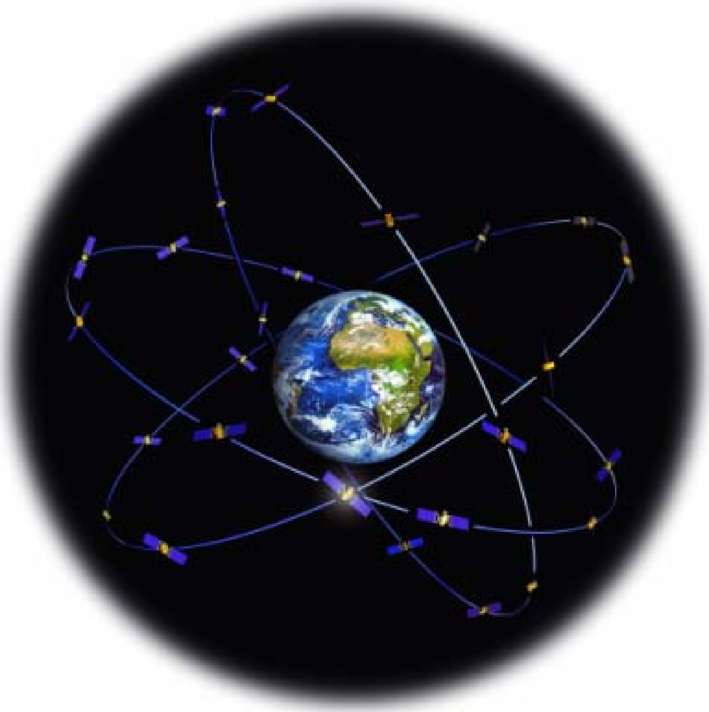
Decoding Galileo and Compass

Grace Xingxin Gao

The GPS Lab, Stanford University

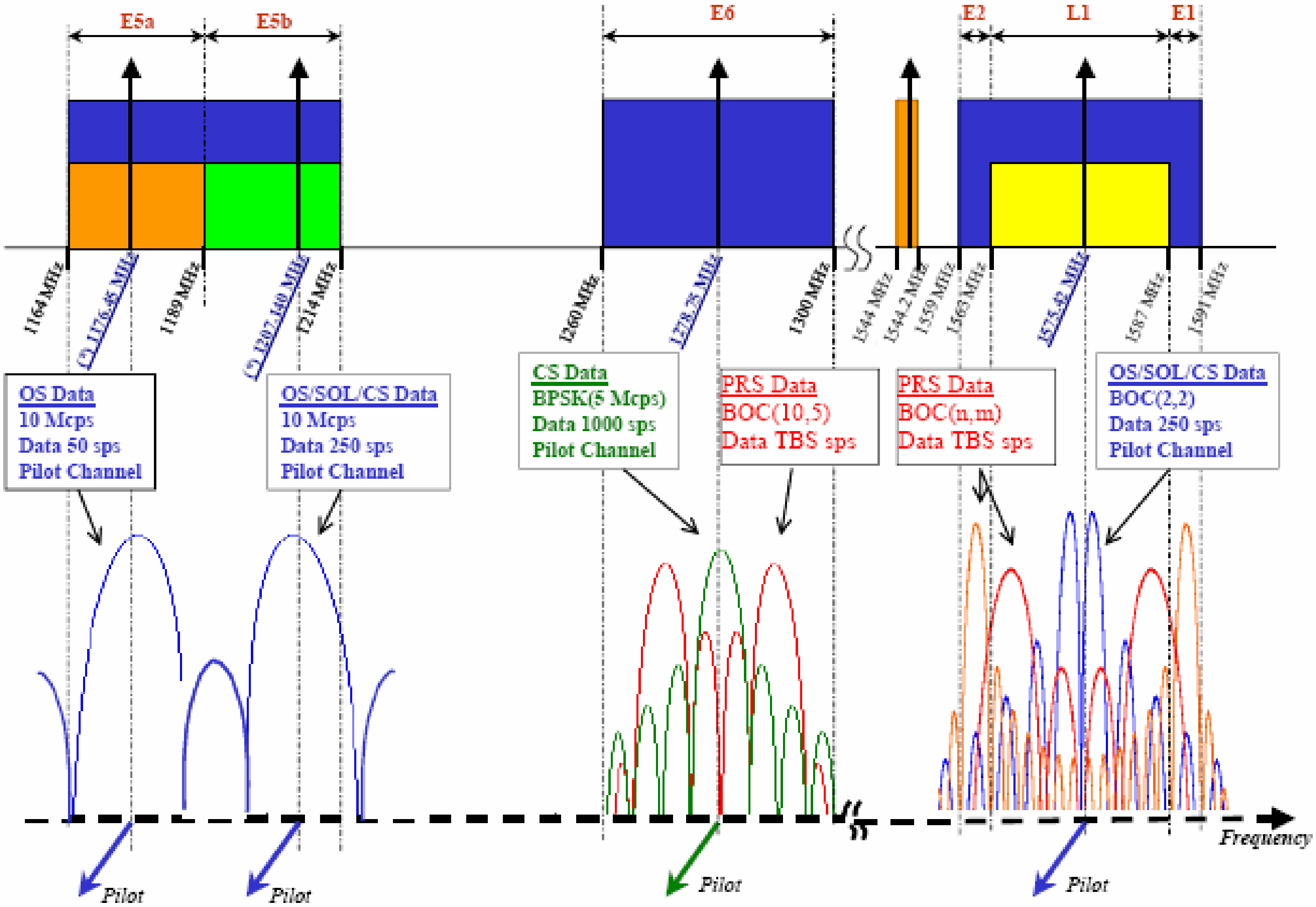
June 14, 2007

What is Galileo System?



- Global Navigation Satellite System built by European Union
  - The first Galileo test satellite – GIOVE-A was launched on Dec. 28, 2005
  - First navigation signals were transmitted by GIOVE-A on Jan. 12, 2006
- Interoperable with GPS
- 30 satellites in three Medium Earth Orbit MEO planes at 23,222km above the earth
  - 9 satellite + 1 spare per plane
  - The inclination of the orbits was chosen to ensure good coverage of polar latitudes
  - One revolution 14 hours 4 min

Galileo Signal Spectrum



OS Data
10 Mcps
Data 50 sps
Pilot Channel

OS/SOL/CS Data
10 Mcps
Data 250 sps
Pilot Channel

CS Data
BPSK(5 Mcps)
Data 1000 sps
Pilot Channel

PRS Data
BOC(10,5)
Data TBS sps

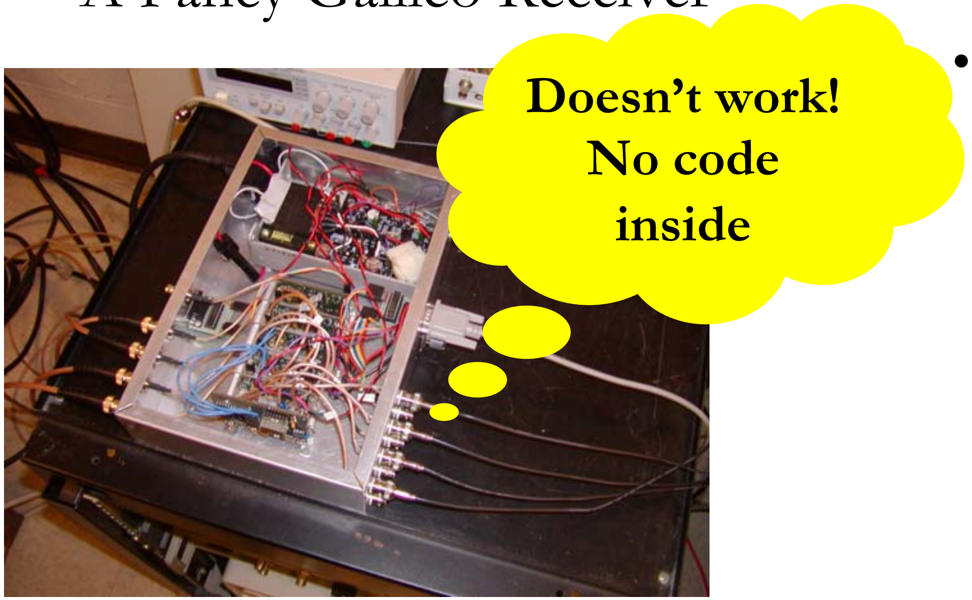
PRS Data
BOC(n,m)
Data TBS sps

OS/SOL/CS Data
BOC(2,2)
Data 250 sps
Pilot Channel

Why Seek the Galileo Codes?

- Galileo provides additional 30 satellites to the US GPS system
  - More accuracy and integrity
- Galileo L1 band overlaps with GPS L1 band
  - Can use the same antenna for the integrated Galileo/GPS receivers

- A Fancy Galileo Receiver

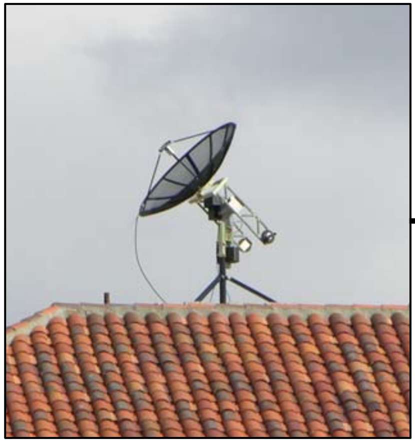


- We are considering designs for new signals from GPS and terrestrial ranging sources that could augment GPS. Thus, we are eager to gain a deep understanding of the recent efforts by our European colleagues.

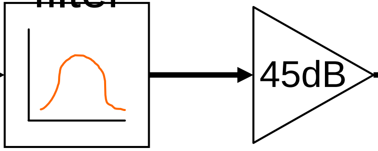
Data Collection – My Antennas

Data Collection - Antennas

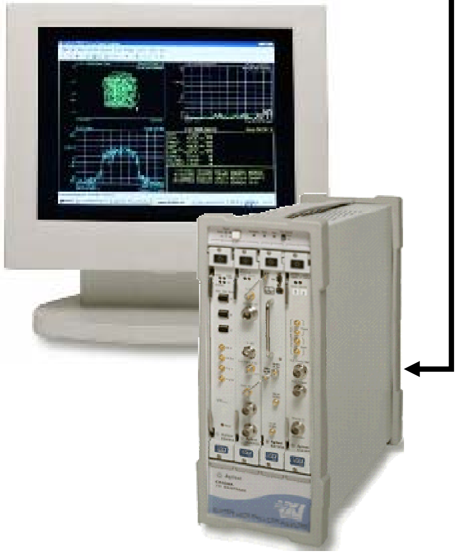
Data Collection
Stanford GNSS Monitor Station



