PRN and GPS decoding using Software Defined Radio

J.-M Friedt, C. Fluhr, G. Cabodevila, E. Rubiola

FEMTO-ST Time & Frequency department, Besançon, France

jmfriedt@femto-st.fr

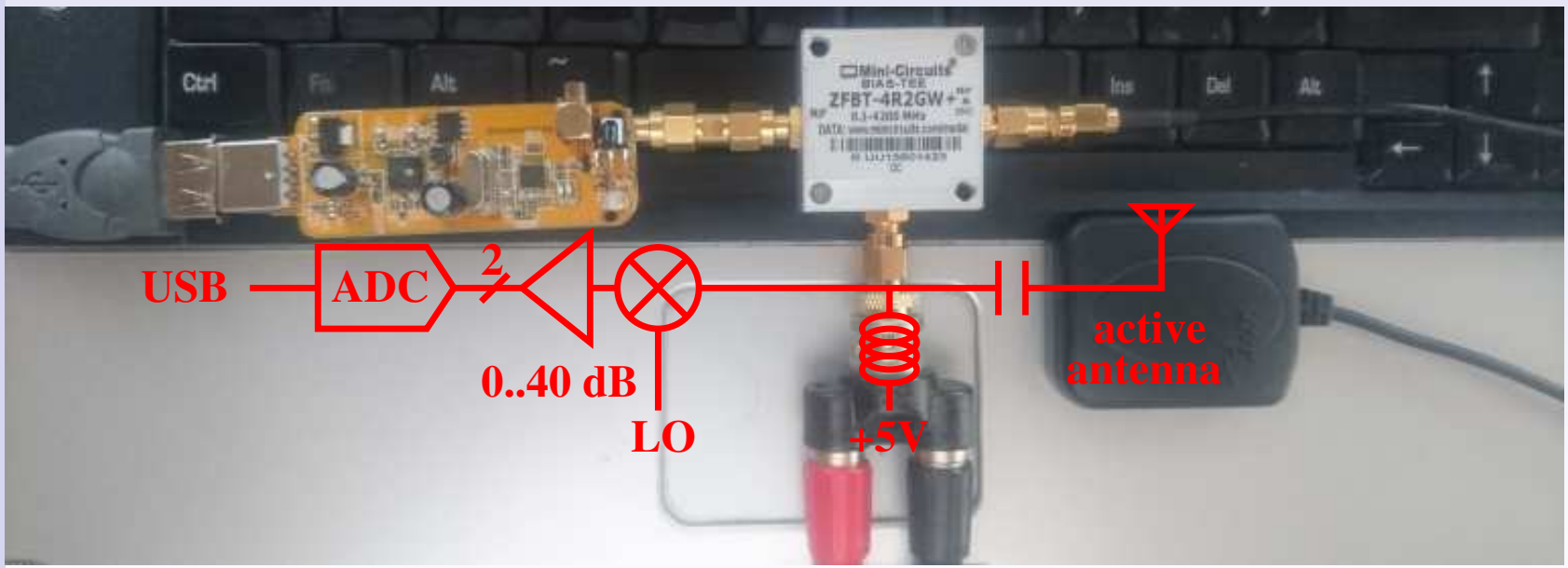
slides and references at
jmfriedt.free.fr

FIRST TF

June 27, 2018

Outline

1. Spectrum spreading for timing capability
2. Cross-correlation computation and relation to Fourier transform
3. Orthogonal coding for Code Division Multiple Access
4. GPS decoding: Doppler frequency offset + PRN detection
   - can I see satellites ? (autocorrelation)
   - what is the coarse frequency offset ? (squaring the signal)
   - PRN-Doppler chart (which satellite is where)
   - navigation message



Software Defined Radio receiver applied to GNSS

Introduction: GNSS

GNSS:

- Spaceborne atomic clocks
- Aim: use of ultrastable time references beyond positioning ...
- ... eg. tide gauge [1], moisture detection [2], phase monitoring (TEC)
- Requires at least phase recovery.
- Educational purpose: detailed understanding of the steps needed to complete a GPS receiver low phase noise LO !
- Towards software defined radio GNSS receivers for improved security and safety (spoofing attacks)

Use a low cost DVB-T receiver for acquisition:

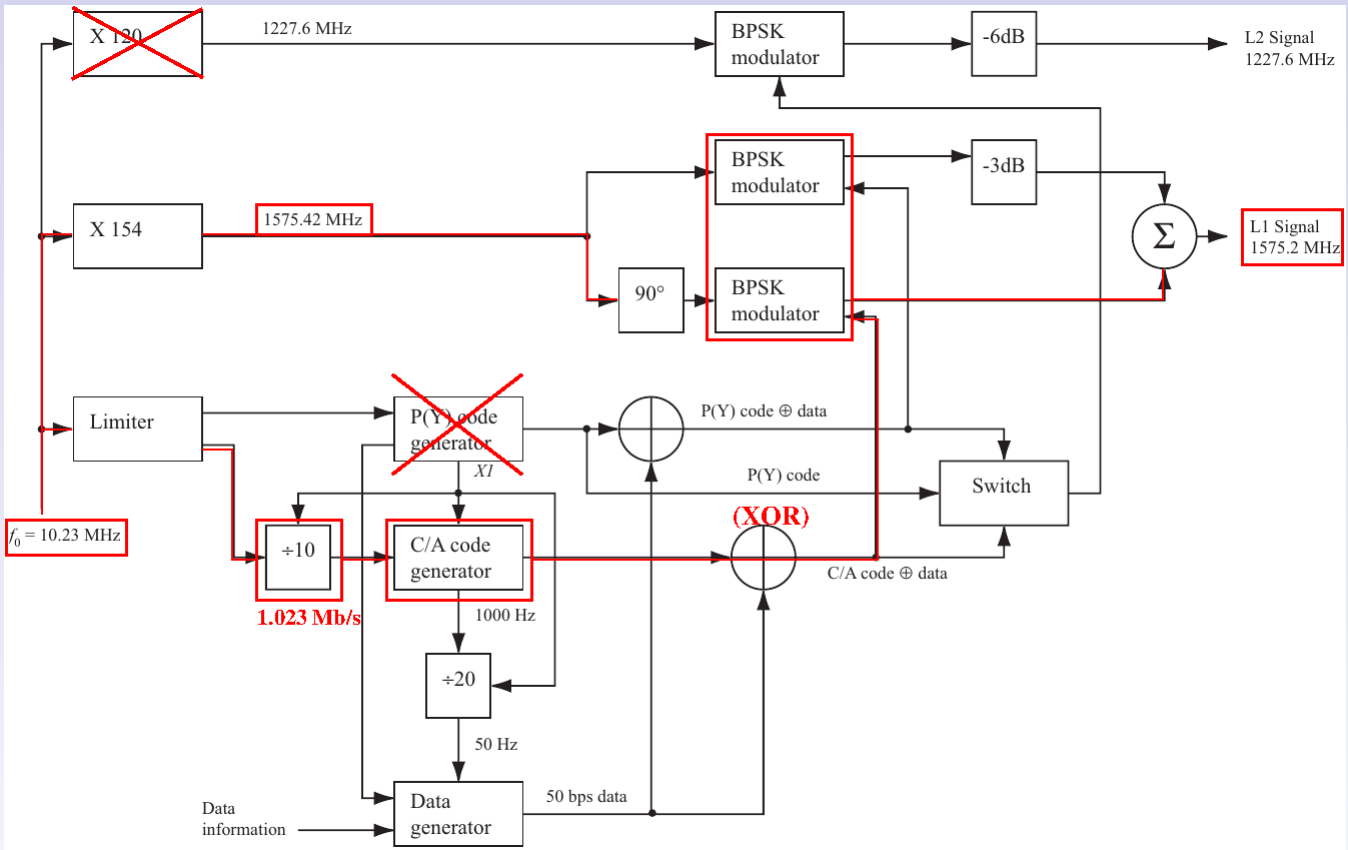
- 8 bit-resolution
- poor sensitivity $\Rightarrow$ pre-amplified antenna
- 2.4 MHz measurement bandwidth limited by USB bandwidth (I, Q components)

[1] K.M. Larson: `spot.colorado.edu/~kristine/Kristine_Larson/Home.html`

[2] Bock et. al., West African Monsoon observed with ground-based GPS receivers ..., J. Geophysical Research 113, D21105 (2008), at `http://onlinelibrary.wiley.com/doi/10.1029/2008JD010327/pdf`

CDMA: decoding GPS

GPS signal encoding principle [3] :



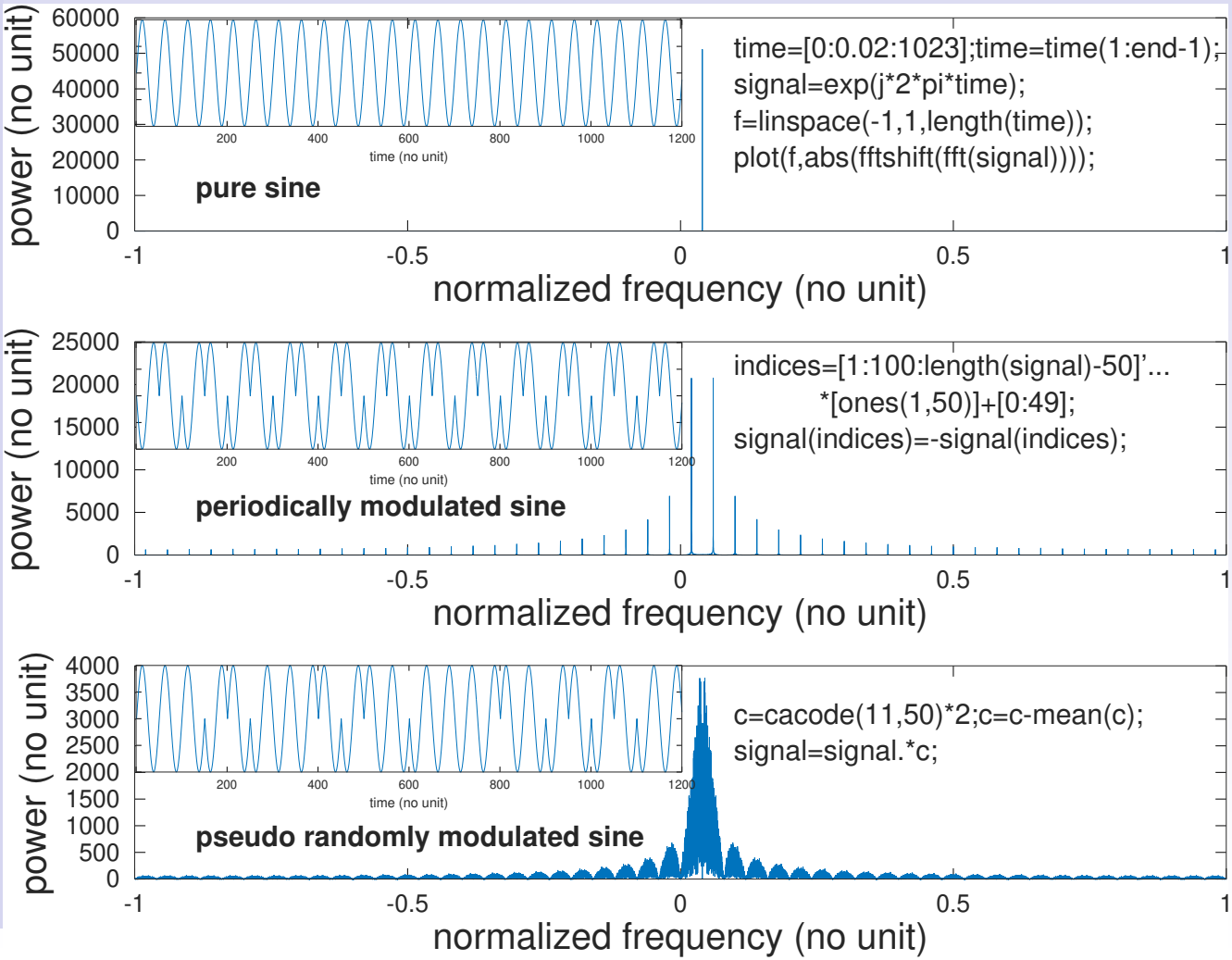
- the carrier is generated by an atomic clock (1575.42 MHz) ...
- ... is phase modulated at 1.023 MHz with a unique satellite identifier ...
- ... and again phase-modulated with the navigation message (50 bps)

[3] K. Borre *et al.*, *A Software-Defined GPS and Galileo Receiver – A Single-Frequency Approach*, Birkhäuser Boston, 2007

Spectrum spreading numerical experiments

Carrier frequency and bandwidth are two unrelated quantities which can be tuned independently for **matching each sensor spectral characteristics**

