CS4457 - Networks Lecture 2 Notes

Josh Laney   Patrick Thomas
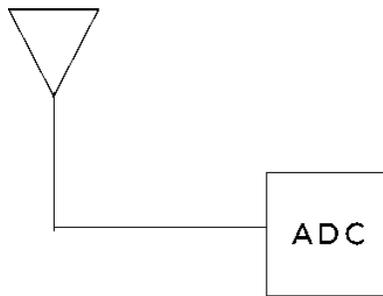
January 16, 2020

IQ Sampling and Modulation

Figure 1: Circuit from last lecture. This circuit cannot sample many signals fast enough to be useful, and this can be solved by adding a mixer to the circuit.
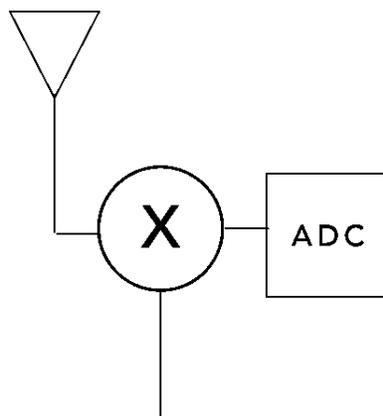

Figure 2: Now we've added a mixer. However, this circuit has another problem – it has problems disambiguating frequencies from the mixer. (See example from *Lecture 1*)
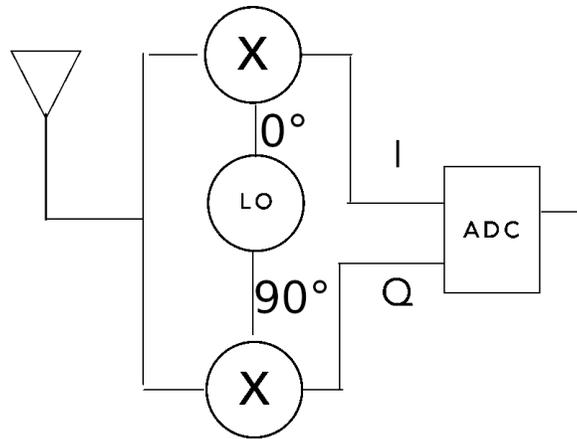
Figure 3: We can solve the frequency ambiguity problem by adding another mixer that outputs a frequency that is shifted 90 degrees from the other mixer input. Additionally, the ADC now outputs our IQ values, which can be represented as phasor samples over time – that is, a series of tuples or complex numbers.
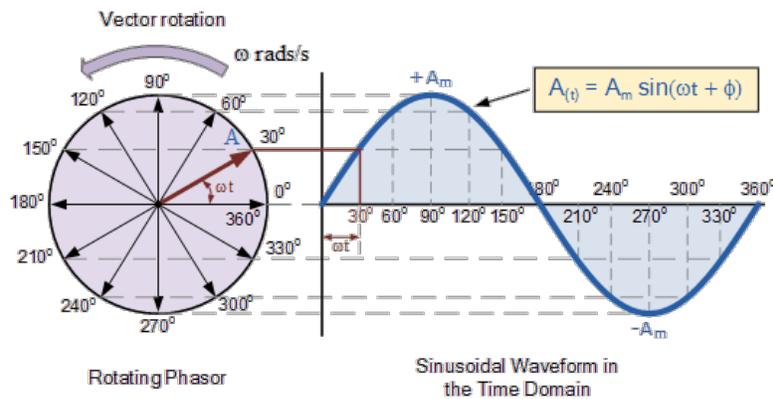
Phasors

Figure 4: Phasor

The equation for a phasor is

$$A_{(t)} = A_m(\omega t + \phi)$$

Where $A_{(t)}$ is the phasor, A_m is the amplitude of our sinusoid, ω is the frequency, and ϕ is the phase shift.