L-band feed

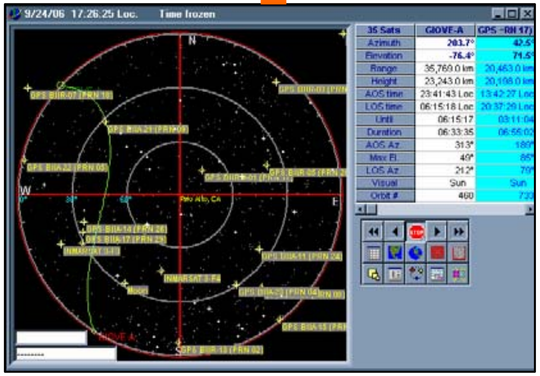


50' cable



Agilent Vector Signal Analyzer

Az/El control



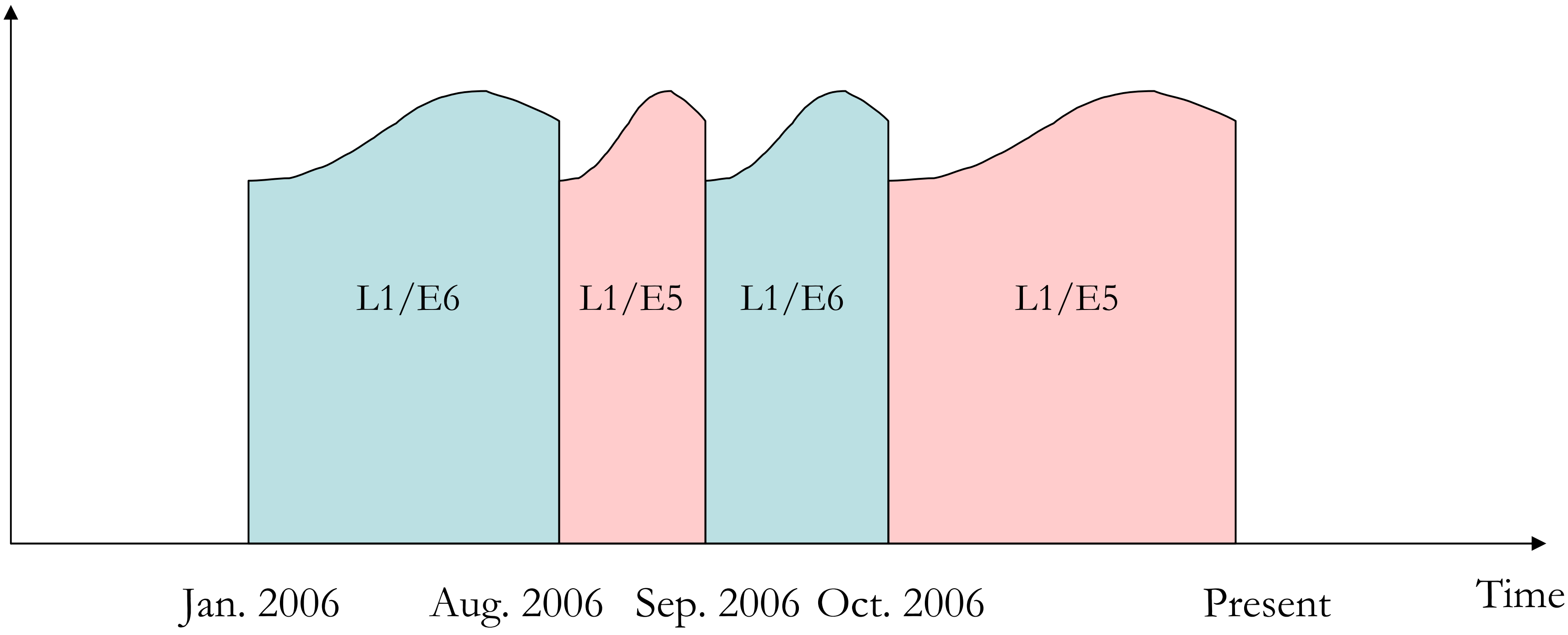
35 Sats	GIOVE-A	GPS -RH 17)
Azimuth	203.7°	42.5°
Elevation	-76.4°	71.5°
Range	35,769.0 km	20,463.0 km
Height	23,243.0 km	20,108.0 km
AOS time	23:41:43 Loc	13:42:27 Loc
LOS time	06:15:18 Loc	20:37:29 Loc
Until	06:15:17	03:11:04
Duration	06:33:35	06:55:02
AOS Az	313°	180°
Max El	49°	86°
LOS Az	212°	70°
Visual	Sun	Sun
Orbit #	460	730

Nova for Windows
Satellite Tracking Software

- On demand operation
- 1.8m steerable dish antenna
  - High gain
  - Directional
- Flexible data collection system

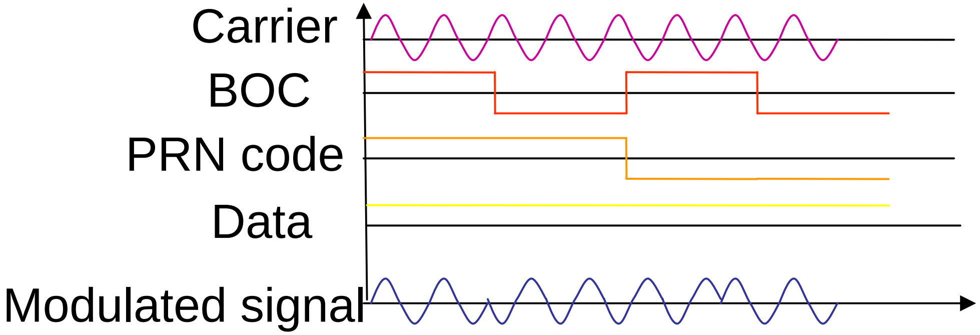
Seek L1 and E6 Codes

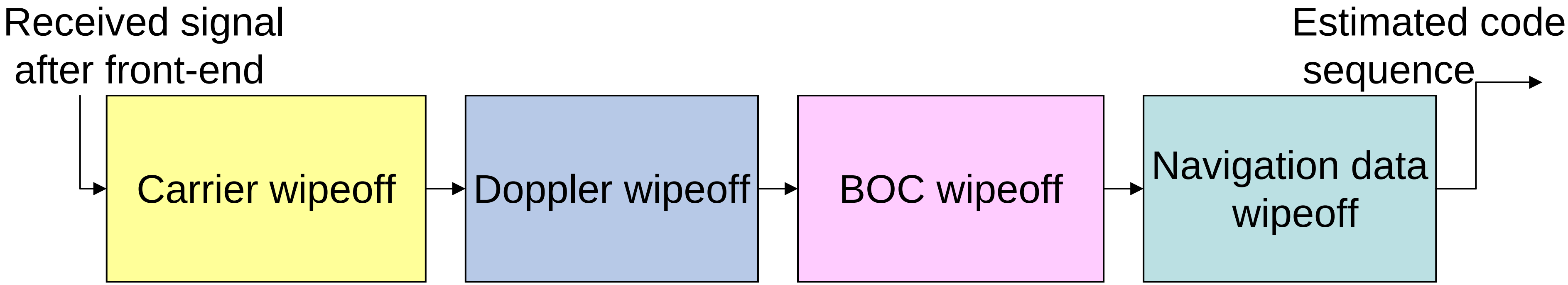
GIOVE-A Transmission Time Chart



Estimate Individual Code Sequences

- Modulated signal is the product of carrier, BOC code, PRN code, and data





Received signal after front-end

Carrier wipeoff

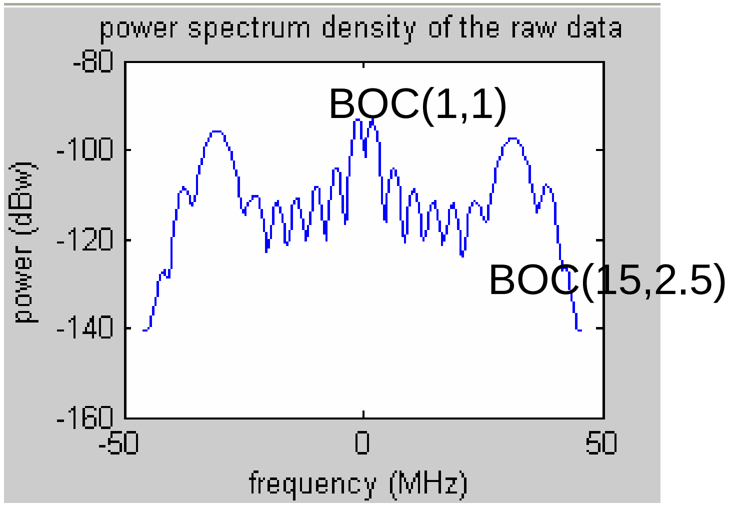
Doppler wipeoff

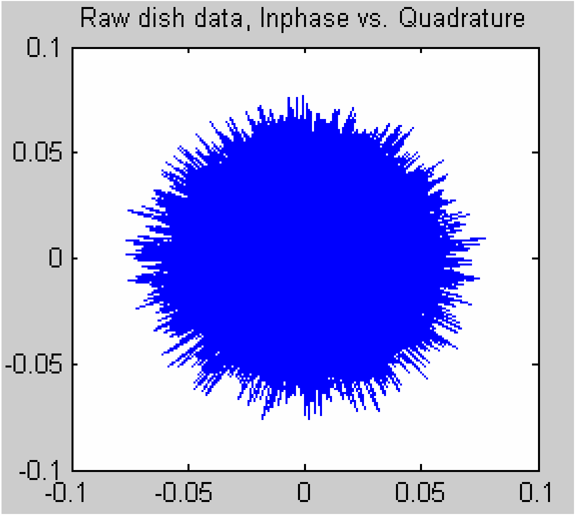
BOC wipeoff

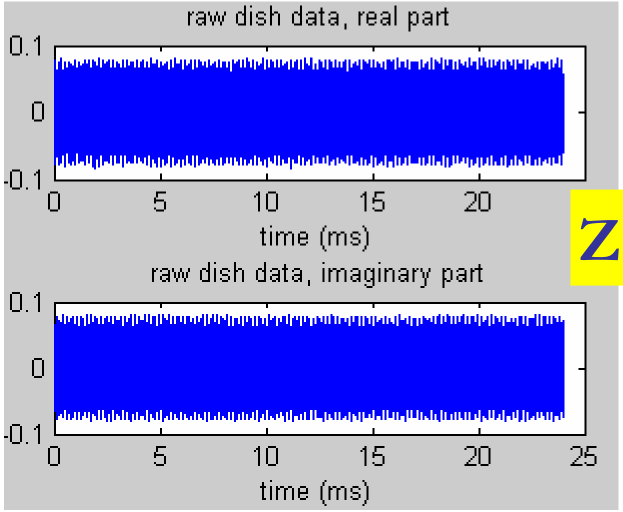
Navigation data wipeoff

Estimated code sequence

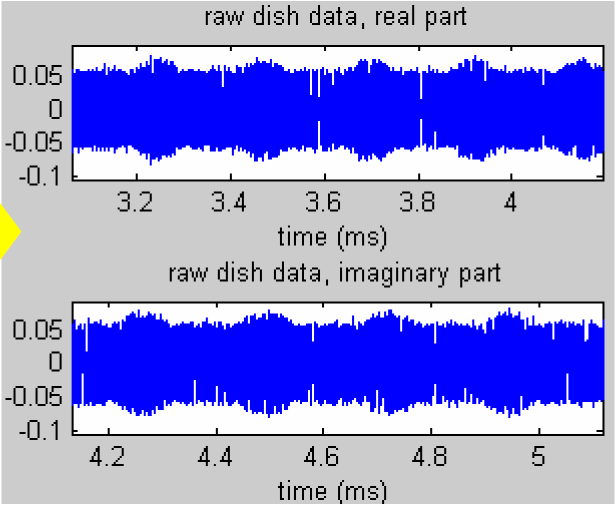
Raw Data Received from the Stanford Big Dish