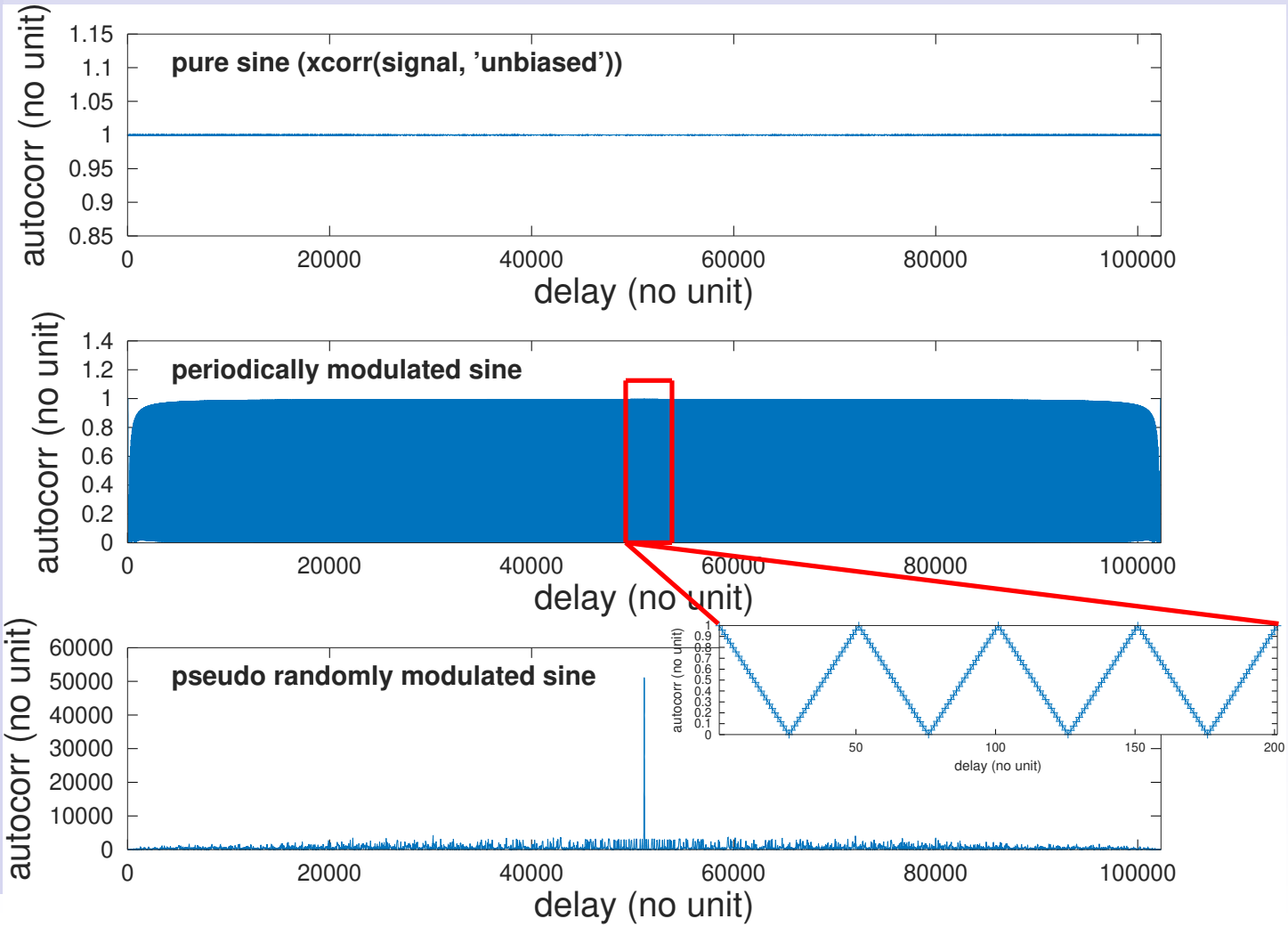
Binary Phase shift keying: $\varphi \in [0; \pi]$ for spectrum spreading



Spectrum spreading numerical experiments

Carrier frequency and bandwidth are two unrelated quantities which can be tuned independently for **matching each sensor spectral characteristics**

Binary Phase shift keying: $\varphi \in [0; \pi]$ for spectrum spreading



Spectrum spreading numerical experiments

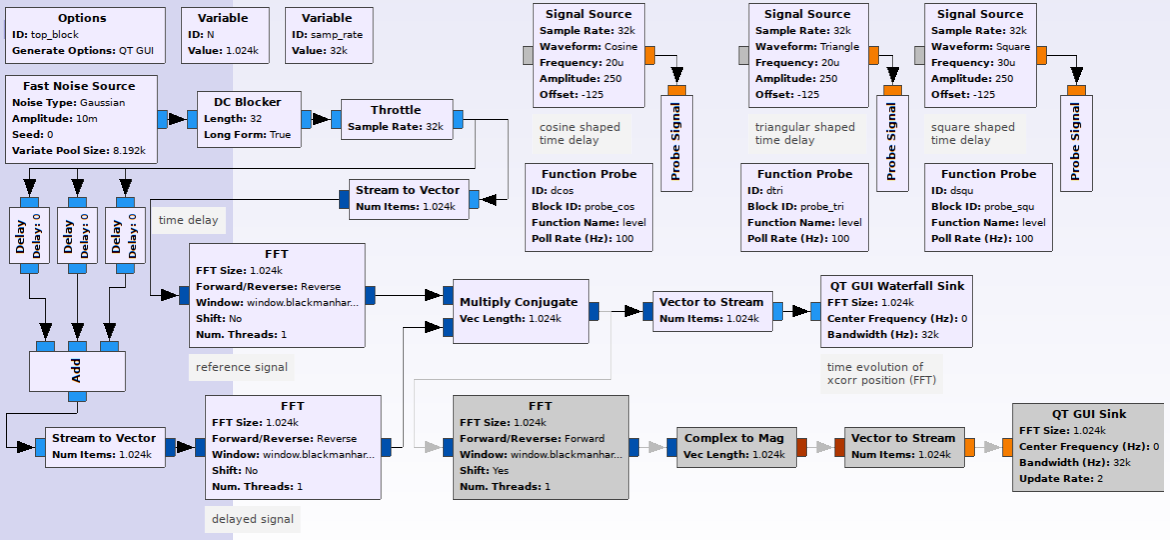
From convolution to correlation:

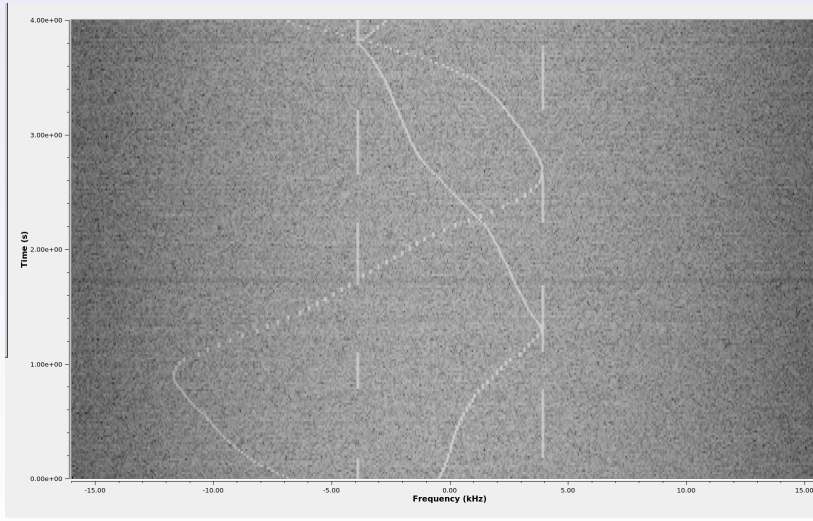
- Convolution: $conv(s,r)(\tau) = \int s(t)r(\tau - t)dt$
- Practical computation of convolution:

$$FT(conv(s,r)) = FT(s) \cdot FT(r)$$

- Correlation: $corr(s,r)(\tau) = \int s(t)r(t + \tau)dt$
- Convolution $\rightarrow$ correlation: time reversal
- since $\exp(j\omega t)^* = \exp(-j\omega t)$, we conclude

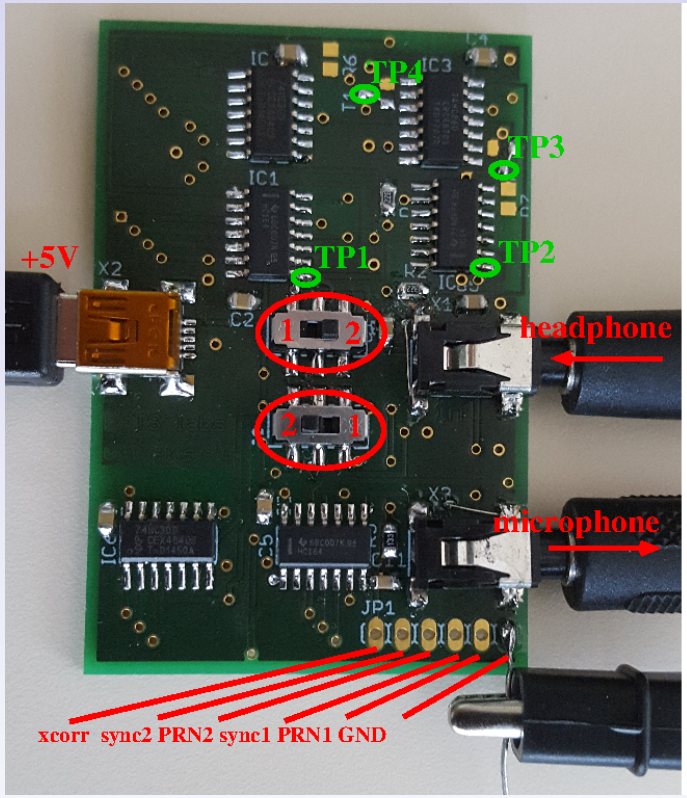
$$FT(corr(s,r)) = FT(s) \cdot FT^*(r)$$





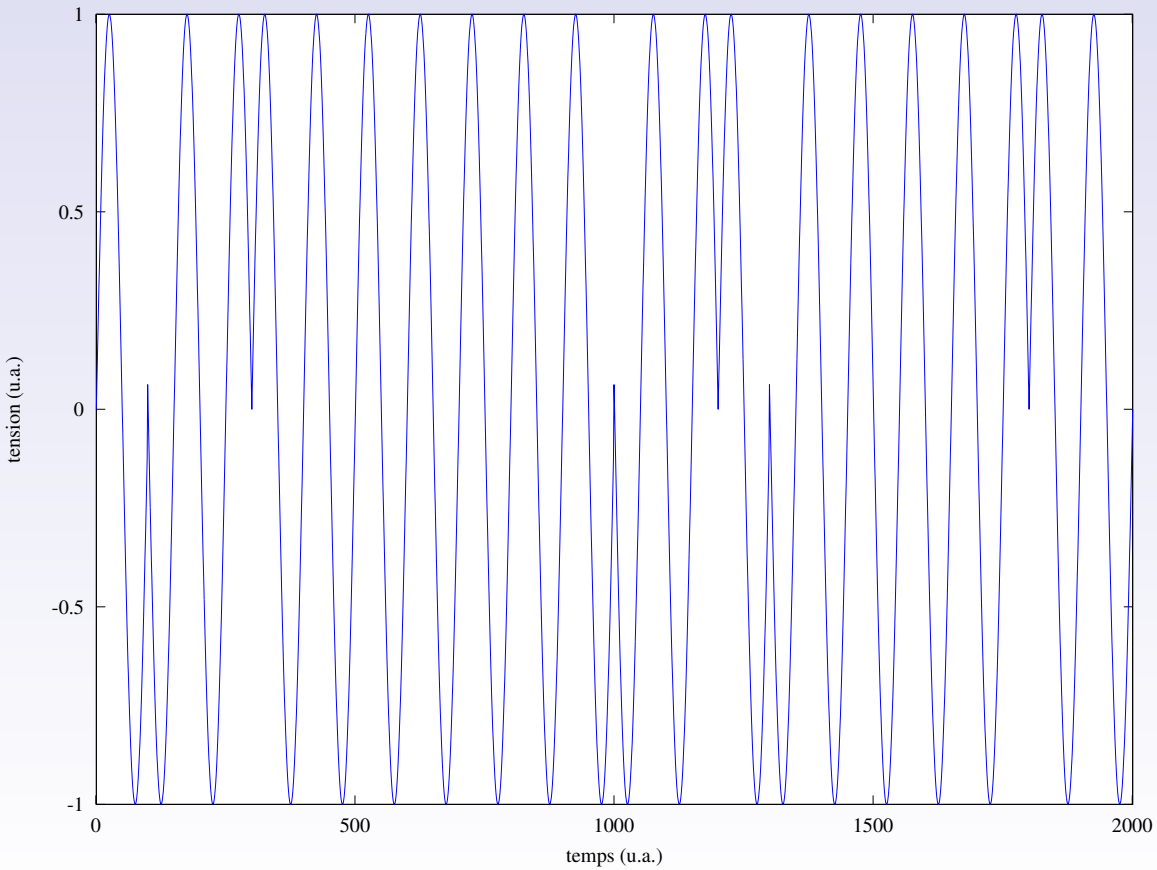
Lab session: hardware PRN

- Clock (carrier) feeds two PRN generators
- XOR/low pass filter as correlator
- Offset clock frequencies to sweep one PRN over the other
- Observe correlator dip when PRN sequences match (1 XOR 1=0 XOR 0=0)
- Introduction to the processing technique used to detect GPS a signal