We can represent the output of the circuit from Figure 3 as a phasor, shown in 5
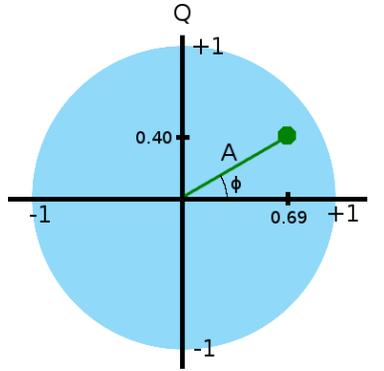
Figure 5: Example of an IQ value plotted as a phasor.

$$Q = \sin\phi$$
$$I = \cos\phi$$

IQ is then represented as either a tuple (Q, I) or as a complex number $I + Qj$. With the IQ values stored as complex numbers in memory, we can then use software to manipulate these values.

Software Defined Radios (SDR)

SDRs can be used to listen in on signals in the RF spectrum, such as WiFi networks, satellite communications, and unencrypted police radios. This gives us access to the physical layer through only using software.
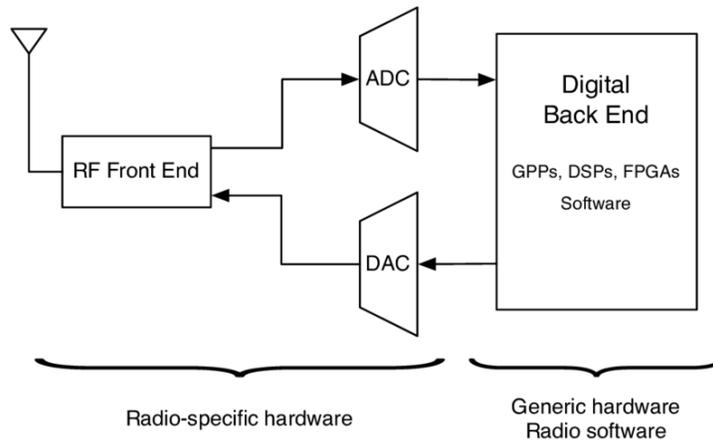

Figure 6: Block diagram of a SDR.

Example code using an SDR:

```
from rtlsdr import RtlSdr

sdr = RtlSdr()
# configure device
sdr.sample_rate = 2.048e6 # Hz
sdr.center_freq = 70e6 # Hz
sdr.gain = 'auto'

print(sdr.read_samples(12))
```

The above code outputs an array or stream of complex numbers like below. These complex numbers represent our IQ values and need to be demodulated and then converted into an audio file for playback.

```
 3.832798814072237246e-03-3.814442118802083975e-03j
-3.841128956818968751e-03-2.064052528090117890e-03j
-2.170216042670042398e-03-1.565552341909755285e-03j
-2.931813835758705859e-03-3.257285920291357832e-03j
-2.513969728080853432e-03-2.934689625757648263e-03j
-3.199319000218817967e-03-1.225806672846709196e-03j
-3.802803683201396064e-03-2.221995624597027357e-03j
-2.425861820519914676e-03-3.992723771607279912e-03j
-2.606126565394079487e-03-2.161200769632450492e-03j
-2.330759742839671675e-03-3.400828605998721418e-04j
```

FM Modulation

Remember that the complex values are our IQ values, each of which we can plot as a phasor (like in Figure 5), which means each of the complex values have an angle and magnitude associated with them (represented as A and ϕ respectively from Figure 5).

The change of the angle ϕ wih respect to time is directly related to a change in frequency. Thus, if we can calculate the change in frequency, we can then recover the original signal.
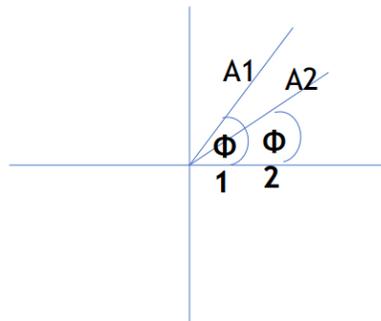
Figure 7: Two pairs of IQ values, plotted to show their angles, ϕ_1 and ϕ_2.