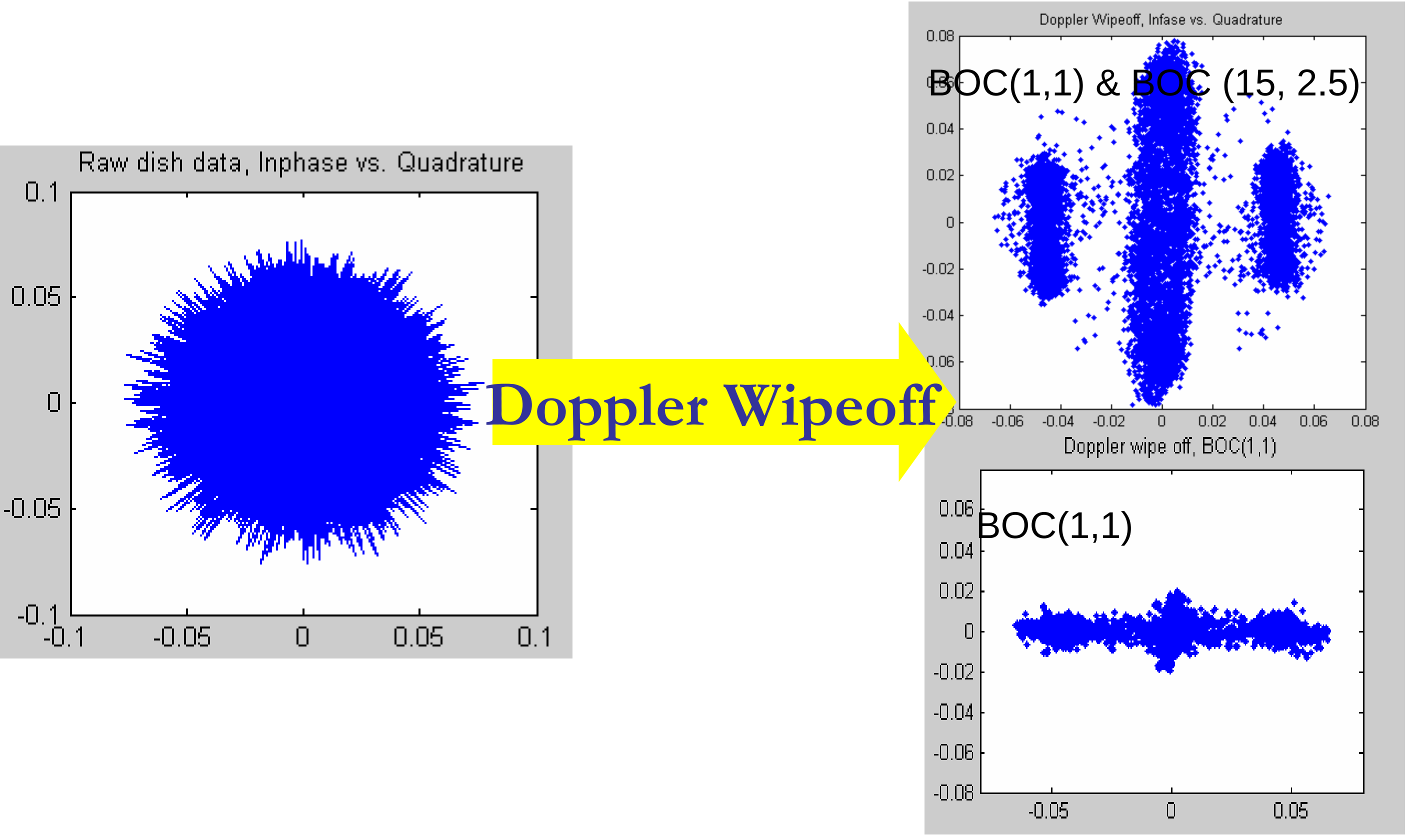




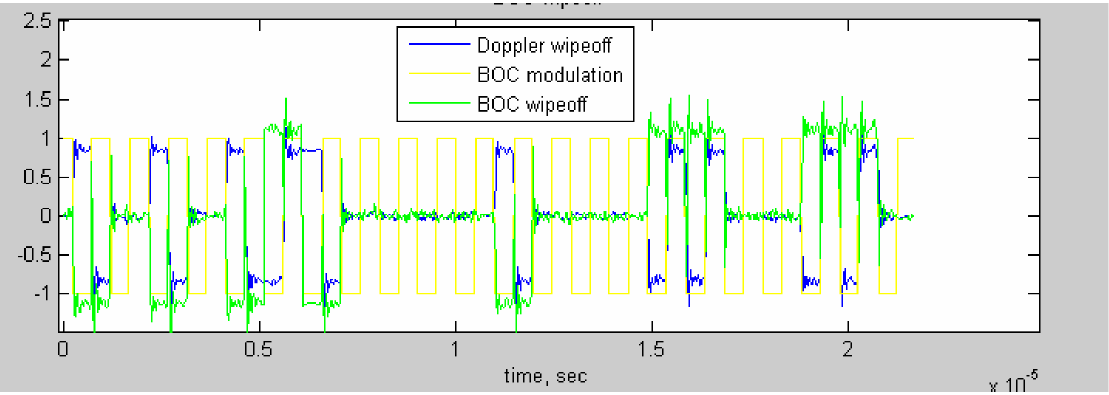
Zoom In

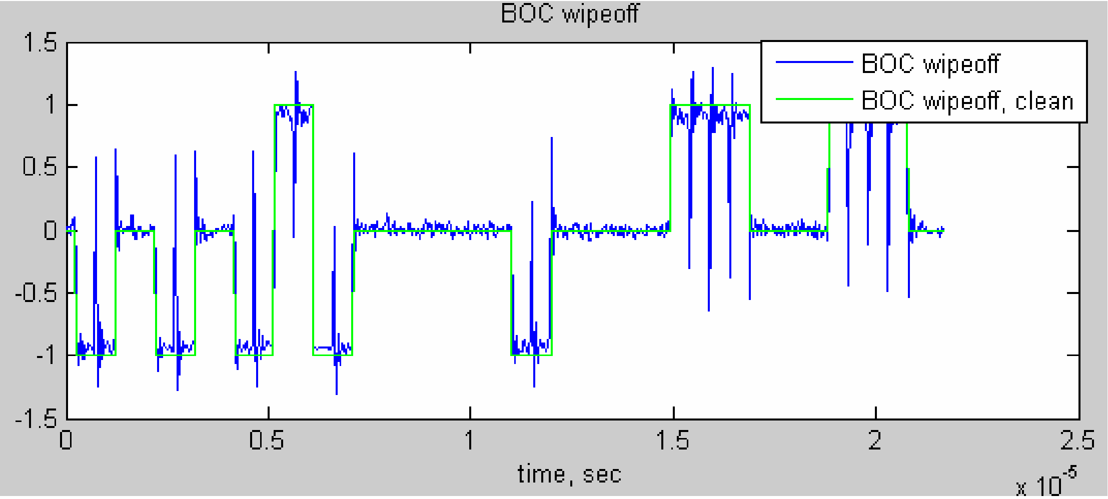


Doppler Wipeoff & Carrier Phase Alignment



BOC Wipeoff

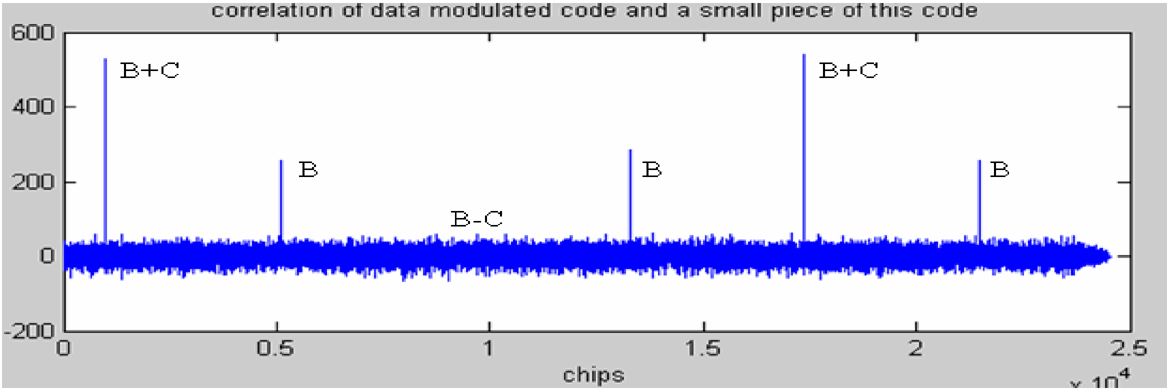




Align BOC code with the Doppler removed signal, and multiply them to wipe of the BOC code

Navigation Data Wipeoff

- Correlate the code sequence with a small slice of it
- The correlation plot shows that there are two codes, code B and code C with different periods.

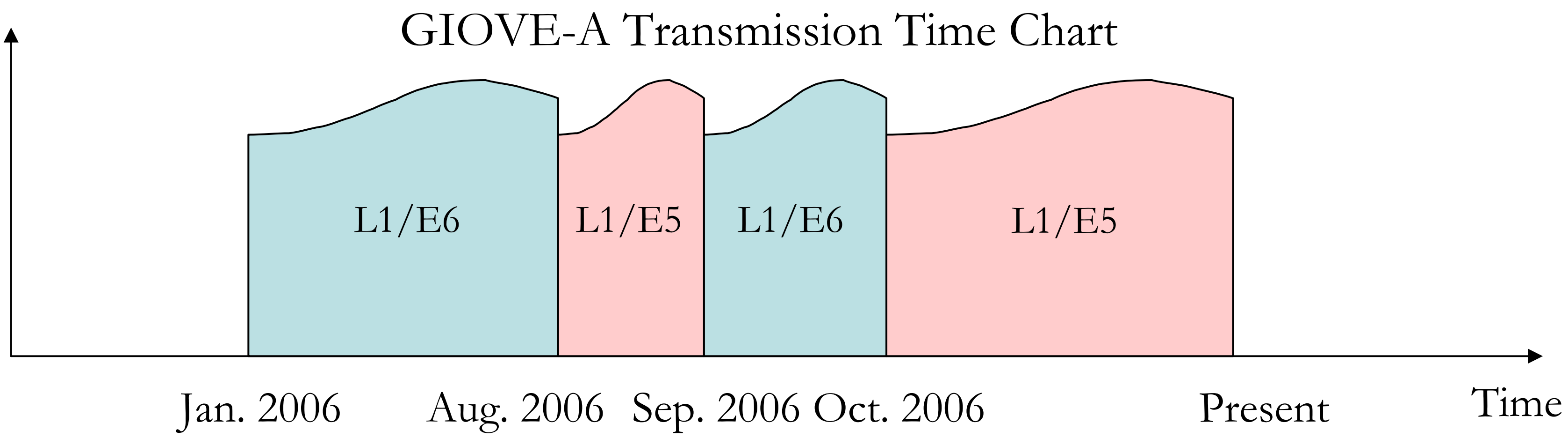


	Period	Data
Code B	4092	[1, 1, 1, 1, 1, 1]
Code C	8184	[1, -1, 1]

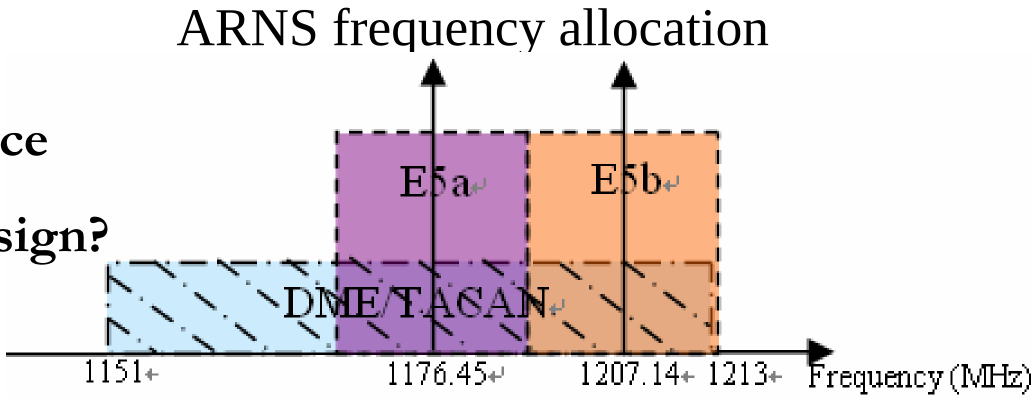
- Code sequences are obtained after wiping off Doppler, BOC and navigation data

  - Note, the sign of code B or code C is possibly flipped. This can be verified after the PRN code polynomials are calculated. If the polynomials contain “1+X”, then the code is flipped. Otherwise, it’s not.

Seek E5a/E5b Codes

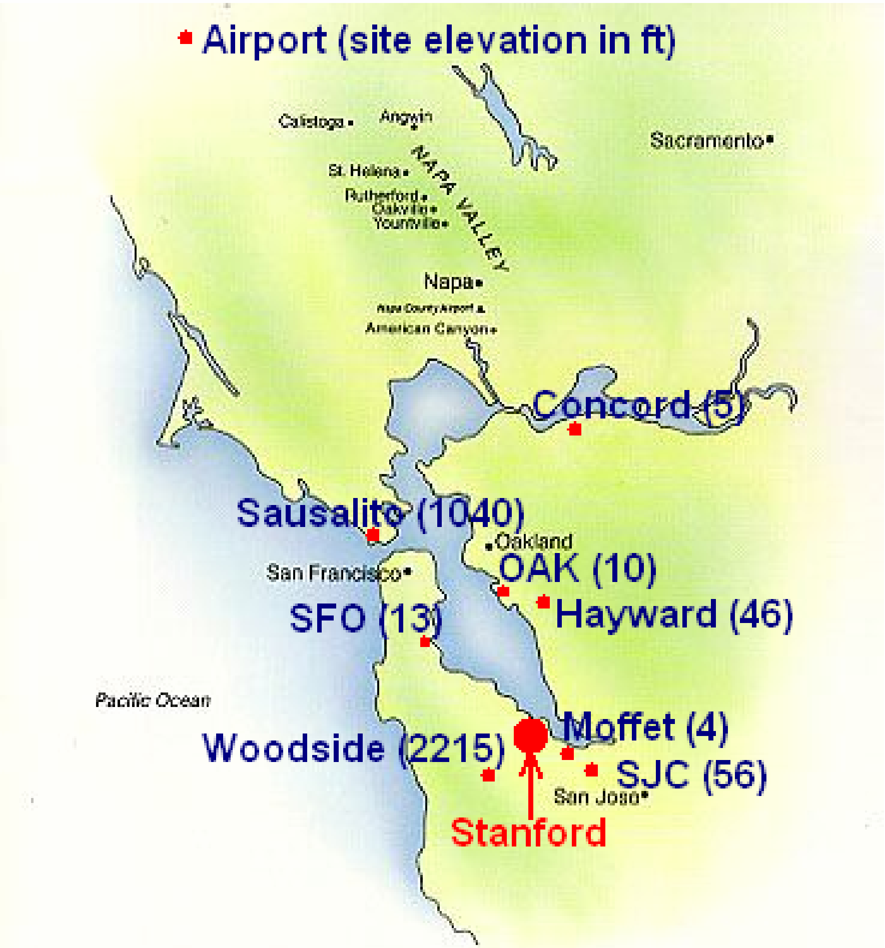


- **New challenges – DME interference**
- **How does DME affect receiver design?**

