

GPS Signal Processing

Pengluo Wang & Yang Mi

Start with Side Dishes

- Use of GPS in the Gulf War
 - Before the Gulf War, localization is mainly achieved by using fixed landmarks as references.
 - Under severe conditions, landmarks will have great uncertainty, making it hard to locate position accurately.
 - GPS allowed the alliance to know their accurate positions, and also enabled precision strike to the enemies.

Start with One More Side

- Xingxin Gao got scolded by Chinese media because of a paper.
 - She derived Beidou's civil PRN code before it has been released by Chinese government four years later.
- Is she really a traitor, as said by some mainstream?
 - No. It actually helped other scientists analyze Beidou signal characteristics on an early stage, which is beneficial for the development of Beidou.
- How did she derive civil code?
 - Can military code be derived in the same manner?

Outline

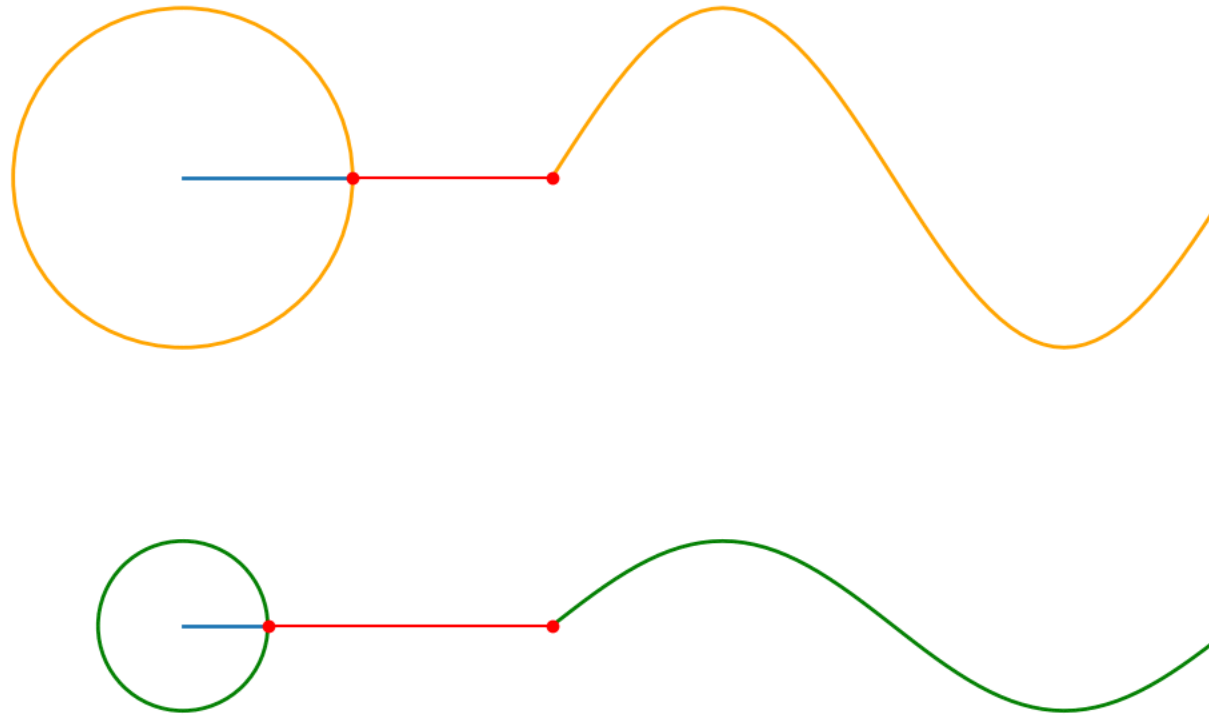
- Digital signal processing (DSP) background
 - Signals, modulation, and correlation
- GPS signal structure
 - Carrier wave, pseudorandom code, and navigation message
- Data demodulation
 - Signal acquisition and tracking

DSP Background

Signals, data modulation, and correlation

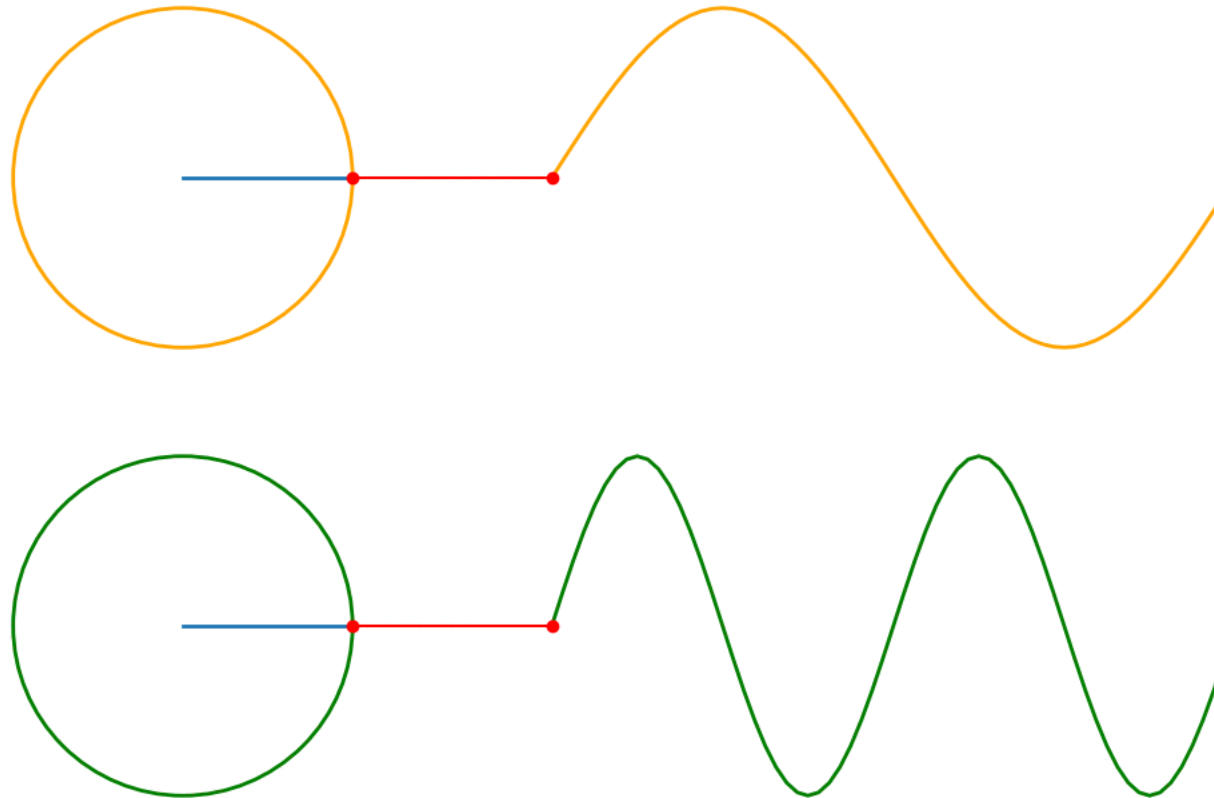
DSP Background – Signals

- Amplitude



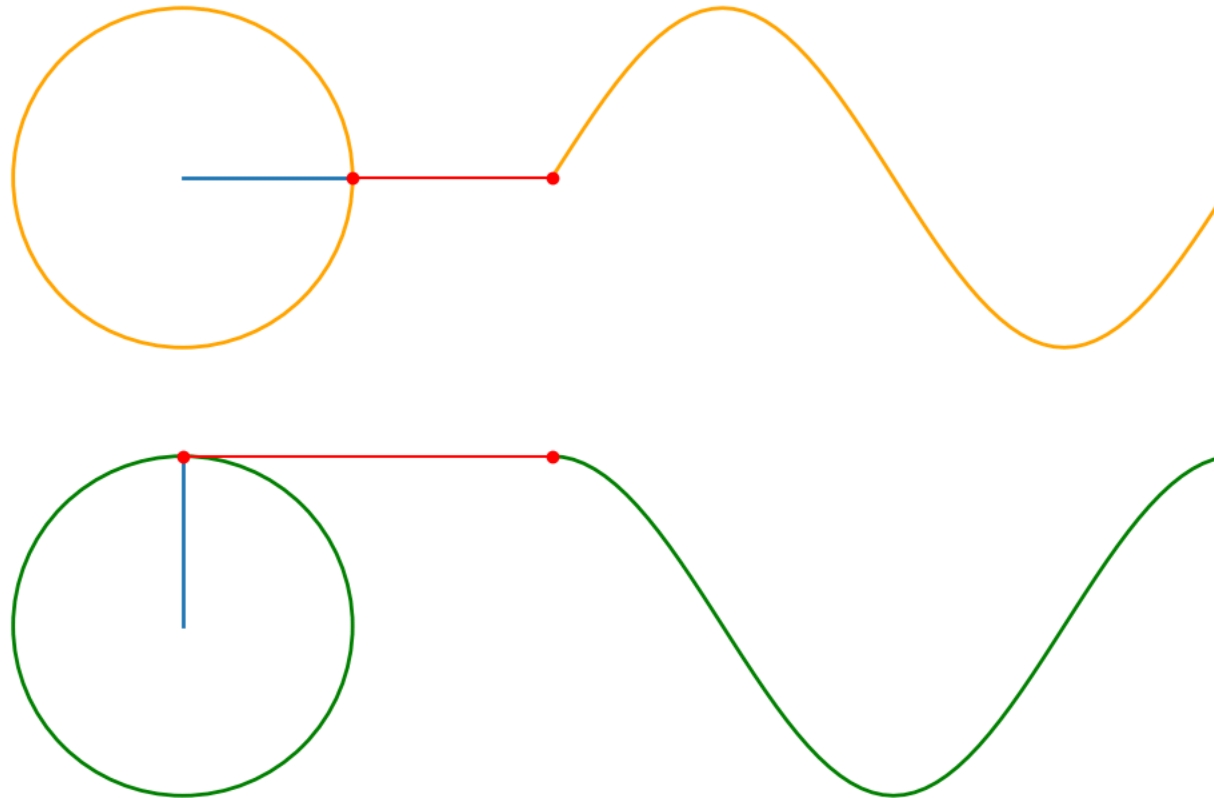
DSP Background – Signals (cont'd)