The angles, calculated from the IQ value pairs.

$$\phi_1 = \tan^{-1}\left(\frac{Q_1}{I_1}\right)$$

4

$$\phi_2 = \tan^{-1}\left(\frac{Q_2}{I_2}\right)$$
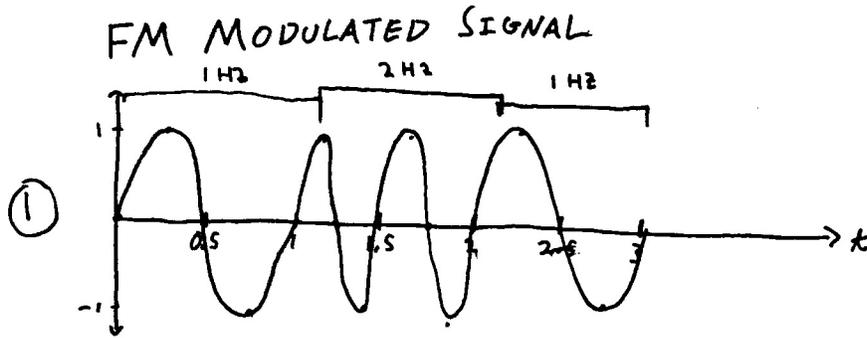
$$f = \phi_1 - \phi_2$$

FM Modulation via Polar Discriminator

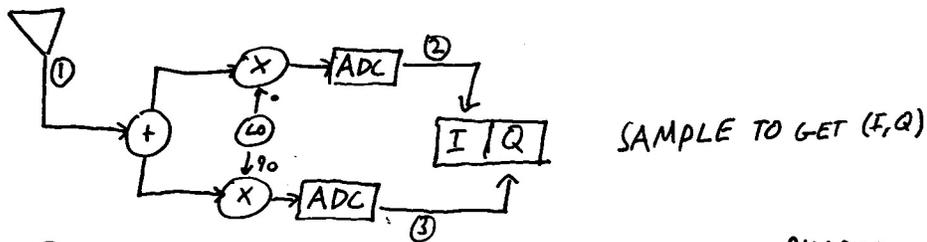The previous method can be improved by taking advantage of Euler's Formula as well as exponent rules.

$$\text{FM}_{\text{baseband 1}} = e^{j\phi_1}$$

$$\text{FM}_{\text{baseband 2}} = e^{j\phi_2}$$

$$e^{j\phi_2} \cdot e^{-j\phi_1} = e^{j(\phi_2 - \phi_1)}$$

This method can easily be done with software via math libraries that support matrix operations.
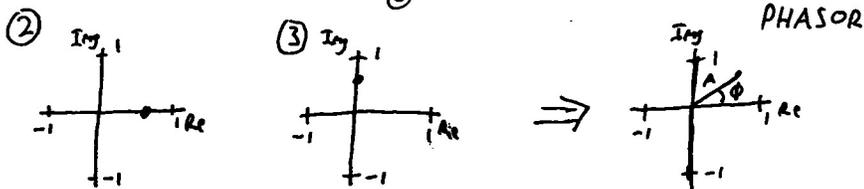
FM Demodulation Example Flow

FM MODULATED SIGNAL
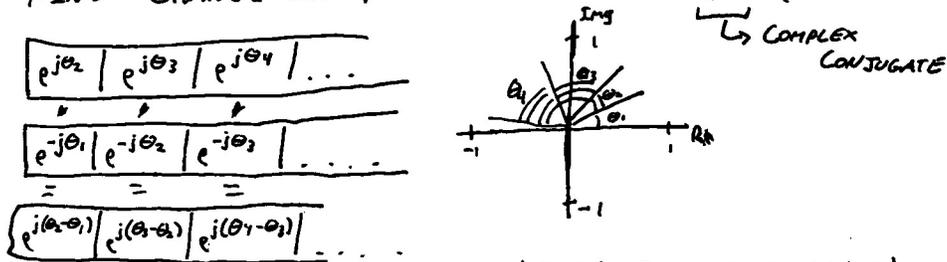
FEEDS INTO RF FRONT END

SAMPLE TO GET (F, Q)

PHASOR

CONVERT (I, Q) SAMPLES INTO PHI SAMPLES $\phi_i = \tan^{-1}\left(\frac{Q_i}{I_i}\right)$

