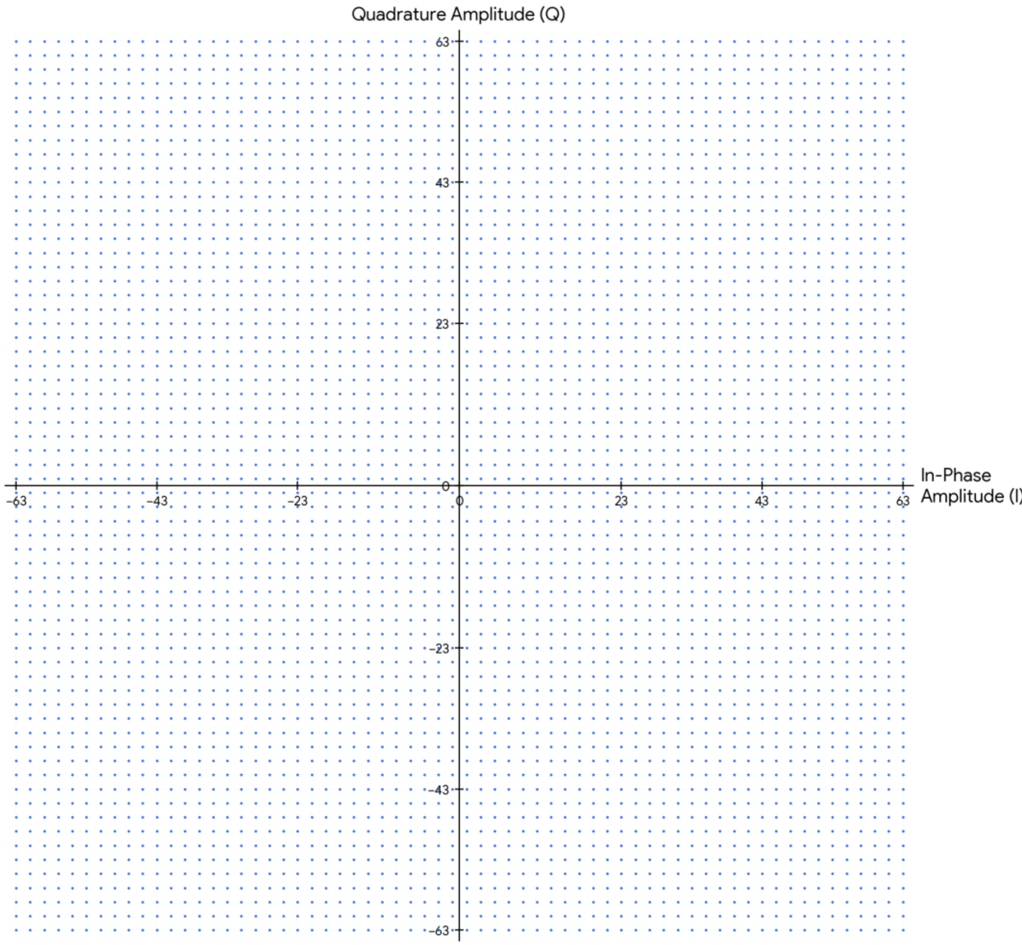
Other Signal Constellations

- Different options for 16 QAM





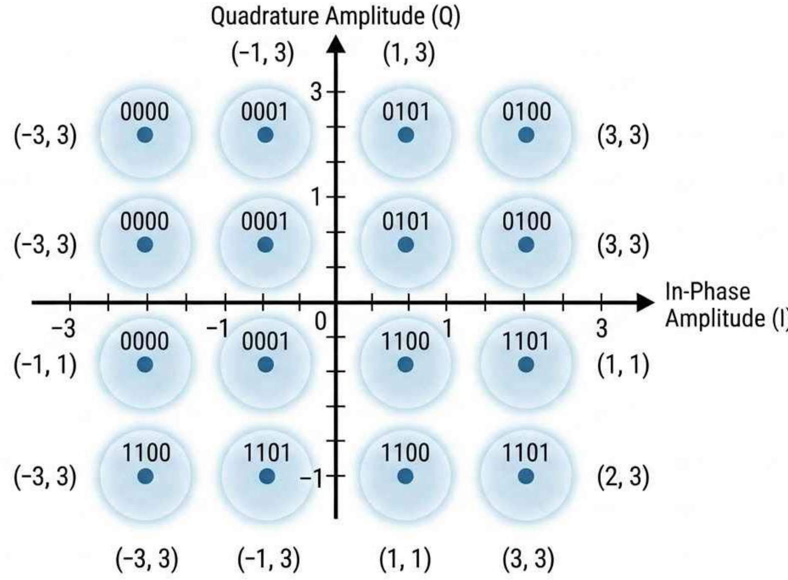
QAM & Wi-Fi Generations



- Wi-Fi 2 & 4 (802.11a & n)
  - Max 64-QAM
  - 6 bits per symbol
- Wi-Fi 5 (802.11ac)
  - Max 256-QAM
  - 8 bits per symbol
- Wi-Fi 6 / 6E (802.11ax)
  - Max 1024-QAM
  - 10 bits per symbol
- Wi-Fi 7 (802.11be)
  - Max 4096-QAM
  - 12 bits per symbol

Adapting to Channel Conditions

- Channel conditions vary
  - Physical environment of the channel
  - Changes over time (slow and fast fading)
- Modulation schemes are only as good as the receiver's ability to differentiate the symbols!



