GRCon '24

Getting Started with GNURadio in the Classroom

UNITED STATES
AIR FORCE
ACADEMY

Disclaimer

The views expressed in this article, book, or presentation are those of the author and do not necessarily reflect the official policy or position of the United States Air Force Academy, the Air Force, the Department of Defense, or the U.S. Government. Approved for public release: distribution unlimited. PA#: USAFA-DF-2024-491.

You First – Introductions

- Name
- School/Organization
- What do you want out of this seminar?

A Huge Caveat

A Huge Caveat

Overview

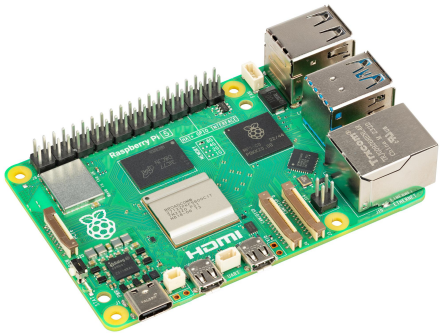
- SDR course/lesson organization
- Hardware
- Software
- "The textbook"
- Sample lesson
- Round table/discussion

Approach

- Theory is needed, but application is foremost
- Student engagement is primary teaching mechanism
- Failure is encouraged
- Exploratory learning

> I'm not building Communications experts
> I'm building critical thinkers

Hardware Options: PC



- 2.4GHz quad-core ARM64
- max 8GB RAM
- USB 3.0 ports @ 5gbps
- Gigabit Ethernet
- Linux-based OS
- Portable, good enough for low sample rates

- 2.4GHz (4.6GHz turbo) quad-core i5
- max 64GB RAM
- USB 3.2, USB 4 via Thunderbolt
- 2.5gb Ethernet
- Good for lab spaces w/ Ubuntu

- 2.4GHz (4.6GHz turbo) 12-core i5/i7
- max 64GB RAM
- USB 3.2, USB 4 via Thunderbolt
- No native Ethernet, need dongle
- Windows 11 (meh)
- Good for students

Hardware Options: SDR

- 100kHz to 1.7GHz (direct sample below 14.7MHz)
- Max 3Msps
- Rx only
- 0-50db gain
- Have to manually install Windows drivers
- $50 (kit)

- 1MHz to 6GHz
- Max 20Msps
- Half duplex (Tx/Rx, one at a time)
- 0 or 14dB of RF gain
- Starting to see version compatibility issues
- $350

- 70MHz to 6GHz
- Max 60MSps
- 2 channles, Full Duplex
- 0-76dB of gain
- $1400

Hardware Options: SDR

Operating Systems

- Linux/Ubuntu
- Windows
- Mac OS X
- Dragon OS

- Makes development/usage most straightforward
- Students may not be familiar
- Will serve them well in the future
- Does require some work if starting from scratch

Operating Systems

- Linux/Ubuntu
- Windows
- Mac OS X
- Dragon OS

- Wait, but why?!?!
- Ubiquitous & well supported
- WSL2 support is significantly improved
- Need USB manager to pass USB signal to WSL2 terminal
- Some tasks may be difficult:
  - Building OOT blocks
  - Running command line tools (direwolf, sox, multimon-ng)
  - Audio passthrough

Operating Systems

- Linux/Ubuntu
- Windows
- Mac OS X
- Dragon OS

- Similar to Ubuntu, but some nuances
- Need X11 to support GUI Applications
- XCode CLI tools
- Conda or Homebrew will install most applications
- USB support is seamless

Operating Systems

- Linux/Ubuntu
- Windows
- Mac OS X
- Dragon OS

- Turnkey solution, if computers support it
- Contains all major tools
- Why don't I use it?

Software Options

- GNURadio
- GQRX
- SDRAngel
- URH
- Python
- Inspectrum

- Best to develop useful applications
- Low barrier of entry, fully-featured
- Obviously, a great community
- OOT blocks
- Usage nuances

Software Options

- GNURadio
- GQRX
- SDRAngel
- URH
- Python
- Inspectrum

- Best to see "big picture"
- Lowest barrier of entry
- Limited demod capability
- Built on GR, bundled with apt or radioconda distribution
- Usage nuances

Software Options

- GNURadio
- GQRX
- SDRAngel
- URH
- Python
- Inspectrum

- Very full featured
- Significant learning curve
- Runs on android devices
- Many built-in demods/decoders

Software Options

- GNURadio
- GQRX
- SDRAngel
- URH
- Python
- Inspectrum

- Narrowly focused on common protocols
- Steep learning curve
- Runs on Windows and Linux
- Must watch tutorial videos to get started
- Nice companion to rtl_433 (command-line utility)

Software Options

- GNURadio
- GQRX
- SDRAngel
- URH
- Python
- Inspectrum

- Good for really understanding the numerical operations
- Not immediately intuitive how things connect
- Simplest infrastructure
- PySDR is a good place to start
- I use it as a supplement to "dig in" to topics like IQ data handling and filters

Software Options

- GNURadio
- GQRX
- SDRAngel
- URH
- Python
- Inspectrum

- Very good for time-independent analysis
- Can be finicky
- Lots of "hand jamming"
- Documentation is sparse
- I have seen dependency conflicts

Curriculum Options

- PySDR
- University of Michigan Book
- GNURadio Wiki
- Ossmann Videos
- Mathys article on PAM

- Good intermediate between theory and GNURadio
- Minimal overhead to get started
- Python snippets are easy to assemble into Jupyter Notebooks
- Great animations
- Consistently updated

Curriculum Options

- PySDR
- University of Michigan Book
- GNURadio Wiki
- Ossmann Videos
- Mathys article on PAM

- Great theoretical foundation
- Free
- Contains modern communications concepts
- Free
- Authors have been responsive to emails

Curriculum Options

- PySDR
- University of Michigan Book
- GNURadio Wiki
- Ossmann Videos
- Mathys article on PAM

- Best place to start to learn GNURadio
- Consistently updated
- Easily adaptable to classroom and extensible for projects
- Recommended tutorials:
  - LPFs
  - QPSK
  - Creating an OOT block
  - PMTs

