INTRODUCTION TO TELECOMMUNICATIONS

SCADA Hackers BNE – April 2020

@beLarge

This Evening's Agenda

1. Introduction and what does a Telecommunications engineer study?
2. Limited Highschool Revision and background
3. The Time Domain
4. The Frequency Domain
5. Filtering
6. Modulation

/whois @beLarge

- Graduated Bachelor Engineering (Telecommunications) First Class Honours at QUT in 2009
- Worked as a telecommunications engineer at QR (QR National -> Aurizon) for 7 and a bit years – as a Data Communications Engineer (IP Route & Switch, Network Security & Network Monitoring)
- Did some other stuff – went back to Uni and studied a Master of Business in Applied Finance and I am now interested in engineering Asset Management
- You might know me from events such as the MC For BSides Brisbane!
- Committee Member of the College of Information Technology, Telecommunications and Electronics Engineers (ITEE), Engineers Australia
- Involved with the Brisbane Branch of the International Society of Automation (ISA)

What is Telecommunications?

Telecommunications is the body of knowledge that enables the transmission of data (*information?*) between participants over distances by manipulating the properties of a transmission medium, for example:

- visual signals (signs, semaphore flags, signal lamps, rude hand gestures)
- written symbols (e.g. letters, books, memes)
- air (sound, yelling, music)
- smoke signals
- electromagnetic radiation (e.g. Electrical, Optical)
- Quantum?

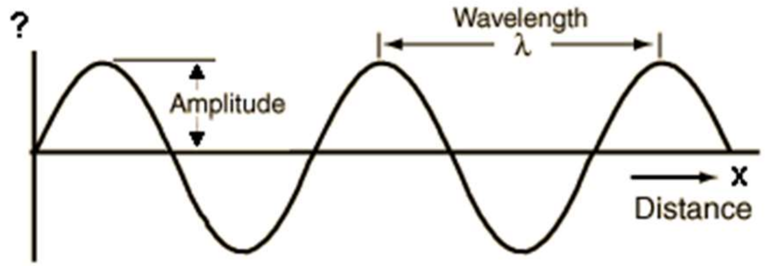
What does a Telecomms Engineer Study?

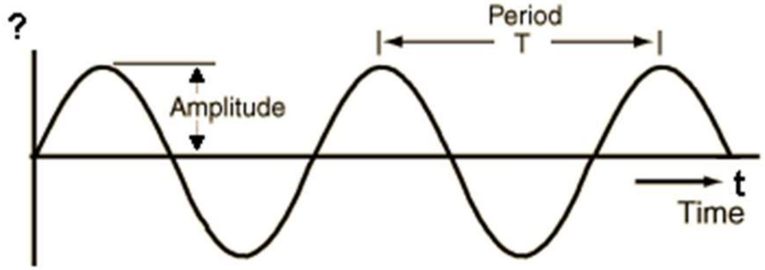
- Telecommunications
  - Introduction to Telecommunications
  - Classical Signal Processing
  - Digital Communications
  - Digital Signal Processing
  - Modern Signal Processing (elective)
- Wireless
  - Fields, Transmission and Propagation
  - Wireless Communications
  - RF Communication Technologies
  - Wireless and Mobile Networks (IT)
- Analogue and Digital Electronics
  - Electrical Circuits and Measurements
  - Analogue and Digital Electronics
  - Advanced Electronics and Embedded Systems
  - Introduction to Design
  - Advanced Design
- Computer Networking
  - Networking Systems (IT)
  - Internet Protocols and Services (IT)
  - Network Planning and Deployment (IT)
- Programming and Real Time Computing
  - Problem Solving and Programming (IT)
  - Object Orientated Programming (IT)
  - Programming Abstraction (IT)
  - Real-Time Computer Based Systems
  - Communication Environments for Embedded Systems
- Elective (yes, 1 - haha)
  - Lasers and Photonics
- Core Units
  - Engineering Mathematics (1A, 1B, 3, 4)
  - Physics
  - “Professional Studies” units x2
- Final year project!

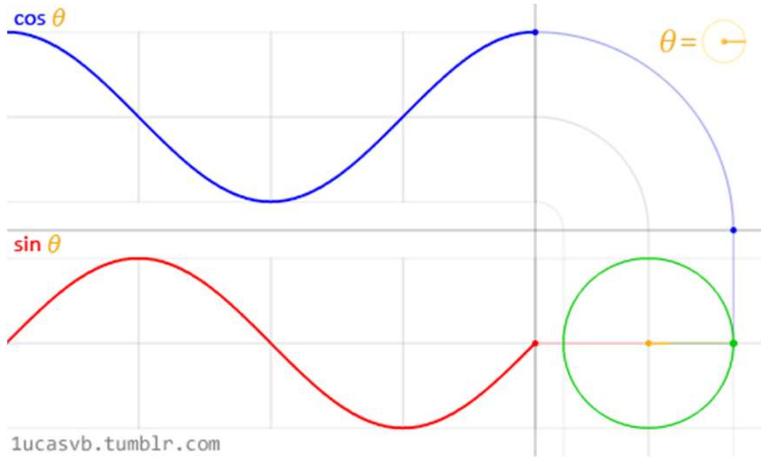
Highschool Revision

- Periodic Functions
  - A - Amplitude
  - Period (T in seconds)
  - Wavelength (λ) (meters) denoted as c = λ.f where c is the speed of light in a vacuum
  - *f* - Frequency (Hz)
  - Frequency (cycle per second) is $\frac{1}{Period}$
  - Phase Offset – how signals of the same frequency can be offset from each other
- Trigonometric Functions (periodic functions)
  - Cosine (cos)
  - Sine (sin)
  - Tangent (tan) (Also, $tan = \frac{sin}{cos}$)

Source - http://www.sengpielaudio.com/calculator-wavegraphs.htm & https://www.iflscience.com/brain/math-gifs-will-help-you-understand-these-concepts-better-your-teacher-ever-did/page-2/