We'll deal with this when we discuss errors

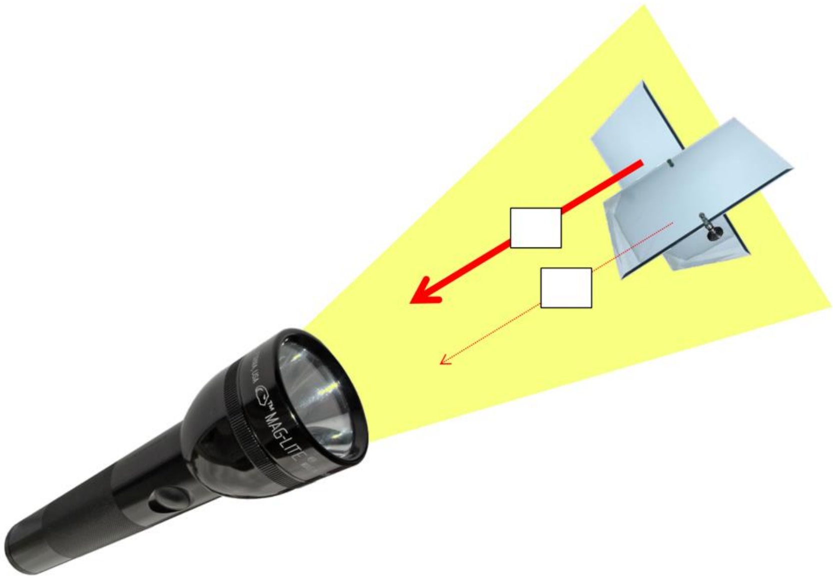
Adapting to Channel Conditions

- Fixed coding/modulation scheme will often be inefficient
  - Too conservative for good channels
  - Too aggressive for bad channels
- Adjust coding/modulation based on channel conditions – "rate" adaptation
  - Controlled by the MAC protocol
  - E.g. 802.11a: BPSK – QPSK – 16-QAM – 64 QAM

Bad Channel ⟷ Good Channel

Using Modulation: Backscatter

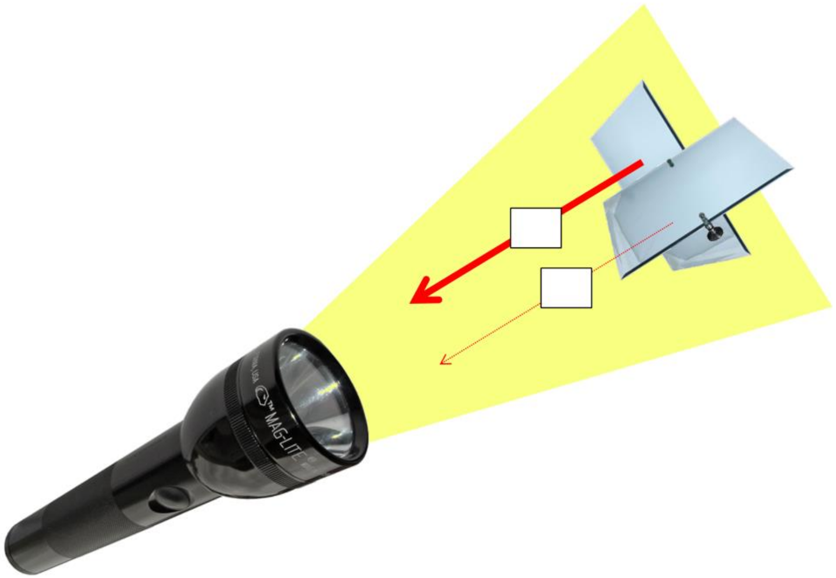
- Consider a flashlight emitting a beam of light
- The light is reflected by the mirror
- The intensity of the reflected beam can be associated with a logical "0" or "1"