Phase modulation

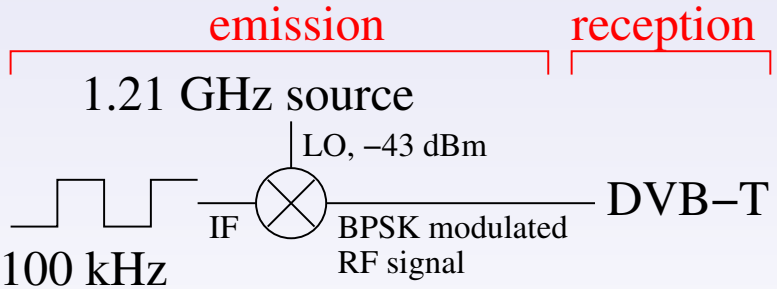
- PSK : Phase Shift Keying
- $\varphi = \arctan(Q/I)$: output of the I/Q demodulator
- local oscillator stability – constellation diagram
- GPS: BPSK (Binary Phase Shift Keying) – demonstration using a saturated mixer controlled by the bits to be transmitted

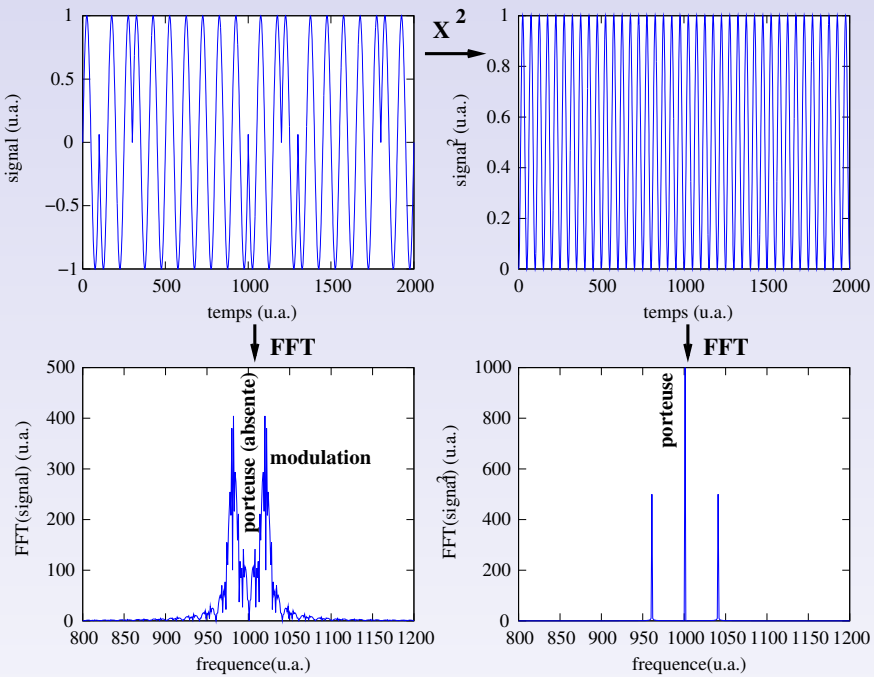


Phase demodulation

Requires accurate reproduction of the unmodulated carrier

$$\exp(j(\Delta\omega t+\varphi))^N = \exp(j(N\Delta\omega t+N\varphi)) = \exp(jN\Delta\omega t) \text{ if } \varphi = 2\pi\cdot n/N$$



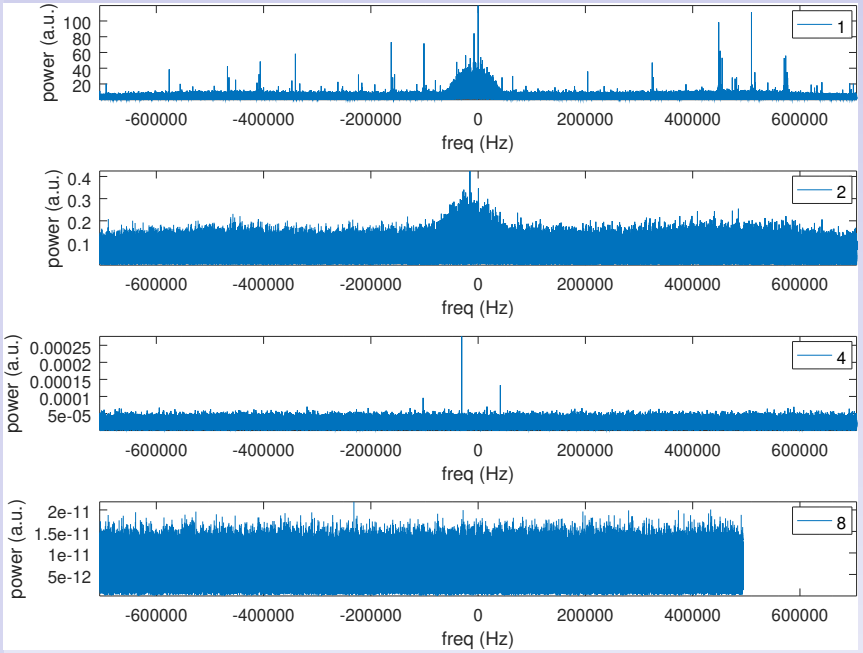


$$\cos(\varphi)^2 \propto \cos(2\varphi)$$
$$\varphi \in [0;\pi] \Rightarrow 2\varphi = 0[2\pi]$$

Carrier recovery by squaring BPSK

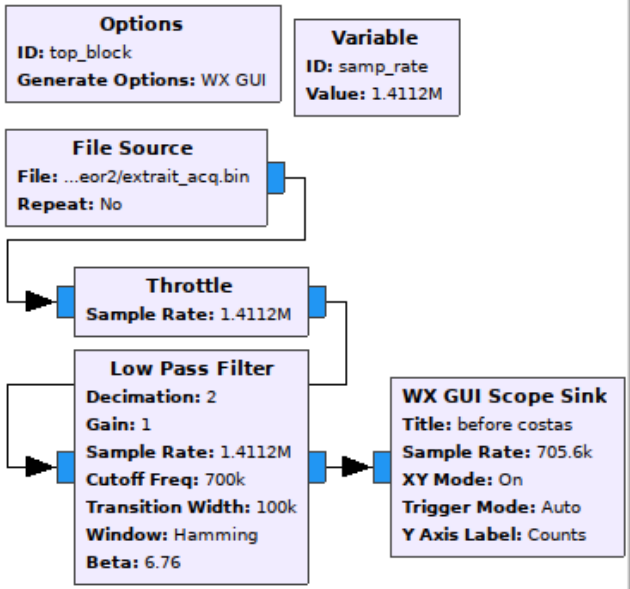
Find N by raising the I/Q signal to various powers until modulation sidebands disappear: **try with the Meteor M2 signal**: `jmfriedt.free.fr/extrait_acq.bin`

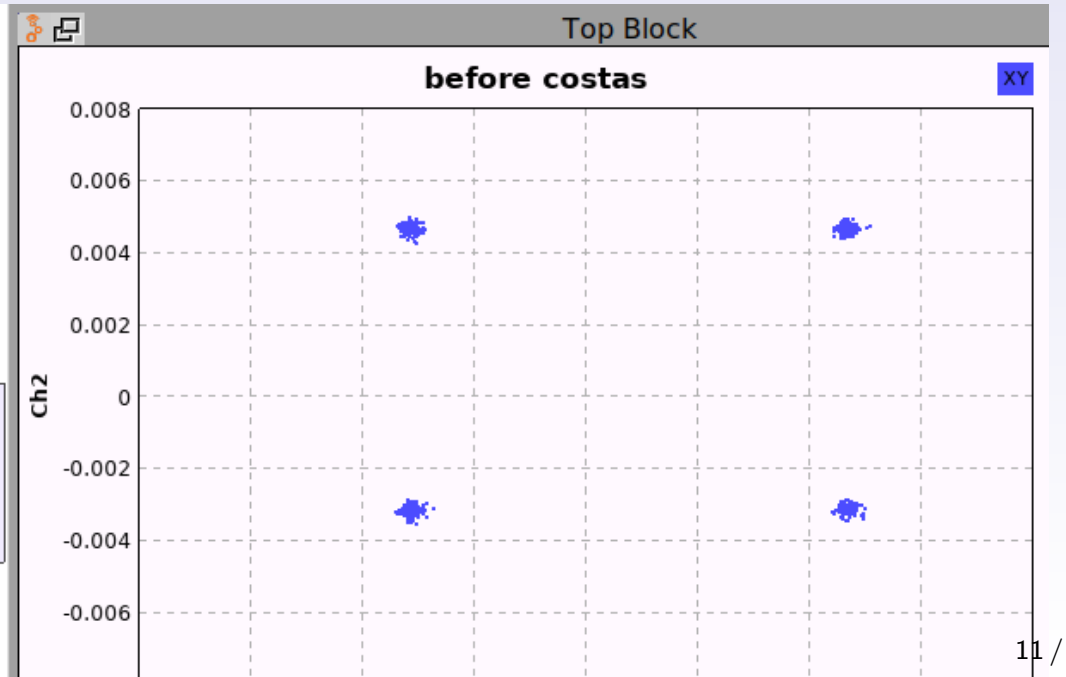
Meteor M2




```
x=read_complex_binary('extrait_acq.bin');
fs=11025*64*2; % 1.4112 MHz
N=300e3;
f=linspace(-fs/2,fs/2,N);
for m=0:3
 subplot(4,1,m+1);
 plot(f,fftshift(abs(fft(x(1:N).^(2^m)))));
 axis tight;
 xlabel('freq (Hz)');ylabel('power (a.u.)');
 legend(num2str(2^m))
end
```

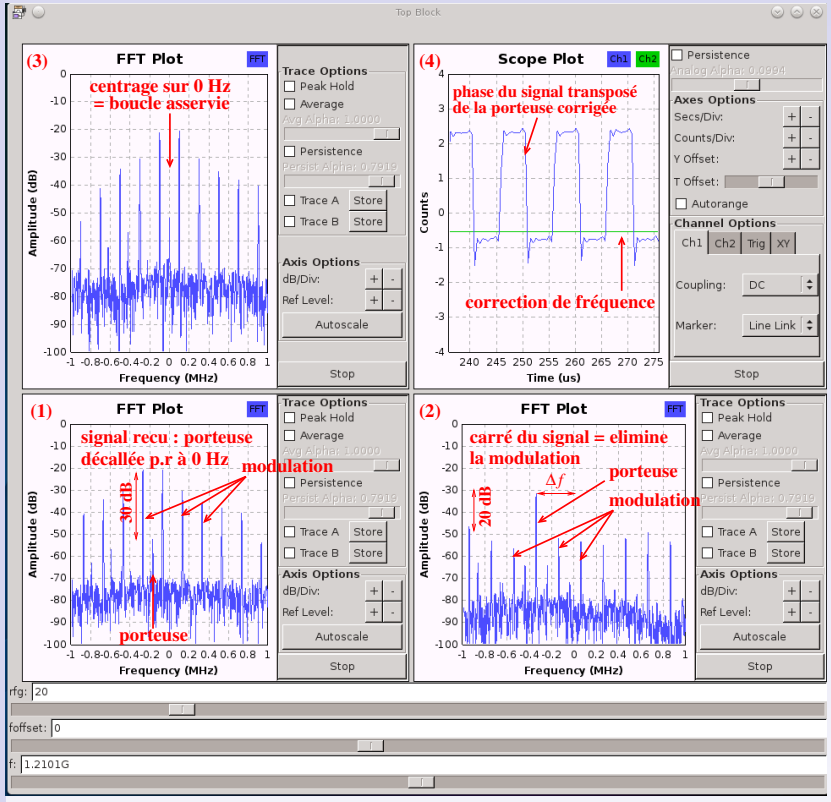
Tune N depending on SNR (e.g. Wifi – IEEE 802.11)