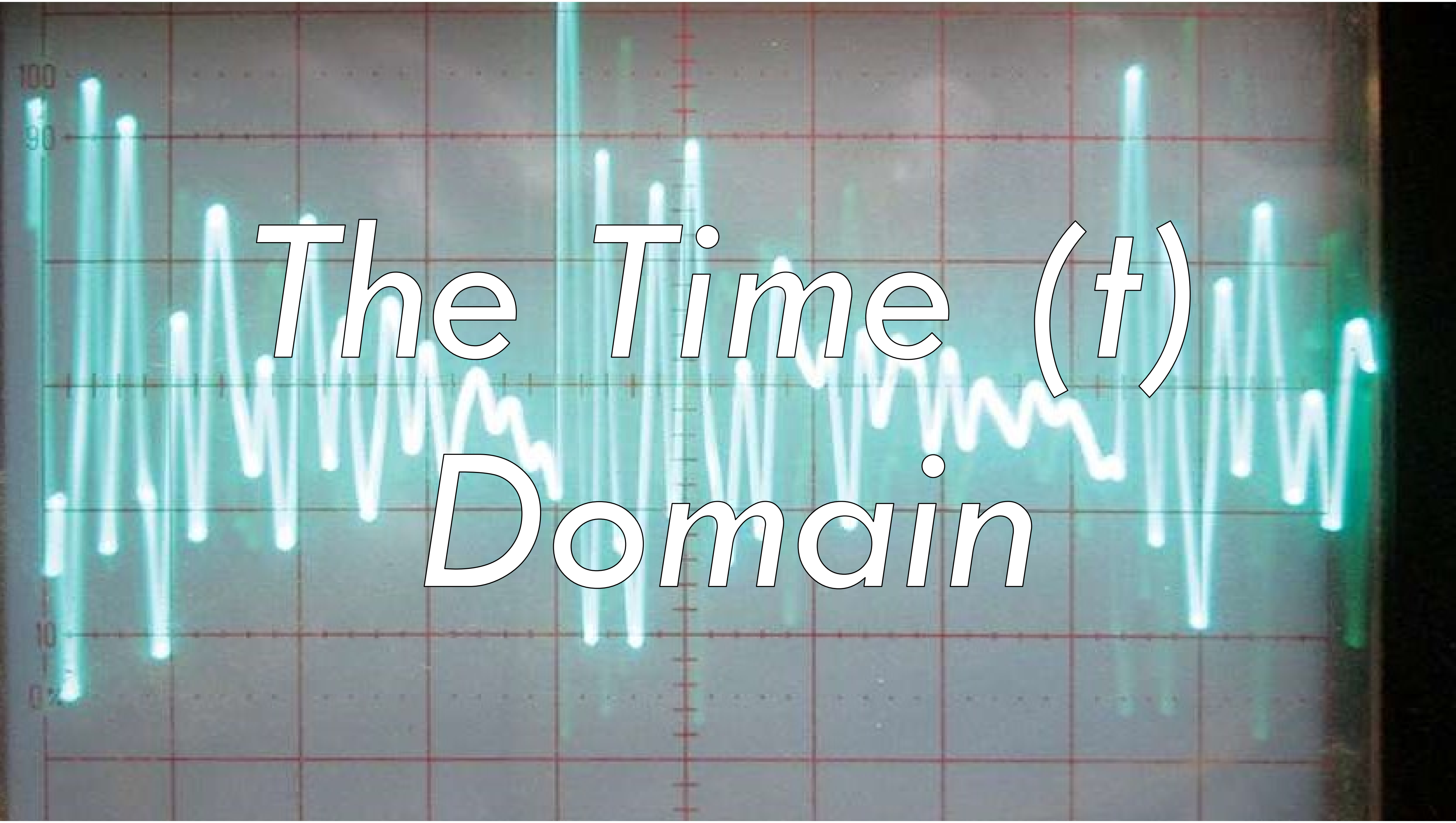
Highschool Revision (pt 2)

- You can have a square root (two even) of a negative number; it's defined as an imaginary number
  - $\sqrt{-1} = i; i^2 = -1;\ i = \frac{1}{-i}$; (but we use $\mathtt{j}$ in electrical engineering because $\mathtt{I}$ denotes Current)
- Electrical engineering uses complex numbers for:
  - The conversion from the time domain to the frequency domain (Fourier Transform, Fourier Series)
  - As a vector notation to denote in phase and out of phase (quadrature) signals
  - Phasor Notation – it allows phase offsets to be considered in circuit calculations
- Euler's Expansion
  - $e^{jwt} = \cos(wt) + j\sin(wt)$ - this is really useful – <u>we will come back to this</u>

Octave (Open Source MATLAB)

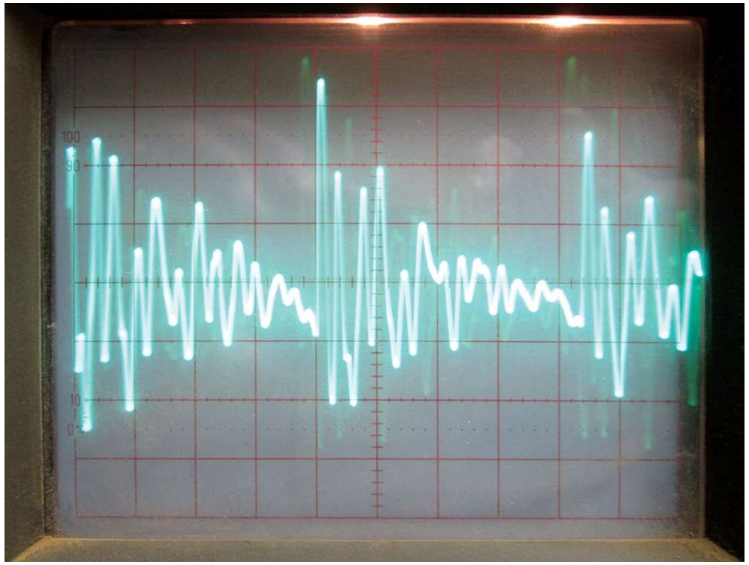
- In my degree I spent **<u>a lot of time</u>** in MATLAB
- Octave is an open source MATLAB project!
  - https://www.gnu.org/software/octave/
- You can follow along with my code if you would like

https://github.com/belarge/IoT-SCADAHackersBNE

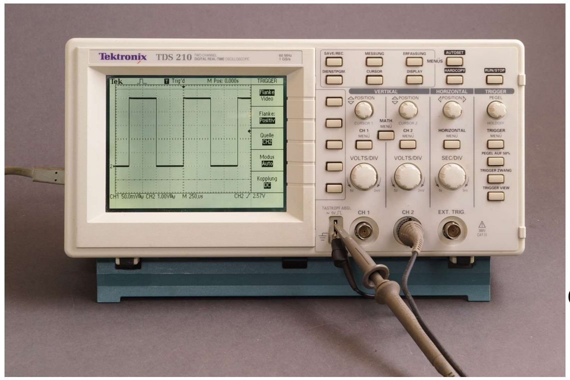

The Time (t)
Domain

The Time Domain

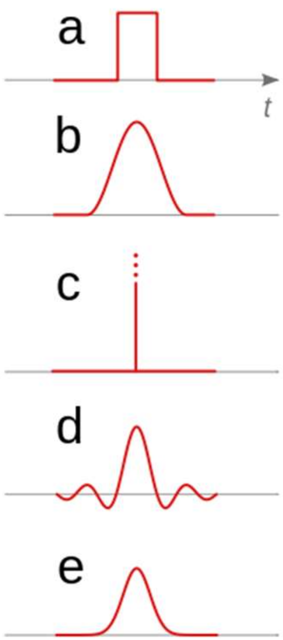
- Everyone understands and has used the time domain!
- Measured using an oscilloscope
- Think in Winamp – it's the oscilloscope