Using Modulation: Backscatter

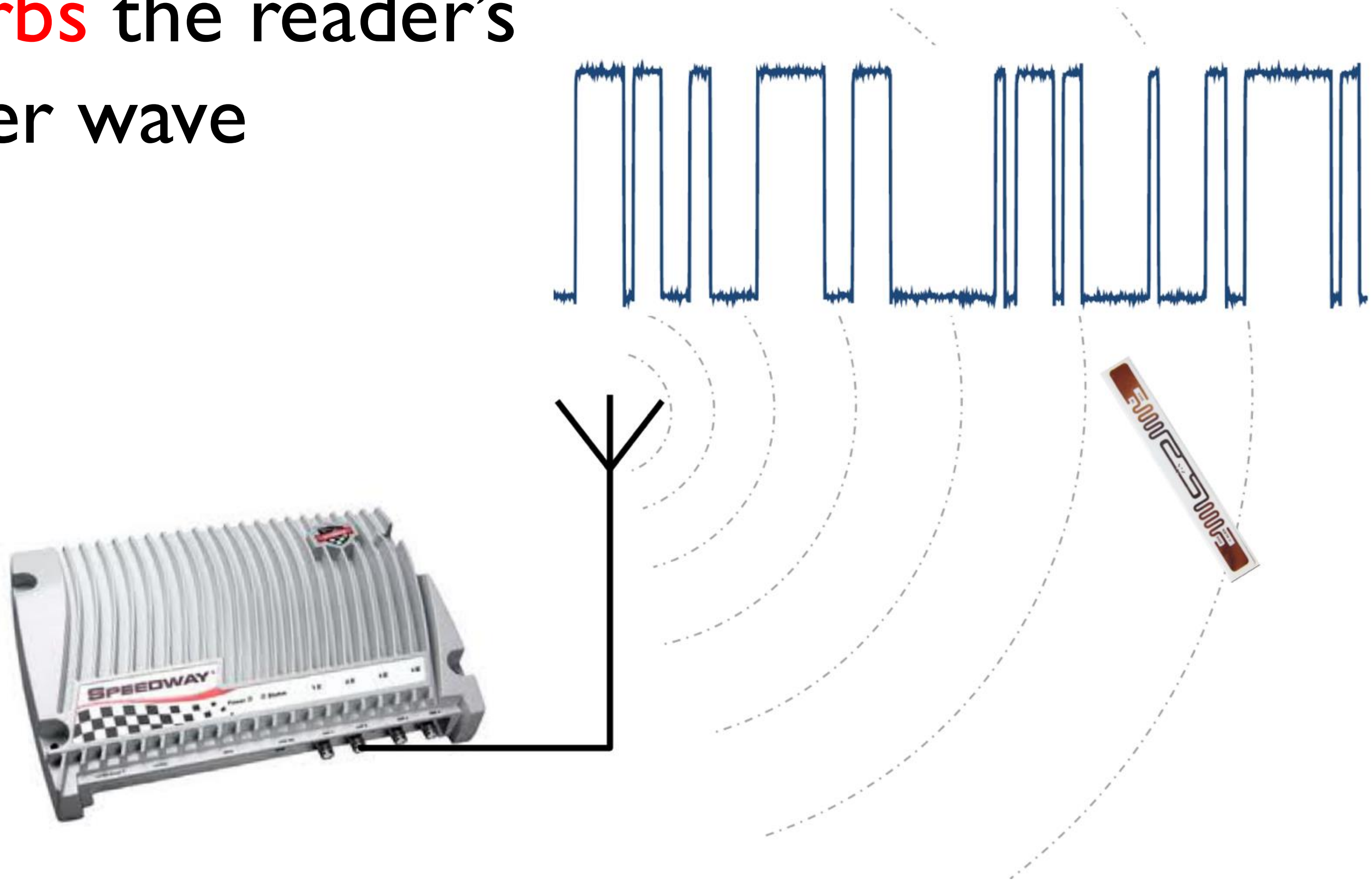
- Switch open
  - Absorbs the wave
  - Nothing bounces back
  - Bit = 0

- Switch closed
  - Reflects the wave back
  - Bit = 1



Backscatter Communication: RFID

- RFID tag reflects or absorbs the reader's carrier wave



Passive RFID: Two Different Physical Mechanisms

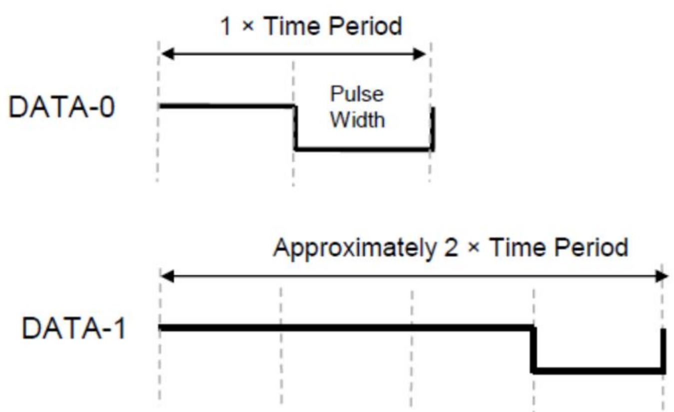
- LF/HF: Inductive Coupling
  - Reader coil generates a magnetic field
  - Tag coil harvests power via mutual inductance (near-field)
  - Tag must sit inside the near-field zone
  - Range: < 1 cm
  - Data rate: bps to few kbps
  - Example: NFC tap-to-pay
- UHF: RF Backscatter
  - Reader radiates a true propagating RF wave;
  - Tag reflects it back by toggling its antenna (far-field)
  - Works at real radio range, not just proximity
  - Range: a few meters
  - Data rate: up to 100s of kbps
  - Example: RFID