FIND CHANGE IN ϕ OVER TIME $e^{j\theta_2} \cdot e^{-j\theta_1} = e^{j(\theta_2 - \theta_1)}$

$\hookrightarrow$ COMPLEX CONJUGATE

CONVERT TO ANGLES (USING EXAMPLE INPUT WAVE)

THE ANGLES MAP TO AMPLITUDE OF

ORIGINAL UN-MODULATED SIGNAL (USING EXAMPLE INPUT
                                        WAVE) ①

Δt = SAMPLE RATE OF ORIGINAL SIGNAL

Modulation

Modulation is just the inverse process of demodulation. There are many different modulation schemes, each with their own pros and cons.
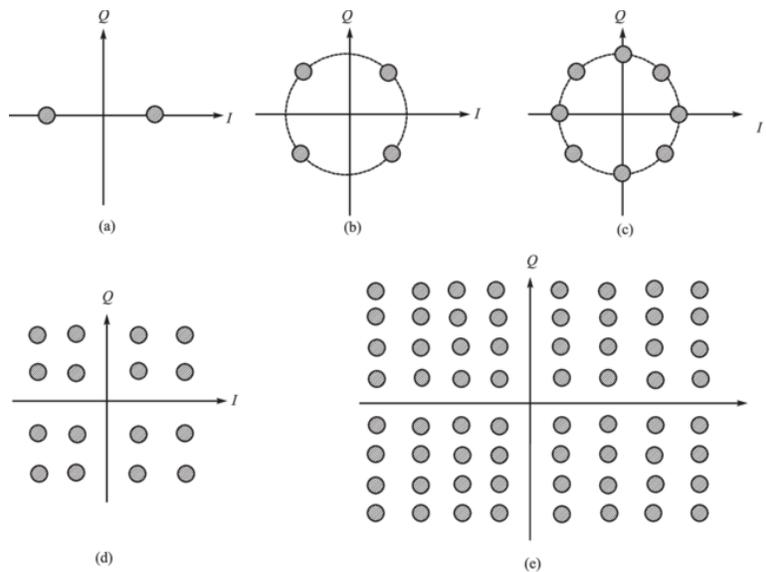

Figure 8: Several modulation schemes.

a. Binary shift keying (BPSK). Our input signal is essentially a binary signal, either on or off. This results in the two possible phasors that we could transmit.
b. QPSK modulation scheme. Now we utilize both I and Q axes, which allows us to represent more possible values and therefore transmit more data per unit time, as we now can represent 00, 01, 10, and 11. However, this scheme is more sensitive to noise.
c. 8PSK modulation scheme. We can continue the idea from QPSK and continue to pack more data at the cost of sensitivity to noise.
d. 16QAM modulation scheme. Note that now instead of placing the desired values around the unit circle, the magnitude of the phasor is now also considered to place the values in a grid.
e. 64QAM. This encoding scheme is much more sensitive to noise than a scheme like BPSK due to the close proximity of values.

7

Actual SDRs

In reality, SDRs are much more complex and have many more features.
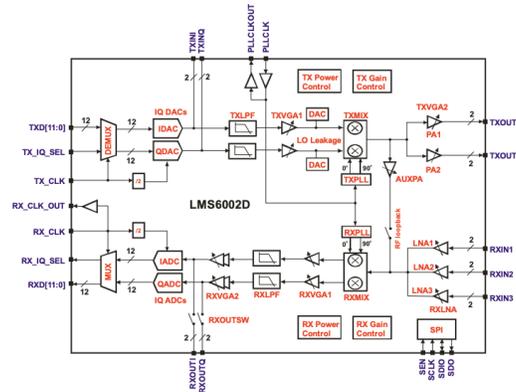

Figure 1: Functional block diagram

Figure 9: A schematic of an actual SDR.

In addition to the physical devices, there are commerical SDR tools, such as

- Redhawk, by the NSA
- Universal Hacker Radio

NOAA Satellite Data

NOAA weather satellites transmit data that anyone can receive and demodulate. It transmits pictures of the Earth that are AM modulated and then FM modulation. In addition to the pictures, some additional data is transmitted to assist in the demodulation and synchronization of the signal.