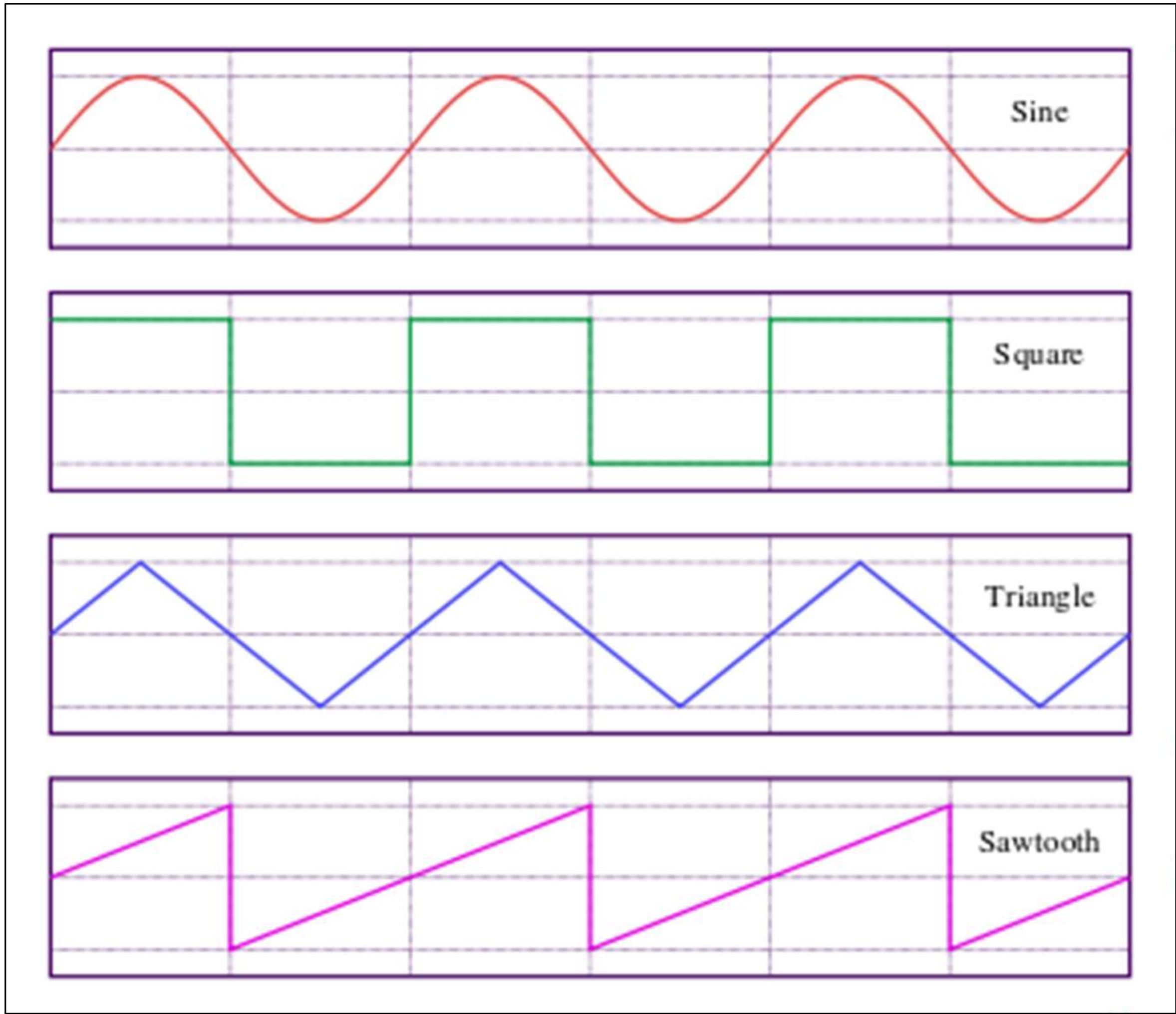


[Image Source - https://www.kitplanes.com/aero-lectrics-13/](https://www.kitplanes.com/aero-lectrics-13/)

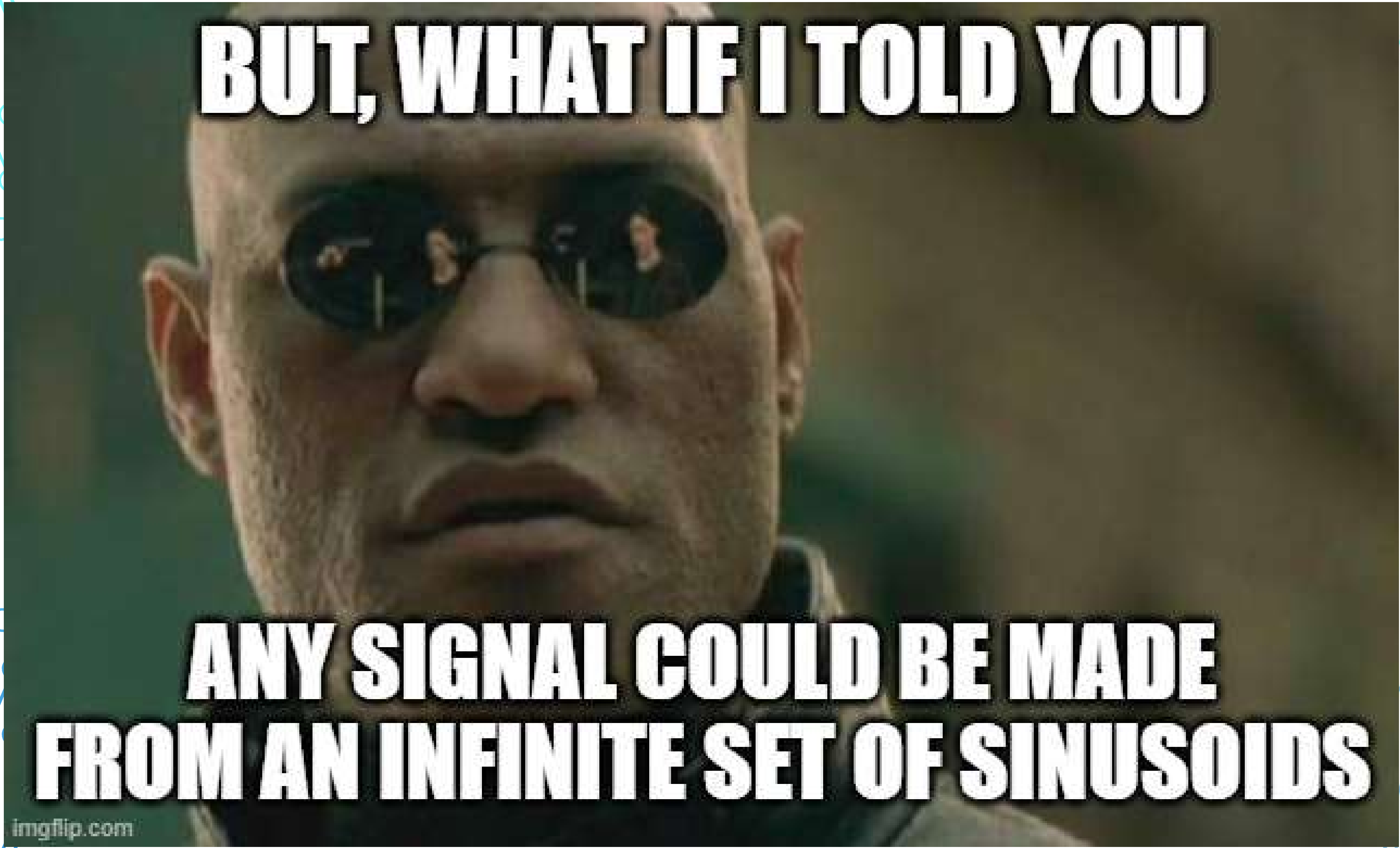


The Time Domain (cont.)





https://en.wikipedia.org/wiki/Waveform
https://en.wikipedia.org/wiki/Pulse_(signal_processing) (Thanks Wikipedia! you should donate!)