Backscatter Frequency and Range

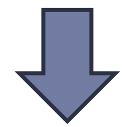
	UHF Backscatter RFID	HF Proximity RFID	NFC (Near Field)
Primary Frequency	860 MHz - 960 MHz	13.56 MHz	13.56 MHz
Typical Scan Range	Up to 12+ meters (40 feet)	Up to 1 meter (3 feet)	Under 10 centimeters (4 inches)
Data Coupling	Electromagnetic Far-Field	Inductive Near-Field	Inductive Near-Field Focus
Comms Direction	Unidirectional (Tag to Reader)	Unidirectional (Tag to Reader)	Bidirectional (Two-Way Comms)
Use Cases	Pallet tracking, bulk retail scans	Keyfob access control, library logs	Apple Pay, secure pairings, smart posters

Backscatter Communication

- Reader-to-tag
  - ON-OFF Keying
  - Pulse Interval Encoding (PIE)



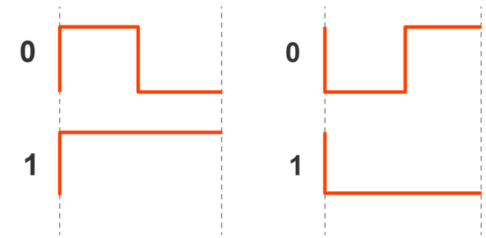
Signal is on for longer time

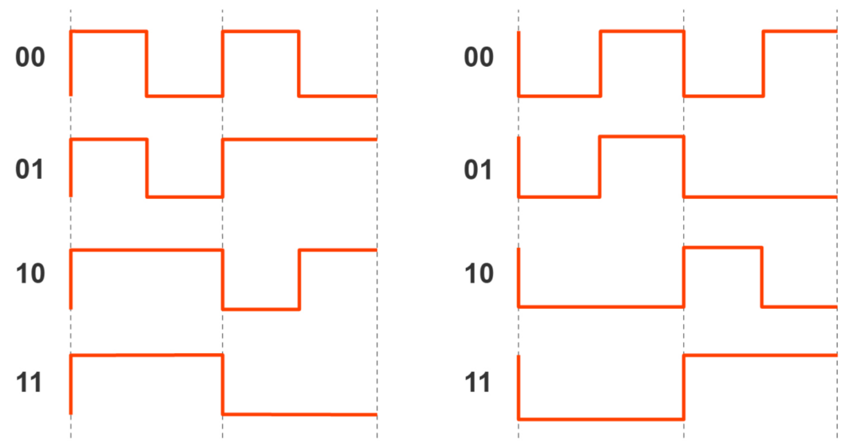


Maximize energy harvesting at the tag

Backscatter Communication

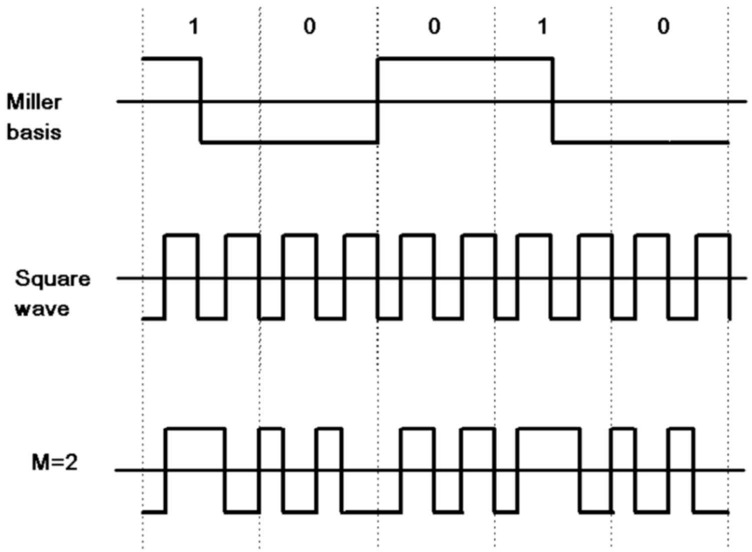
- Tag-to-reader
  - ON-OFF Keying
  - FM0
    - Inverts switch at every symbol
    - 0 bits has extra switch mid-symbol





Backscatter Communication

- Tag-to-reader
  - ON-OFF Keying
  - Miller
    - Inverts switch between two consecutive 0 bit symbols
    - Inverts the switch in the middle of 1 bit symbol