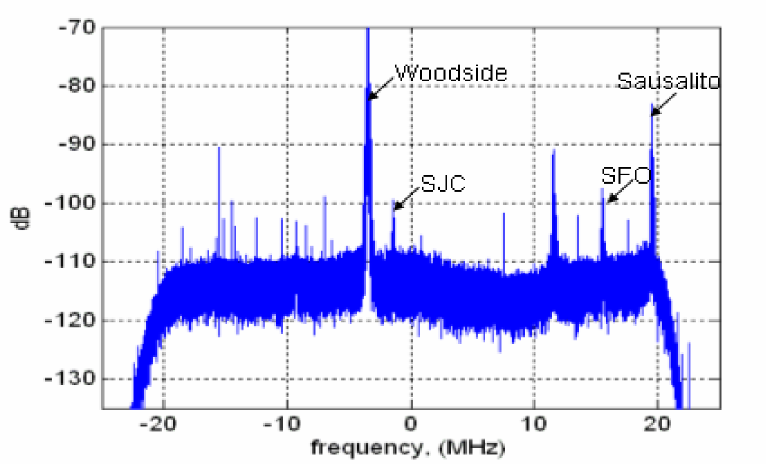


E5 Signal Environment

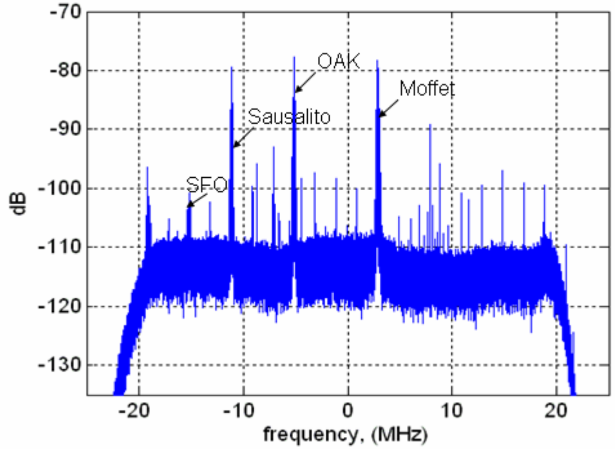
E5 signal environment in the bay area
– DME/TACAN inference from nearby airports



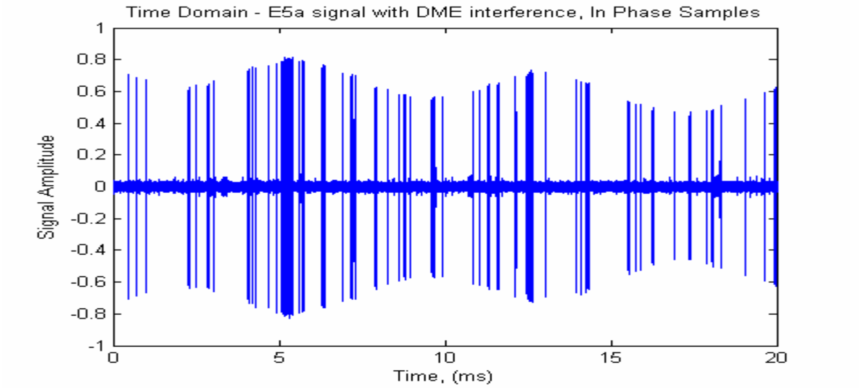
Received Raw Data



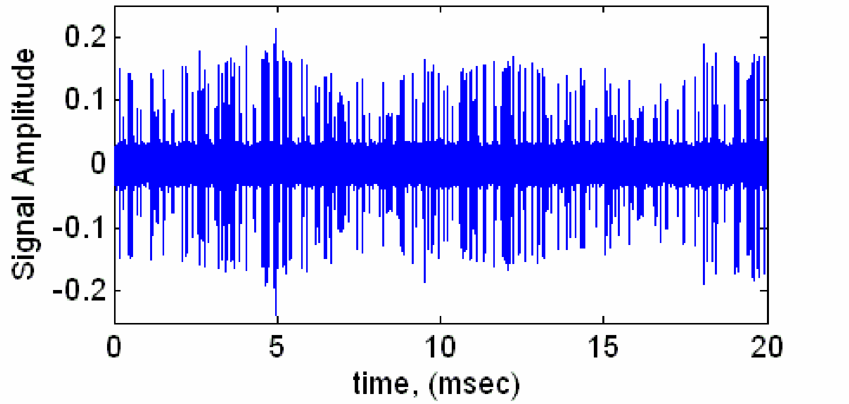
E5a Power spectral density



E5b Power spectral density

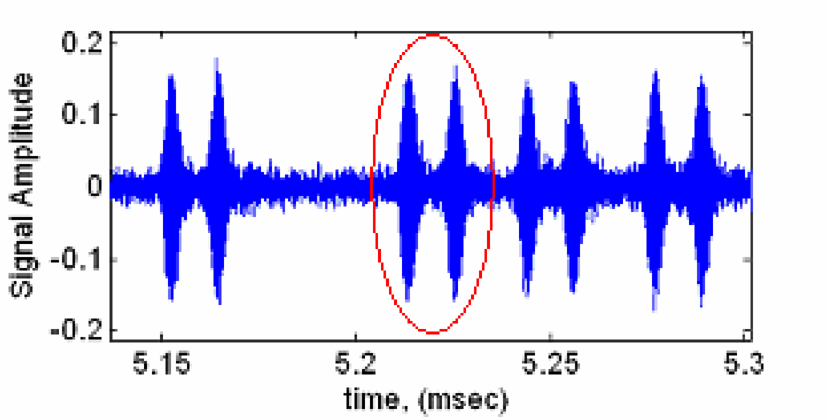


Time domain E5a signal, inphase samples

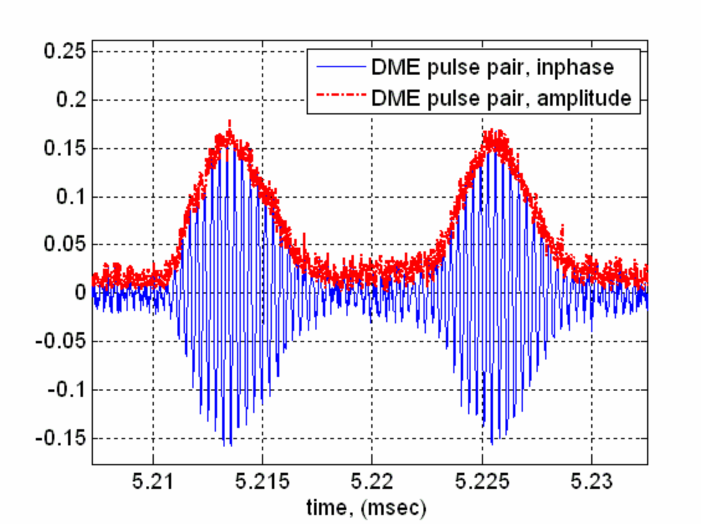


Time domain E5b signal, inphase samples

Raw Data, Zoom In



Time domain E5b signal with DME interference, inphase samples

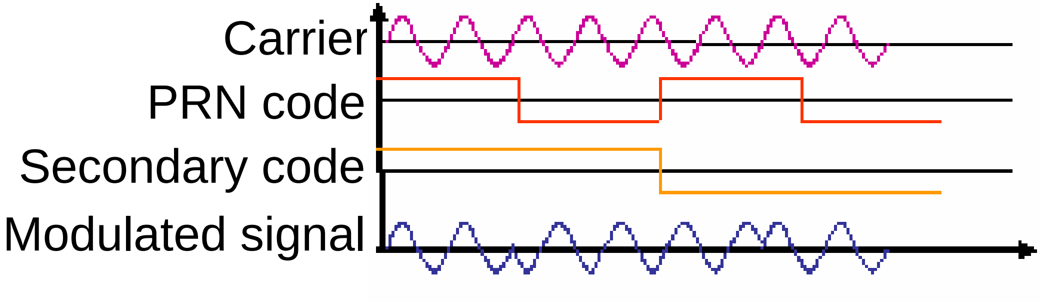


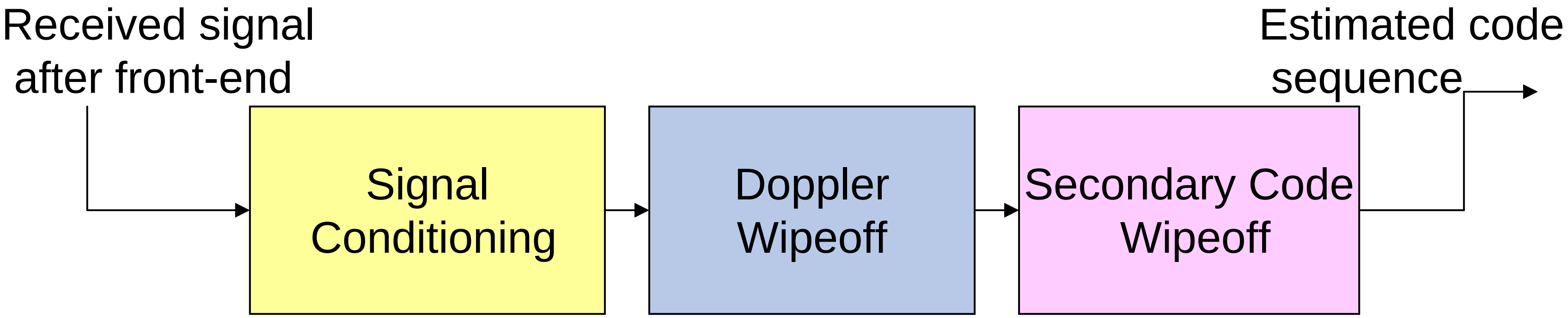
Time domain E5b signal with DME interference, inphase samples, zooming in

- The DME pulse amplitude is 5~100 times greater than the noise floor
- E5 signal is even buried in noise
- DME interference occurs 10-14% of the time
- DME comes in pairs with an inter-pulse interval of 12 μsec

Estimate Individual Code Sequences

- Modulated signal is the product of a carrier, a PRN code, and a secondary code





Received signal after front-end

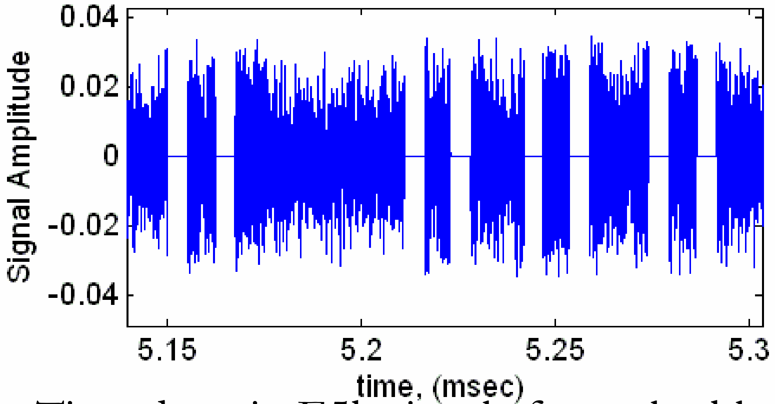
Signal Conditioning

Doppler Wipeoff

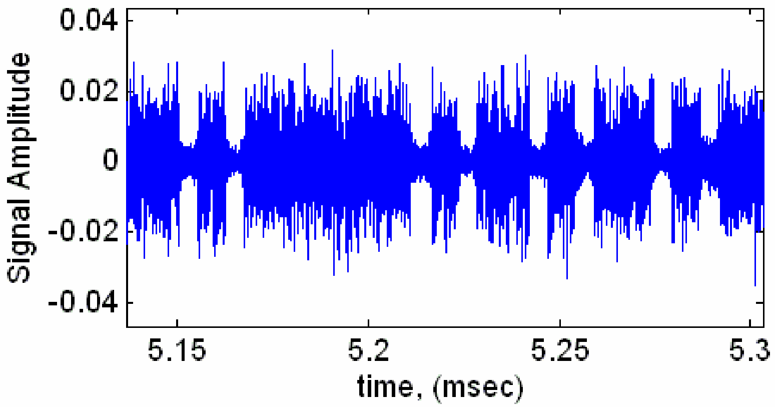
Secondary Code Wipeoff

Estimated code sequence

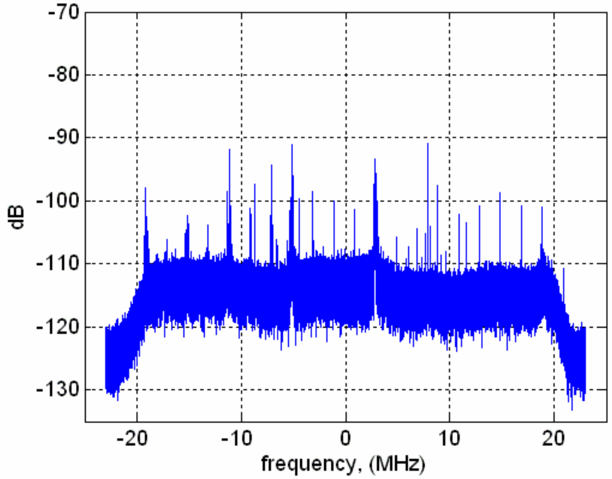
Signal Conditioning, Pulse Blanking & Notch Filtering