Curriculum Options

- PySDR
- University of Michigan Book
- GNURadio Wiki
- Ossmann Videos
- Mathys article on PAM

- Dated version of GNURadio
- Otherwise, fantastic information
- Easily adaptable to newer versions of GR
- Recommended tutorials:
  - LPFs
  - QPSK
  - Creating an OOT block
  - PMTs
  - FSK

Curriculum Options

- PySDR
- University of Michigan Book
- GNURadio Wiki
- Ossmann Videos
- Mathys article on PAM

- Fantastic as an introduction to GR and Comms
- OR as a mid-level lesson
- Built on an old version of GR, but I can share updated flowgraph
- HIGHLY Recommended

ECE 447 Schedule: Midterm

Lesson	Topics	Reading	Graded Event
1	Introduction to Comms Systems & SDRs	Ch. 1	
2	Theory: Power & Energy Signals	2.1-2.2	2.4; 2.6
3	Theory: Fourier Series/Transform	2.3-2.4	Skills Review due ; 2.10;
4	Theory: Spectral Density, Correlation	2.5-2.6	2.15; 2.16
5	Theory: Frequency Domain	PySDR: Frequency Domain	
6	Intro to SDRs	Supplemental	
7	Theory: Sampling Theory & Hilbert Transform	Ch. 2.7-2.8	
8	Theory: IQ Sampling & Filters	PySDR: IQ Sampling	
9	Introduction to GNURadio	Supplemental	
10	Theory: Linear Modulation (AM)	4.1-4.4	4.1, 4.7
11	Theory: Linear Modulation (AM)/Mixing/Shifting	4.5-4.8	4.9, 4.11
12	Lab: Linear Modulation (AM)		
13	GRC: Data Types/Sampling/Basics	Supplemental	
14	GRC: AM Simulation	Supplemental	
15	GRC: AM Receiver	Supplemental	
16	Flex Day		
17	GR 1		
18	Theory: Angle Modulation	4.11-4.12	4.13, 4.20
19	Theory: Angle Demodulation	4.11-4.12	
20	Lab: Analog FM		

ECE 447 Schedule: Final

Lesson	Topics	Reading	Graded Event
1	Introduction to Comms Systems & SDRs	Ch. 1	
2	Theory: Power & Energy Signals	2.1-2.2	2.4; 2.6
3	Theory: Fourier Series/Transform	2.3-2.4	Skills Review due ; 2.10;
4	Theory: Spectral Density, Correlation	2.5-2.6	2.15; 2.16
5	Theory: Frequency Domain	PySDR: Frequency Domain	
6	Intro to SDRs	Supplemental	
7	Theory: Sampling Theory & Hilbert Transform	Ch. 2.7-2.8	
8	Theory: IQ Sampling & Filters	PySDR: IQ Sampling	
9	Introduction to GNURadio	Supplemental	
10	Theory: Linear Modulation (AM)	4.1-4.4	4.1, 4.7
11	Theory: Linear Modulation (AM)/Mixing/Shifting	4.5-4.8	4.9, 4.11
12	Lab: Linear Modulation (AM)		
13	GRC: Data Types/Sampling/Basics	Supplemental	
14	GRC: AM Simulation	Supplemental	
15	GRC: AM Receiver	Supplemental	
16	Flex Day		
17	GR 1		
18	Theory: Angle Modulation	4.11-4.12	4.13, 4.20
19	Theory: Angle Demodulation	4.11-4.12	
20	Lab: Analog FM		

ECE 448 Schedule: Midterm

Lesson	Topics	Notes
2	Course Overview & Introduction	
3	Noise Figure & Link Budget	
4	Signal Space	
5	PAM Theory	
6	ASCII/PAM	**Theory HW Due**
7	ASCII/PAM	
8	GRC: OOT Modules	
9	GRC: Custom Blocks	
10	GRC: Custom Blocks	
11	Narrowband FM	
12	CW	**Custom Block HW due**
13	WBFM Radio	
14	HD Radio	**CW HW due**
15	HD Radio	
16	mPSK Theory	
17	mPSK	**HD Radio HW due**
18	mPSK	**Assign CTF**
19	FHSS - Tx	
20	FHSS - Rx	
21	GR1/Fox Hunt	**CTF Proj due**

ECE 448 Schedule: Final

Lesson	Topics	Notes
22	RF Reverse Engineering	**Final Project Intro**
23	RF Reverse Engineering	
24	RF Reverse Engineering	
25	DTMF	**Remote HW due**
26	DTMF	**Project Proposal due**
27	DTMF	
28	flex day	
29	ADS-B	
30	Project Work Day	
31	ADS-B	**Background Research due**
32	ADS-B	
33	AIS	
34	AIS	
35	Project Work Day	
36	HD Radio	**Design Description due**
37	HD Radio	
38	QAM	**Prototype Description due**
39	Project Day	**GR2 due**
40	Final Project Presentations	**Final Project due**

Comms in Two Courses

ECE 447: Theory of Comms

1. Signals
2. Intro to SDRs
3. Analog AM
4. Analog AM in GR
5. Analog Angle Modulation
6. FM in GR
7. Noise
8. Digital Modulation
9. FSK in GNURadio
10. Final Exam

ECE 448: SDR Applications

1. Advanced Comms Theory
2. GR PAM
3. GR OOT Modules
4. Common Signals
5. mPSK
6. FHSS
7. RF Remote Hacking
8. Special Topics
9. Final Project

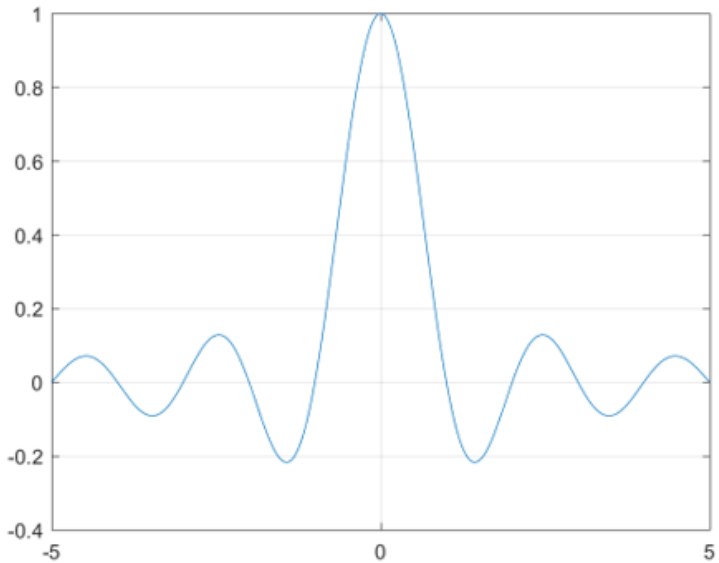
Note: Red text indicates a hands-on component.