BUT, WHAT IF I TOLD YOU
ANY SIGNAL COULD BE MADE FROM AN INFINITE SET OF SINUSOIDS
imgflip.com

The Time Domain (cont.)

- A time signal, `s(t)` can be made by adding many periodic signals together
- The Classic Example is the Square wave - the source of this image is a cool visualisation tool

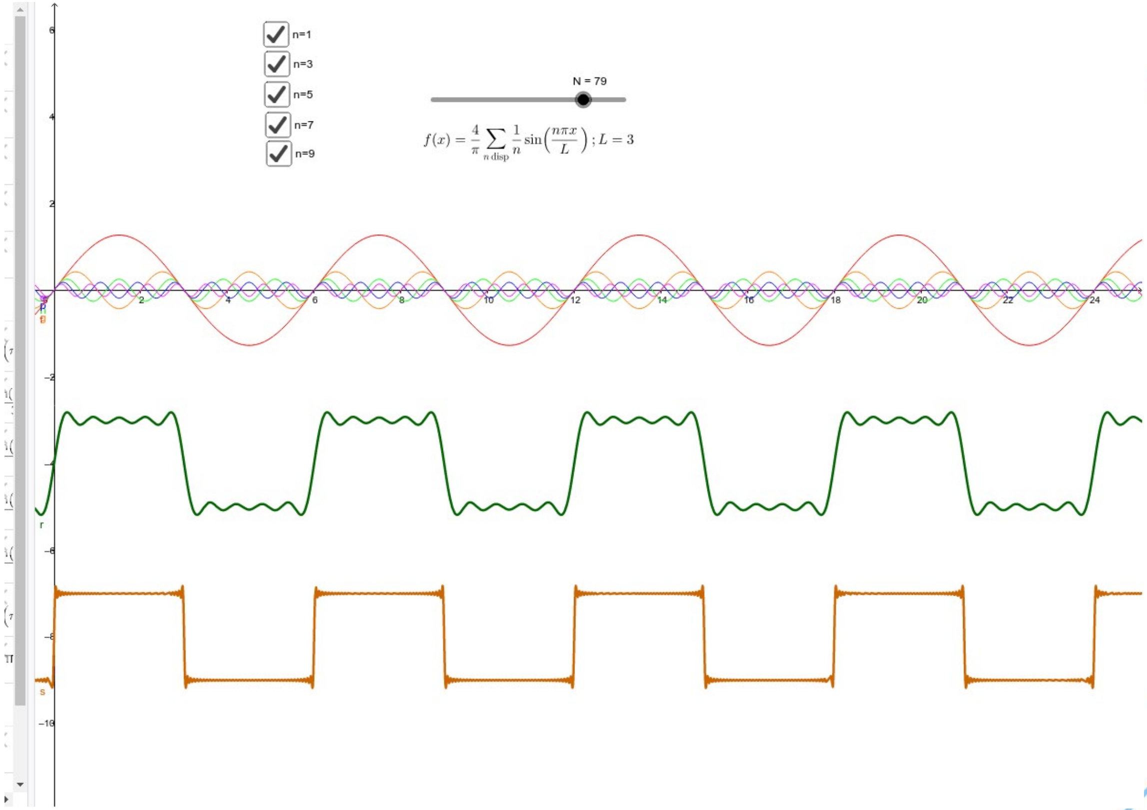
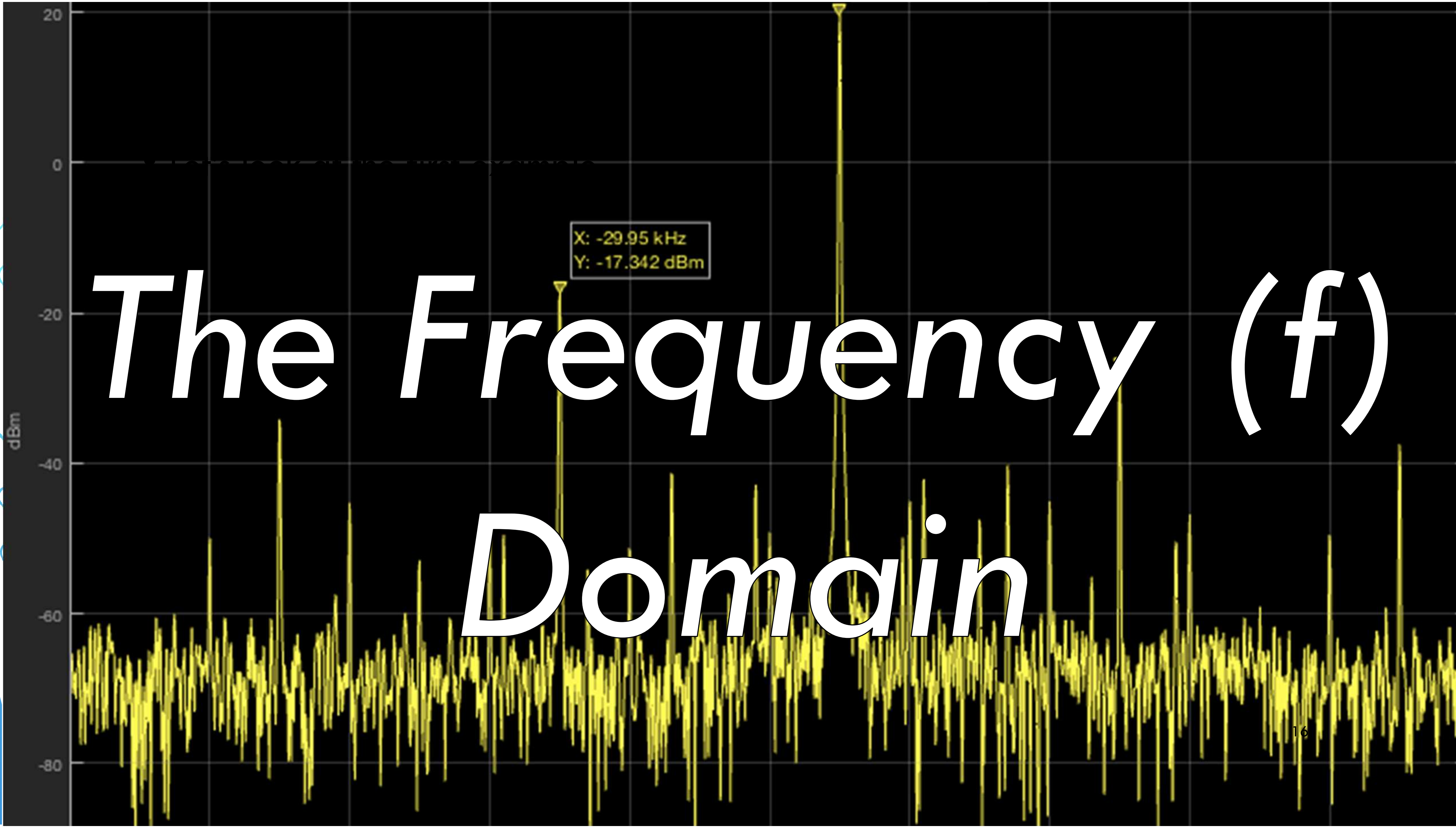


Image source - https://www.geogebra.org/m/wUanseCs

Demo Time (Octave)

Questions?