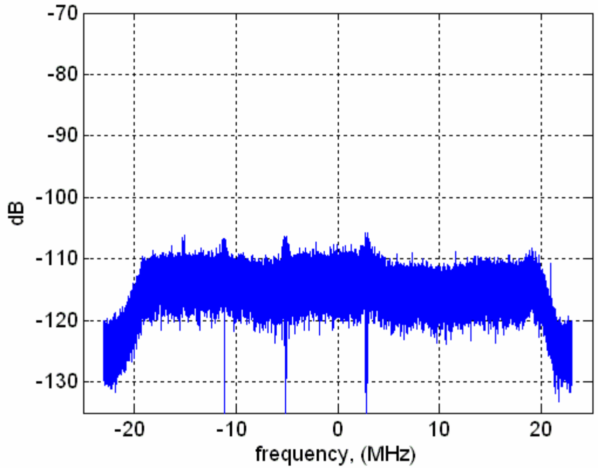
Time domain E5b signal after pulse blanking



Time domain E5b signal after notch filtering

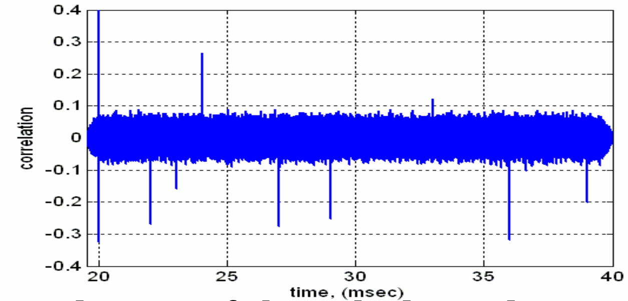


E5b signal spectrum after pulse blanking

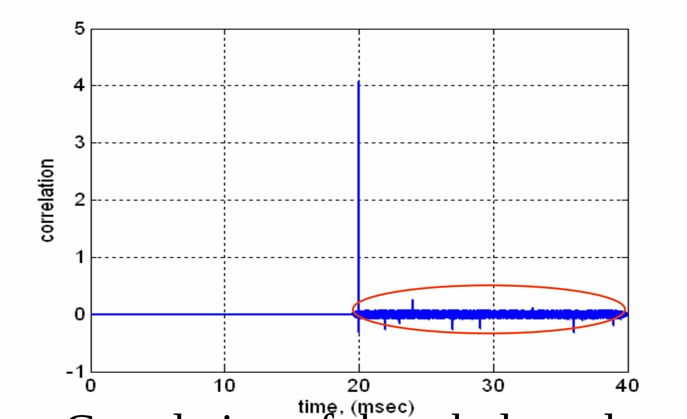


E5b signal spectrum after notch filtering

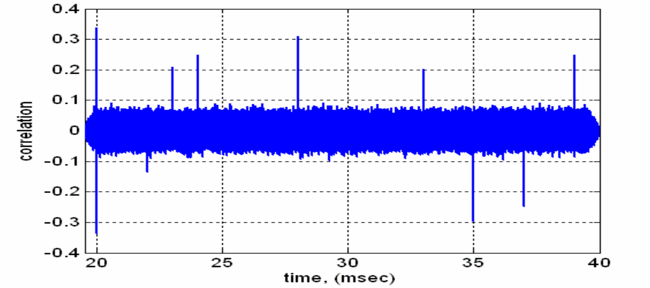
Calculate Code Periods



Correlation of the whole code sequence with a small slice of itself, inphase



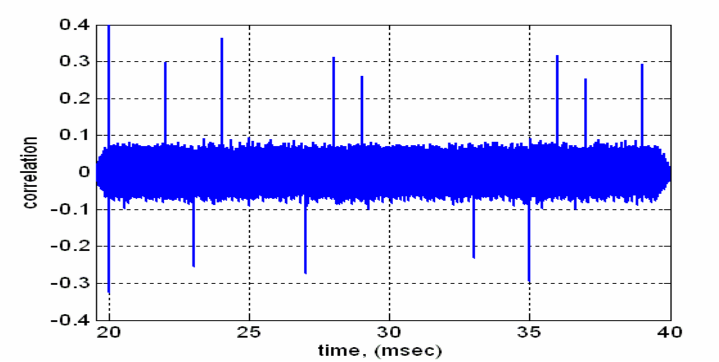
Correlation of the whole code sequence with a small slice of itself



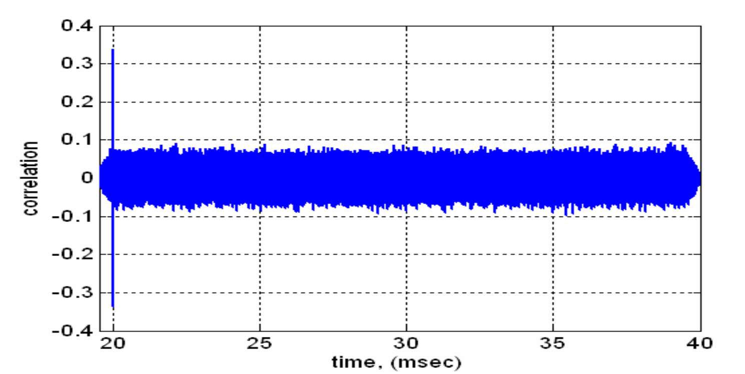
Correlation of the whole code sequence with a small slice of itself, quadrature

- Correlate the whole code sequence with a small slice of itself
- The intervals between pairs of peaks indicate a code period of 1ms
- Doppler results in constant phase variation, creating peaks in the inphase and quadrature channels and causing the peak heights to vary.

Doppler Wipeoff



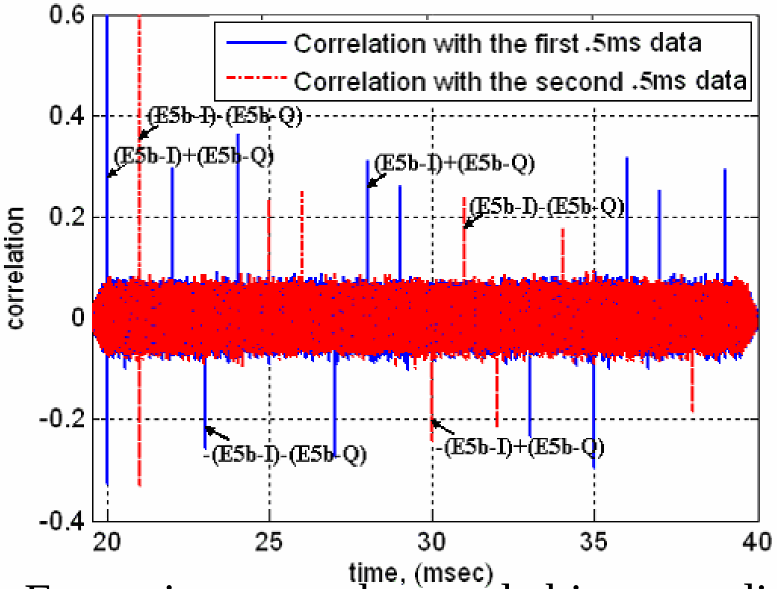
Correlation of the whole code sequence with a small slice of itself, inphase, after Doppler removal



Correlation of the whole code sequence with a small slice of itself, quadrature, after Doppler removal

- We search the whole Doppler domain from -5000 Hz to 5000 Hz and minimize the peak height variation after Doppler compensation
- After Doppler wipeoff and initial-phase adjustment, peaks with more uniform heights appear in the inphase channel and no peak in the quadrature channel.
- Null peaks indicate two codes added on top of each other

Secondary Code Wipeoff



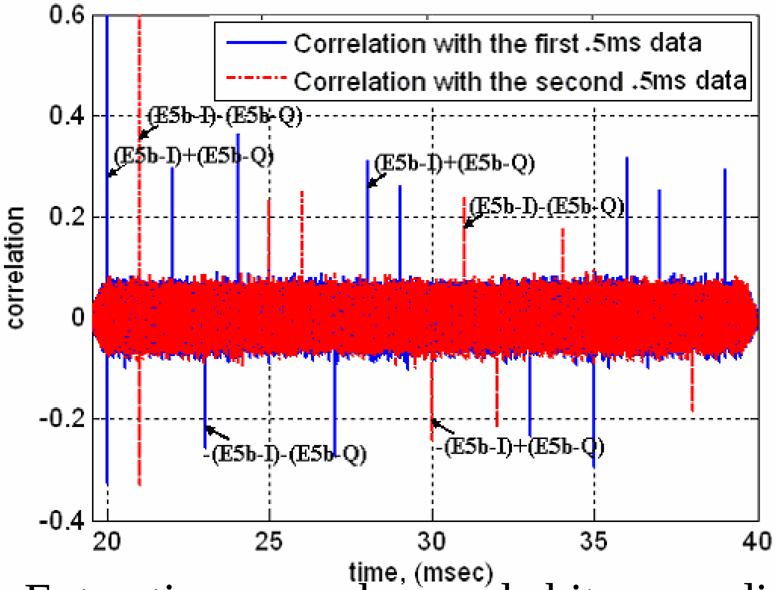
Extracting secondary code bits according to correlation peaks

	Period	Secondary code
E5b-I code	10230	[1, 1, 1, -1, 1, 1, 1, -1, 1, 1, -1, 1, -1, -1, 1, -1, 1, 1, -1, 1…]
E5b-Q code	10230	[1, -1, 1, -1, 1, -1, -1, -1, 1, 1, 1, -1, 1, -1, -1, -1, 1, 1, 1, 1…]

Secondary code reading of E5b-I and E5b-Q

- Choose the slice length to be 0.5 msec to avoid bit transition within the small slice of data. Compute two consecutive slices of 0.5 msec and use the one with relatively larger peaks.
- Pick another slice of data that corresponds to a null peak to solve the ambiguity
- The sign of E5b-I code or E5b-Q code is possibly flipped. This can be verified after the PRN code polynomials are calculated. If the polynomials contain “1+X”, then the code is flipped. Otherwise, it’s not.