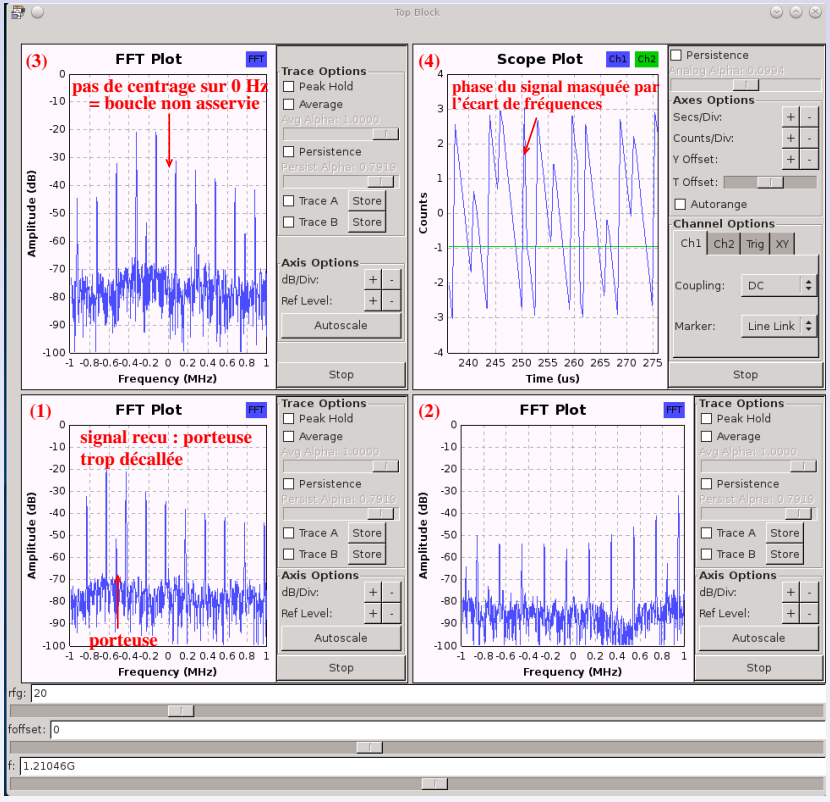


Phase demodulation

Software defined carrier recovery (feedback loop not allowed between GNURadio blocks): use the ready made Costas loop block:



Locked Costas loop

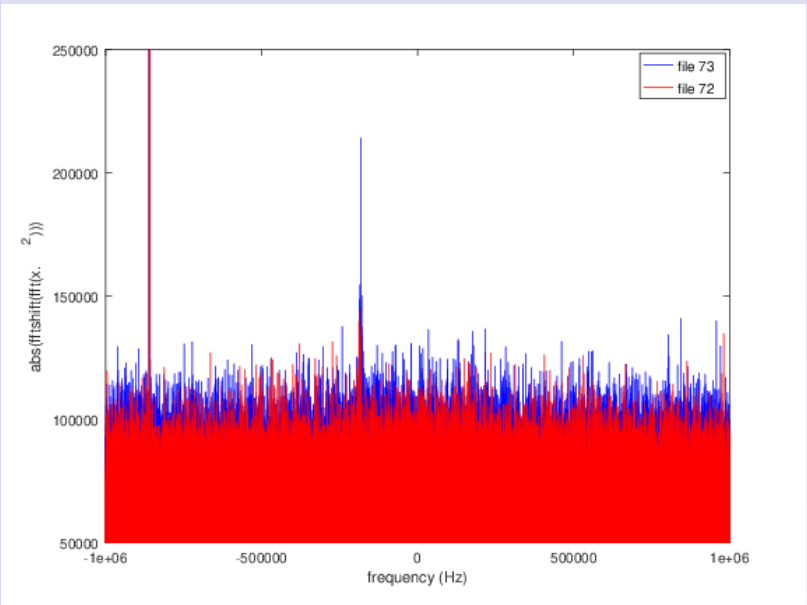


Unlocked Costas loop

Carrier offset: $\Delta\omega$ + Modulation: $\varphi = [0;\pi] \rightarrow \sin(\underbrace{\Delta\omega \cdot t + \varphi}_{separate})$

Example of GPS (BPSK)

Squaring a BPSK signal gets rid of modulation and collects all the energy in the carrier (requires averaging multiple Fourier transforms to get the squared signal spectrum out of the noise)

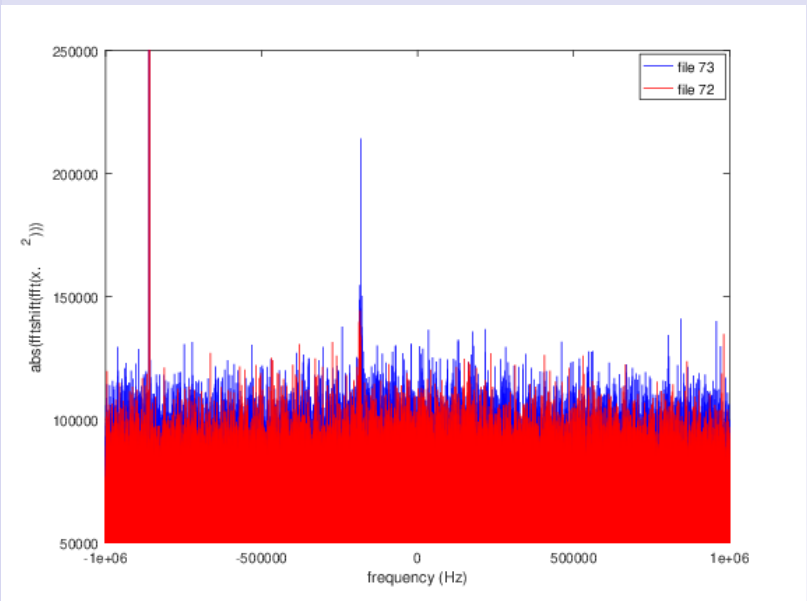


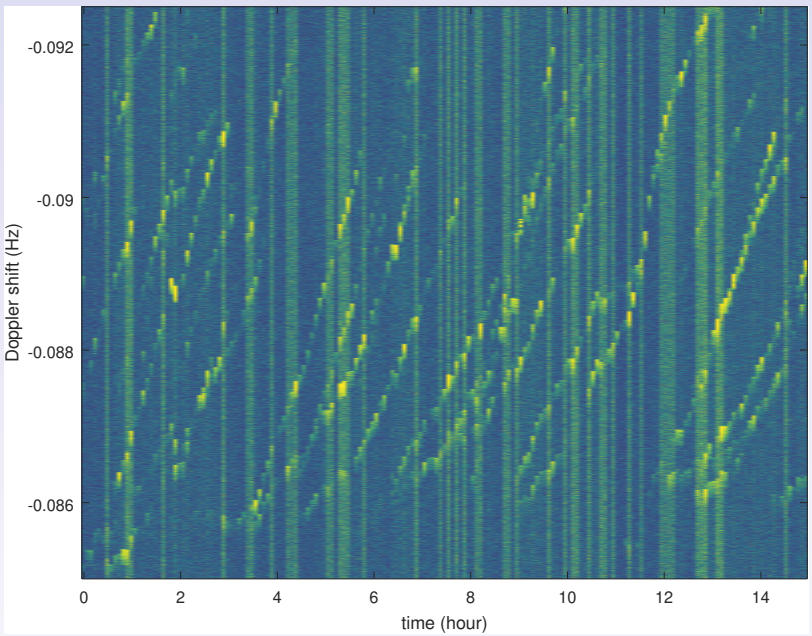
Coarse estimate of (twice) the Doppler shift+frequency offset[4]

[4] P. Boven, *Observe, Hack, Make: GPS* (2013): used in Vaisala RS80 radiosonde

Example of GPS (BPSK)

Squaring a BPSK signal gets rid of modulation and collects all the energy in the carrier (requires averaging multiple Fourier transforms to get the squared signal spectrum out of the noise)





Coarse estimate of (twice) the Doppler shift+frequency offset[4]

[4] P. Boven, *Observe, Hack, Make: GPS* (2013): used in Vaisala RS80 radiosonde

CDMA: software decoding of GPS

- GPS: 31-satellite fleet [5] orbiting Earth at a distance of 20000 km
- Time reference (Cs+Rb and then Rb only)
- Time of flight computation for positioning
- Offsets introduced by electromagnetic wave velocity fluctuations (ionosphere, troposphere) impossible to compensate for if a single frequency carrier is monitored
- Satellite ephemeris + time of flight = position of receiver on Earth
- Multiple applications beyond positioning [6] [7]

All satellites transmit on the same carrier frequency

---

[5] `http://spaceflightnow.com/2014/10/13/gps-modernization-continues-with-quick-pace-of-launches/`

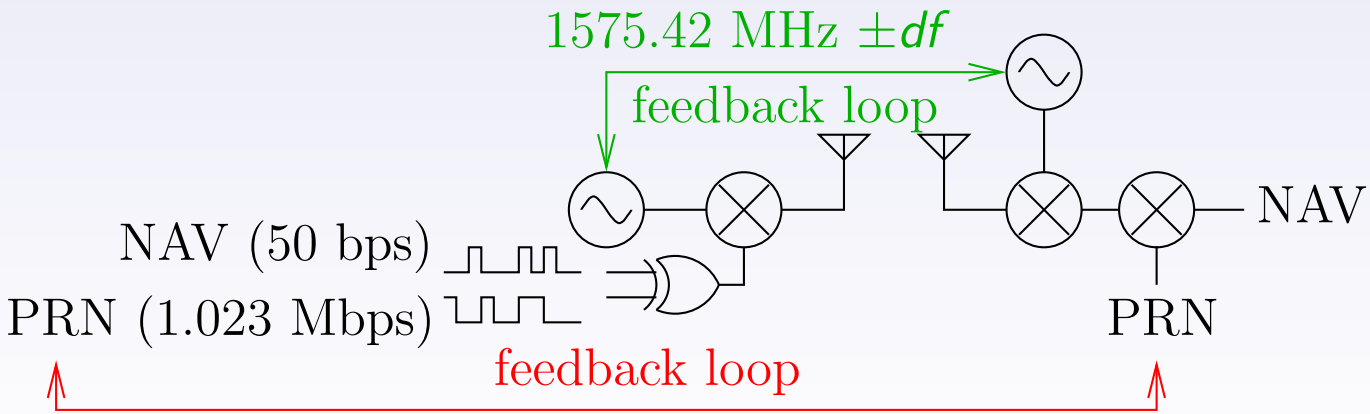
[6] J.-M Friedt, G. Cabodevila, *Exploitation de signaux des satellites GPS reçus par récepteur de télévision numérique terrestre DVB-T*, OpenSilicium 15, Juil.-Sept. 2015

[7] L. Lestarquit *et al.*, *Reflectometry With an Open-Source Software GNSS Receiver: Use Case With Carrier Phase Altimetry*, IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing **9** (10), pp. 4843–4853 (2016)

Objectives

- a modulator generates the information, here encoded in the phase of the carrier
- the information is carried on a signal whose frequency varies (Doppler, thermal drift of LO)
- recovering the transmitted information is a matter of eliminating carrier information
- two degrees of freedom (carrier frequency and CDMA for satellite identification) will require two feedback loops to recover the information

$\Rightarrow$ carrier recovery and code position (delay) recovery



CDMA: decoding GPS

Cross-correlation: search for a (known) pattern $m(t)$ in the received signal $s(t)$.

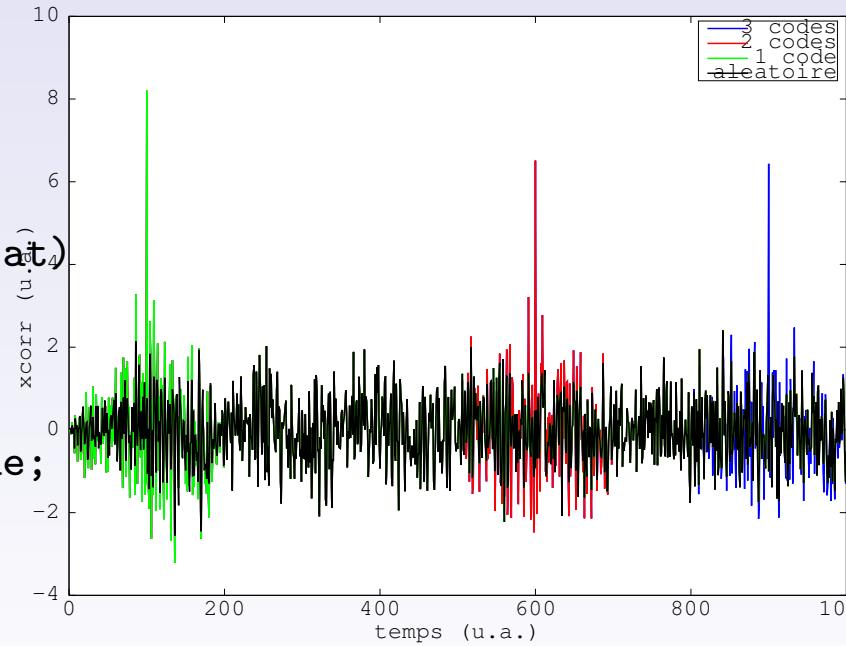
$$xcorr(\tau) = \int_{-\infty}^{+\infty} s(t) \times m(t+\tau)dt$$

becoming for discrete time

$$xcorr(n) = \sum_{k=-\infty}^{+\infty} s(k) \times m(k+n)$$

Searching for a known pattern in an apparently random sequence:

```
aleat=rand(1000,1);aleat=aleat-mean(aleat);
code=rand(100,1);code=code-mean(code);
aleat(1:100)=aleat(1:100)+code;
plot(xcorr(code,aleat))
aleat(end-99:end)=aleat(end-99:end)+code;
plot(xcorr(code,aleat))
aleat(end-500-99:end-500)= \
  aleat(end-500-99:end-500)+code;
plot(xcorr(code,aleat))
```



\+ **magnitude** of the cross-correlation indicates whether a bit is found

CDMA: decoding GPS

Cross-correlation: search for a (known) pattern $m(t)$ in the received signal $s(t)$.

