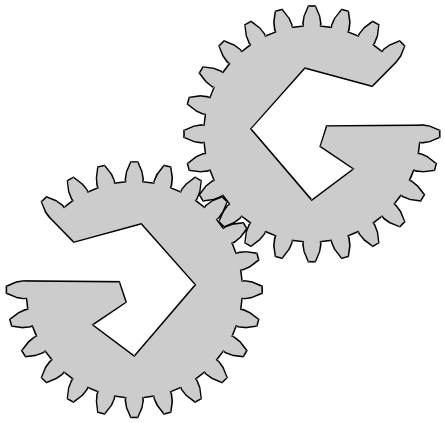


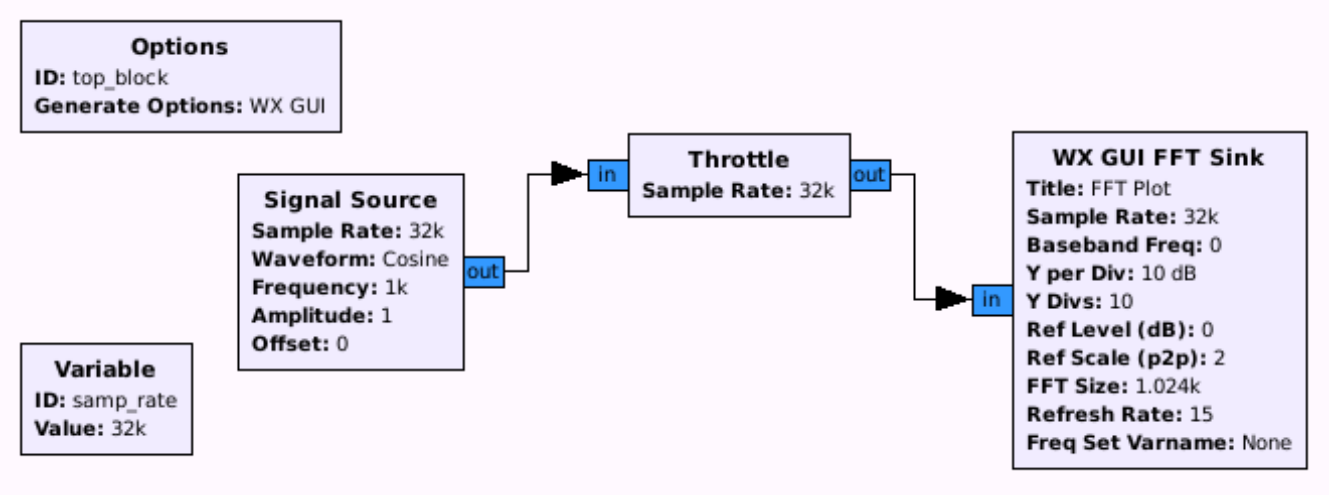
GREAT SCOTT GADGETS

Software Radio Workshop Exercises

October 2012

Exercise 1

Create a flow graph in GRC (gnuradio-companion):



Execute the flow graph.

A) Does it behave differently if you remove the throttle block?

B) Does the FFT sink correctly indicate the frequency produced by the source? What if the source and sink have different sample rates configured?

C) What happens if you configure the signal source with various frequencies between 0 and 16k?

D) What if you specify frequencies greater than 16k? Any idea why?

E) What if you specify negative frequencies? Mathematically, is there a difference between cos(x) and cos(-x)?

F) Does the plot indicate the presence of any frequencies other than the one produced by the source? (hint: autoscale) What is the average amplitude of this noise? What is the signal to noise ratio (SNR) in dB? As a ratio? Why is there any noise at all? Could an analog system achieve a better SNR?

G) Try multiple signal sources added together. Are there any other interesting operations you could try?

H) Try various waveforms (instead of cosine) in the signal source.

Exercise 2

(adapted from *Practical Signal Processing* by Mark Owen)

A weather station measures wind direction once per minute. Write a program to indicate the average direction over a five minute period. Try it on the following sets of readings:

- 12°, 15°, 13°, 9°, 16°
- 358°, 1°, 359°, 355°, 2°
- 210°, 290°, 10°, 90°, 170°

A) Modify your program to handle wind speed input in addition to direction.

Exercise 3

Create a flow graph in GRC as shown in Exercise 1. Add a scope sink.

A) How do the scope and FFT change if you change the data type of every block from complex to float?

B) When using the float data type, what happens if you specify a negative source frequency? (see Exercise 1E)

Exercise 4

Find the FCC filing for the XyLoc tag (ID: NW5MK). Use the information found there to answer the following questions.

A) At what frequency does the device transmit?

B) What modulation scheme (such as ASK, FSK, or PSK) is employed?

C) What is the duration of a single transmission (packet)?