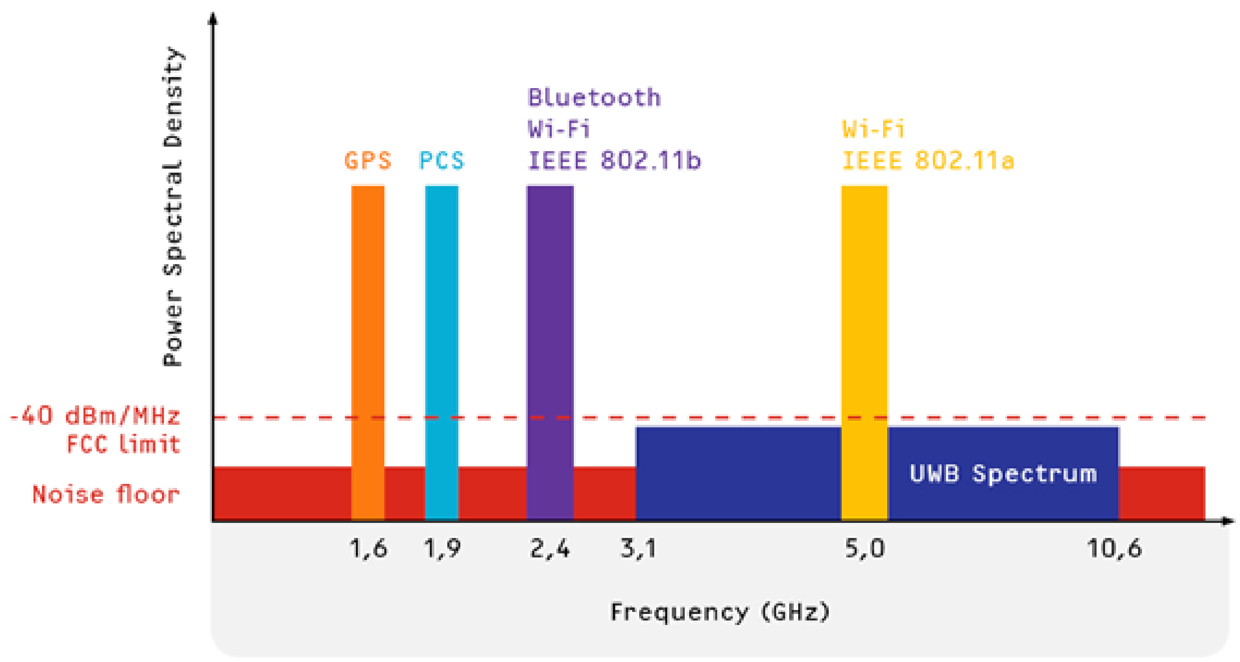


Backscatter Communication

- Tag-to-reader
  - ON-OFF Keying
  - Miller
    - Inverts switch between two consecutive 0 bit symbols
    - Inverts the switch in the middle of 1 bit symbol
- Benefits
  - Multiple switches per bit
  - Robust to Multi-Reader, Multi-Tag scenarios
  - Robust to noise
  - M=2, Data Rate
    - 20 Kbps – 320 Kbps
  - M=4, Data Rate
    - 10 Kbps – 160 Kbps
  - M=8, Data Rate
    - 5 Kbps – 80 Kbps

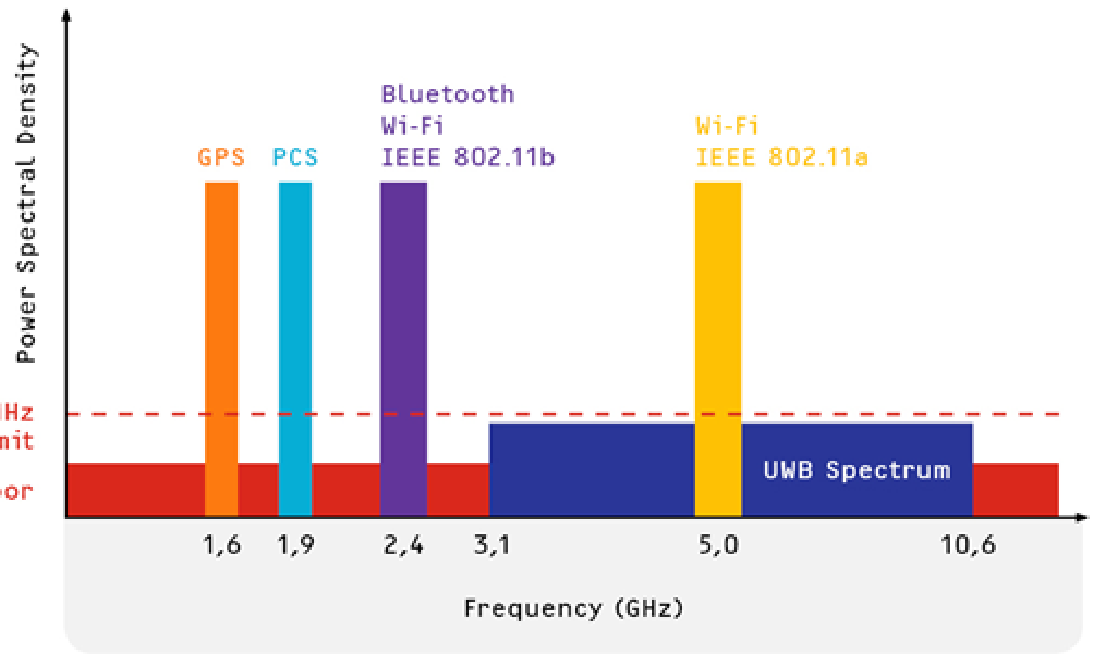
Ultrawide Band (UWB)

- UWB sends extremely short pulses (nanoseconds), spreading energy across a huge bandwidth (500+ MHz, often several GHz)