The Frequency (f) Domain



The Frequency domain

- The frequency domain is the most important concept to understand for telecommunications!
- Think of the VU meter setting in Winamp

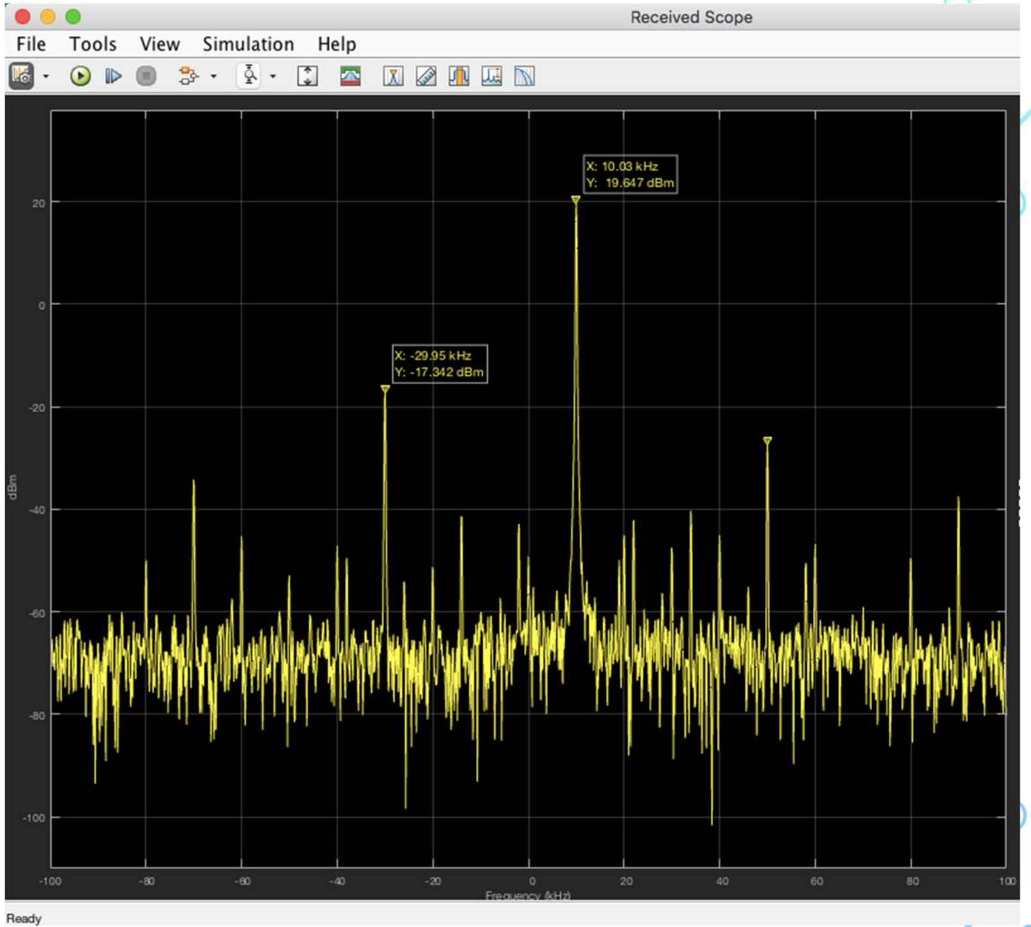
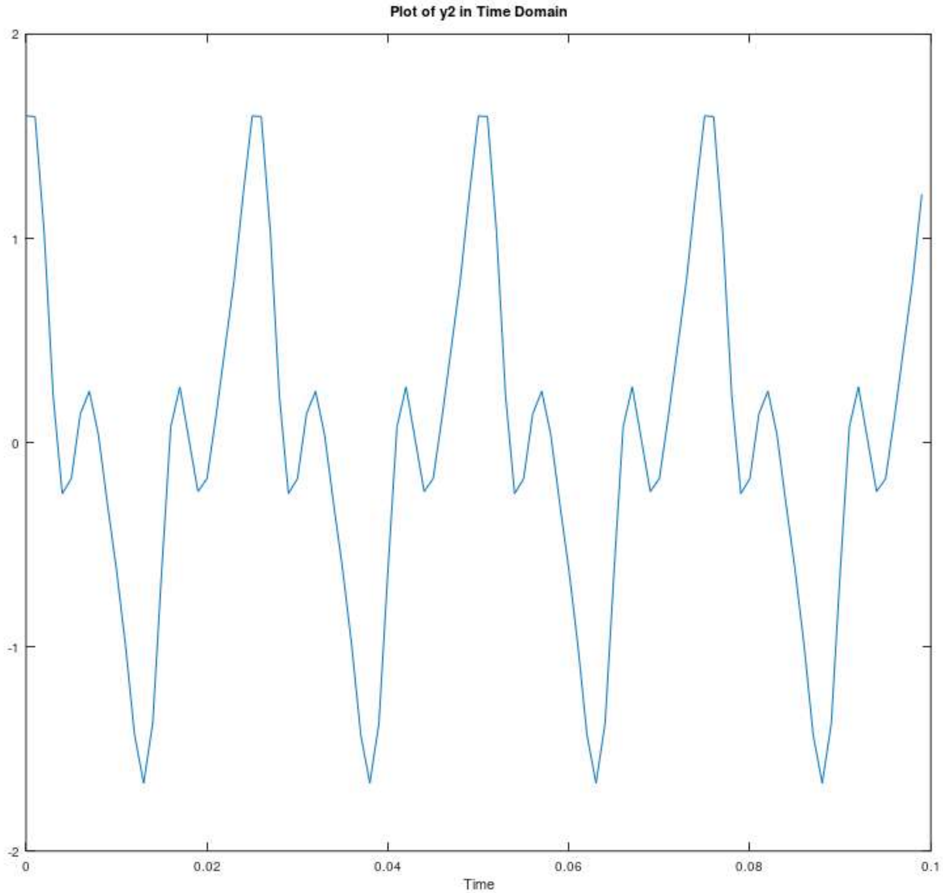
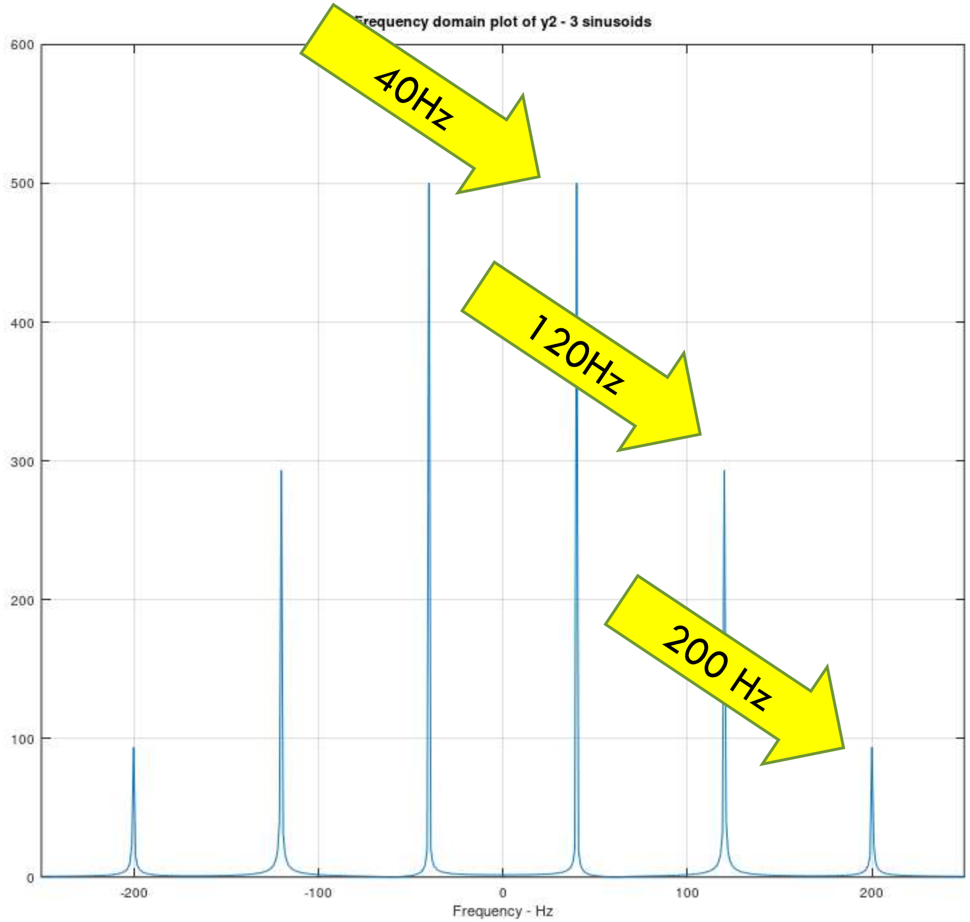