- Frequency



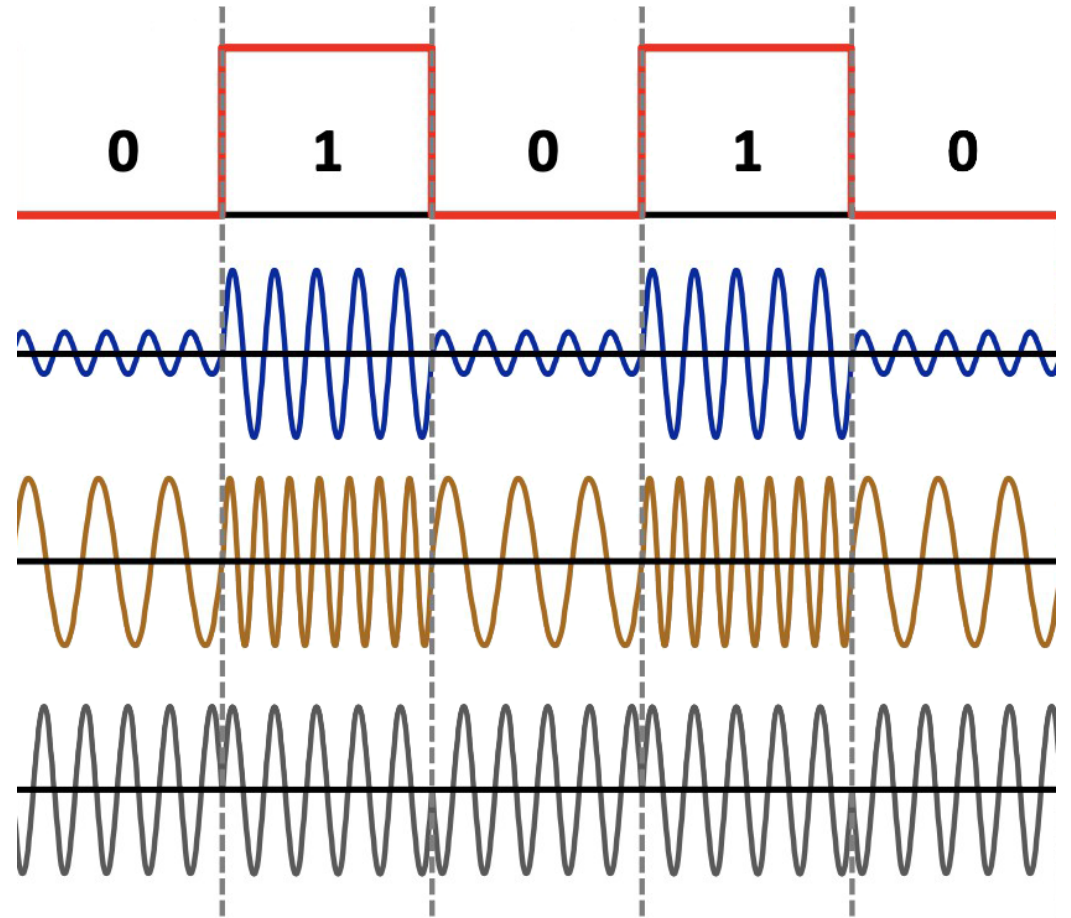
DSP Background – Signals (cont'd)

- Phase



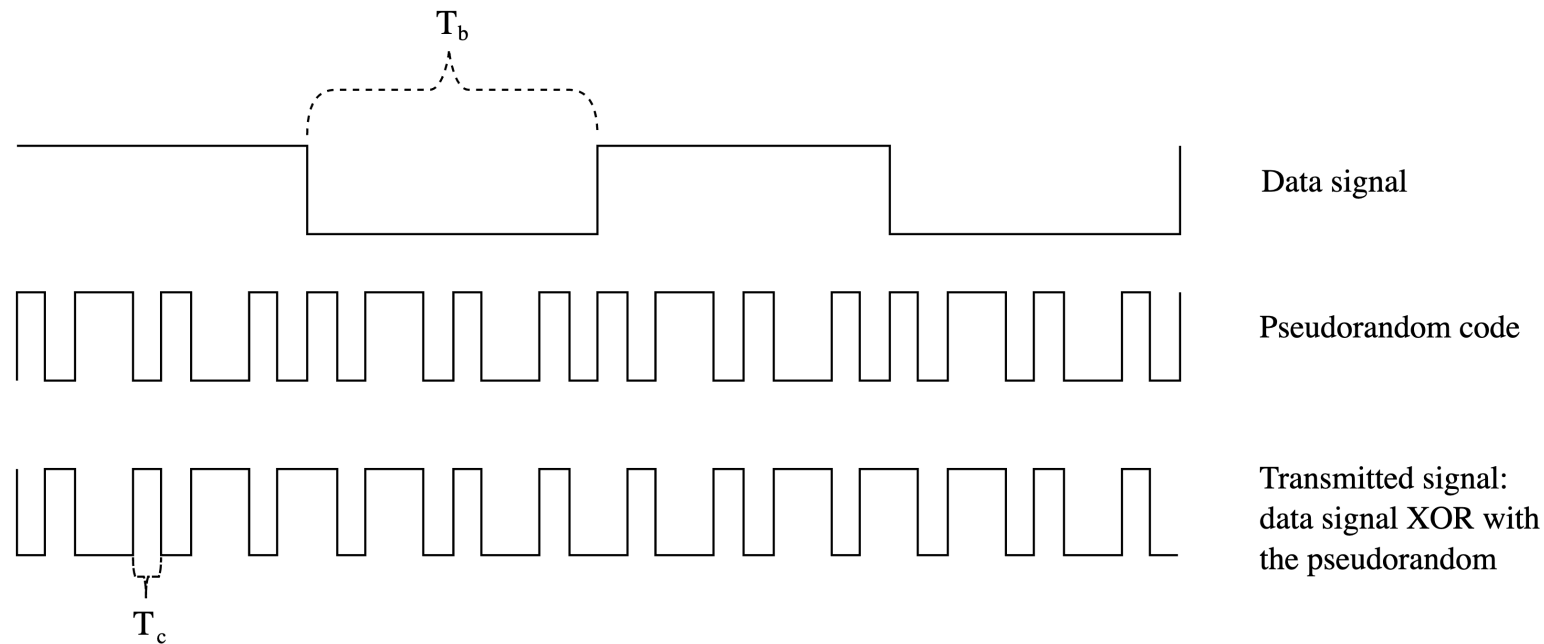
DSP Background – Modulation

- Amplitude Shift Key (ASK)
 - modulate on amplitude
- Frequency Shift Key (FSK)
 - modulate on frequency
- Phase Shift Key (PSK)
 - modulate on phase
- Only one user is allowed for one frequency band.



DSP Background – CDMA

- Code-division multiple access (CDMA) is used for allowing *multiple* users on one frequency band at the same time.
 - Each user has a specific pseudorandom noise (PRN) code for identification.