ECE 447 Topic Details

ECE 447: Theory of Comms

1. Signals
2. Intro to SDRs
3. Analog AM
4. Analog AM in GR
5. Analog Angle Modulation
6. FM in GR
7. Noise
8. Digital Modulation
9. FSK in GNURadio
10. Final Exam

- Power & Energy
- Fourier Analysis
- Convolution & Correlation



ECE 447 Topic Details

ECE 447: Theory of Comms

1. Signals
2. Intro to SDRs
3. Analog AM
4. Analog AM in GR
5. Analog Angle Modulation
6. FM in GR
7. Noise
8. Digital Modulation
9. FSK in GNURadio
10. Final Exam

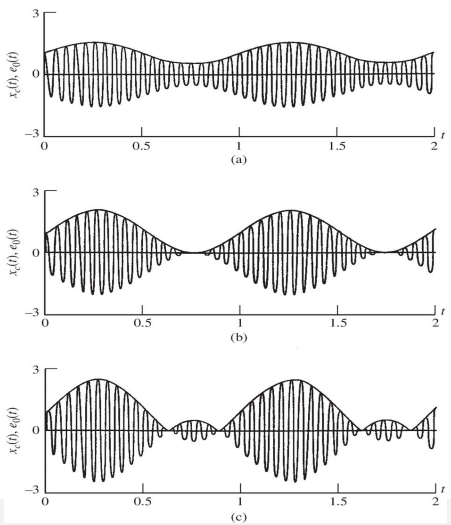
- SDR hardware/software
- IQ Sampling & Data
- Intro to GR
- GR Data types, sampling rate, filters
- ZMQ, data files

ECE 447 Topic Details

ECE 447: Theory of Comms

1. Signals
2. Intro to SDRs
3. Analog AM
4. Analog AM in GR
5. Analog Angle Modulation
6. FM in GR
7. Noise
8. Digital Modulation
9. FSK in GNURadio
10. Final Exam

- AM Theory & Mixing
- DSB-LC
- SSB
- Pulse Modulation
- Analog AM Lab*

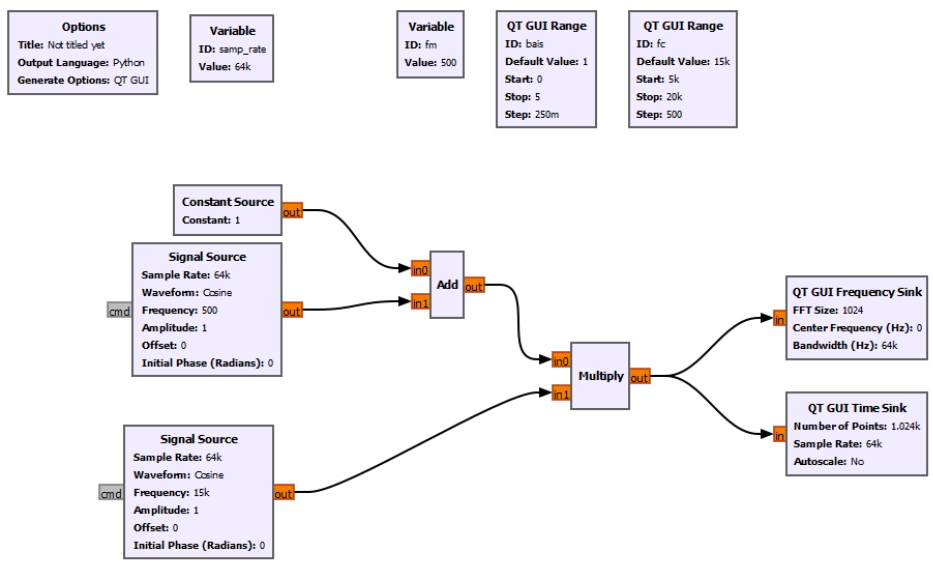


ECE 447 Topic Details

ECE 447: Theory of Comms

1. Signals
2. Intro to SDRs
3. Analog AM
4. Analog AM in GR
5. Analog Angle Modulation
6. FM in GR
7. Noise
8. Digital Modulation
9. FSK in GNURadio
10. Final Exam

- AM Simulation
- AM Receiver



ECE 447 Topic Details

ECE 447: Theory of Comms

1. Signals
2. Intro to SDRs
3. Analog AM
4. Analog AM in GR
5. Analog Angle Modulation
6. FM in GR
7. Noise
8. Digital Modulation
9. FSK in GNURadio
10. Final Exam

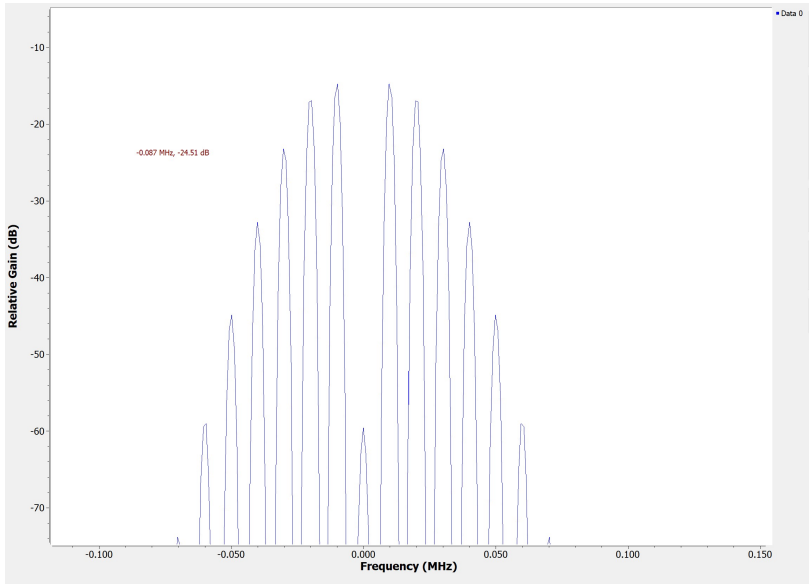
- FM Modulation
- FM Demodulation
- FM Lab*