Secondary Code Wipeoff



Extracting secondary code bits according to correlation peaks

	Period	Secondary code
E5b-I code	10230	[1, 1, 1, -1, 1, 1, 1, -1, 1, 1, -1, 1, -1, -1, 1, -1, 1, 1, -1, 1…]
E5b-Q code	10230	[1, -1, 1, -1, 1, -1, -1, -1, 1, 1, 1, -1, 1, -1, -1, -1, 1, 1, 1, 1…]

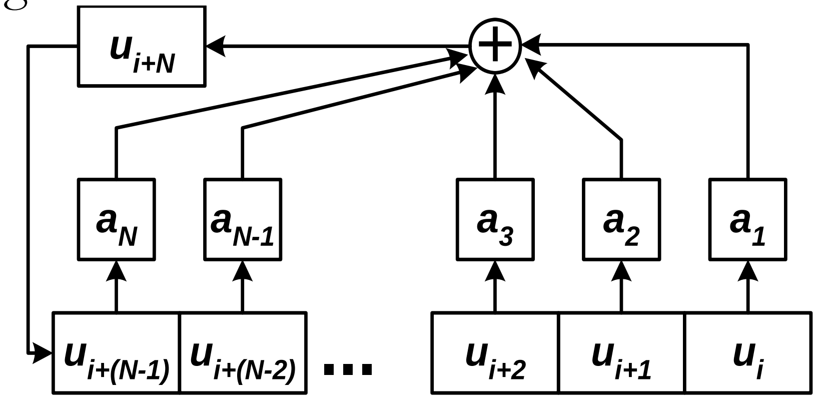
Secondary code reading of E5b-I and E5b-Q

- With secondary codes available, we can coherently add multiple periods of signal together until the SINR ratio is high enough to boost the code chips above the noise floor

- **PRN code sequences are obtained!**

Calculate Code Generator Stages (1/2)

- Start with linear codes
  - Linear codes can be generated by linear shift registers (LSR)
- Linear Shift Register

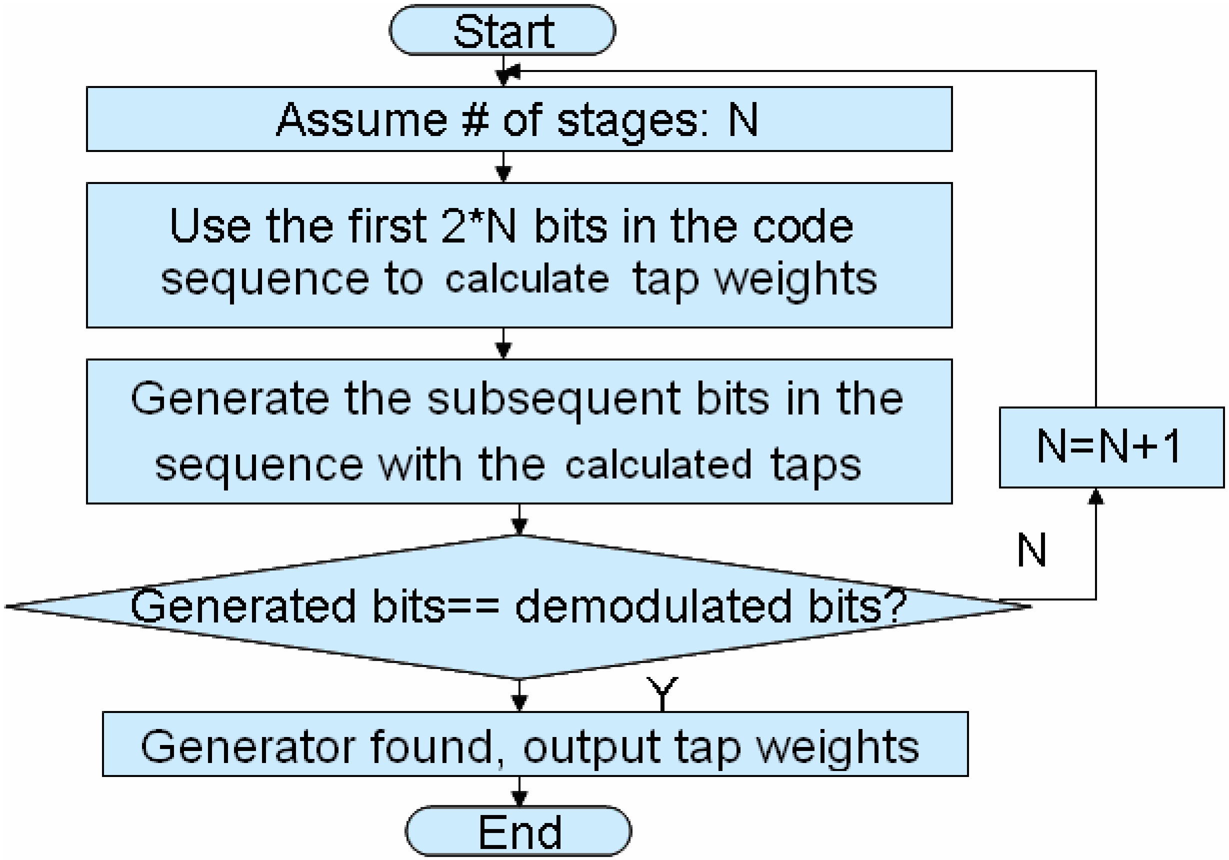


$$\boxed{u_{i+N} = \mathrm{a}_N * u_{i+(N-1)} \oplus \mathrm{a}_{N-1} * u_{i+(N-2)} \oplus \cdots \oplus \mathrm{a}_2 * u_{i+1} \oplus \mathrm{a}_1 * u_i}$$

- 2*N bits contain all information of the whole 2^N-1 bits sequence
  - We have *ui*, i = 1, …, 2*N, …
  - The relationship for N distinct values of i yields N equations
  - Tapping weights are N unknown variables in N equations
  - Solve the equation, determine which taps are on or off (*an* = 0 or 1)

Calculate Code Generator Stages (2/2)

Calculate generator tap weights


Start
Assume # of stages: N
Use the first 2*N bits in the code sequence to calculate tap weights
Generate the subsequent bits in the sequence with the calculated taps
Generated bits== demodulated bits?
N
N=N+1
Y
Generator found, output tap weights
End

Obtain Code Generators, L1 Signal

- Obtain code generator polynomials
  - Both codes are linear codes
  - Each code is generated by a 26 order polynomial
  - The obtained code generator polynomials can be factorized
  - Ambiguity of sign flipping is solved
  - The code sequence can be generated by modulo 2 adding maximal length sequences of the factor polynomials – **Gold codes!**
- Code B (Gold code)
  - Poly1_code1 = $X^{13}+X^{10}+X^{9}+X^{7}+X^{5}+X^{4}+1$, initial state 1111111111111
  - Poly2_code1 = $X^{13}+X^{12}+X^{8}+X^{7}+X^{6}+X^{5}+1$, initial state 1101110000011
- Code C (Gold code)
  - Poly1_code2 = $X^{13}+X^{10}+X^{9}+X^{7}+X^{5}+X^{4}+1$, initial state 1100110000011
  - Poly2_code2 = $X^{13}+X^{4}+X^{3}+X+1$, initial state 1111111111111
- Secondary code of C
  - 25 bits long
  - [1 0 1 1 0 1 1 0 0 1 0 0 0 1 1 1 0 0 0 0 0 0 0 1 0]

Obtain Code Generators, E6 Signal

- E6-B code: 5115 bits, 1ms, gold code
  - Poly_E6_B_1: X^13+X^12+X^11+X^1+1;
    - initial state: 0 1 0 1 0 1 1 1 0 0 0 0 0
  - Poly_E6_B_2: X^13+X^10+X^8+X^5+1;
    - initial state: 1 1 1 1 1 1 1 1 1 1 1 1 1
- E6-C code: primary code* secondary code=511500 bits, 100ms
  Primary code: 10230 bits, 2ms, gold code
  - Poly_E6_C_1: X^14 +X^8+X^7+X^4+X^3+X^2+1;
    - initial state: 0 1 1 0 1 0 0 0 0 1 1 1 0 1
  - Poly_E6_C_2: X^14+X^11+X^6+X^1+1;
    - initial state: 1 1 1 1 1 1 1 1 1 1 1 1 1 1
  - Secondary code: 50 bits
    - E6_C_secondary=[0 1 0 1 1 1 1 1 0 0 1 0 1 1 1 0 1 0 1 1 0 0 0 0 1 0 0 1 0
      1 0 0 0 0 1 1 1 0 1 1 0 0 1 1 0 0 0 1 0];

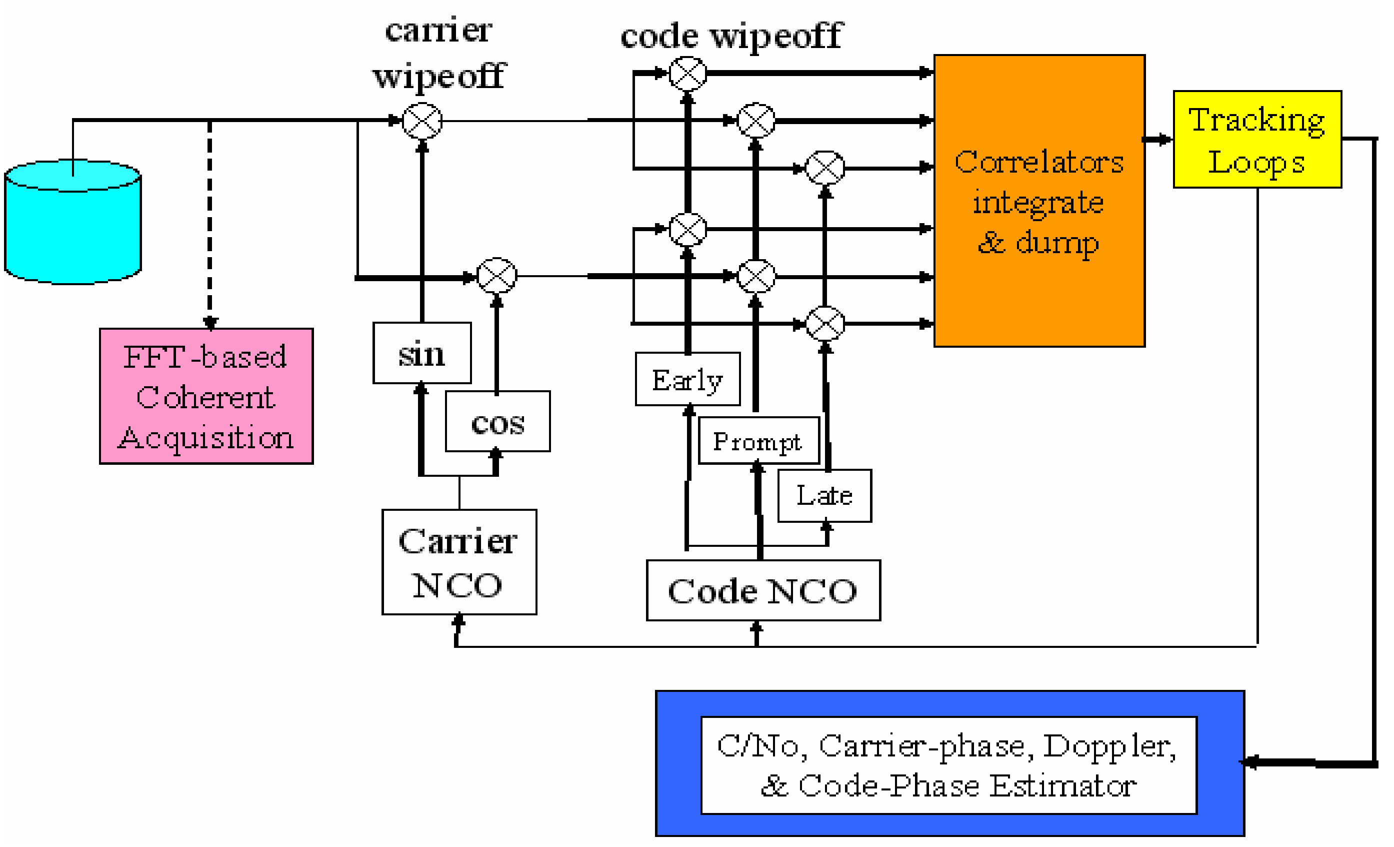
Obtain Code Generators, E5 signal

E5b-I code (10230 bits, 1msec, 14-stage Gold code)	
Polynomial_1	$X^{14}+X^{13}+X^{11}+X^{4}+1$
Initial State_1	[1 1 1 1 1 1 1 1 1 1 1 1 1 1]
Polynomial_2	$X^{14}+X^{12}+X^{9}+X^{8}+X^{5}+X^{2}+1$
Initial State_2	[1 1 1 0 0 0 1 0 1 0 0 0 1 0]
E5b-Q code (10230 bits, 1msec, 14-stage Gold code)	
Polynomial_1	$X^{14}+X^{13}+X^{11}+X^{4}+1$
Initial State_1	[1 1 1 1 1 1 1 1 1 1 1 1 1 1]
Polynomial_2	$X^{14}+X^{12}+X^{9}+X^{8}+X^{5}+X^{2}+1$
Initial State_2	[1 1 0 0 0 0 0 0 0 0 0 1 0 0]

E5a-I code (10230 bits, 1msec, 14-stage Gold code)	
Polynomial_1	$X^{14}+X^{8}+X^{6}+X+1$
Initial State_1	[1 1 1 1 1 1 1 1 1 1 1 1 1 1]
Polynomial_2	$X^{14}+X^{12}+X^{8}+X^{7}+X^{5}+X^{4}+1$
Initial State_2	[1 1 1 0 1 0 1 0 1 1 1 1 1 1]
E5a-Q code (10230 bits, 1msec, 14-stage Gold code)	
Polynomial_1	$X^{14}+X^{8}+X^{6}+X+1$
Initial State_1	[1 1 1 1 1 1 1 1 1 1 1 1 1 1]
Polynomial_2	$X^{14}+X^{12}+X^{8}+X^{7}+X^{5}+X^{4}+1$
Initial State_2	[0 1 1 0 1 1 0 0 1 0 1 0 1 0]