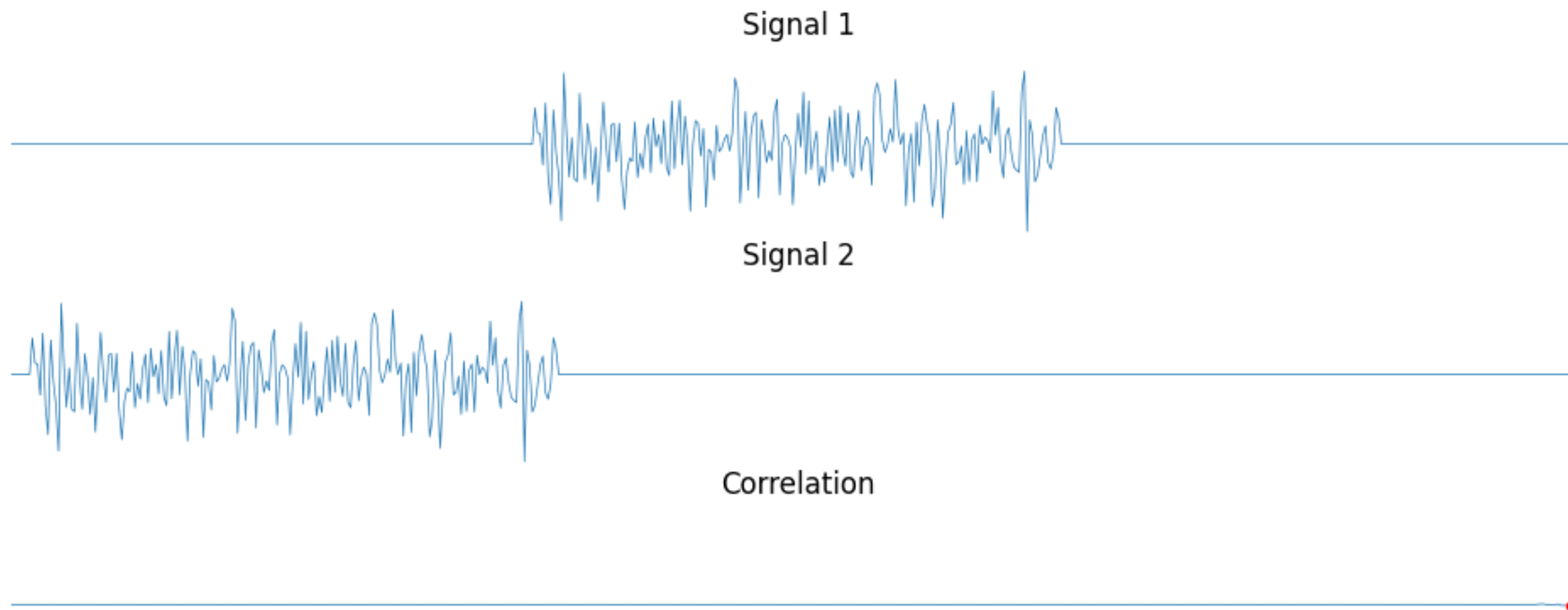


DSP Background – Demodulation of CDMA

- PRN code functions as a key for communication with received signal and the user.
 - Different users have different keys (PRN codes).
 - One door (data modulated for one user) can be only opened by one key.
 - Inserting the key into the door is done by *correlation*.
- User will generate PRN code locally to correlate with received signal.
 - If signal matches the local PRN code, the correlation will be high.
 - Data information is indicated by the sign (\pm) of correlation result, this process is called data *demodulation*.

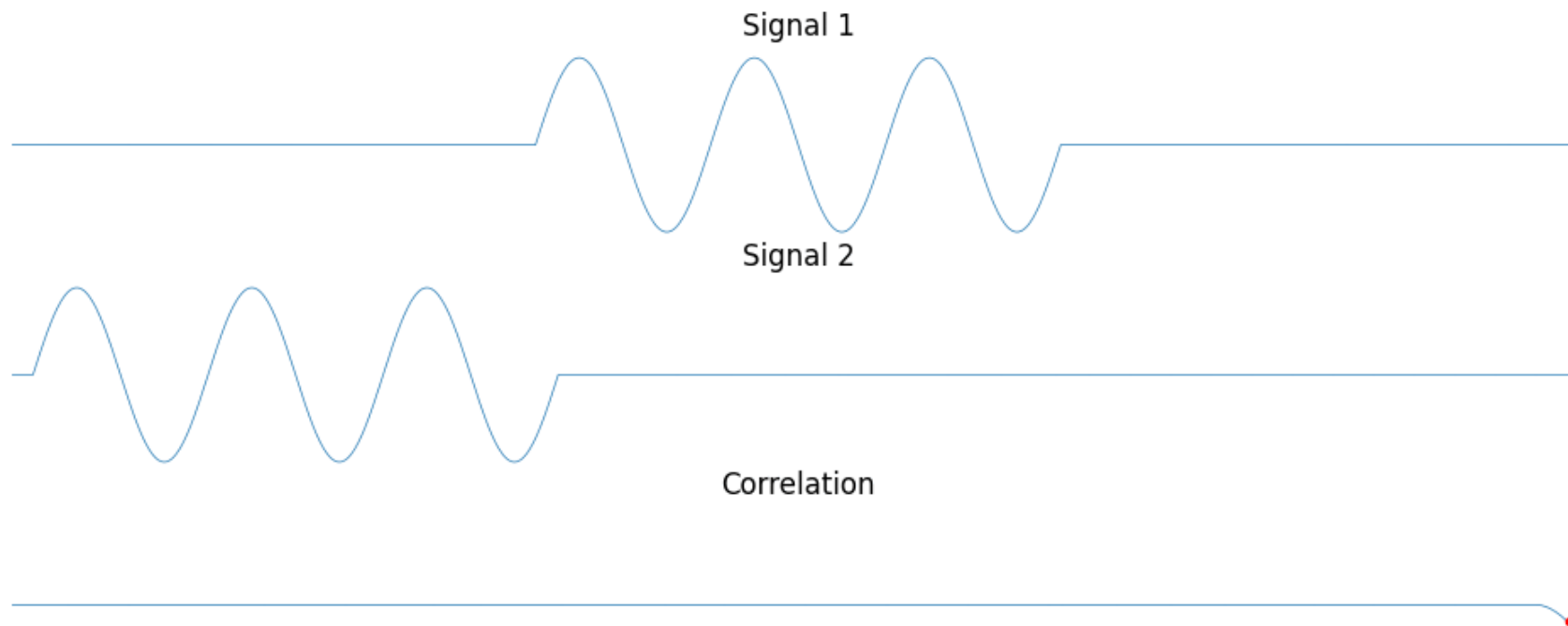
DSP Background – Correlation

- Correlation measures the similarity of two signals.



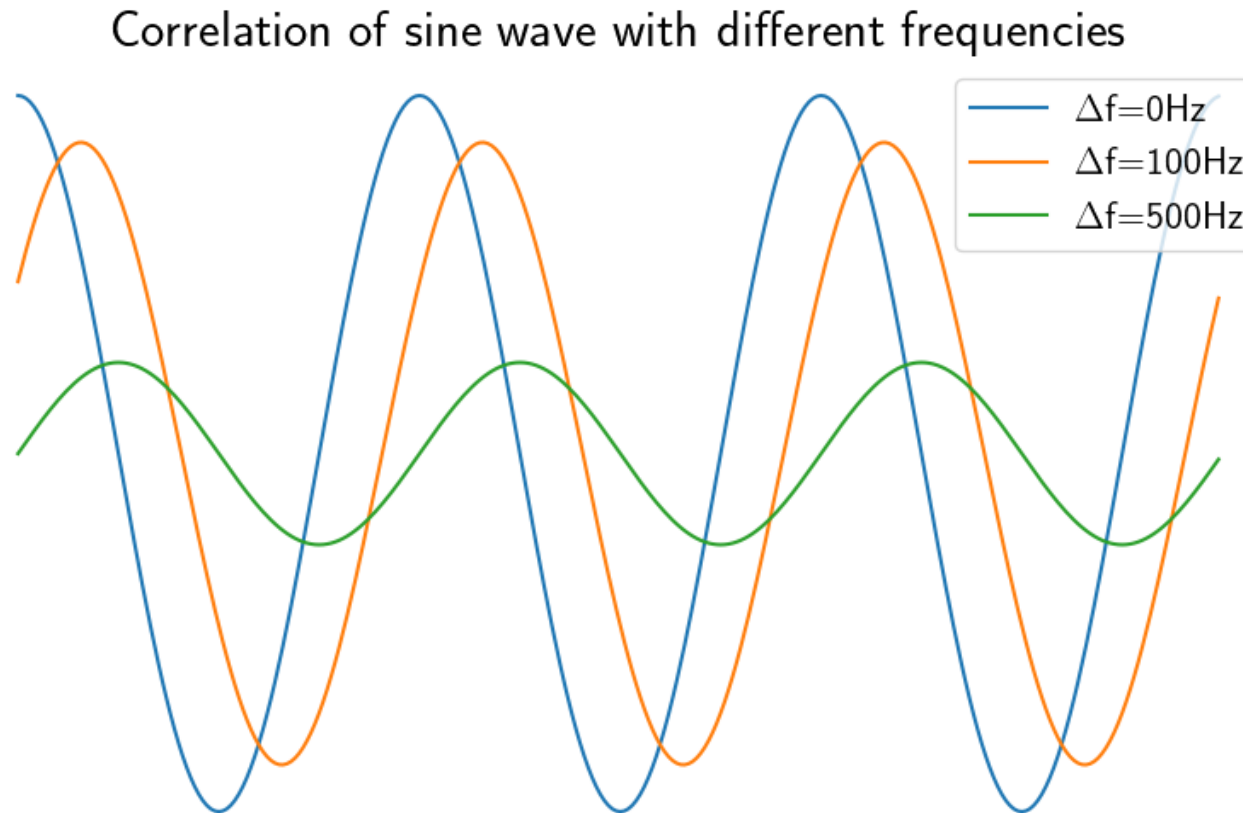
DSP Background – Correlation (cont'd)

- Correlation measures the similarity of two signals.