D) What is the bandwidth of the transmission?

E) How often is a packet transmitted? What is the duty cycle?

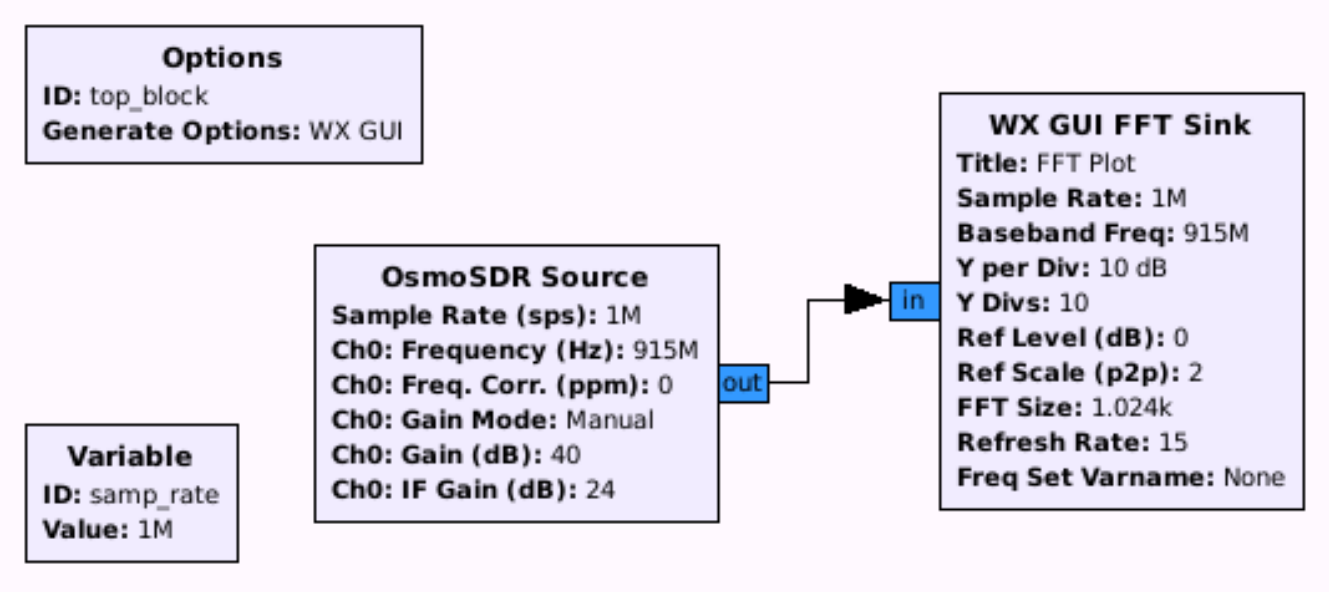
F) Can you identify any integrated circuits or other particular components used in the device?

G) Does the tag receive, transmit or both? How about the dongle (ID: NW5LKA)?

H) What is the symbol rate or what might it be?

Exercise 5

Create a flow graph in GRC:



Tune the receiver (by setting the frequency in the source block) according to the information learned in Exercise 5.

A) Do you see bursts that might be produced by the tag? Do you see them as often as you expect?

B) Try a waterfall sink instead of the FFT sink.

C) Add a file sink and run the flow graph for a few seconds. Then open the file in Baudline. (hint: raw format, 2 channels, quadrature, flip complex, 32 bit float, little endian)

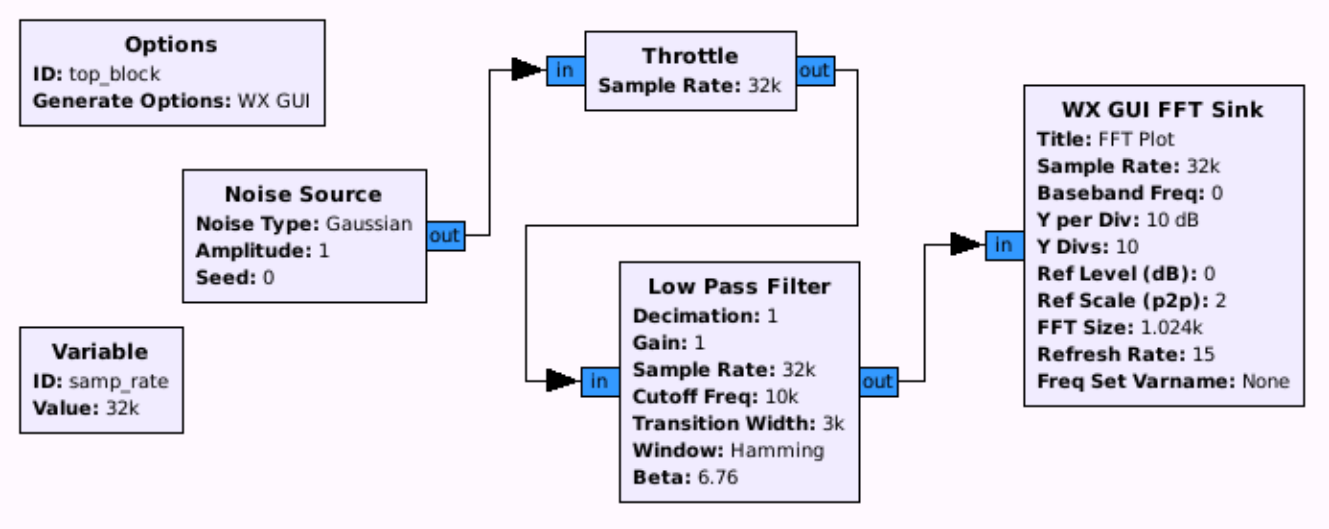
D) Try zooming in and out of the spectrogram in Baudline. Open a waveform window. Try zooming in and out in this window.