Ultrawide Band (UWB)

- Energy is spread across spectrum
  - Transmit power density stays very low
  - FCC lets UWB share spectrum used by other services

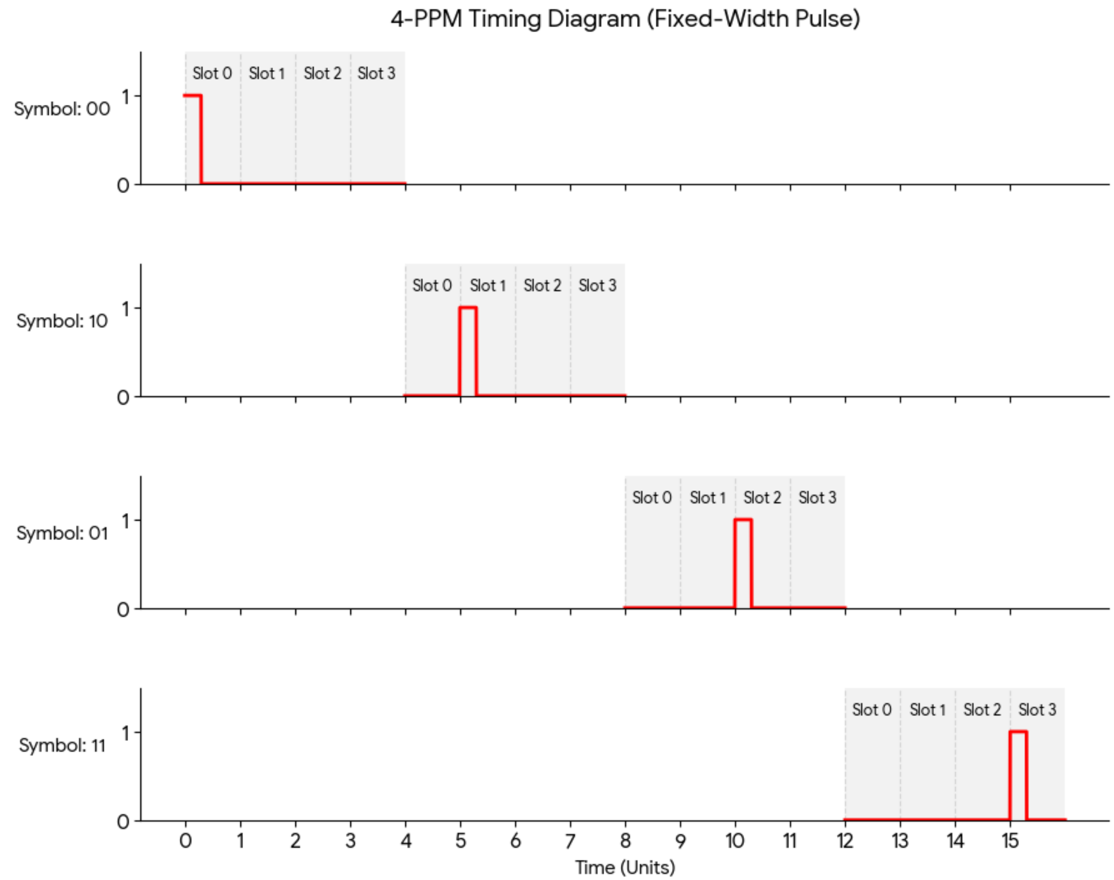


Ultrawide Band (UWB)

- Precise timing enable PPM (Pulse Position Modulation)
  - Pulses are narrow and identical
    - Transmitter uses very steady, low power.
  - Amplitude noise does not corrupt the message
    - Data relies only on timing, not height.
  - Receiver must match the sender's clock precisely

Ultrawide Band (UWB)

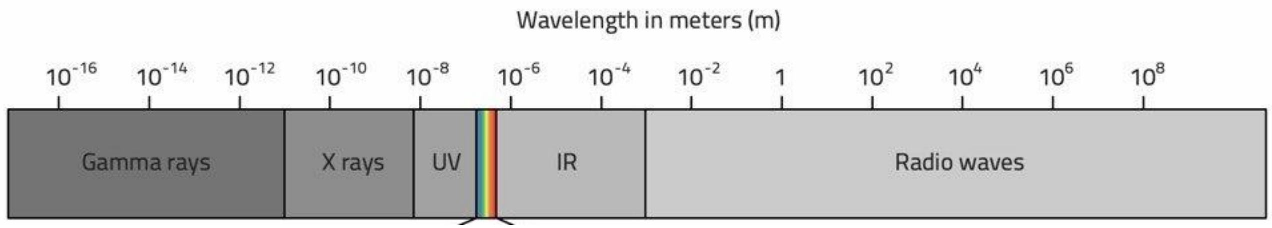
- Precise timing enable PPM (Pulse Position Modulation)