DSP Background – Correlation (cont'd)

- Correlation measures the similarity of two signals.



DSP Background – Correlation (cont'd)

- Correlation definition

$$R_{xy}[m] = \sum_{n=-\infty}^{\infty} x[n]y^*[n - m]$$

- Some key points:

- Random noise $r[n]$ only correlates with itself

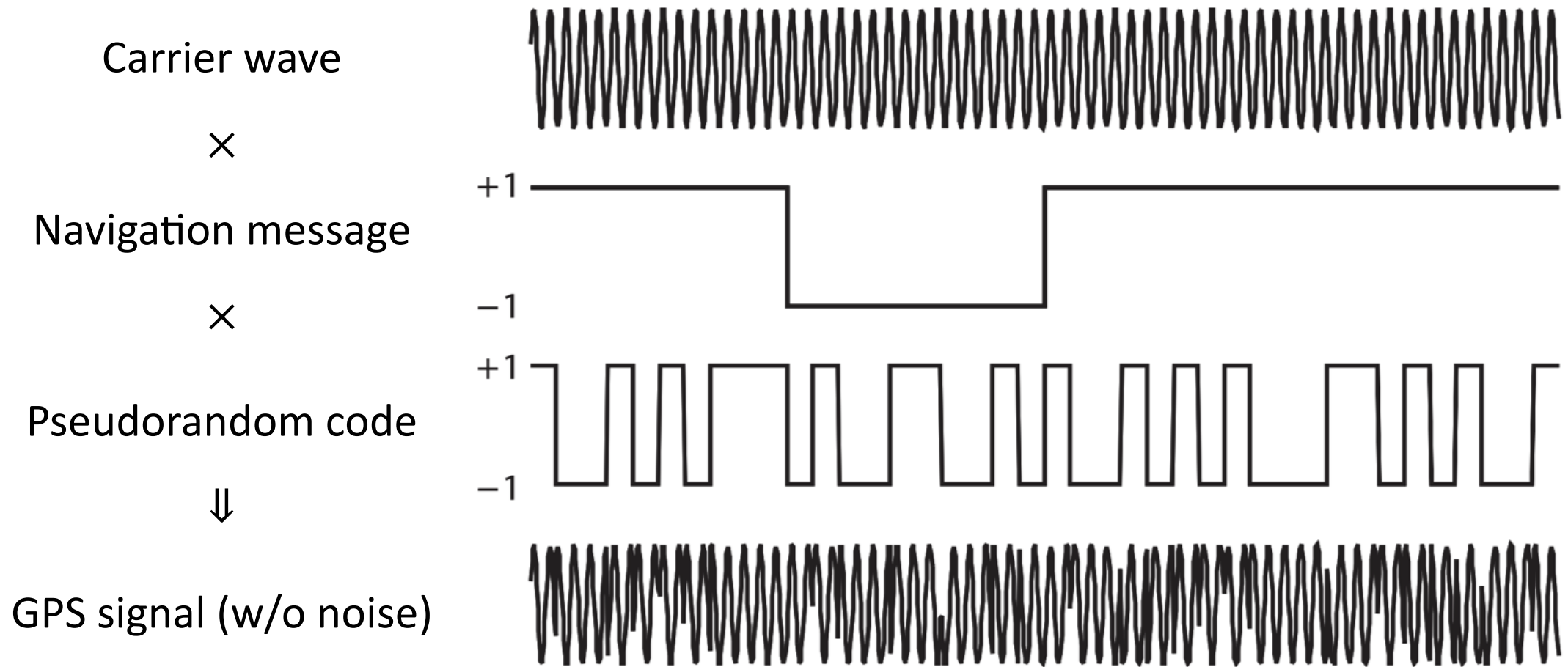
$$R_{rr}[m] = \begin{cases} 1, & m = 0 \\ 0, & \text{otherwise} \end{cases}$$

- The more sinusoid signal frequencies differ, the less their correlation will be.

GPS Signal Structure

Carrier wave, pseudorandom code, and navigation message

GPS Signal Structure



Carrier Wave

- Sine wave with frequency of 1575.42 MHz .
 - High frequency ensures users to receive accurate data under all weather conditions.
 - High frequency will also lead to strong degradation, thus received signals are rather weak, like the light from a 25W lightbulb shining 20,00 km away.
- Due to Doppler effect, received carrier frequency may be different.
 - The faster the user moves, the bigger the frequency difference will be.
 - Typically Doppler shift (frequency difference) is within $\pm 10 \text{ kHz}$.

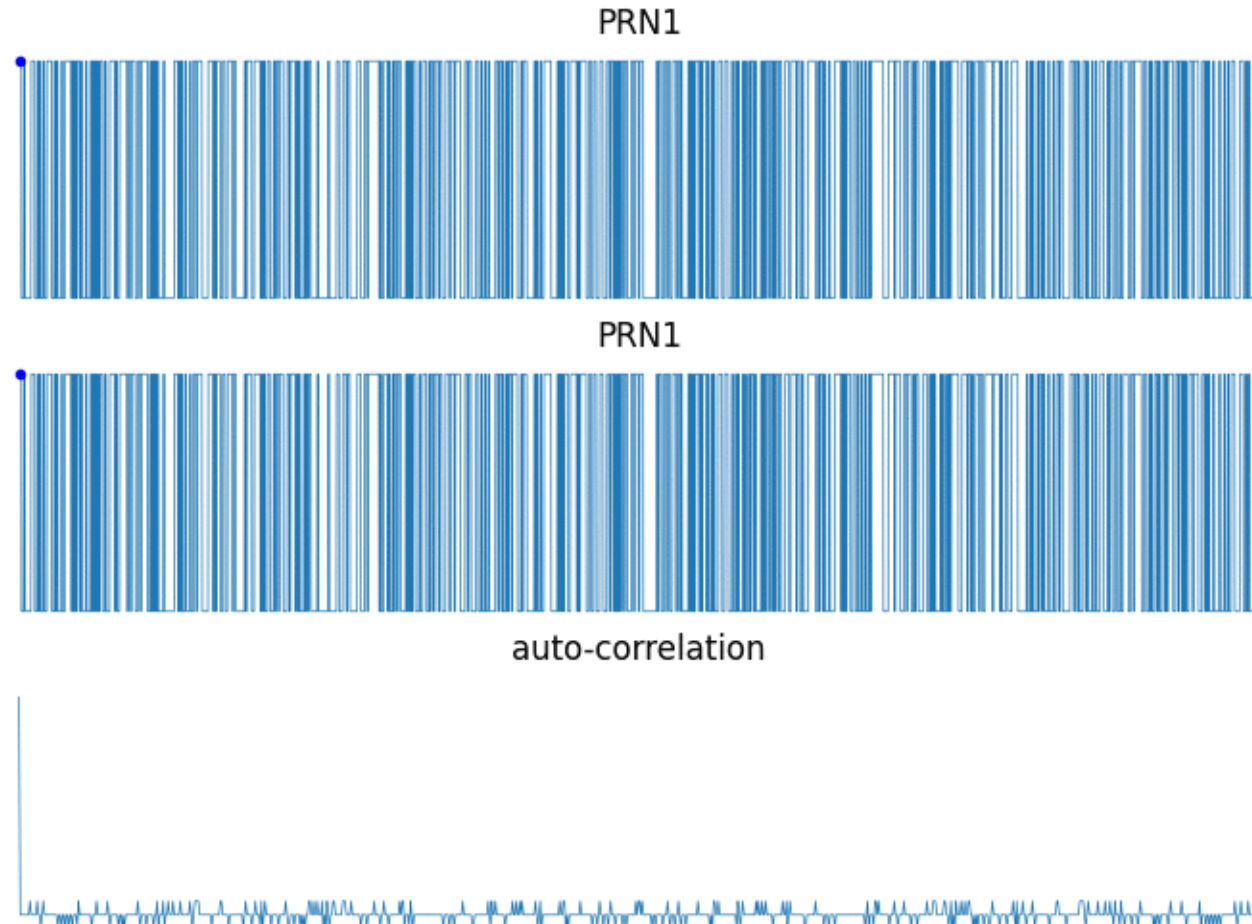
C/A Code and P code

- Two kinds of *pseudorandom noise* (PRN) codes are modulated.
- Coarse/acquisition (C/A) code with 1023 chips, chip rate 1.023 *MHz*.
 - Code sequence is open for civil use.
 - Each satellite will have a specific code with a period of 1 *ms*.
- Precise (P) code with 2.35×10^{14} chips, chip rate 10.23 *MHz*.
 - The original period of P code is more than half a year, it's been cut to a period of 1 week when broadcast by each satellite.