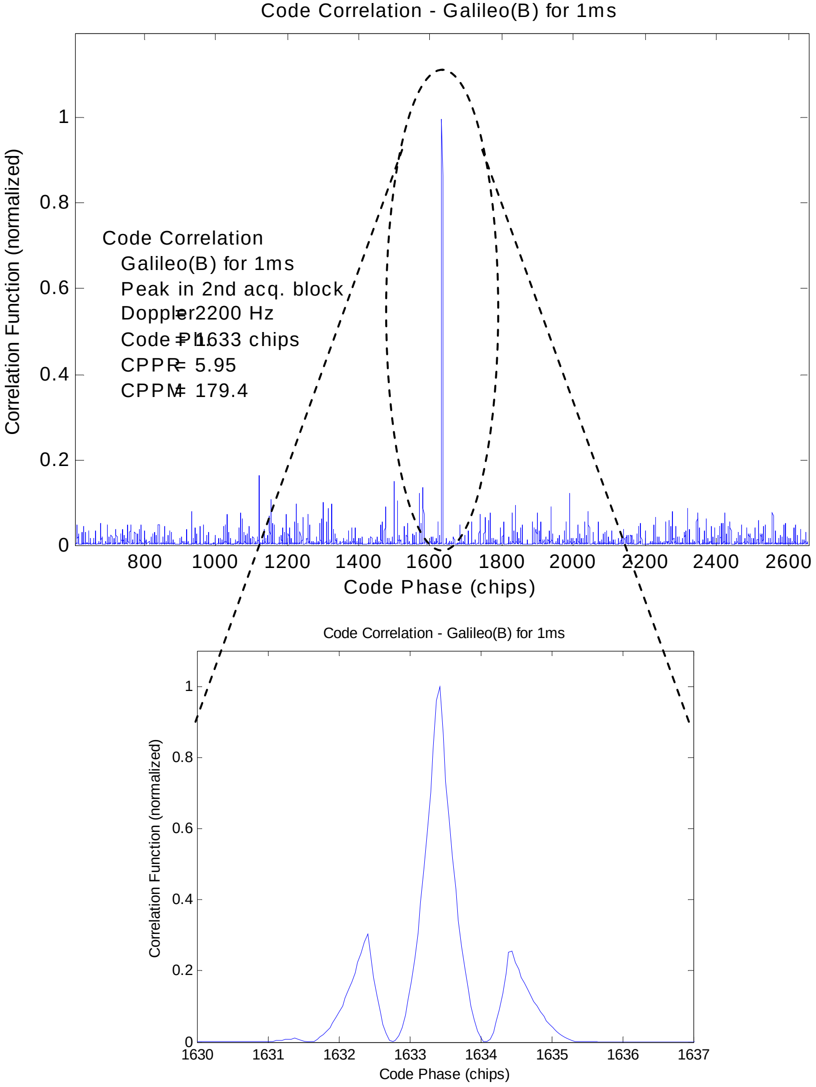
- All four codes are linear codes, can be generated by a 28 order polynomial
- The obtained code generator polynomials can be factorized
- Ambiguity of sign flipping is solved
- **Gold codes!**

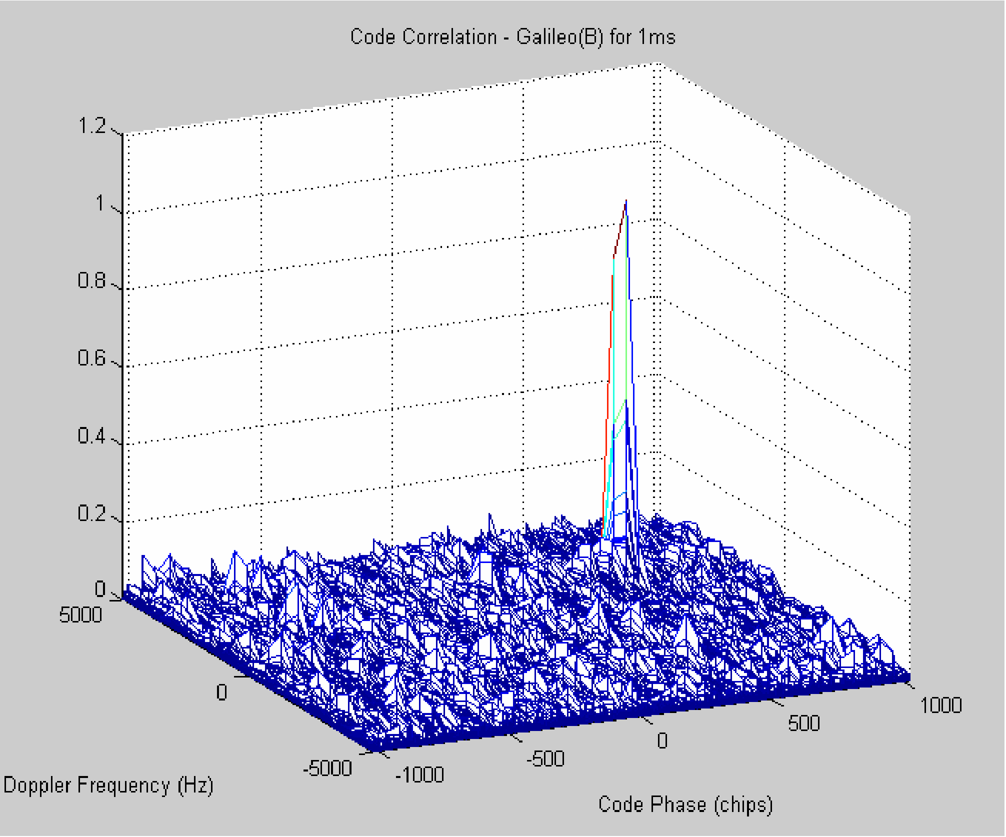
Applying the Codes for Acquisition and Tracking Real Broadcast signal


carrier wipeoff
code wipeoff
Correlators integrate & dump
Tracking Loops
FFT-based Coherent Acquisition
sin
cos
Carrier NCO
Early
Prompt
Late
Code NCO
C/No, Carrier-phase, Doppler, & Code-Phase Estimator