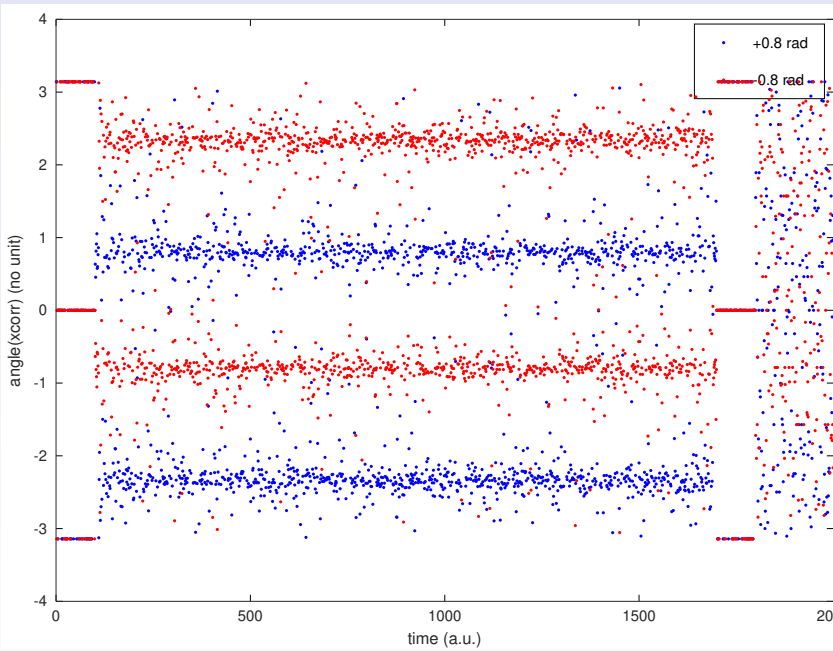
$$xcorr(\tau) = \int_{-\infty}^{+\infty} s(t) \times m(t+\tau)dt$$

becoming for discrete time

$$xcorr(n) = \sum_{k=-\infty}^{+\infty} s(k) \times m(k+n)$$

Searching for a known pattern in an apparently random sequence:

```
a=rand(1000,1);a=a-mean(a);
code=rand(800,1);code=code-mean(code);
a2=a;P=[101:900];
a2(P)=a(P)+10*code*exp(j*0.8);
r=angle(xcorr(code,conj(a2))); r(800)
a3=a;
a3(P)=a(P)+10*code*exp(-j*0.8);
r=angle(xcorr(code,conj(a3))); r(800)
```

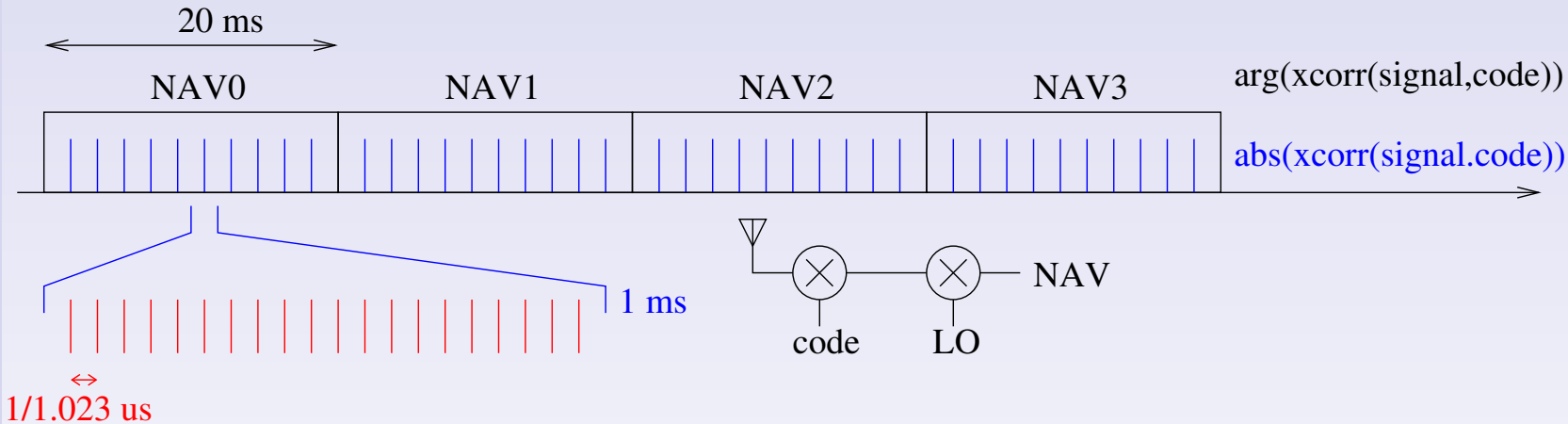


+ **phase** of the complex signal is transferred to the cross-correlation

CDMA: decoding GPS

Modulation steps:

- the carrier is binary-phase shift keying modulated with the satellite identifier at a rate of 1.023 MHz (phase rotations 0-180°)
- the message is additionnally binary-phase shift keying modulated over the previous signal (50 bps)



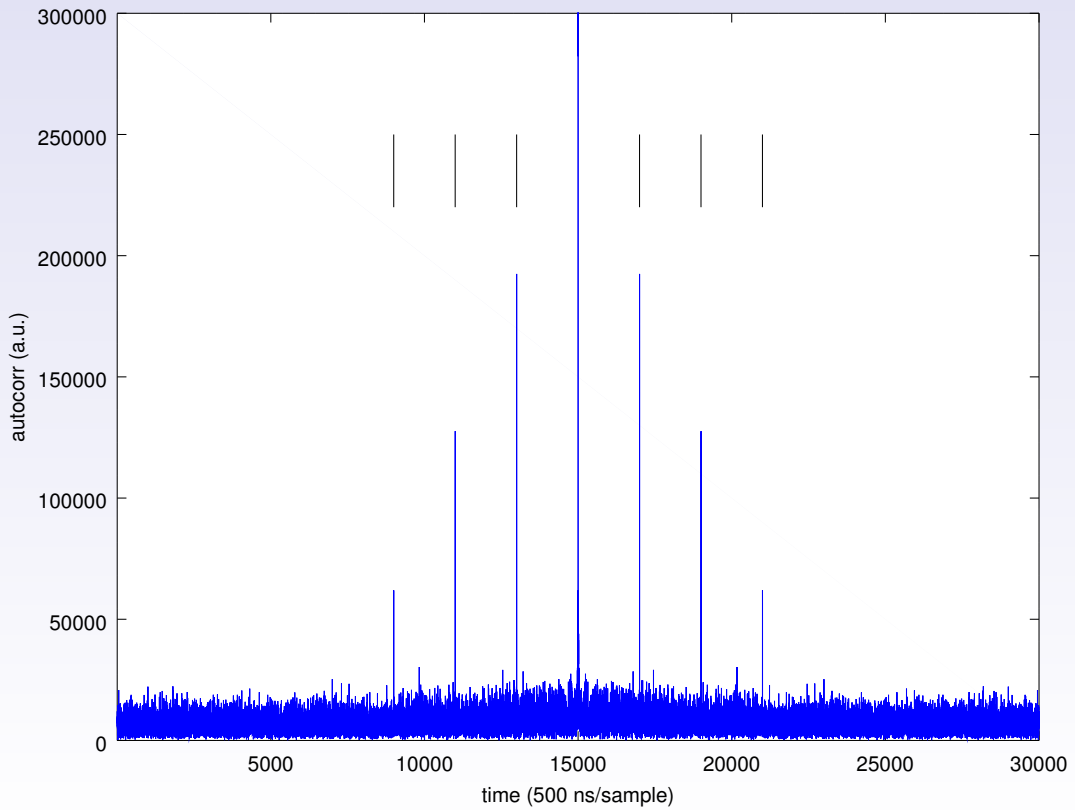
- when demodulating; first eliminate the code, ...
- ... to identify and eliminate the carrier,
- in order to recover the message.

The carrier frequency is not accurately known (Doppler shift): **what LO offset is acceptable for demodulating the message ?**

CDMA: decoding GPS

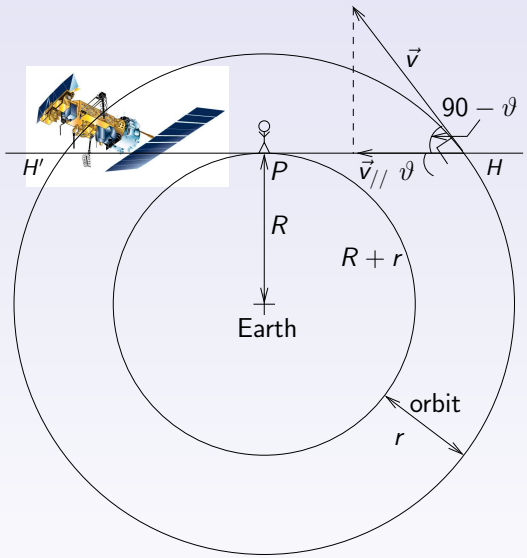
Even if we did not know the GPS encoding scheme, knowing that this code repeats is enough to assess whether a GPS signal is usable: **autocorrélation**

```
f=fopen('fichier.bin');d=fread(f,inf,'uchar');fclose(f);
d=d(1:2:end)-127+i*(d(2:2:end)-127);
time=[-10000:10000];
dx=abs(xcorr(d-mean(d),d-mean(d)));
plot(time,dx(2e6-10000:2e6+10000)); ylim([0 1e6]) % 2 MHz
```



CDMA: decoding GPS

- Decoding GPS is *only* possible if the carrier frequency is accurately known ...
- ... whcih can only be identified after removing the code from the received signal !
- Initial **exaustive** (*Acquisition*) search of all possible codes and frequency offsets (brute force) for later only *tracking* satellites known to be visible.
- What frequency offset should we look for ?



Doppler shift: $(R+r) = 20000 + 6400$ km in 12 h ($T^2/R^3 = \text{cst}$) $\Rightarrow |\vec{v}| = 3830$ m/s

Since $\sin(\theta) = \frac{R}{r+R}$ or $R \simeq 6400$ km

$\Rightarrow |\vec{v}_{//}| = |\vec{v}| \cos(90-\theta) = |\vec{v}| \sin(\theta) = |\vec{v}| \frac{R}{r+R}$