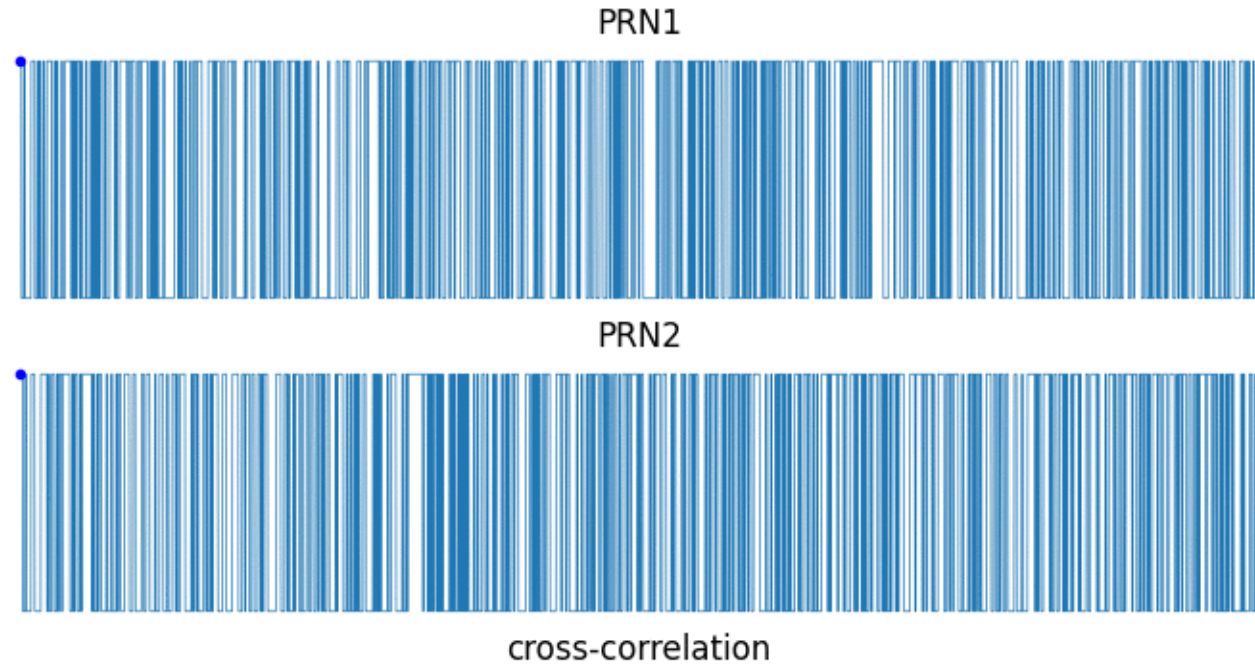
More on C/A Code and P Code (cont'd)

- Recall Xingxin Gao's work to derive BeiDou C/A code.
- Deriving C/A code sequence is not hard, but
 - it requires a received signal lasting for 50 C/A code period (50 *ms*).
- Well, using same method for hacking military code, you have to
 - collect signal for almost a year (50 weeks), and
 - gamble that the military encrypted code won't change during that time.

PRN Code – Auto-correlation



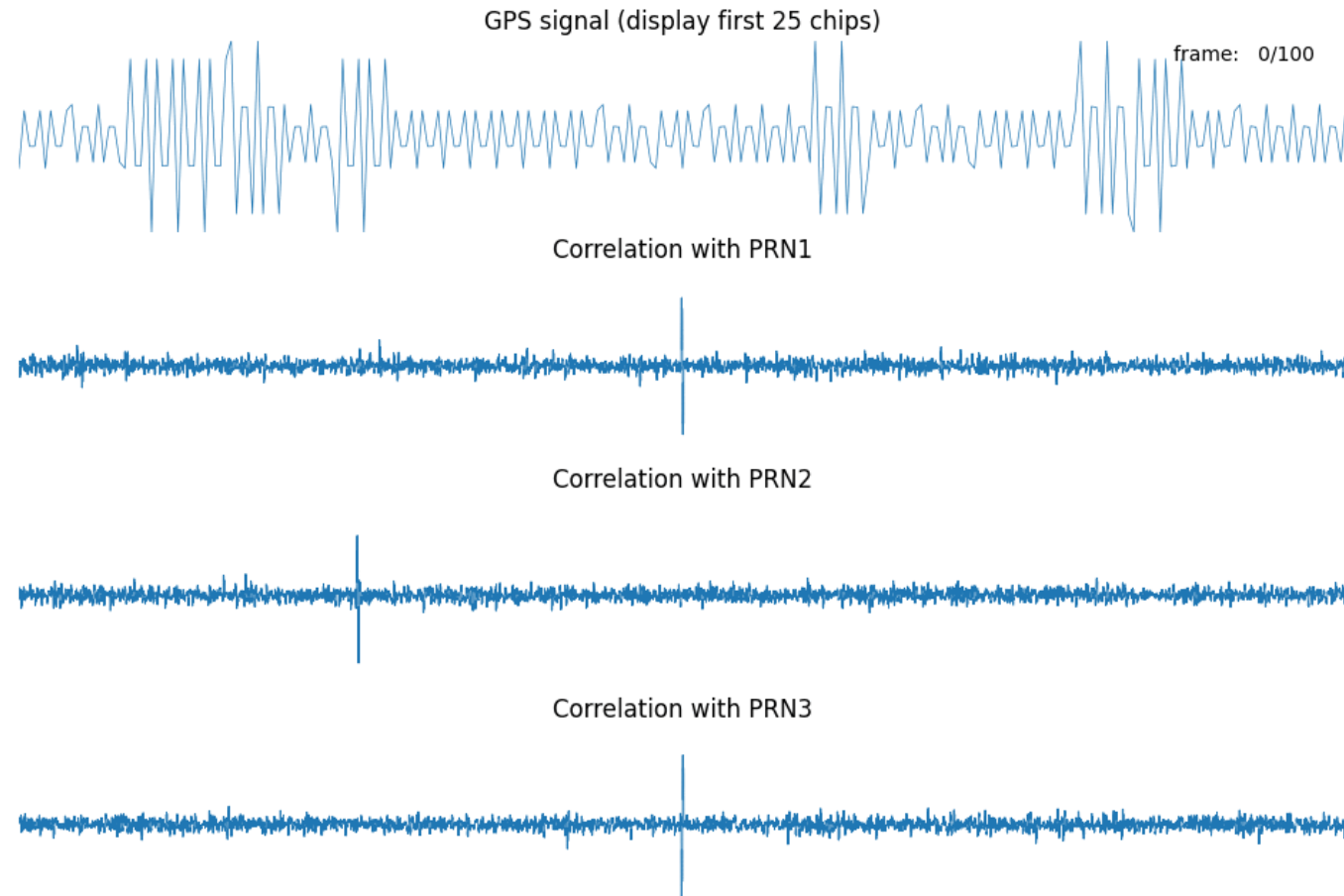
PRN Code – Cross-correlation



PRN Code – GPS Signal Correlation

- Signal received by the user is a combination of
 - signals transmitted from different satellites,
 - plus noise caused by receiver, multipath, etc.
- What would be the results if we correlate received signal with different PRN code?
 - Received signal will have signals transmitted by three satellites.
 - PRN1 will have no phase shift, no Doppler (carrier frequency difference).
 - PRN2 will have phase shift, no Doppler.
 - PRN3 will have no phase shift, but Doppler is changing across time.