ECE 447 Topic Details

ECE 447: Theory of Comms

1. Signals
2. Intro to SDRs
3. Analog AM
4. Analog AM in GR
5. Analog Angle Modulation
6. FM in GR
7. Noise
8. Digital Modulation
9. FSK in GNURadio
10. Final Exam

- FM Receiver
- Dual FM Receiver



ECE 447 Topic Details

ECE 447: Theory of Comms

1. Signals
2. Intro to SDRs
3. Analog AM
4. Analog AM in GR
5. Analog Angle Modulation
6. FM in GR
7. Noise
8. Digital Modulation
9. FSK in GNURadio
10. Final Exam

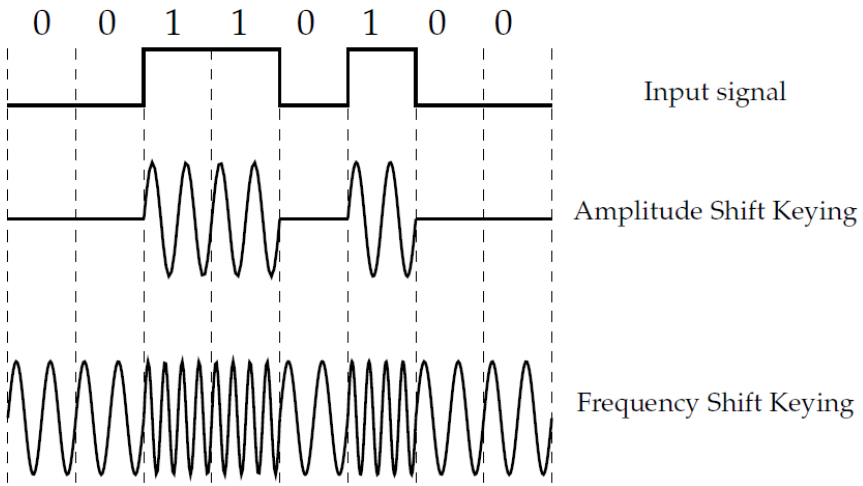
- Random Signals
- Noise in Digital Systems
- Probability of Error

ECE 447 Topic Details

ECE 447: Theory of Comms

1. Signals
2. Intro to SDRs
3. Analog AM
4. Analog AM in GR
5. Analog Angle Modulation
6. FM in GR
7. Noise
8. Digital Modulation
9. FSK in GNURadio
10. Final Exam

- ASK
- FSK
- PSK
- Digital Modulation Lab*



ECE 447 Topic Details

ECE 447: Theory of Comms

1. Signals
2. Intro to SDRs
3. Analog AM
4. Analog AM in GR
5. Analog Angle Modulation
6. FM in GR
7. Noise
8. Digital Modulation
9. FSK in GNURadio
10. Final Exam

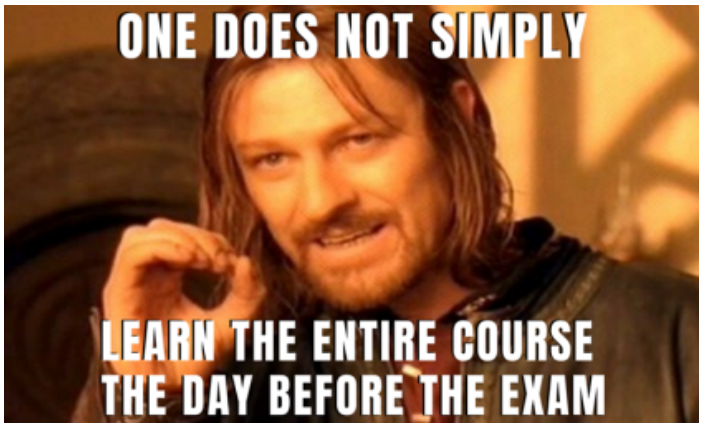
- FSK Tutorial
- FSK Project
  - End-to-end tutorial from Wiki
  - Students provided modulated file data
  - Must build decoder
  - Must be resilient to (low) sample errors

ECE 447 Topic Details

ECE 447: Theory of Comms

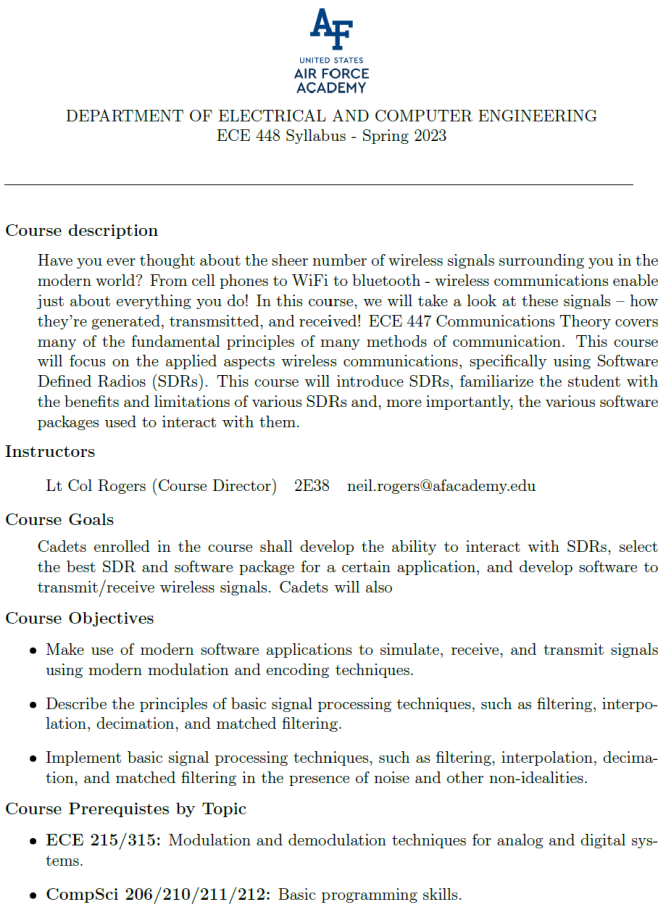
1. Signals
2. Intro to SDRs
3. Analog AM
4. Analog AM in GR
5. Analog Angle Modulation
6. FM in GR
7. Noise
8. Digital Modulation
9. FSK in GNURadio
10. Final Exam