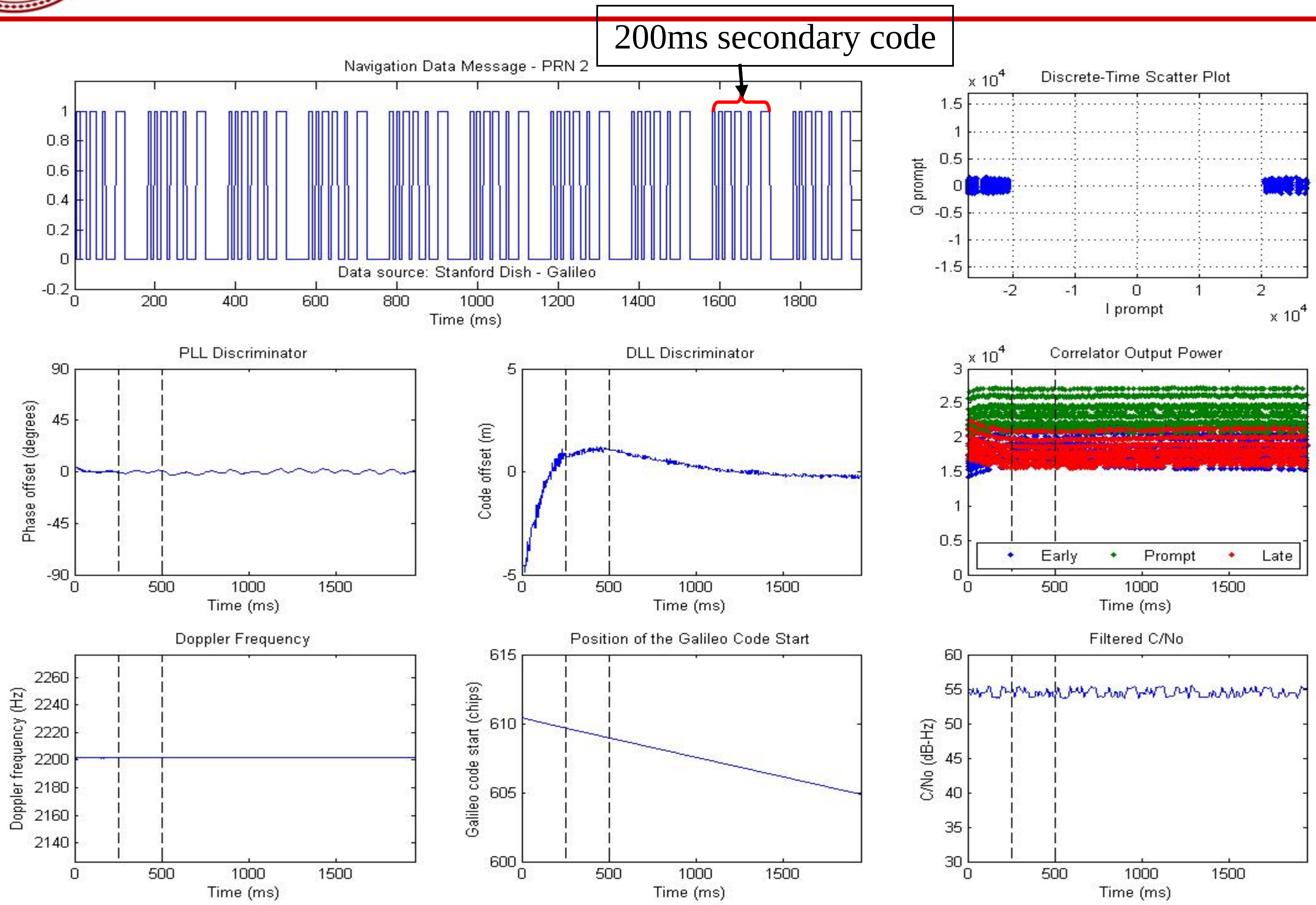
Software receiver block diagram

Acquisition of Broadcast L1-C Signal





Tracking of Broadcast L1-C Signal


200ms secondary code

Navigation Data Message - PRN 2

Data source: Stanford Dish - Galileo

Discrete-Time Scatter Plot

PLL Discriminator

DLL Discriminator

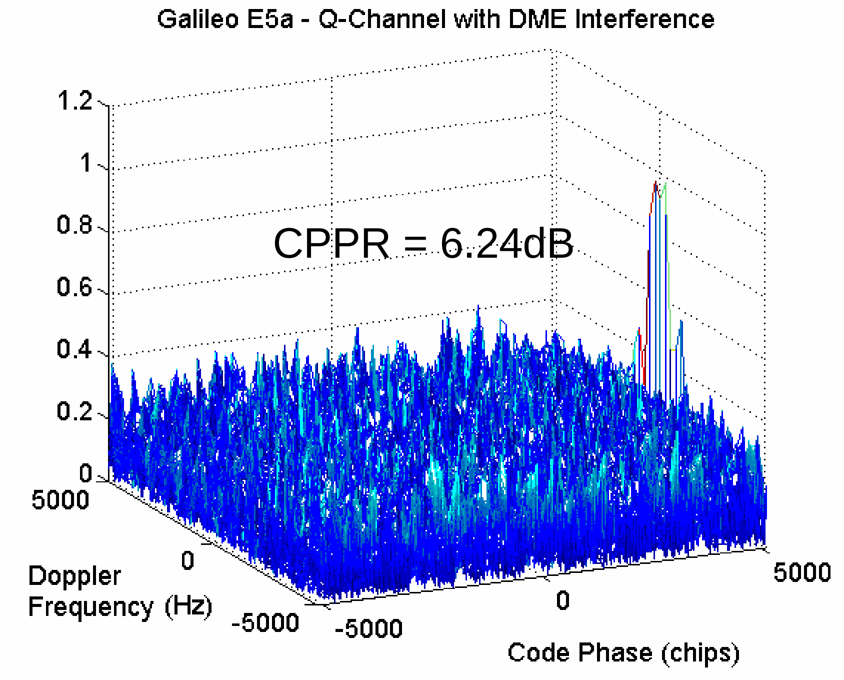
Correlator Output Power

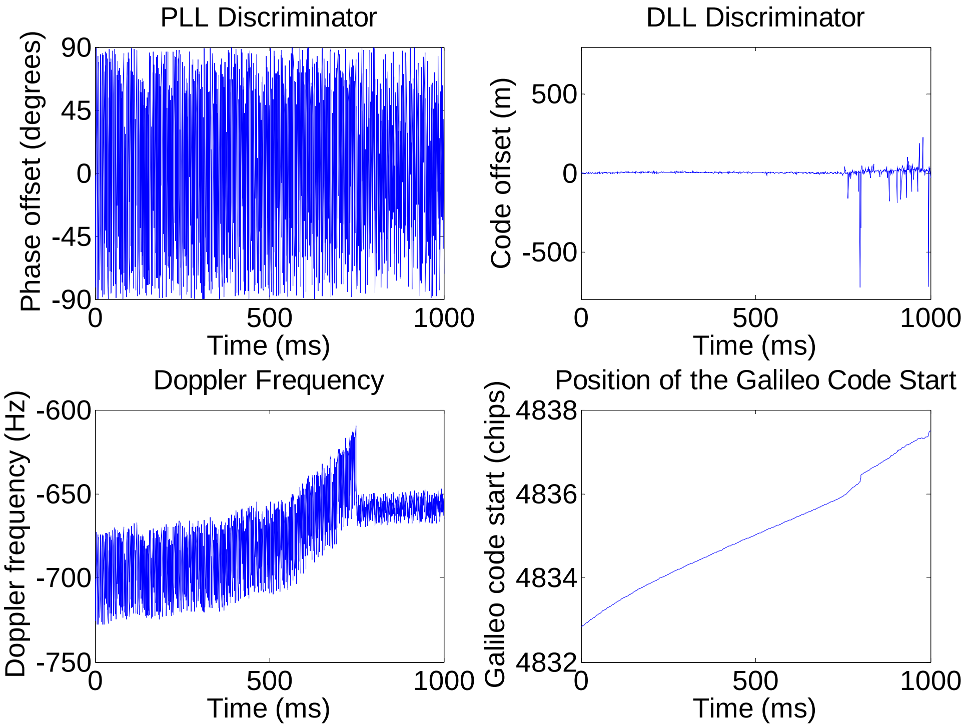
Doppler Frequency

Position of the Galileo Code Start

Filtered C/No

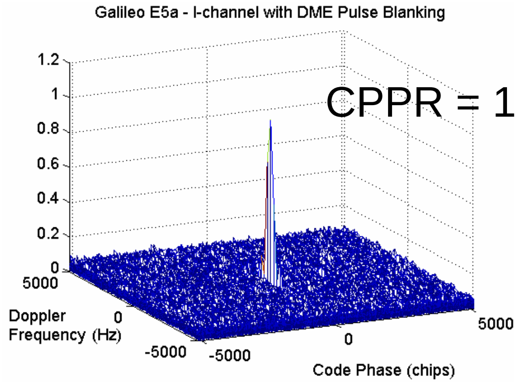
Acquire and Track Raw Data without any Signal Processing



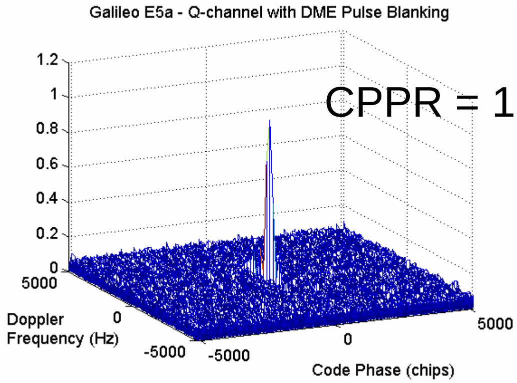


- Acquisition “successful” but tracking does not converge – too much error in initial Doppler estimate
- Doppler should be -450 Hz, but PLL incorrectly locks onto -650 Hz; poor aiding to DLL causes periodic large discriminator errors

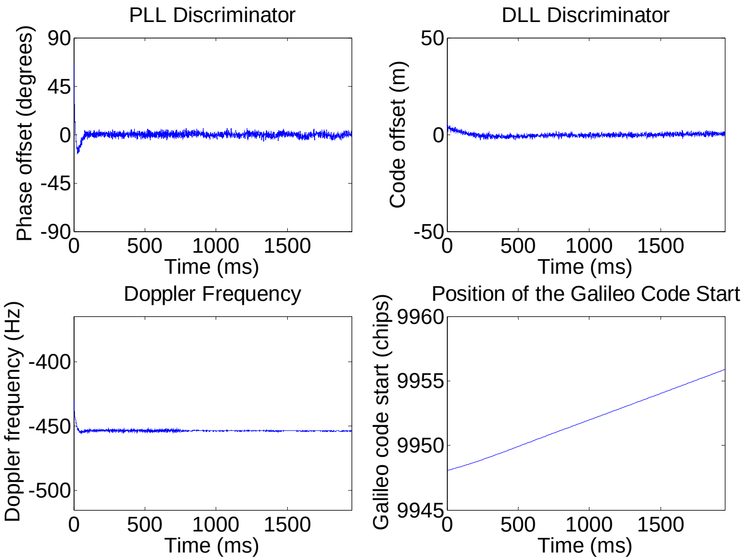
Acquire and Track Pulse-blanked Data

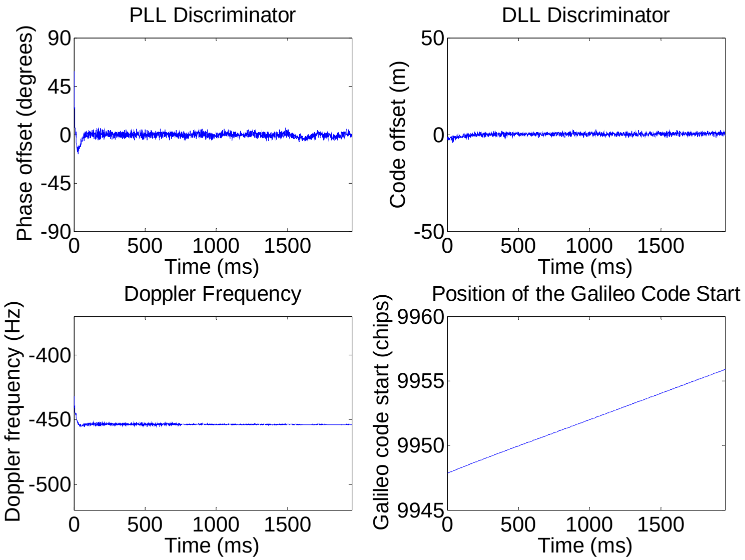


CPPR = 19.44 dB



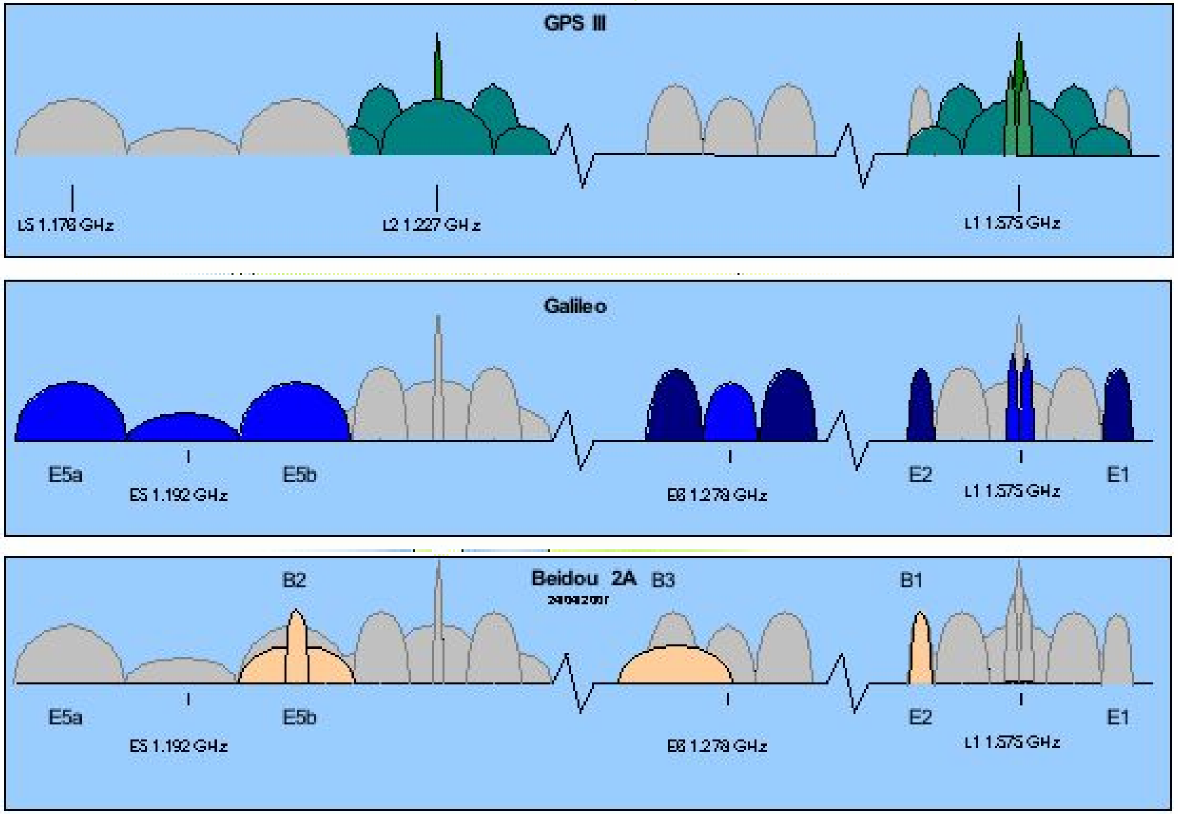
CPPR = 18.82 dB





Compass Frequency Plan Compared with GPS and Galileo

- On April 13 China launched the first MEO satellite in its Compass GNSS system, 21,550 km above the Earth. (GPS: 20,184 km; Galileo: 23,222 km)
- It has been transmitting on L1, E6 and E5b.

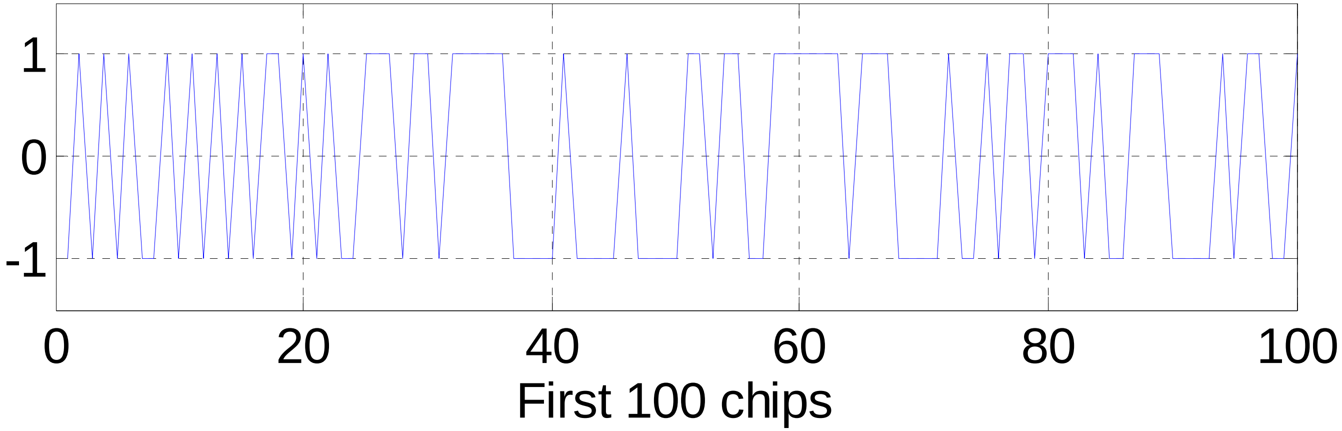


http://www.insidegnss.com/compass.php

Decoded Chinese Compass PRN Codes

The L1 PRN code is decoded to be an 11-order Gold Code.

L1 code (2046 bits, 1msec, 11-stage Gold code)	
Polynomial_1	$X^{11}+X^{10}+X^{9}+X^{8}+X^{7}+X+1$
Initial State_1	[0 1 0 1 0 1 0 1 0 1 0]
Polynomial_2	$X^{11}+X^{9}+X^{8}+X^{5}+X^{4}+X^{3}+X^{2}+X+1$
Initial State_2	[0 0 0 0 0 0 0 1 1 1 1]



Summary

- Decode all broadcast codes in L1, E6, E5a and E5b frequency bands of GIOVE-A test satellite.
- Decode Compass L1 code.
- Prove codes to be truncated Gold Codes
- Find code generators – linear shift feedback register
- Implement the code generators in software receivers
- Be able to acquire and track real broadcast signals
- Interference mitigation is desirable and beneficial for E5 signals

Questions?