Image source https://ez.analog.com/adieducation/university-program/f/q-a/77831/generating-cw-tones-with-pluto-in-matlab

The Frequency domain (cont.)






```
y2 = cos(2*pi*f*t) + 0.6*cos(2*pi*f*t*3) + 0.2*sin(2*pi*f*t*5); %f = 40Hz
```

The Fourier Transform

- To convert between the Time domain (t) and the Frequency domain (f) we use a Fourier Transform

s(t) $\xrightarrow{\mathscr{F}}$ S(f)

- Because we are using discrete mathematics we are going to use a discrete Fourier transform tonight and a special one at that – the Fast Fourier Transform (FFT)

MORE ABOUT THIS NEXT TIME!!!!

$$s(t) = \int_{-\infty}^{+\infty} S(f) e^{-2\pi i f t} df$$

$$S(f) = \int_{-\infty}^{+\infty} s(t) e^{2\pi i f t} dt$$

Image Source - https://towardsdatascience.com/fun-with-fourier-591662576a77 &

The Fourier Transform (the hard bit)

¿Some sort of elvish?

S(f) $= \int_{-\infty}^{\infty} s(t).e^{j2\pi f t} dt$ $(Remember\ \omega = 2\pi f)$

$\boxed{\text{S(f)} = \int_{-\infty}^{\infty} s(t).Z(t)dt}$

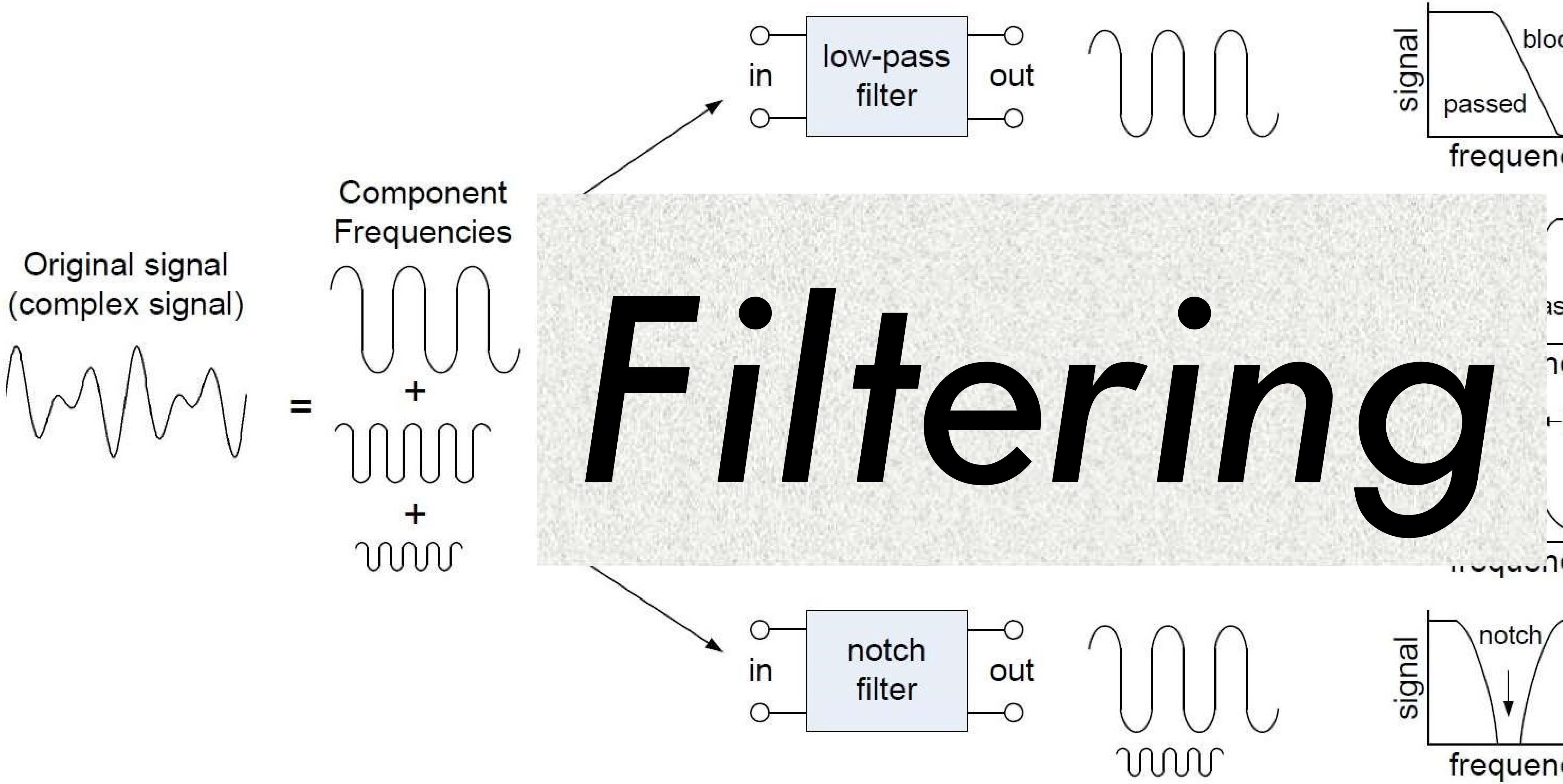
S(f) $= \int_{-\infty}^{\infty} s(t).(\cos(2\pi f t) + j\sin(2\pi f t)\ dt$

<u>"This integral finds the inner product of a sweep of sinusoids from –infinity to +infinity with the inputted signal"</u>

Demo Time (Octave)

Questions?