- Institutionally required
- Comprehensive
- Includes sample flowgraphs w/ errors
- Includes questions to test GR literacy



ECE 448: Pick Up Where We Left Off...

- Can't start the course without the syllabus...
- syllabus.sigmf ⟶ syllabus.pdf
- Provided Modulated data of PDF bytes
- Must demodulate to PDF document



UNITED STATES AIR FORCE ACADEMY

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING
ECE 448 Syllabus - Spring 2023

Course description

Have you ever thought about the sheer number of wireless signals surrounding you in the modern world? From cell phones to WiFi to bluetooth - wireless communications enable just about everything you do! In this course, we will take a look at these signals – how they're generated, transmsitted, and received! ECE 447 Communications Theory covers many of the fundamental principles of many methods of communication. This course will focus on the applied aspects wireless communications, specifically using Software Defined Radios (SDRs). This course will introduce SDRs, familiarize the student with the benefits and limitations of various SDRs and, more importantly, the various software packages used to interact with them.

Instructors

Lt Col Rogers (Course Director) 2E38 neil.rogers@afacademy.edu

Course Goals

Cadets enrolled in the course shall develop the ability to interact with SDRs, select the best SDR and software package for a certain application, and develop software to transmit/receive wireless signals. Cadets will also

Course Objectives

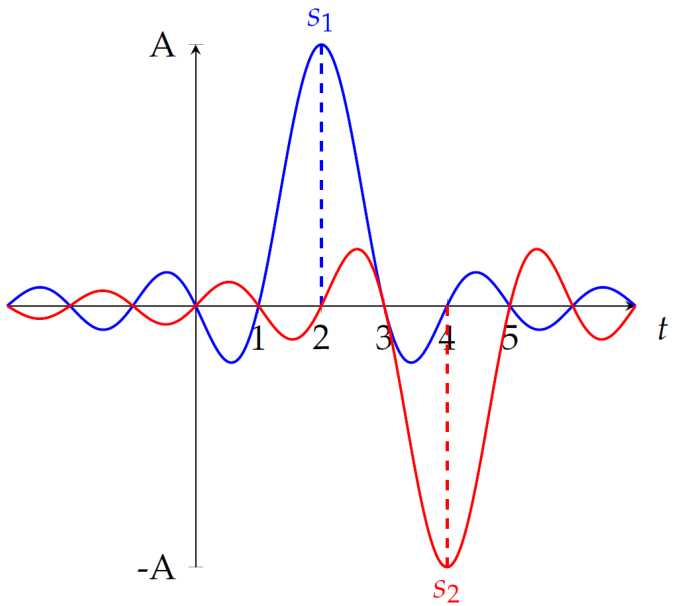
- Make use of modern software applications to simulate, receive, and transmit signals using modern modulation and encoding techniques.
- Describe the principles of basic signal processing techniques, such as filtering, interpolation, decimation, and matched filtering.
- Implement basic signal processing techniques, such as filtering, interpolation, decimation, and matched filtering in the presence of noise and other non-idealities.

Course Prerequistes by Topic

- **ECE 215/315:** Modulation and demodulation techniques for analog and digital systems.
- **CompSci 206/210/211/212:** Basic programming skills.

ECE 448 Topic Details

- Course Intro & Motivation
- Link Budgets & Comms Systems
- Signal Space

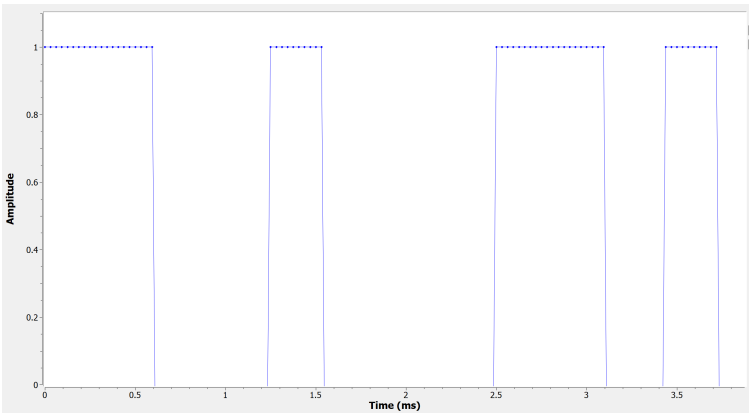


ECE 448: SDR Applications

1. Advanced Comms Theory
2. GR PAM
3. GR OOT Modules
4. Common Signals
5. mPSK
6. FHSS
7. RF Remote Hacking
8. Special Topics
9. Final Project

ECE 448 Topic Details

- PAM Tutorial (Mathys, 2016)
- Hier blocks
- Matched filter project
  - Build new MF hier block
  - Must incorporate multiple pulse shapes



ECE 448: SDR Applications

1. Advanced Comms Theory
2. GR PAM
3. GR OOT Modules
4. Common Signals
5. mPSK
6. FHSS
7. RF Remote Hacking
8. Special Topics
9. Final Project