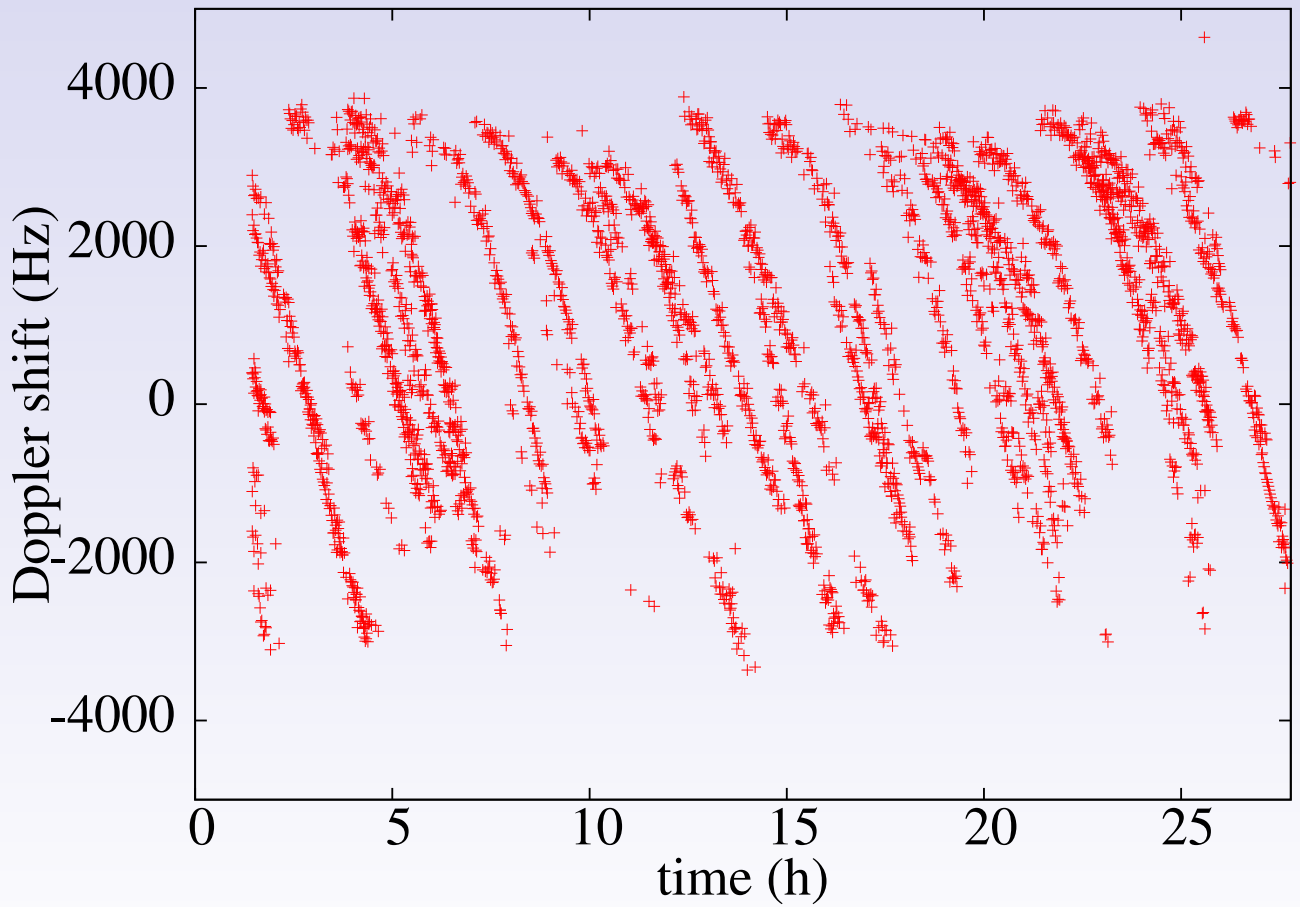
Result: $|\vec{v}_{//}| \in [\pm 4880]$ Hz

+ local oscillator contribution (bias and random fluctuations) !

Application: decode an acquired signal, using the GPS pseudo-random code generator available at `fr.mathworks.com/matlabcentral/fileexchange/14670-gps-c-a-code-generator/`

Observed Doppler shift

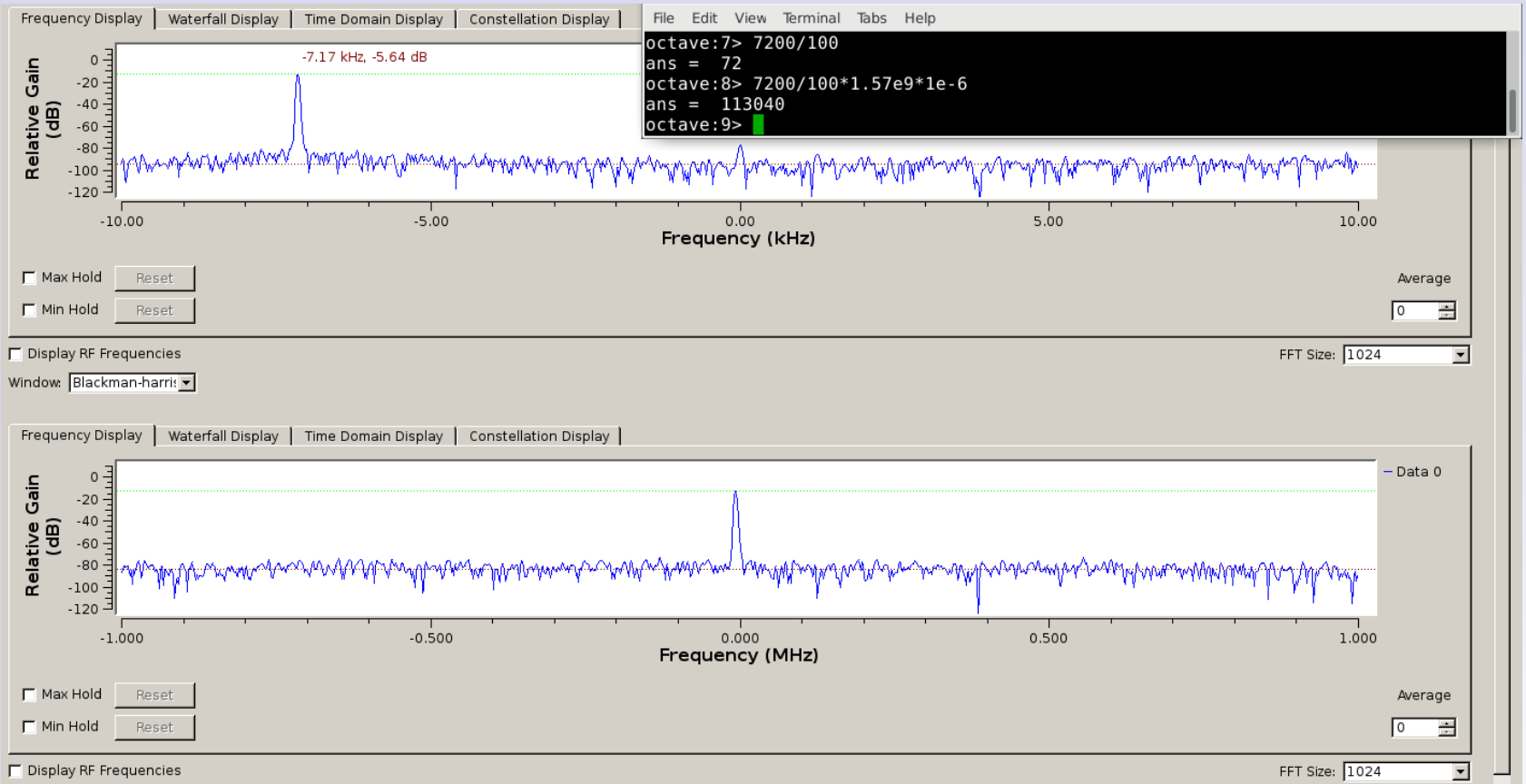
Record Doppler offset provided by `gnss-sdr` as a function of time for all visible satellites



Doppler indeed $\in [\pm 4000]$ Hz accounting for minimum elevation for detectable signal

On the need for high stability LO: offset v.s Doppler

Recording a 100 MHz carrier referenced to a Cs clock:

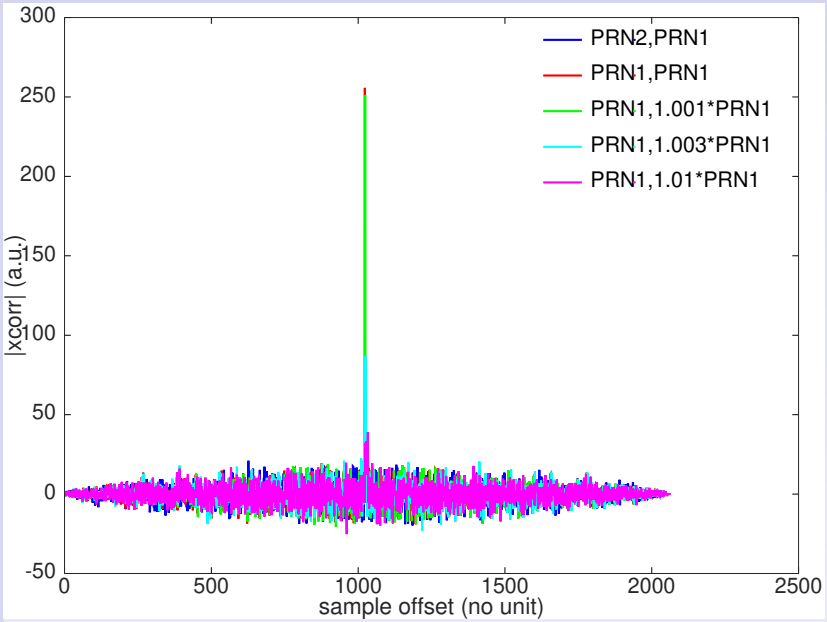


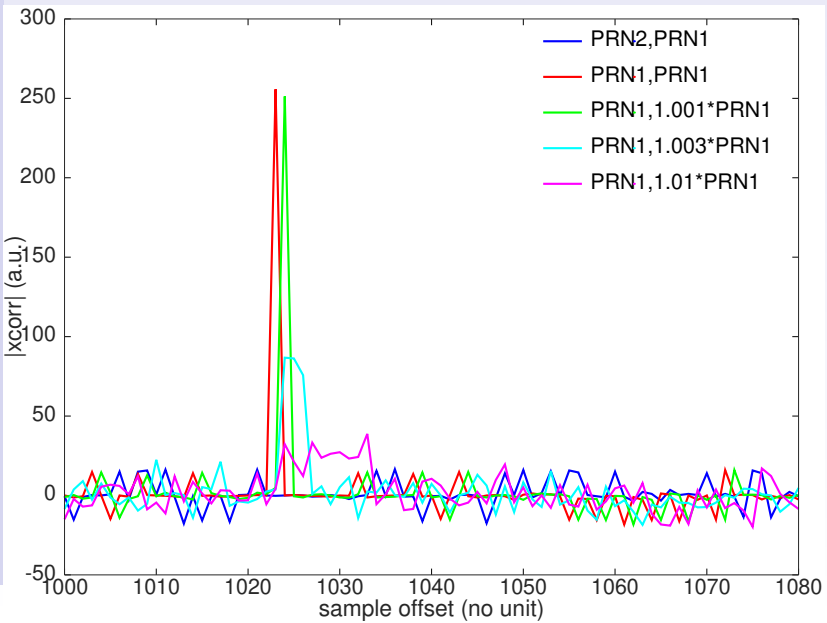
-75 ppm offset or 120 kHz at 1.57 GHz

$\Rightarrow$ rather than **20** Doppler frequencies ($\pm$5 kHz with 500 Hz steps) we must probe $\geq$ **500** Doppler frequencies

Doppler analysis frequency step

How accurately should the Doppler shift be known ?

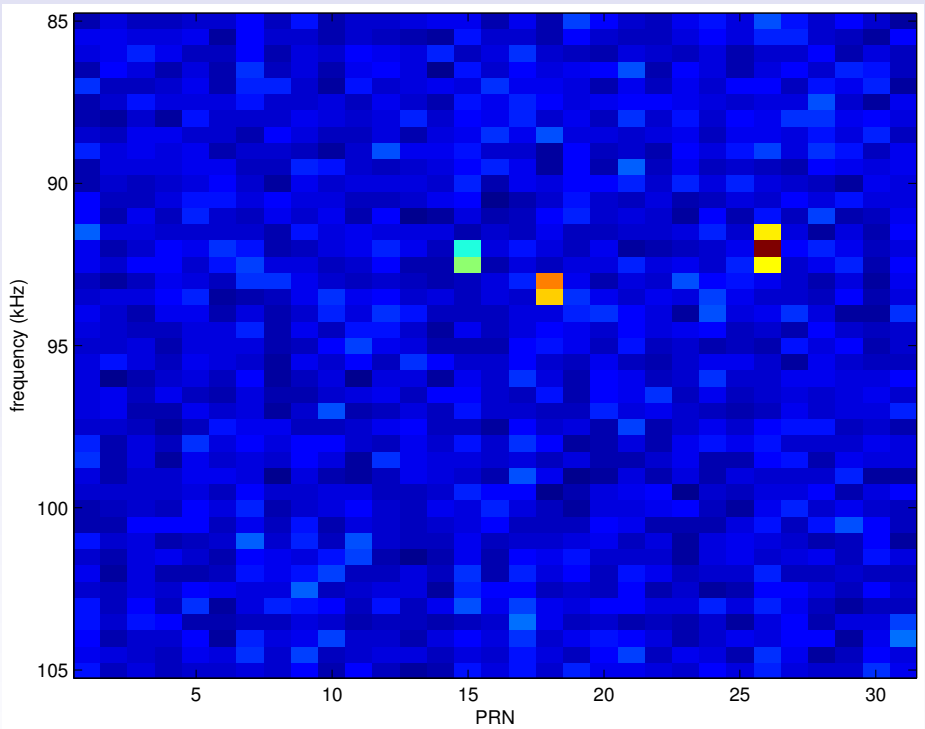




- 1023 kb/s $\simeq$ 1 μs/bit
- 1 ms long sentence: if the last bit mismatches: $dt/t = 10^{-6}/10^{-3} = 10^{-3}$
- $df/f = dt/t \Rightarrow df = 10^{-3} \times 1023$ kb=1 kHz
- to be safe, we select df=500 Hz