Filtering


Original signal
(complex signal)
=
Component
Frequencies
+
+
in
low-pass
filter
out
signal
passed
frequenc
in
notch
filter
out
signal
notch
frequenc

Filtering

- At the core of telecommunications systems is the ability to filter signals

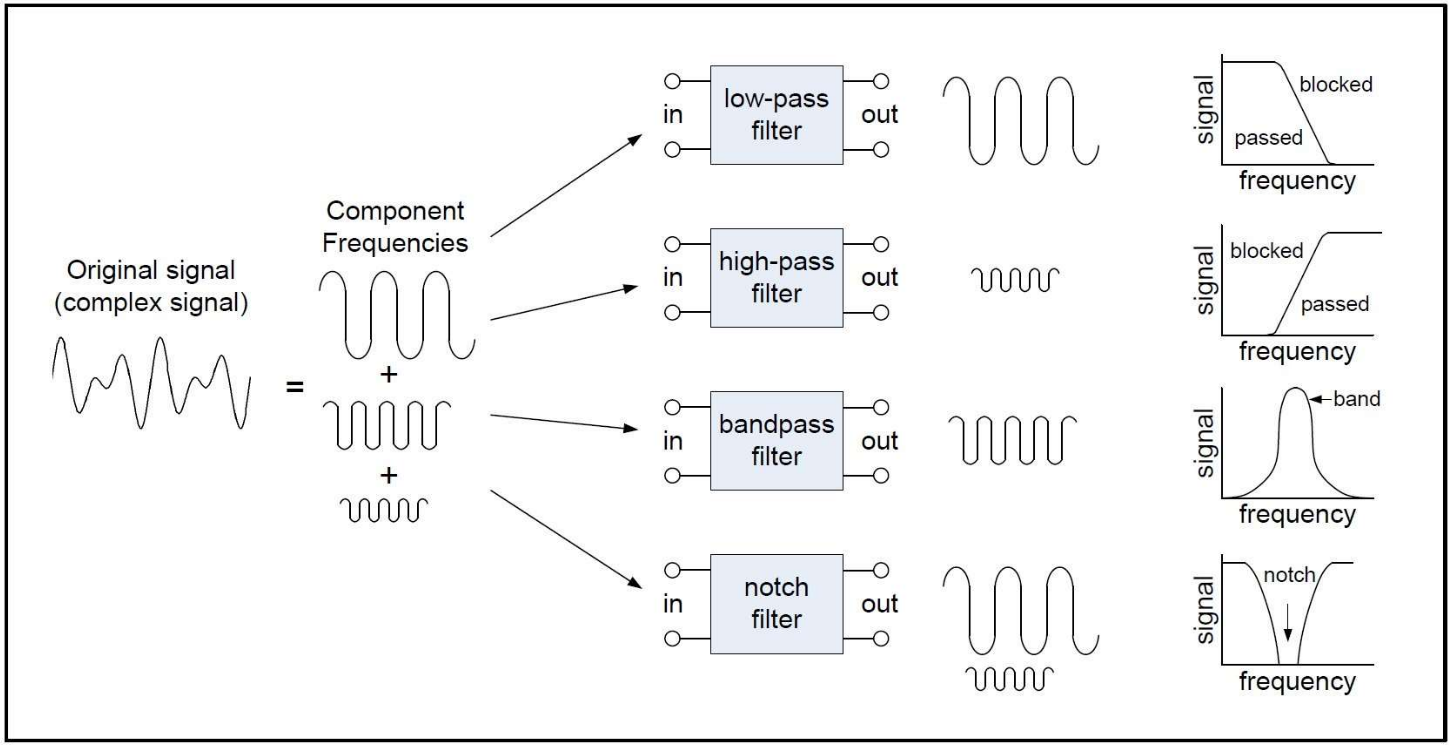


Image source https://www.allaboutcircuits.com/technical-articles/an-introduction-to-filters/

Filtering (cont.)

To understand how to apply filters you need to understand the Input and the System Response (system transfer function)

$$Output\ (f) = Input(f).System\ Response\ (f)$$

Great! Life is easy and I am happy normal person!

$$Output\ (t) = Input(t) \circledast System\ Response\ (t)$$

Suffering, Pain, Despair!

Your boy – convolution!!!

Convolution – definition

Image Source - https://en.wikipedia.org/wiki/Convolution

$$(f * g)(t) \triangleq \int_{-\infty}^{\infty} f(\tau)g(t-\tau)\,d\tau.$$

1. Take two functions, f(t), g(t) – figure out which is the easiest to flip
2. Then, move the flipped function back to –infinity, then move it forwards (i.e. to the right) to its first overlap position with the other function.
3. Define the integral of those two functions multiplied – start integrating until the waveform changes the overlap
4. Take note of where it changes, break the integral, start the process at step 3 again
5. Repeat until you get to + infinity

If the lecture is nice, they will give you at least one function where it is constant
(This is why you ***never*** take the second exam – sit the exam even if you are dead!)