ECE 448 Topic Details

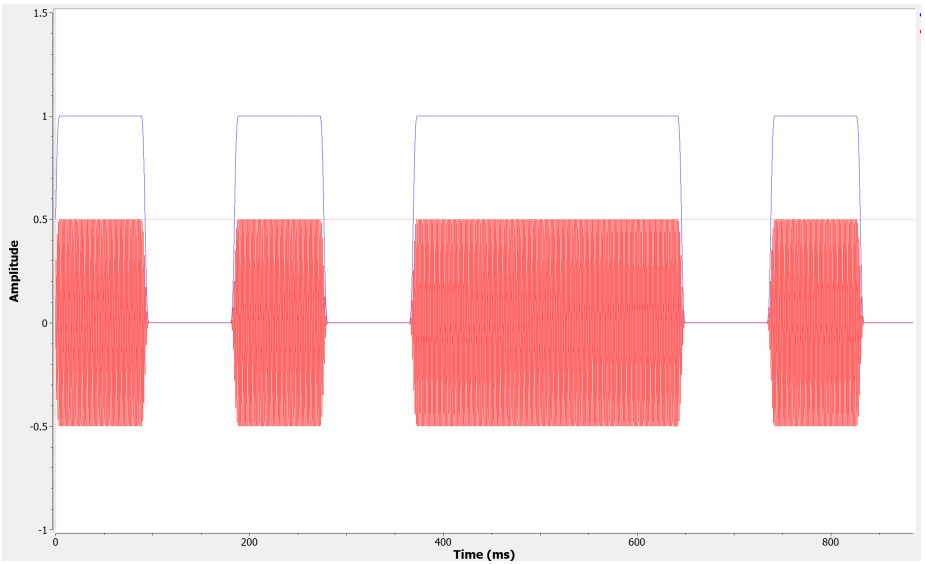
- OOT Module Usage
- Common OOT Modules
- Custom blocks
- Custom block project
  - Build non-trivial block
  - C++ or Python

ECE 448: SDR Applications

1. Advanced Comms Theory
2. GR PAM
3. GR OOT Modules
4. Common Signals
5. mPSK
6. FHSS
7. RF Remote Hacking
8. Special Topics
9. Final Project

ECE 448 Topic Details

- CW generator (@duggabe)
- Build CW decoder

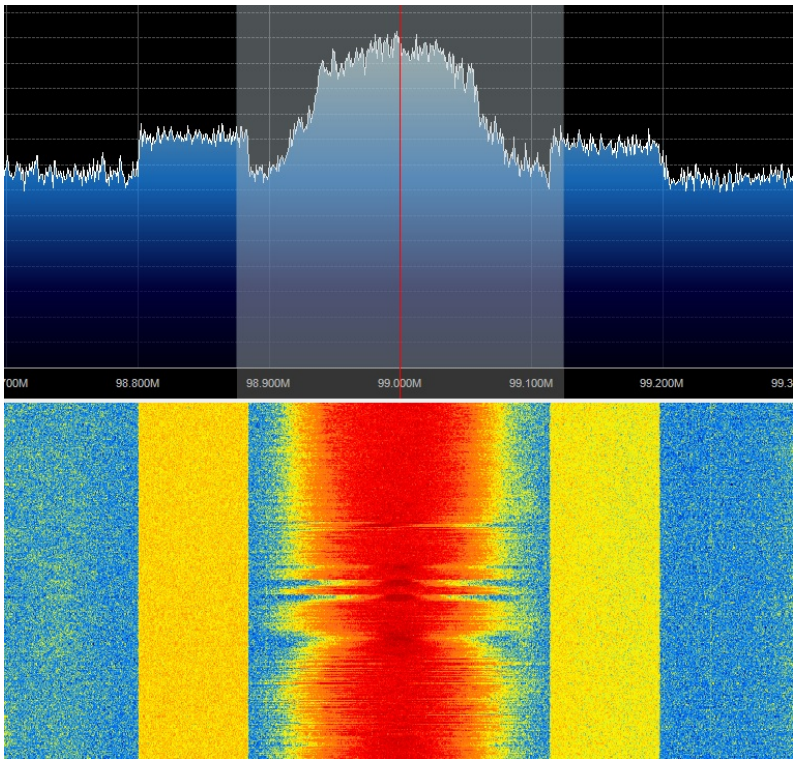


ECE 448: SDR Applications

1. Advanced Comms Theory
2. GR PAM
3. GR OOT Modules
4. Common Signals
5. mPSK
6. FHSS
7. RF Remote Hacking
8. Special Topics
9. Final Project

ECE 448 Topic Details

- HD Radio (thanks @Vlad!)



ECE 448: SDR Applications

1. Advanced Comms Theory
2. GR PAM
3. GR OOT Modules
4. Common Signals
5. mPSK
6. FHSS
7. RF Remote Hacking
8. Special Topics
9. Final Project

ECE 448 Topic Details

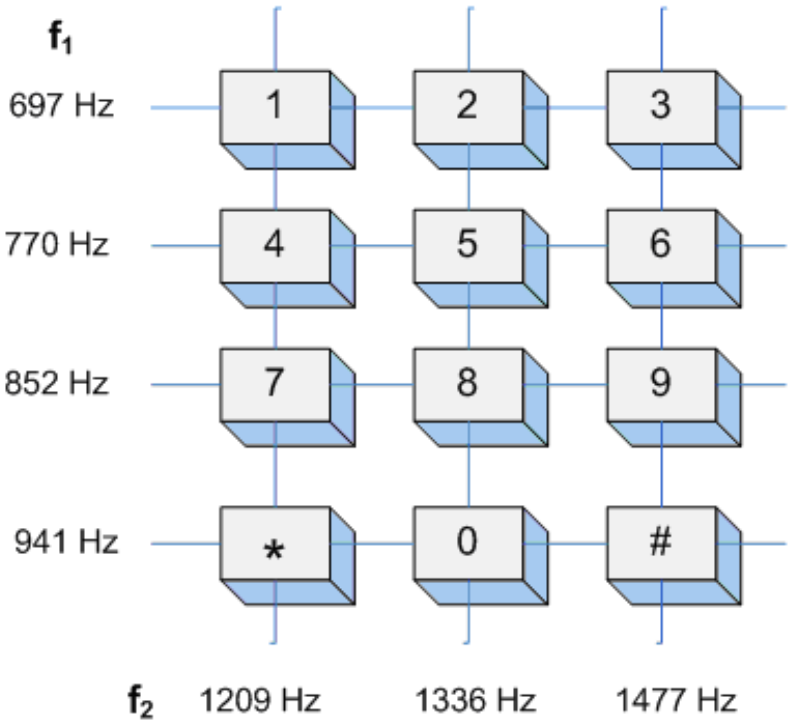
- ADS-B
  - Mode S message breakdown
  - Pymodes, gr-air-modes
  - Mobile device receiving
- AIS
  - NMEA Message structure
  - AIVDM generator, NRZI encoding, GMSK mod
  - AIS Simulator
  - @vtmichael?!