PRN Code – GPS Signal Correlation (cont'd)



PRN Code – GPS Signal Correlation (cont'd)

- Location of correlation peak indicates code phase shift value.
 - Peak should locate at the center to demodulate data successfully.
 - Need to know initial code phase of received signal to “move” the peak at the center, by generating a local PRN signal with same phase.
- Doppler frequency difference will impact correlation peak amplitude.
 - PRN code is modulated on carrier wave, and a large difference of sine wave frequency or phase will lead to small correlation peak
 - Need to know initial Doppler frequency and phase to ensure a correlation peak with carrier wave.

Navigation Message

- Broadcast at 50 bps.
 - A total of 25 frames, each frame takes 30 seconds to be transmitted.
 - Each satellite transmits its own navigation messages all the time.

Satellite parameters	Contains signal transmission time, SV health status, etc.	Data will be updated per frame.
Ephemeris	Contains detailed orbital information for each satellite	Data will be updated per frame.
Almanac	Contains inaccurate position over time for <i>all</i> satellites	Data are broadcast across 25 frames, will be updated every 2 hours.

Data Demodulation

Signal acquisition and tracking

GPS Signal Demodulation

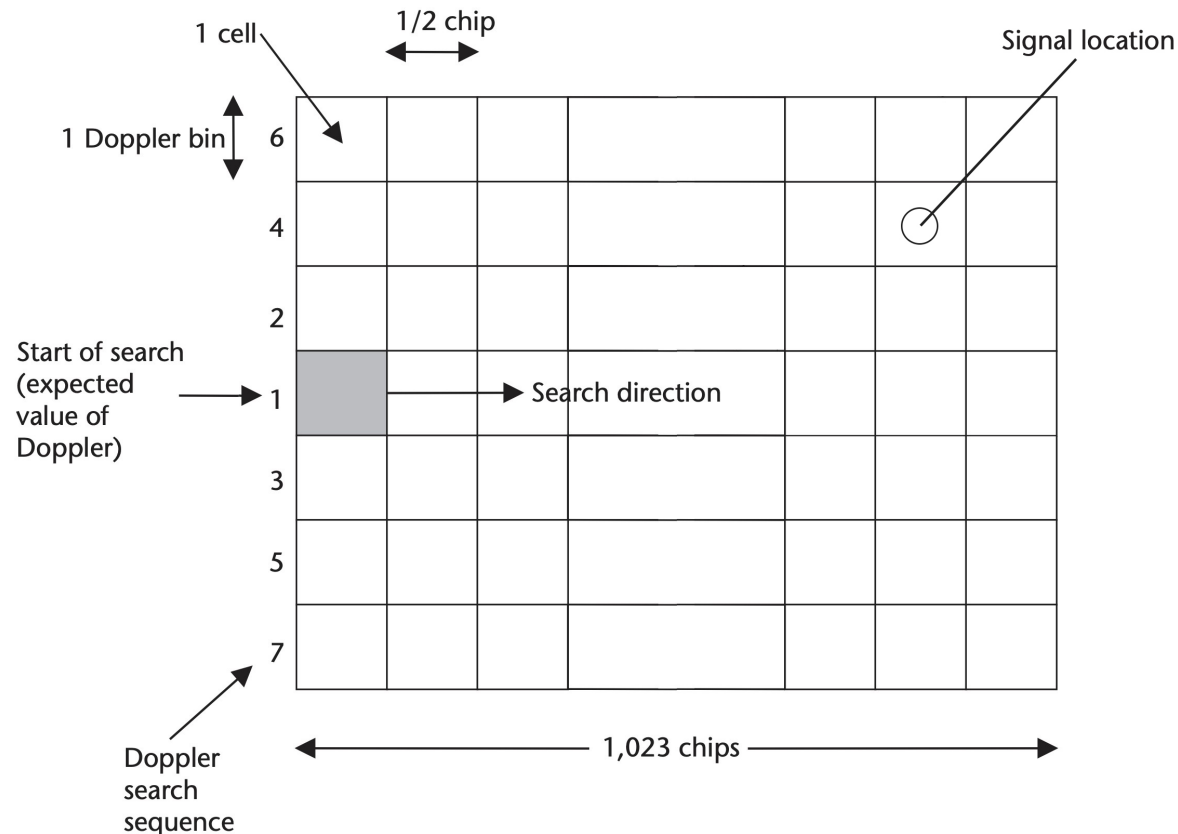
- Data modulation can be implemented by correlation.
 - After receiving GPS signal, the user will also generate a local signal with carrier wave and PRN code signal.
 - Sign of the correlation results indicates if the data modulated is 1 or -1.
- For generating suitable local signals, the user needs to know
 - satellite ID (if satellite is visible),
 - carrier frequency (with Doppler shift),
 - initial carrier phase, and
 - initial PRN code phase.

Signal Acquisition

- Satellites have different distance and relative speed w.r.t. user,
 - thus received satellite signals have different carrier/code phase (decided by distance), and difference Doppler shift (decided by relative speed).
- Signal acquisition is a 3D search in the following dimensions:
 - satellite ID (PRN code sequence) \Rightarrow satellite dimension
 - carrier frequency (with Doppler shift) \Rightarrow frequency dimension
 - initial PRN code phase \Rightarrow code dimension

Search Space

- Considering search only in 2D, search in carrier frequency and code.



Search Space (cont'd)

- Signal acquisition search space:
 - satellite dimension = 31 (total number of GPS satellites)
 - frequency dimension = 41 (if step size = 500 *Hz* within ± 10 *kHz* range)
 - code dimension = 1023 (if step size = 1 chip for C/A code)
 - thus total search space = $31 \times 41 \times 1023$. (It's HUGE!)
- It would be very slow if searching each bin one by one.
 - Doppler and code phase search can be speeded up using FFT.
 - Some prior can be used when searching.

Priors for Signal Acquisition

- With almanac data, the user will know beforehand the visible satellites, thus reducing one dimension for satellite search.
- With ephemeris data, the user could estimate Doppler shift and initial code phase, greatly reducing the remaining 2D search space.
- After signal acquisition, almanac is no longer useful.

More on C/A Code and P Code

- For P code the search space at code dimension is 6.18×10^{12} !
 - It's impossible to acquire code phase in real time without any help of prior.
 - The previous search method requires receiving signal for at least one PRN code period. Recall that P code period is one week!
- After tracking using C/A code to obtain current time first, the user can estimate P code phase, reducing the 2D search space.
- That's why C/A code is called **coarse** acquisition code.

Signal Tracking

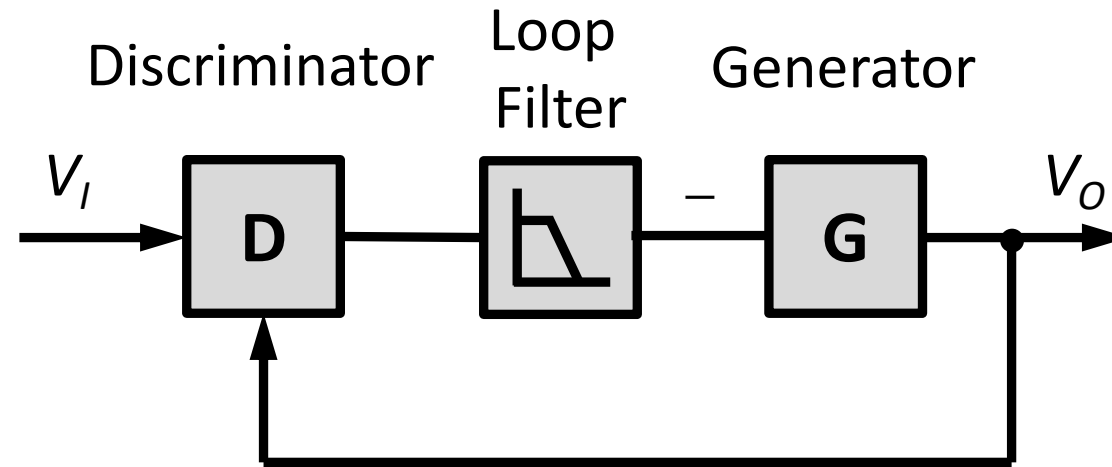
- After signal acquisition, the user has a rough estimate for Doppler shift and code phase.
- Signal tracking can fine-tune the estimation to an accurate level, and also obtain carrier phase accurately.
- User will track the status of received signal.
 - Adjust the estimation of carrier frequency, carrier phase, and code phase, which may slowly across time.

Tracking Modules

- Frequency-locked loop (FLL) \Rightarrow tracking carrier frequency
 - Phase-locked loop (PLL) \Rightarrow tracking carrier phase
 - Delay lock loop (DLL) \Rightarrow tracking code phase
-
- All these lock loops are electronic control systems based on *negative feedback loop*.