CDMA: decoding GPS

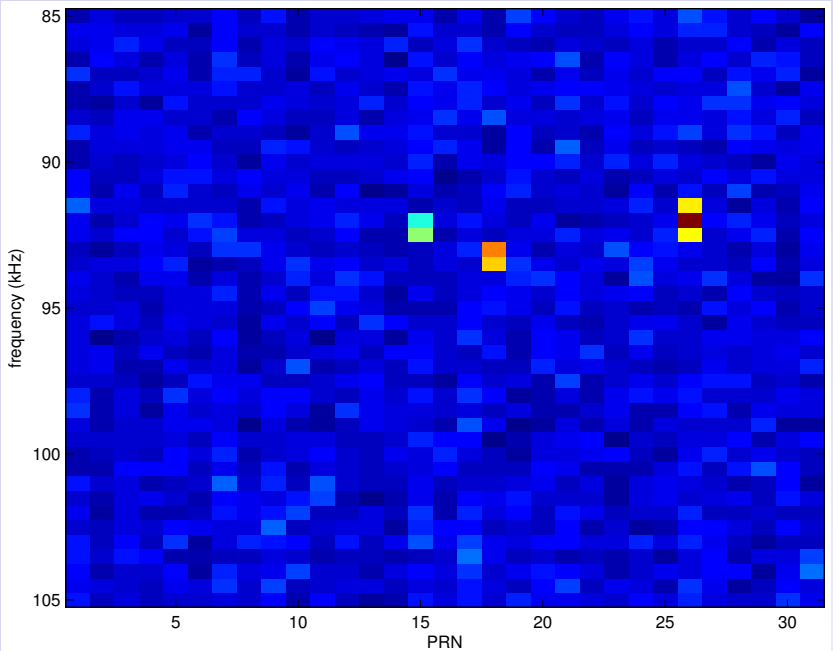
- CDMA basics: each useful bit (*navigation data*) is transmitted with its associated satellite identifier (SV PRN).
- All satellites transmit on the same carrier (1575.42 MHz), only their unique identifier allows differentiating each source.
- Each identifier is repeated every millisecond, NAV is at 50 bps so 20 samples/bit.

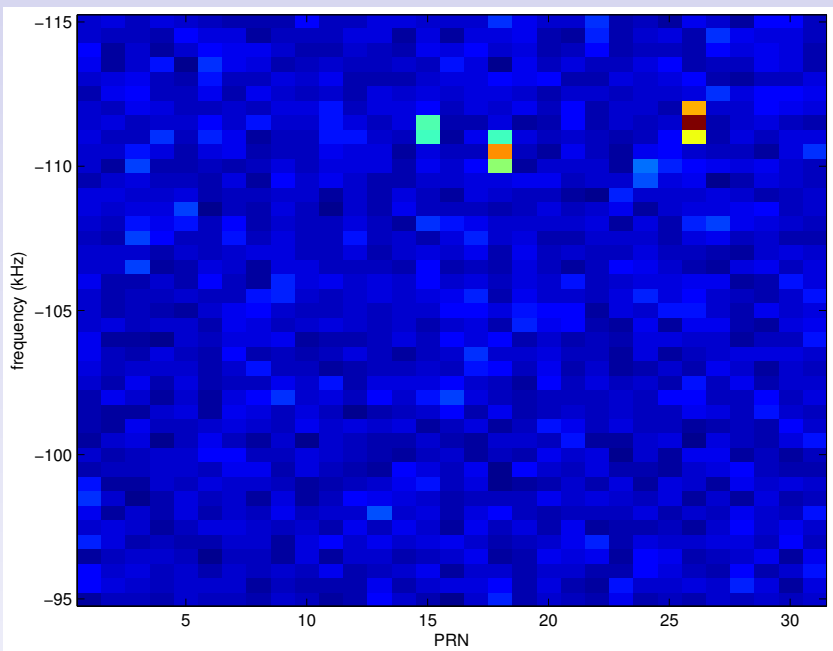


GNU/Octave v.s. `gnss-sdr` SV 15, 18, 26 are visible

CDMA: decoding GPS

Why do we need accuracte oscillators ?





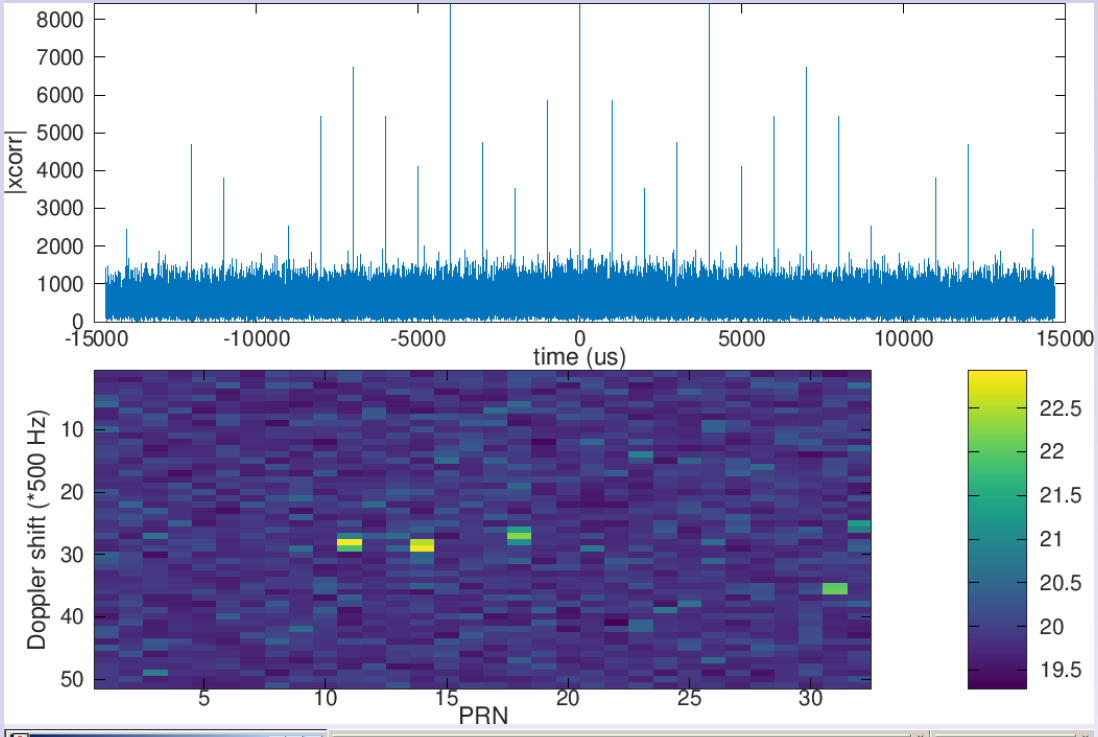
E4000 DVB-T
+59 ppm bias
=+91 kHz at 1575.42 GHz

R820T DVB-T
-68 ppm bias
=-107 kHz at 1575.42 GHz

Instead of searching a ±5 kHz range (Doppler) with 500 Hz steps, we must search ±150 kHz range ⇒ computation time[8] multiplied by 30 !

[8] 20 kHz range with 500 Hz steps on $2 \cdot 10^5$ samples: 302 seconds with Matlab R2010, 342 seconds with GNU/Octave 3.8.2

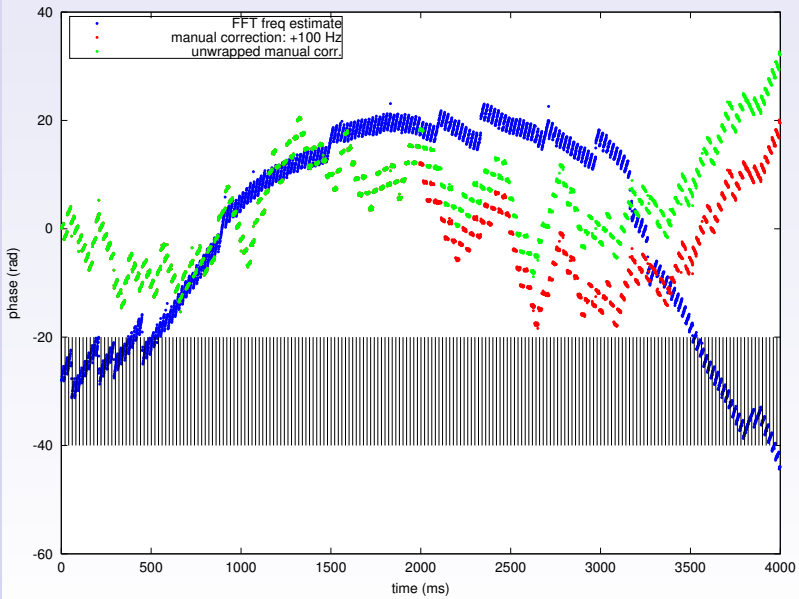
SDR v.s U-Blox

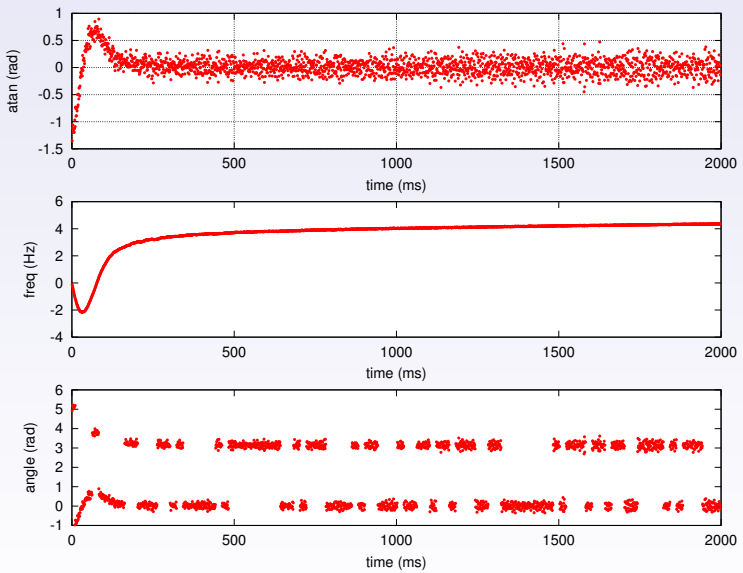


SV 10, 20, 27, 32 best visible with both receivers recording at the same time

CDMA: decoding GPS

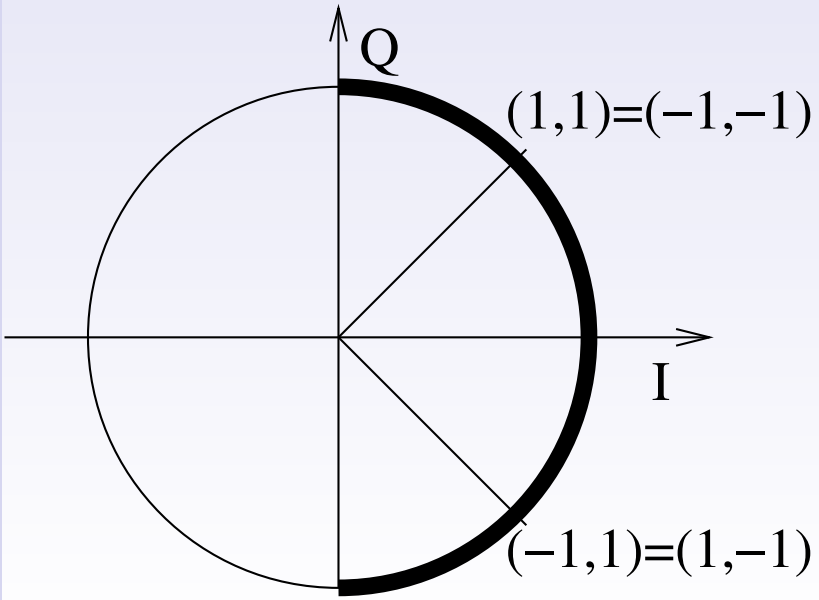
- Cross-correlating the received RF signal with orthogonal codes allows for identifying the source of the signal, but the message is lost
- once the **acquisition** phase is completed, **tracking** by controlling LO on the received carrier
- challenge: the phase is used both to encode the message and track the carrier
- how to eliminate the phase modulation to control the frequency ?
- N-PSK : $\varphi^N = 0[2\pi]$ but reduction by a factor N of the allowed frequency offset

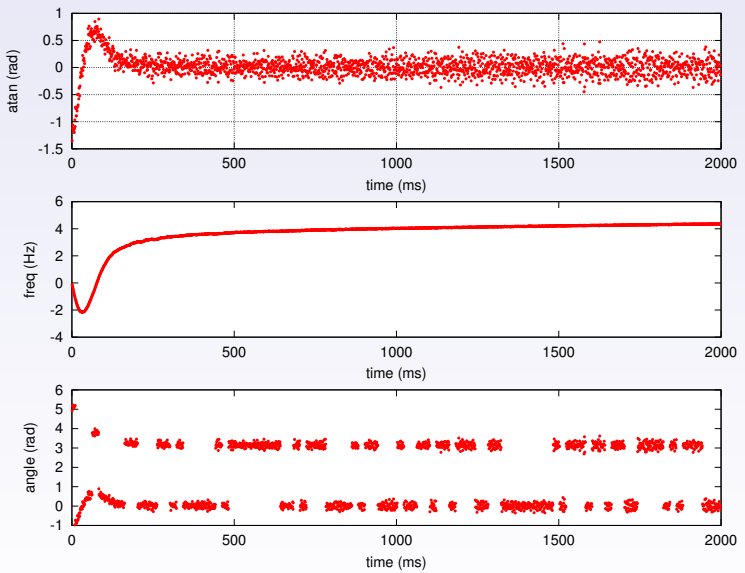




CDMA: decoding GPS

- Cross-correlating the received RF signal with orthogonal codes allows for identifying the source of the signal, but the message is lost
- once the **acquisition** phase is completed, **tracking** by controlling LO on the received carrier
- challenge: the phase is used both to encode the message and track the carrier
- how to eliminate the phase modulation to control the frequency ?
- atan(Q/I) v.s atan2(Q, I): Q/I cannot detect 180° phase rotation, while atan2 provides NAV..