ECE 448: SDR Applications

1. Advanced Comms Theory
2. GR PAM
3. GR OOT Modules
4. Common Signals
5. mPSK
6. FHSS
7. RF Remote Hacking
8. Special Topics
9. Final Project

ECE 448 Topic Details

- DTMF generator
- DTMF receiver

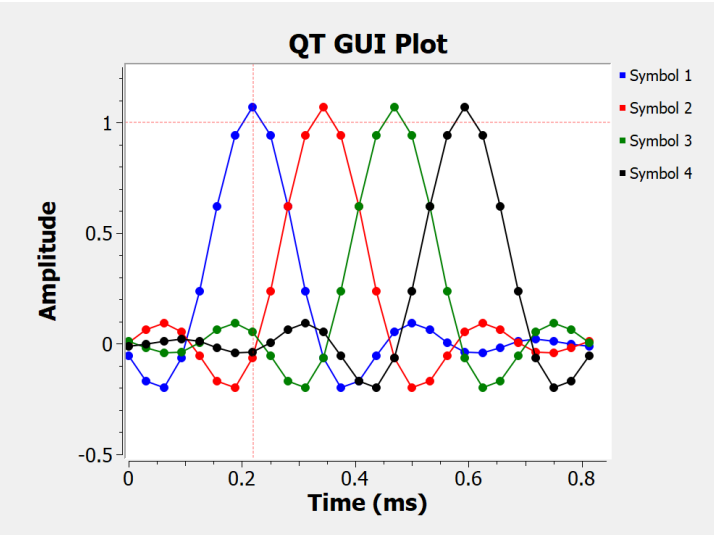


ECE 448: SDR Applications

1. Advanced Comms Theory
2. GR PAM
3. GR OOT Modules
4. Common Signals
5. mPSK
6. FHSS
7. RF Remote Hacking
8. Special Topics
9. Final Project

ECE 448 Topic Details

- mPSK Overview
- mPSK Tutorial

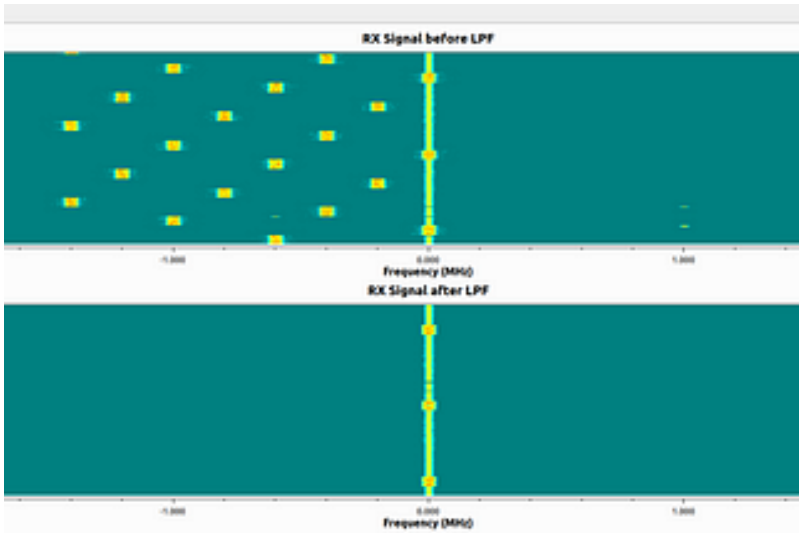


ECE 448: SDR Applications

1. Advanced Comms Theory
2. GR PAM
3. GR OOT Modules
4. Common Signals
5. mPSK
6. FHSS
7. RF Remote Hacking
8. Special Topics
9. Final Project

ECE 448 Topic Details

- FHSS (Medium @Solomon)
- Modify FHSS generator to be random



ECE 448: SDR Applications

1. Advanced Comms Theory
2. GR PAM
3. GR OOT Modules
4. Common Signals
5. mPSK
6. FHSS
7. RF Remote Hacking
8. Special Topics
9. Final Project

ECE 448 Topic Details

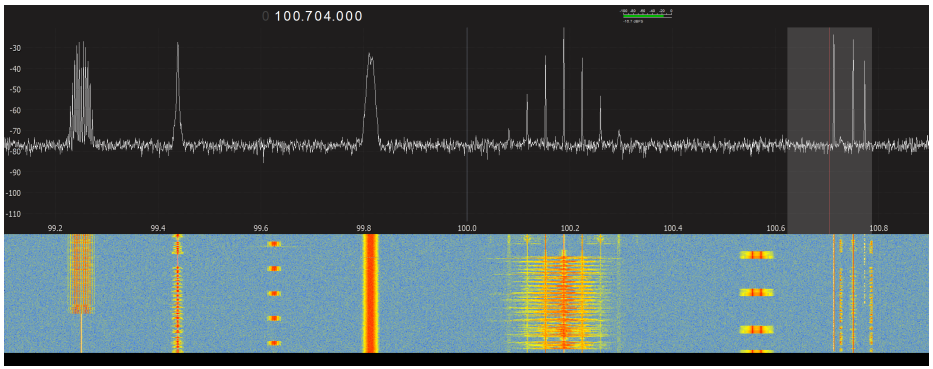
- URH Intro
- PPM
- Remote Reverse Engineering
- Build flowgraph to Tx remote signal