Negative Feedback Loop

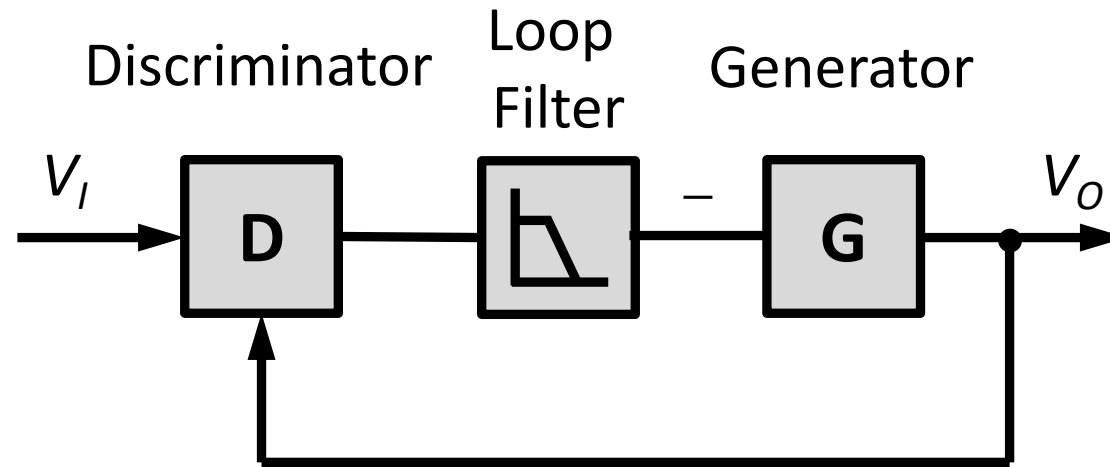
- Negative feedback loop structure



- Discriminator will calculate difference between input and output.
 - Either frequency (FLL), carrier phase (PLL), or code phase (DLL).

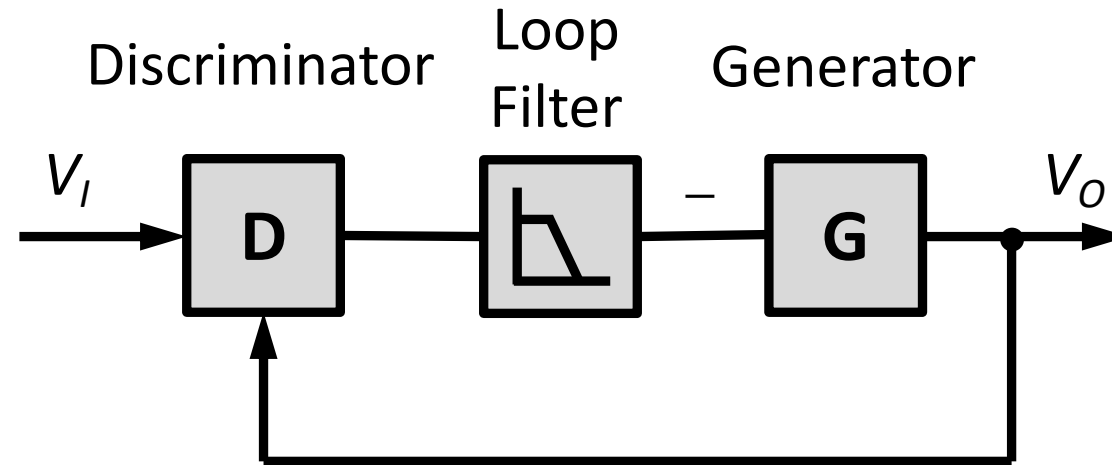
Negative Feedback Loop (cont'd)

- Negative feedback loop structure



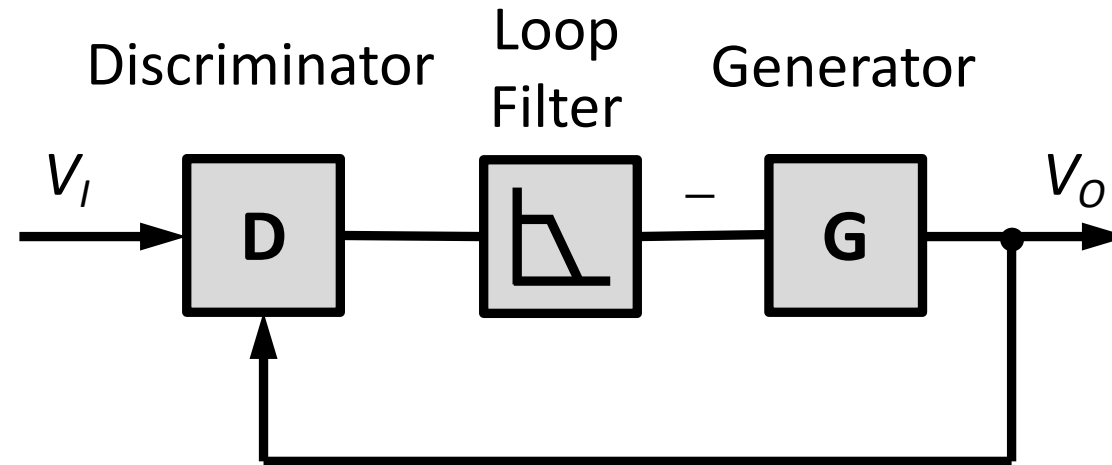
- Loop filter will output a value to control generator.
 - The value is calculated based on previous history.
 - Filter output is the negative of generator's input, hence "negative" feedback.

Negative Feedback Loop (cont'd)



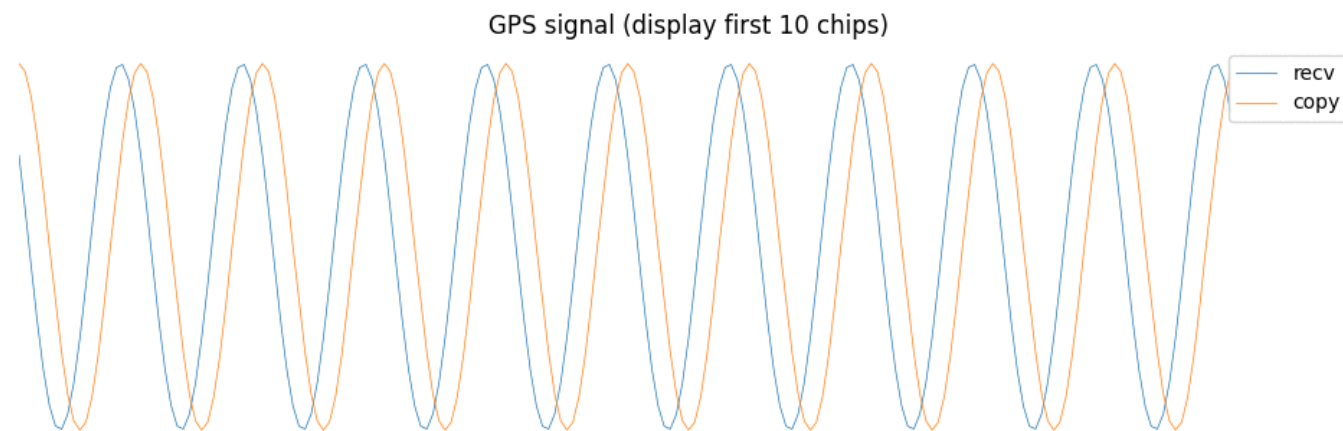
- Generator will generate new output signal based on its input.
 - Taking FLL as an example.
 - If generator input is f_i , and previously the generated signal frequency is f_o .
 - Next time generator will generate new output signal with frequency $f_i + f_o$.

Negative Feedback Loop (cont'd)



- If input and output signal are the same:
 - Discriminator's output will be 0 ($f_I = f_O$).
 - Loop filter's output will be 0 after a short time (considering the filter history).
 - Generator will have zero input ($f_i = 0$), thus keep generating previous output with frequency $f_o = f_i + f_o = f_o$.