Convolution - GIF

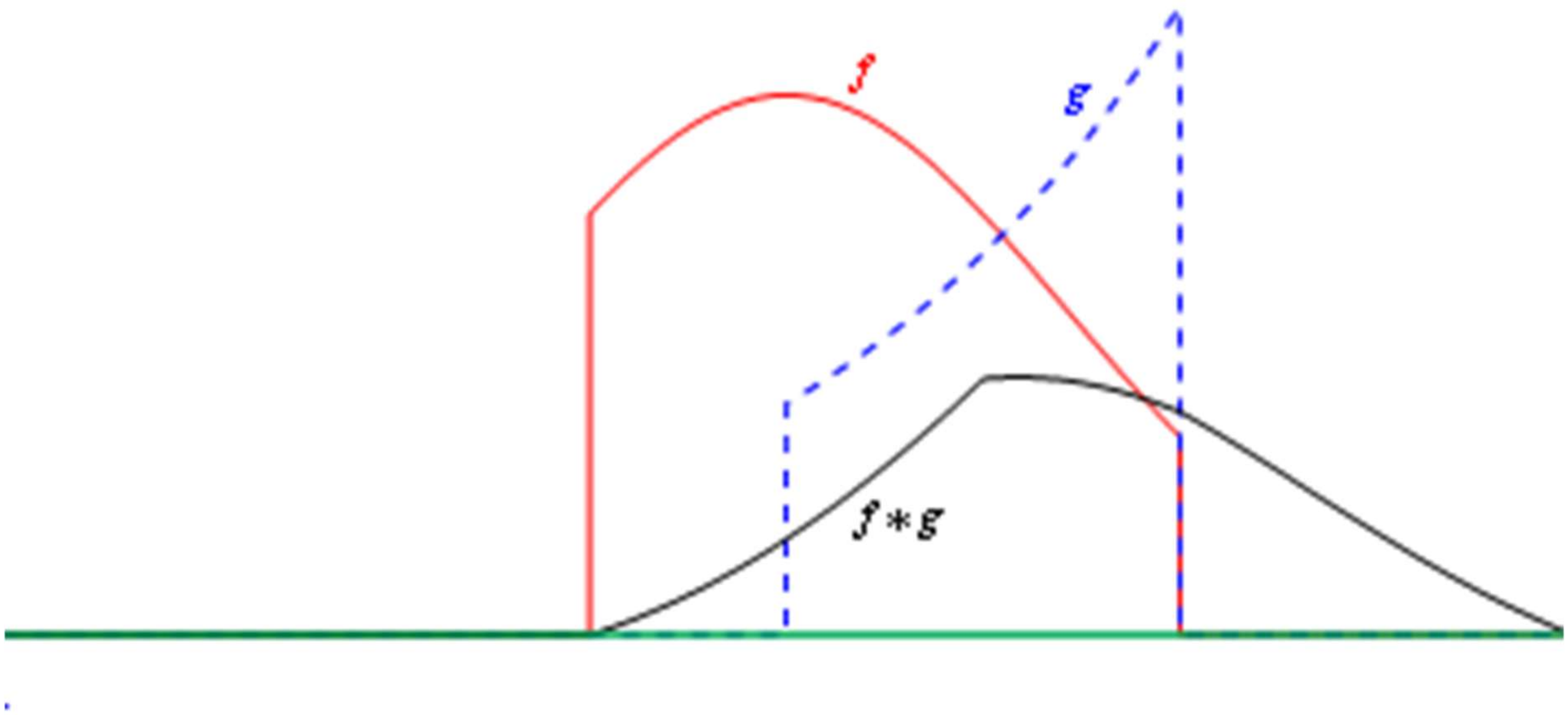


Image source
https://commons.wikimedia.org/wiki/File:Convolution_Animation_(Exponential_and_Gaussian).gif

Convolution – **what** if there was another way?

Convolution in one domain, is the same as multiplication in the other domain!

i.e.

OUPTUT (t) = INPUT (t) ⊛ FILTER (t)

Is the same result as

OUTPUT (F) = OUTPUT (F) x FILTER (F)

Similarly,

OUTPUT(t) = INPUT (t) x FILTER (T)

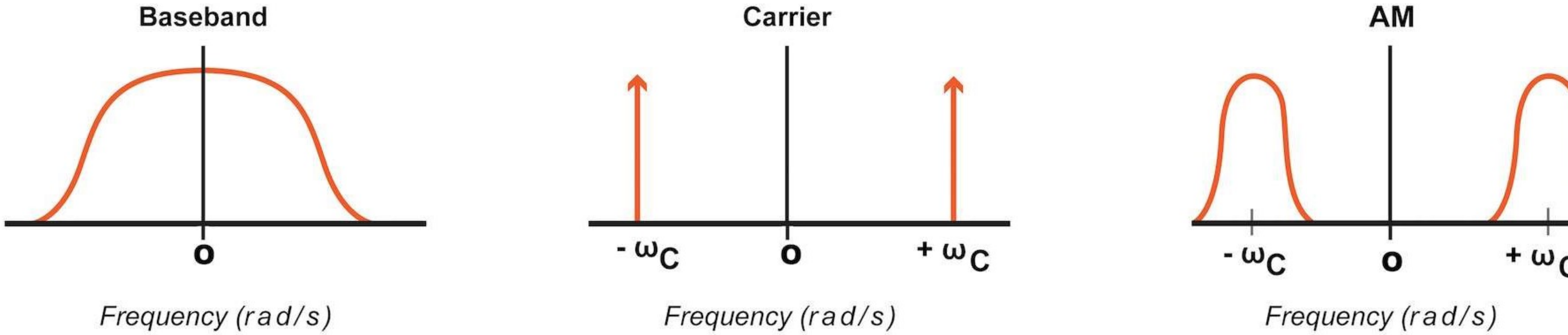
OUTPUT(F) = INPUT (F) ⊛ FILTER (F)

More on this later!

Demo Time (Octave)

Questions?

Modulation


Baseband
o
Frequency (rad/s)
Carrier
- ωC
o
+ ωC
Frequency (rad/s)
AM
- ωC
o
+ ω
Frequency (rad/s)

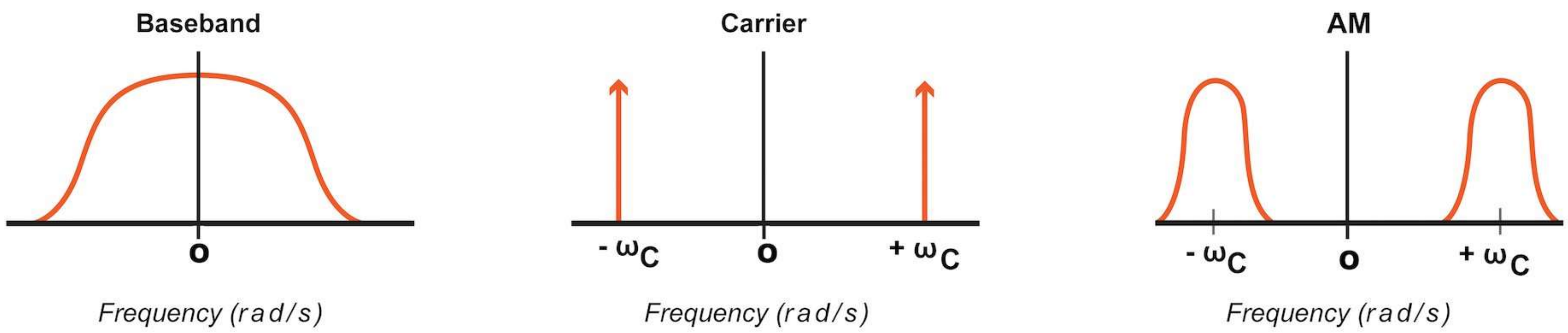
Modulation

- How to encode (modulate) one signal onto another
- You will be familiar with:
  - Amplitude Modulation (AM)
  - Frequency Modulation (FM)
- Think back to multiplication in one domain is convolution in another …

Image source https://www.allaboutcircuits.com/technical-articles/an-introduction-to-filters/

Amplitude Modulation

- Take your signal you want to transmit (for example voice – bandwidth 4000 Hz) – called the baseband signal
- Modulate onto a Carrier Signal (Something in the Hundreds of KHz (i.e. 100,000 times higher)
- Multiple the two together in the time domain – convolve in frequency



https://www.allaboutcircuits.com/textbook/radio-frequency-analysis-design/radio-frequency-modulation/amplitude-modulation-theory-time-domain-frequency-domain/

Demo Time (Octave)

Questions?