E) What block could be added to the flow graph to eliminate much of the gaps between packets?

F) Try opening the saved file with other tools such as Octave, SciPy, GNU Radio executables, od -f, etc.

Exercise 6

Create a flow graph in GRC:



Add variable sliders to control the filter's cutoff frequency and transition width (minimum: samp_rate/1000, maximum: samp_rate/2).

A) Observe how the filter's frequency response changes when adjusting the sliders.

B) Check your CPU utilization with the transition width set to the minimum (samp_rate/1000). How does it compare to the utilization observed with the transition width set to a moderate value (samp_rate/10)?

C) Try band pass and high pass filters.

D) Change all the data types from complex to float and try low pass, band pass, and high pass filters.

Exercise 7

Use a transmitter to replay transmissions from a XyLoc tag.

A) Can you reliably spoof the original tag?

B) Consider adding a filter to your flow graph. Good idea or bad idea?

C) What methods might you use to pre-process a captured waveform before re-transmission?

Exercise 8

Identify the modulation schemes used in the transmissions captured in the modulation-samples directory of the workshop flash drive. (hint: use both the spectrogram and waveform views in Baudline)

A) mod1-314MHz-4Msps.cfile was captured at 314 MHz at a rate of 4 million samples per second (4 Msps). Any idea what common device might have produced this signal?

B) mod4.wav: Use “auto magic” file format to open this acquisition in Baudline. What is the sample rate of the file?

C) mod3-917MHz-1Msps.cfile: Locate the signal with the highest power in this acquisition. (hint: zoom out in the waveform window) What is the duration of each transmission? Can you identify any other transmissions in this sample?

D) mod2-0Hz-250ksps.cfile: Can you find a signal at 60 kHz? Try various FFT sizes (process -> transform size). What is the bandwidth of this signal? What is the symbol rate? Can you identify the source of this signal?

Exercise 9

Decode a packet from an acquisition of a XyLoc transmission.

1. Based on your knowledge of the transmitter, what demodulation method should be used? Plot the output of the demodulator.

2. What sort of output does the demodulator produce between packets? Is there a way to eliminate or reduce this?

3. Can the quality of the demodulator output be improved by filtering the signal before demodulation?

4. How many symbols appear to be used? Is it a binary modulation (two symbols) or something more complicated?

5. Can you determine the symbol rate?

6. Run the demodulator output through a symbol synchronizer. Try the Clock Recovery MM block in GRC with the following parameters:

   - Omega: the number of samples per symbol
   - Gain Omega: 0.0075
   - Mu: 0
   - Gain Mu: 0.175
   - Omega Relative Limit: 0.005

   Verify that the block produces one output item per symbol.

7. It is common for a wireless communication protocol to begin each transmission with a static frame synchronization sequence. Determine the sequence used by XyLoc.

8. Use a Correlate Access Code block to flag occurrences of the frame synchronization sequence.

9. Look at the symbols of a frame following the synchronization sequence. Do you see any trends? Can you guess what encoding method is used?

10. Can you determine how the tag ID number is encoded in the frame? (hint: compare transmissions from multiple tags)

11. Write a program (or GNU Radio block) that automatically decodes the ID number for each frame that is detected.

Exercise 10

Write a program to compute the DFT of a signal. What is the DFT of the following sequences?

A) 0.3535, 0.3535, 0.6464, 1.0607, 0.3535, -1.0607, -1.3535, -0.3535

B) 1, 0+j, -1, 0-j, 1, 0+j, -1, 0-j

C) 1, 0, 0, 0, 0, 0, 0, 0

D) 1, 0, 0, 0

E) 1, 1, 0, 0, 0, 0, 0, 1