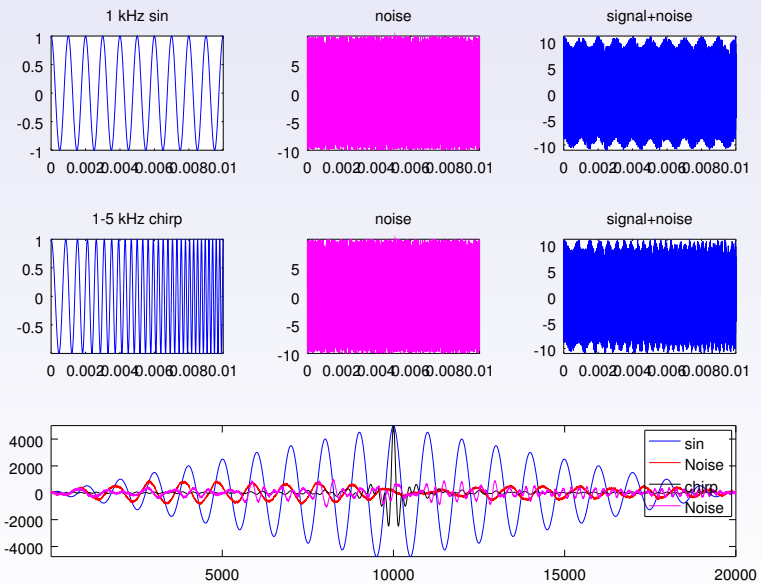




Pulse compression basics

- The longer the code (T), the longer the time during which the integral of xcorr accumulates energy and **smoothes noise**,
- but long pulse induces **loss of time resolution** $\Rightarrow$ cross-correlation is a broad peak
- strong variation of code over time $\Rightarrow$ increased bandwidth B $\Rightarrow$ cross correlation peak width $1/B$

pulse compression ratio (PCR) $= B \cdot T$

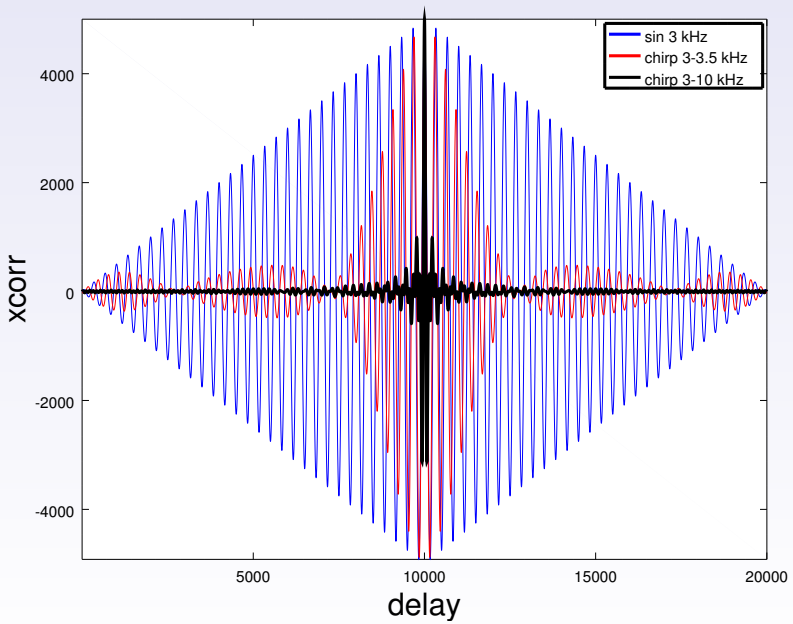



```
time=[0:1e-6:1e-2]; %samp. rate=1 us

x=chirp(time,1e3,time(end),1e3);
noise=20*rand(length(x),1)';
noise=noise-mean(noise);
xx=xcorr(x,x); xb=xcorr(x,noise);
plot(xx,'b-');hold on;plot(xb,'r-');

x=chirp(time,1e3,time(end),5e3);
xx=xcorr(x,x); xb=xcorr(x,noise);
plot(xx,'k-');hold on;plot(xb,'m-');
```

Pulse compression basics

- The longer the code (T), the longer the time during which the integral of xcorr accumulates energy and **smoothes noise**,
- but long pulse induces **loss of time resolution** $\Rightarrow$ cross-correlation is a broad peak
- strong variation of code over time $\Rightarrow$ increased bandwidth B $\Rightarrow$ cross correlation peak width $1/B$

pulse compression ratio (PCR) $= B \cdot T$

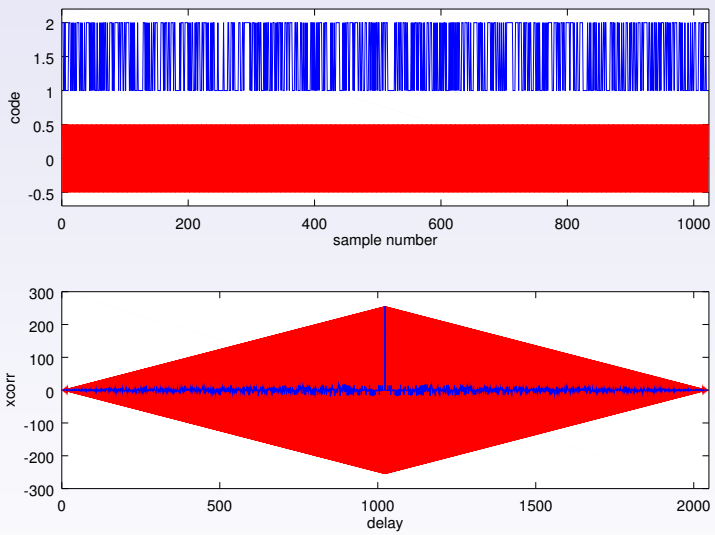



```
time=[0:1e-6:1e-2]; %samp. rate=1 us

x=chirp(time,1e3,time(end),1e3);
noise=20*rand(length(x),1)';
noise=noise-mean(noise);
xx=xcorr(x,x); xb=xcorr(x,noise);
plot(xx,'b-');hold on;plot(xb,'r-');

x=chirp(time,1e3,time(end),5e3);
xx=xcorr(x,x); xb=xcorr(x,noise);
plot(xx,'k-');hold on;plot(xb,'m-');
```

Pulse compression basics

- The longer the code (T), the longer the time during which the integral of xcorr accumulates energy and **smoothes noise**,
- but long pulse induces **loss of time resolution** $\Rightarrow$ cross-correlation is a broad peak
- strong variation of code over time $\Rightarrow$ increased bandwidth B $\Rightarrow$ cross correlation peak width $1/B$

pulse compression ratio (PCR) $= B \cdot T$



Remember: GPS is designed for **timing signals** with better than one "chip" resolution.

```
noise=rand(1023,1)'*7;
noise=noise-mean(noise);
b=[1:1023];
b=mod(b,2);b=b-mean(b);
plot(xcorr(b+noise,b),'r');hold on

a=cacode(1,1);a=a-mean(a);
plot(xcorr(a+noise,a));
plot(a+1.5);hold on;plot(b,'r');
```

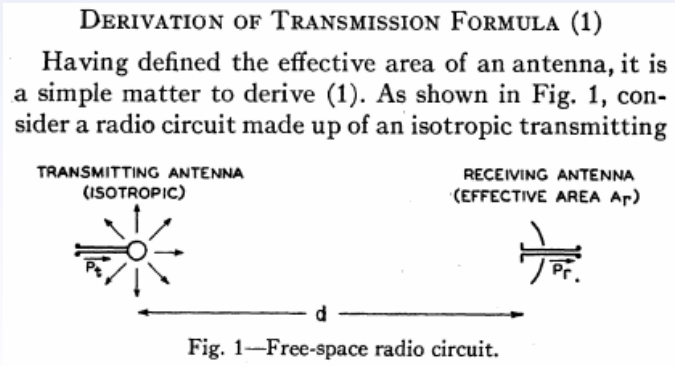
Link budget

- a radiofrequency (electrical) power is emitted, either isotropically or in a directional pattern with an antenna gain G_1: $P_E \times G_1$
- this power spreads on a sphere centered on the emitter: in the case of isotropic emitter, the area of this sphere is, at a distance d, $4\pi d^2$
- if $G_1 > 1$, then only a fraction $4\pi d^2/G_1$ of the sphere is illuminated
- this sphere intersects the receiver, which can detect any incoming signal on a 4π-steradian sphere on a typical area of λ^2
- this receiver might exhibit a reception antenna gain G_2

$$\frac{P_R}{P_E} = G_1 G_2 \left(\frac{\lambda}{4\pi d}\right)^2 : \text{Friis [9] equation}$$

or Free Space Propagation Loss (FSPL), since $20\log_{10}(c/4/\pi) = 147.5$ dB

$$FSPL = 20\log_{10}(f) + 20\log_{10}(d) - 147.55 \text{ dB}$$



DERIVATION OF TRANSMISSION FORMULA (1)

Having defined the effective area of an antenna, it is a simple matter to derive (1). As shown in Fig. 1, consider a radio circuit made up of an isotropic transmitting

Fig. 1—Free-space radio circuit.

[9] H.T. Friis *A Note on a Simple Transmission Formula*, Proc. I.R.E. 254-–256 (1946)

Link budget

- a radiofrequency (electrical) power is emitted, either isotropically or in a directional pattern with an antenna gain G_1: $P_E \times G_1$
- this power spreads on a sphere centered on the emitter: in the case of isotropic emitter, the area of this sphere is, at a distance d, $4\pi d^2$
- if $G_1 > 1$, then only a fraction $4\pi d^2/G_1$ of the sphere is illuminated
- this sphere intersects the receiver, which can detect any incoming signal on a 4π-steradian sphere on a typical area of λ^2
- this receiver might exhibit a reception antenna gain G_2

$$\frac{P_R}{P_E} = G_1 G_2 \left(\frac{\lambda}{4\pi d}\right)^2 : \text{Friis equation}$$

Application:

1. a GPS satellite emits 50 W (17 dBW=47 dBm) at 1575.42 MHz with an antenna gain of 13 dBi and flies at 20000 km over the Earth
2. $FSPL = 182$ dB$\Rightarrow P_R = -152$ dBW$= -\mathbf{122}$ dBm
3. receiver sensitivity: typically around -159 dBm (`usglobalsat.com/store/download/53/et312_ug.pdf`)
4. DVB-T: detection limit around -95 dBm (10 dB SNR) + 27 dB antenna gain = **-122 dBm** detection limit

Link budget

- a radiofrequency (electrical) power is emitted, either isotropically or in a directional pattern with an antenna gain G_1: $P_E \times G_1$
- this power spreads on a sphere centered on the emitter: in the case of isotropic emitter, the area of this sphere is, at a distance d, $4\pi d^2$
- if $G_1 > 1$, then only a fraction $4\pi d^2/G_1$ of the sphere is illuminated
- this sphere intersects the receiver, which can detect any incoming signal on a 4π-steradian sphere on a typical area of λ^2
- this receiver might exhibit a reception antenna gain G_2

$$\frac{P_R}{P_E} = G_1 G_2 \left(\frac{\lambda}{4\pi d}\right)^2 : \text{Friis equation}$$

What is the thermal noise power ?

1. 1 MHz bandwidth (1023 kHz) so that $10\log_{10}(10^6) = 60$ dB
2. $-174 + 60 = -\mathbf{114}$ dBm> -122 dBm !
3. but 30 dB=1023 kHz/1 kHz pulse compression: $-122 + 30 = -\mathbf{92} > 114$ dBm ($SNR \simeq 22$ dB after compression)
4. the cross-correlation brings the signal out of the noise: a spectral analysis (FFT) **cannot display** the GPS signal !