ECE 448: SDR Applications

1. Advanced Comms Theory
2. GR PAM
3. GR OOT Modules
4. Common Signals
5. mPSK
6. FHSS
7. RF Remote Hacking
8. Special Topics
9. Final Project

ECE 448 Topic Details

- FMCW
- GRCon CTF fun
- Other interesting topics



ECE 448: SDR Applications

1. Advanced Comms Theory
2. GR PAM
3. GR OOT Modules
4. Common Signals
5. mPSK
6. FHSS
7. RF Remote Hacking
8. Special Topics
9. Final Project

ECE 448 Topic Details

ECE 448: SDR Applications

1. Advanced Comms Theory
2. GR PAM
3. GR OOT Modules
4. Common Signals
5. mPSK
6. FHSS
7. RF Remote Hacking
8. Special Topics
9. Final Project

ECE 448 Final Project

- Starts around midterm
- Milestones drive work
- FPV Decoder (mod gr-ntsc)
- GR RC Control
- NOAA Image Decoding

ECE 448 Final Project

- Starts around midterm
- Milestones drive work
- FPV Decoder (mod gr-ntsc)
- GR RC Control
- NOAA Image Decoding

Project Proposal

Background Research

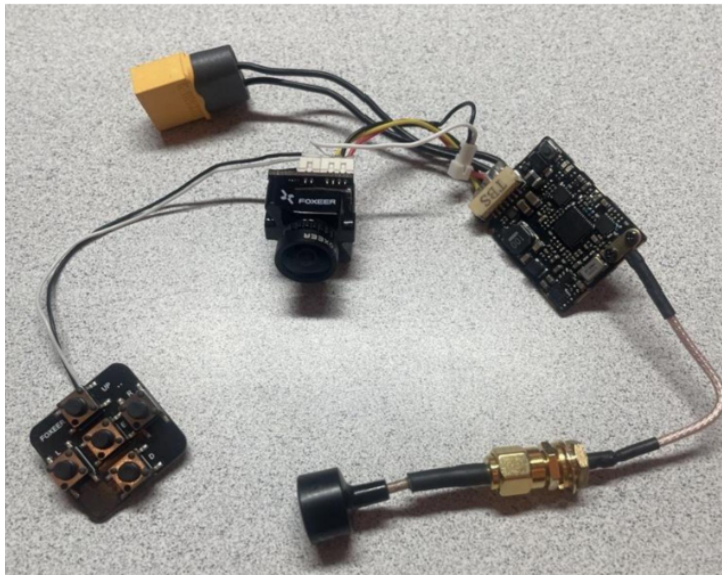
Design Description

Prototype Description

Final report & demo

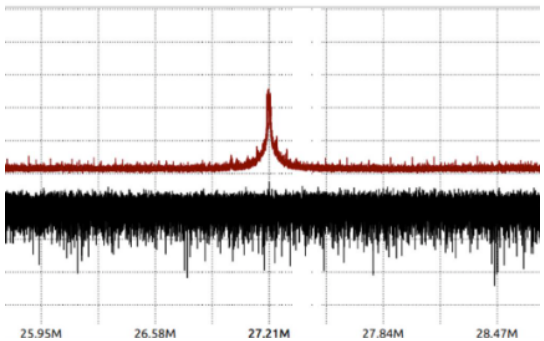
ECE 448 Final Project

- Starts around midterm
- Milestones drive work
- FPV Decoder (mod gr-ntsc)
- GR RC Control
- NOAA Image Decoding



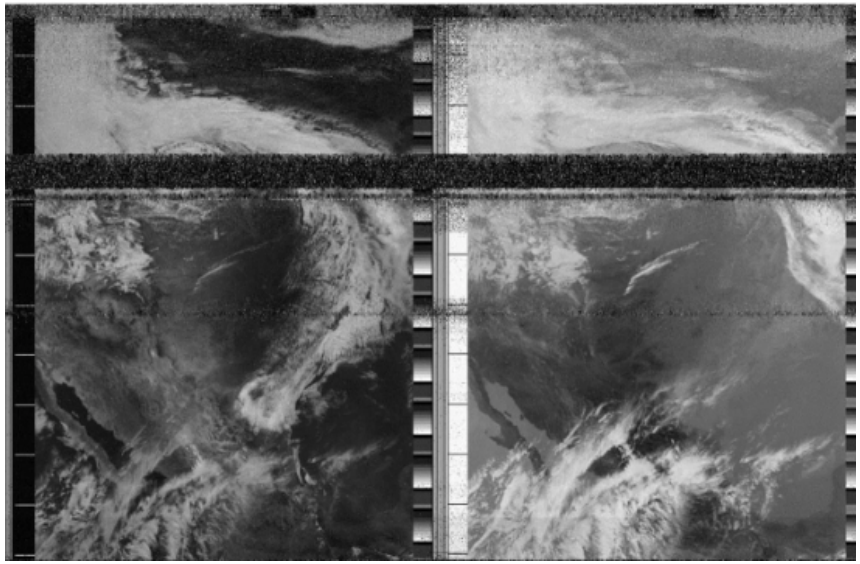
ECE 448 Final Project

- Starts around midterm
- Milestones drive work
- FPV Decoder (mod gr-ntsc)
- GR RC Control
- NOAA Image Decoding



ECE 448 Final Project

- Starts around midterm
- Milestones drive work
- FPV Decoder (mod gr-ntsc)
- GR RC Control
- NOAA Image Decoding



Questions/Discussion

1. What topics are you interested in teaching that are not on the schedule?
2. What labs/activities have you taught that weren't reflected in our lesson?
3. What tools do you prefer to use?
4. What resources do you prefer to use?
5. What gaps do you see in my plan?
6. What resources do you wish you had?
7. Is anything holding you up from moving forward in what you want to do?
8. How can I help you get started with GNURadio in the classroom?
9. What is your favorite hardware combination to use?

Thank You!

Neil Rogers
Email: neil.rogers@afacademy.af.edu
Matrix Chat: @livethisdream