FLL



Loop filter output

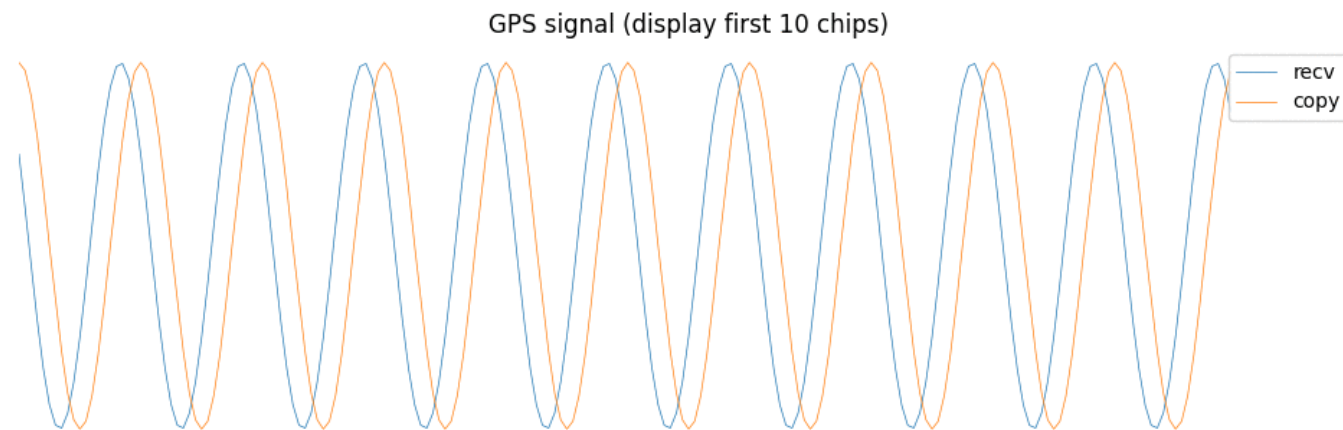


status: FLL

phase diff: 17.2°

freq diff: 100.0Hz

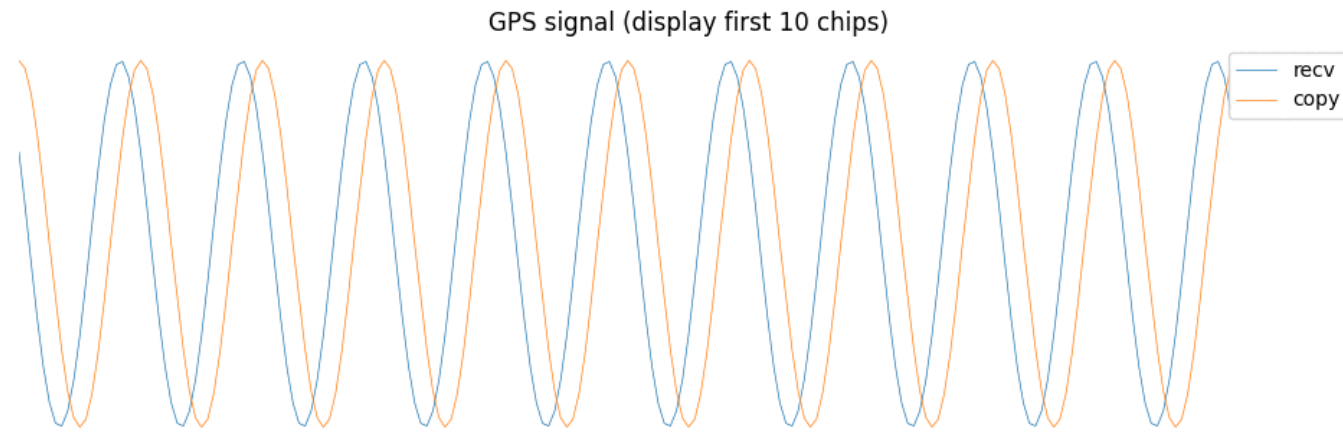
PLL



Loop filter output

status: PLL
phase diff: 17.2°
freq diff: 100.0Hz

FLL + PLL



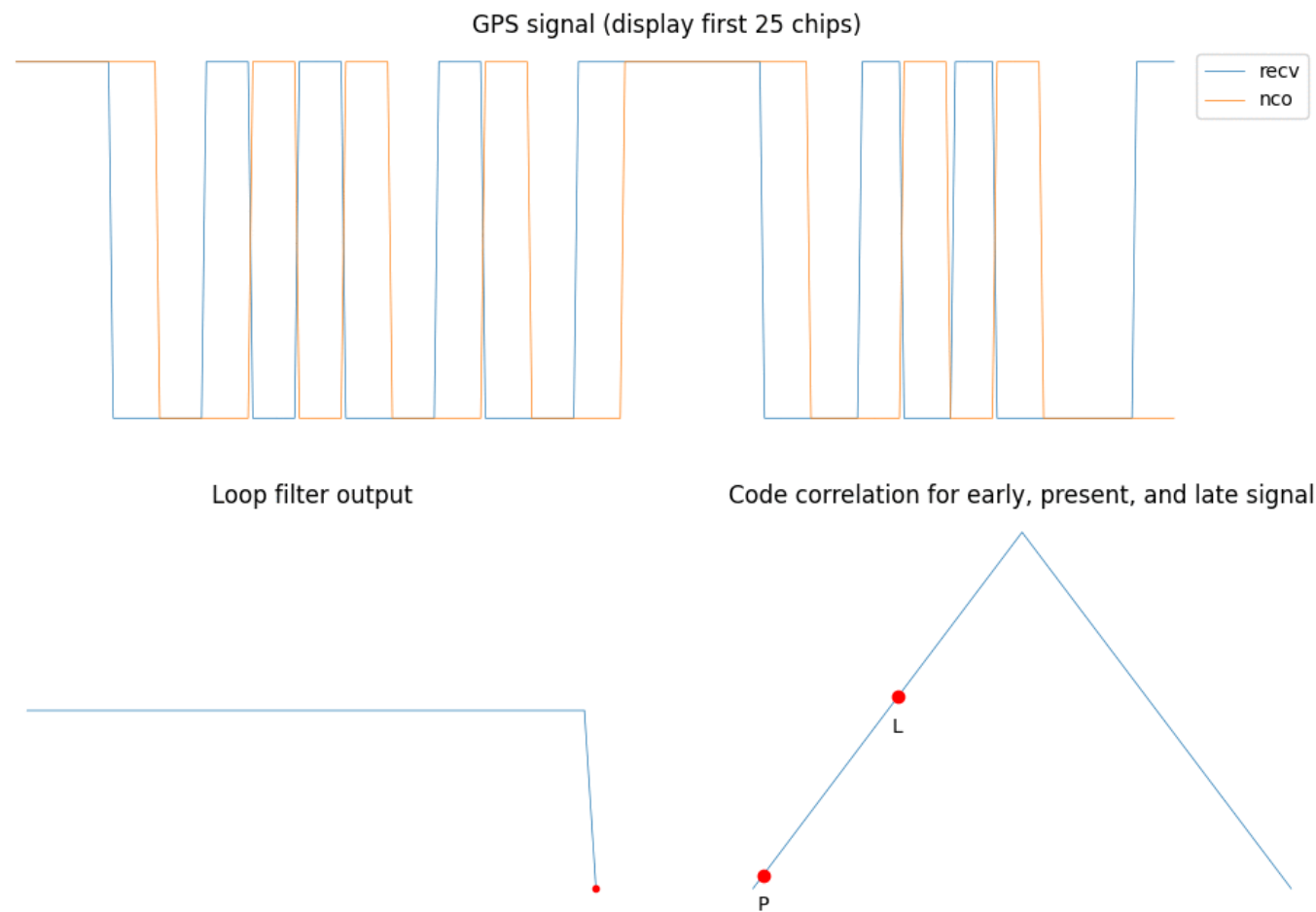
Loop filter output

status: FLL

phase diff: 17.2°

freq diff: 100.0Hz

DLL

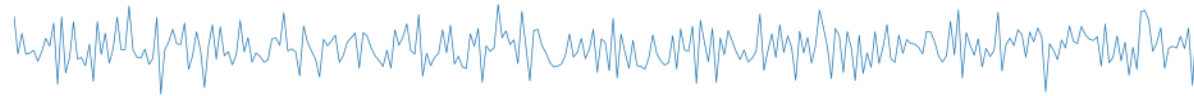


Demodulation

- PLL and DLL make sure the copied signal has the maximum correlation results with the received signal.
- Data demodulation is then indicated by correlation result.
 - If correlation is above 0, then the data modulated on the signal is +1, otherwise it's -1.

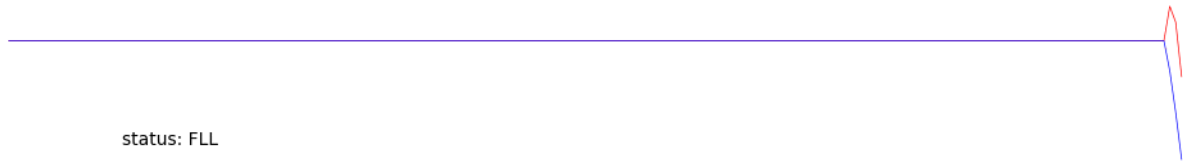
Demodulation

GPS signal (display first 30 chips)



Code & carrier stripping for PRN1

I
Q



status: FLL

Code & carrier stripping for PRN2

I
Q



status: FLL

Some Takeaways

- Pseudorandom noise (PRN) code is used for GPS signal modulation.
- C/A code is released for public use and can be easily hacked, but military code is impossible to hack.
- User will generate a local signal matching with signal through signal acquisition and tracking.
- Data demodulation is achieved by correlation.