Packets

Packets are a means to contextual data into a meaningful and useful form.

For example, 000100100 → [0001|0010|0] → [send number|receiver number|bit].

Upsampling

Upsampling is used to better detect data by interpolating between samples. Essentially, by "guessing" the values of samples between actual observed samples gives more samples overall and a better set of samples.
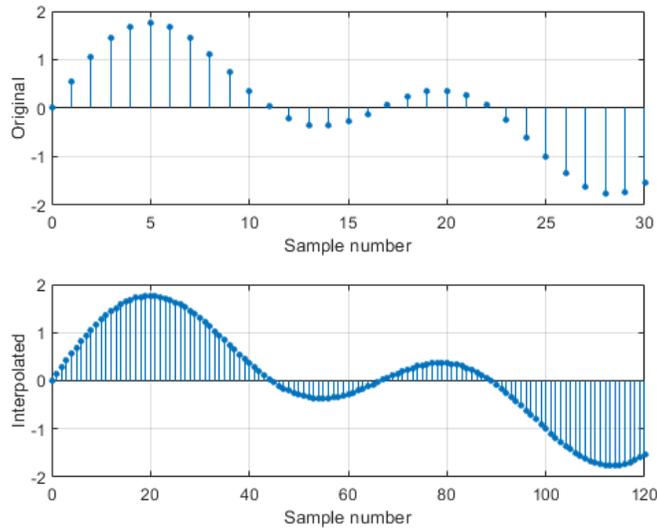
Figure 10: An upsampled signal. See how there are now more samples.

Amplitude Demodulation and Envelope Detection

Amplitude modulation is done by multiplying a information signal (variable frequency and amplitude) with a carrier signal (fixed frequency and amplitude). This puts the carrier signal into "envelopes" of data.
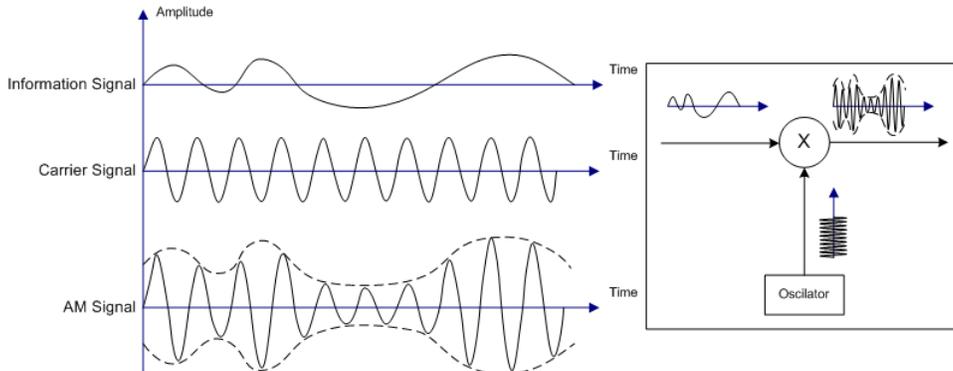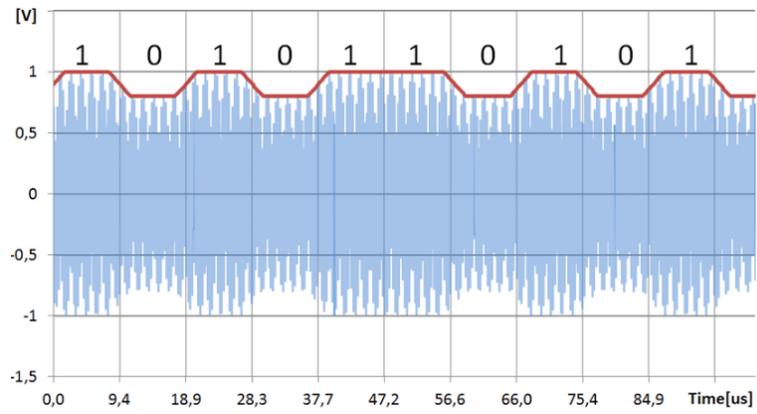

Figure 11: Visualization of amplitude modulation.

Figure 12: An AM signal with envelopes.