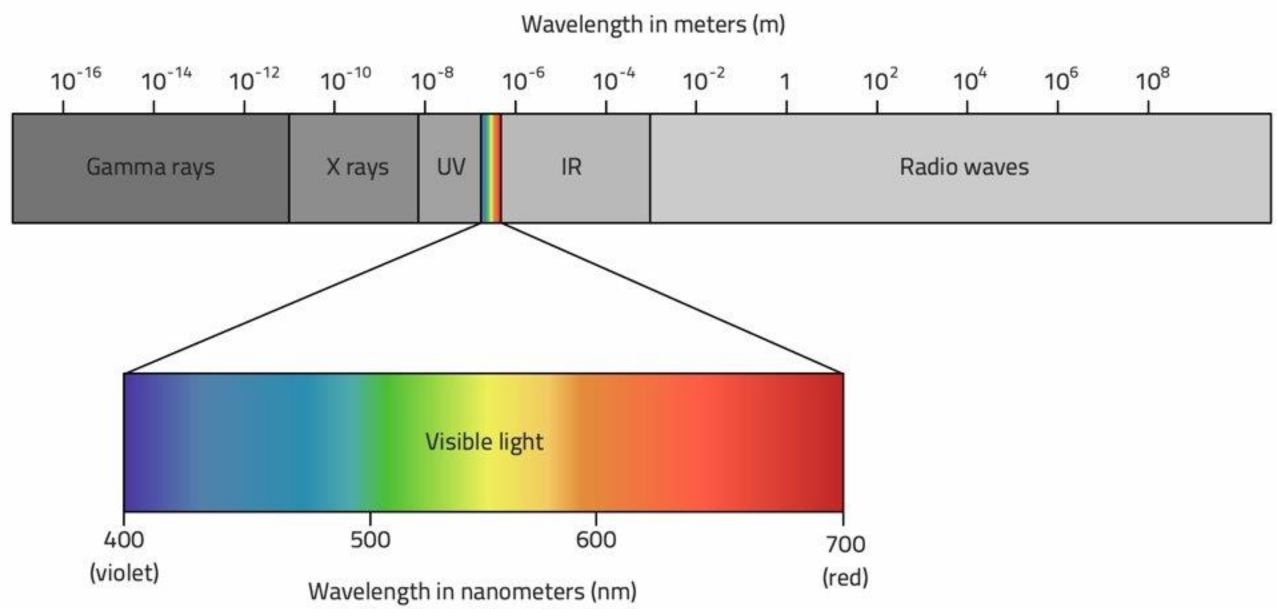
Ultra-Wideband (UWB)

- The huge bandwidth gives extremely fine time resolution
  - Individual multipath reflections arrive far enough apart in time to be resolved separately
    - No equalizer needed to fight ISI
  - Time-of-flight can be measured to centimeter-level accuracy
    - UWB is primarily a precision ranging/localization technology
- Short range (tens of meters)

Wireless Spectrum: What's Missing?



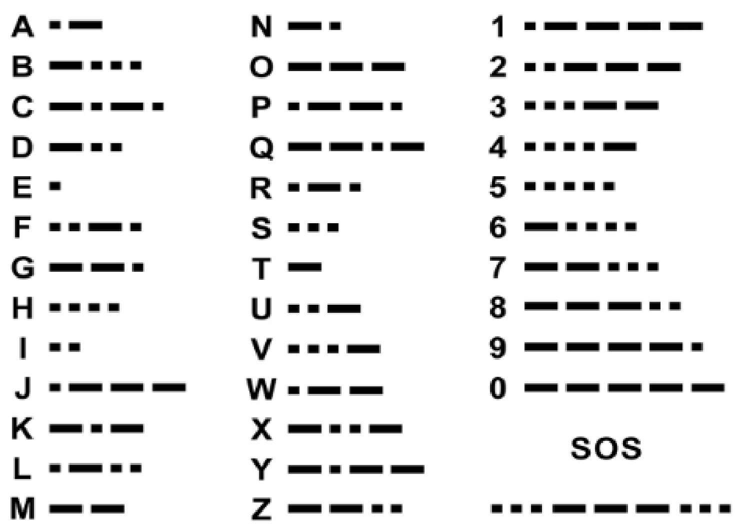
Wireless Spectrum: Light!



- 10,000 times larger than the entire radiofrequency spectrum
- Can we send data through visible light waves?

Early Visible Light Communication

- Flashes of a lamp
  - Morse Code
  - Used by ships to communicate over long distances



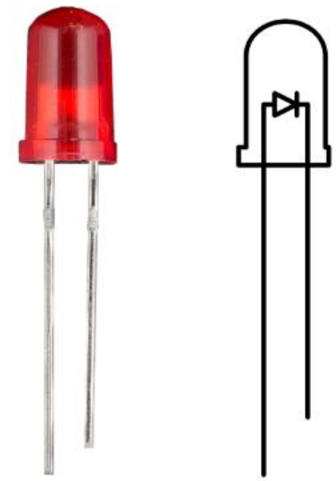
Early Visible Light Communication

- Flashes of a lamp
  - Morse Code
  - Used by ships to communicate over long distances

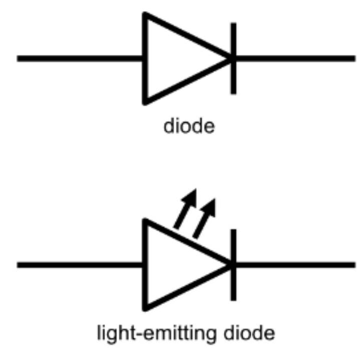
- Limitations
  - Human operators
  - Low data rate
  - Weather affects reliability
  - Light doesn't pass through walls
    - A natural security and interference boundary, but also a coverage limitation

VLC Transmitter: Light Emitting Diode (LED)

- Diode
  - One-way switch for electric current
  - LED emits light when current passes through

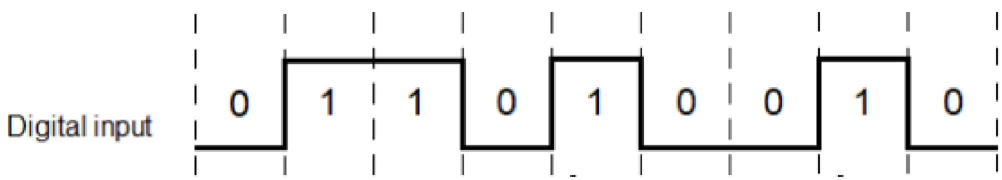


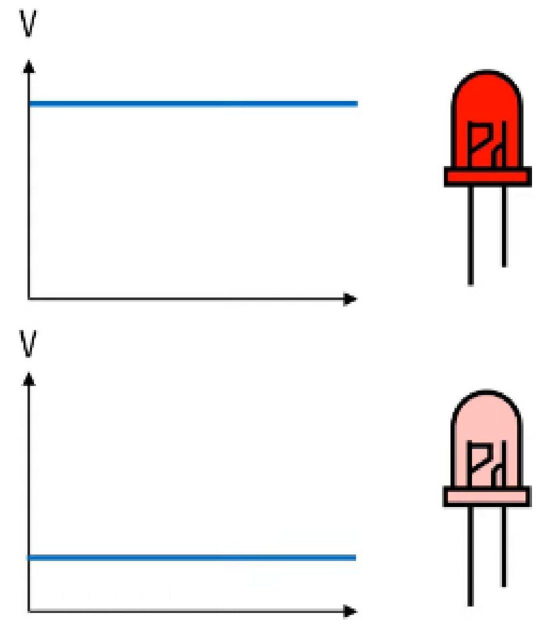
- A photodiode receiver detects the intensity changes and recovers the bitstream



VLC Modulation

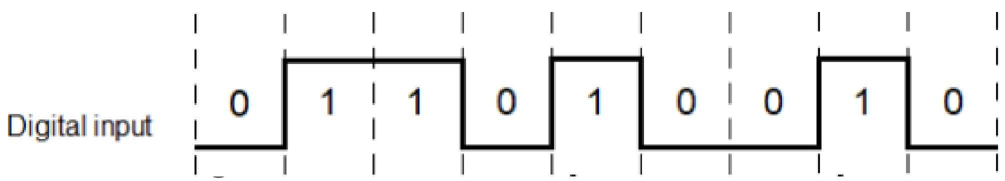
- On-Off Keying
  - 1: turn on the LED
  - 0: turn off the LED

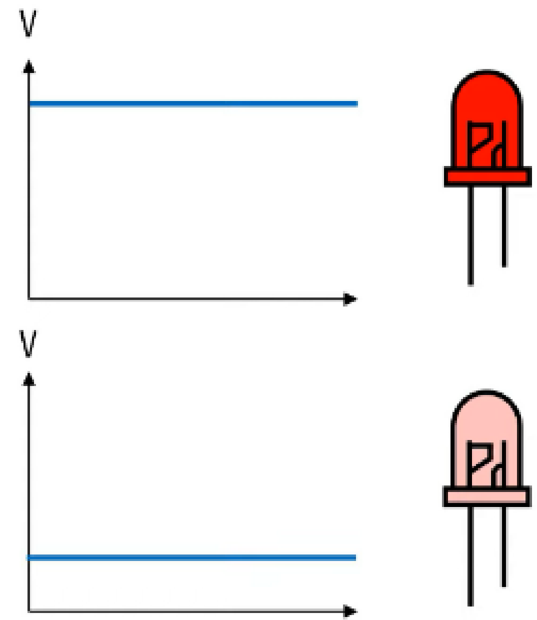




VLC Modulation

- On-Off Keying
  - 1: turn on the LED
  - 0: turn off the LED





- Flickering
- Transitions must be faster than the human eye can perceive

VLC: Tradeoffs vs. RF

- Advantages
  - No RF interference
    - Safe for hospitals, aircraft, and RF-sensitive environments
  - Inherent physical security
    - signal is contained to a lit room
  - Can piggyback on existing LED lighting infrastructure
- Limitations
  - Requires line-of-sight
    - Blocked by obstacles
    - Doesn't work in the dark or through walls
  - Uplink is awkward
    - Needs a return path (often RF or infrared)
    - Ambient light usually isn't attacker-free
  - Mobility and multi-user access are open problems