Radio logicielle 3/4 : corrélations pour la mesure de temps, application à la navigation par satellites

J.-M Friedt

FEMTO-ST/département temps-fréquence, Besançon

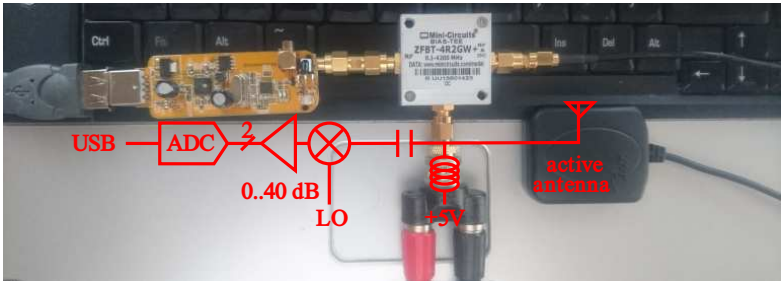
jmfriedt@femto-st.fr

transparents à `jmfriedt.free.fr`

16 janvier 2025

Plan de la présentation

1. Étalement de spectre pour permettre la mesure fine de temps de vol
2. Orthogonalité de la communication multiplexée sur code (CDMA)
3. Décodage de GPS : décallage Doppler et identification du satellite (PRN)
   - est-ce que les satellites sont visibles ? (autocorrélation)
   - quel est l'écart de fréquence grossier ? (mise au carré du signal)
   - cartes PRN-Doppler (quel satellite avec quel écart de fréquence) : *acquisition*
   - messages de navigation : *tracking*
4. Accès aux données IQ brutes : détection de leurrage, annulation de leurrage et annulation de brouillage (CRPA)



Récepteur DVB-T comme SDR générique (R820T2) pour la réception de signaux GNSS (antenna active avec T de polarisation)

Principe de la navigation par satellite

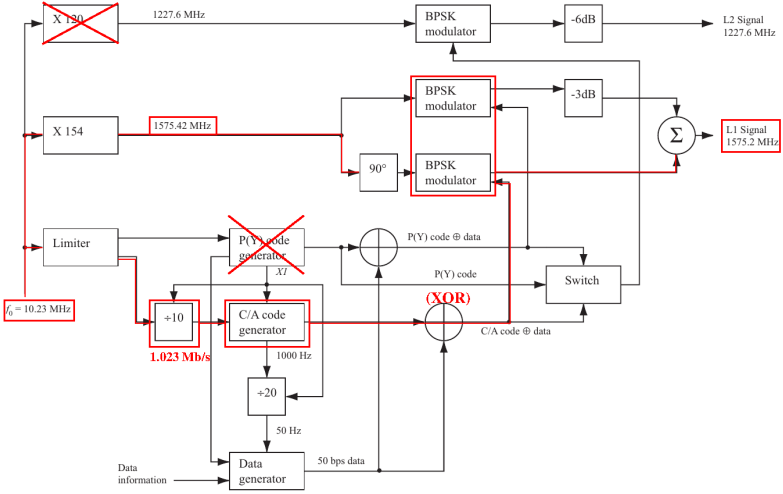
- Navigation par signaux satellitaires : constellations de satellites en orbite intermédiaire ($\simeq$ 20000 km) embarquant des horloges atomiques pour communiquer des signaux horaires
- Positionnement par trilatération comme solution de Position, Vitesse et Temps (PVT) : 4 satellites au moins nécessaires
- **acquisition** (quel satellite est visible) suivi de *tracking* (boucles à verrouillage de retard et de phase pour suivre les signaux des satellites)
- Messages de navigation incluent les éphémérides des satellites et informations sur leurs horloges

SDR donne accès au niveau le plus bas du signal, seule étape permettant de garantir **l'intégrité du signal** [1]

1. https ://www.defense.gouv.fr/aid/actualites/defi-developper-solutions-innovantes-traitements-antibrouillage-radionavigation

Décoder GPS

Principe du signal GPS [2] :



- la porteuse est générée par une horloge atomique(1575,42 MHz) ...
- ... modulée en phase à 1,023 MHz avec une séquence unique à chaque satellite ...
- ... et encore une fois modulée par le message de navigation (50 bps)

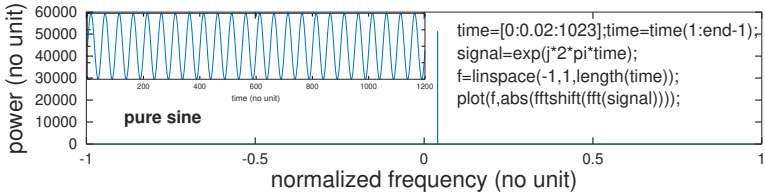
2. K. Borre *et al.*, *A Software-Defined GPS and Galileo Receiver – A Single-Frequency Approach*, Birkhäuser Boston, 2007

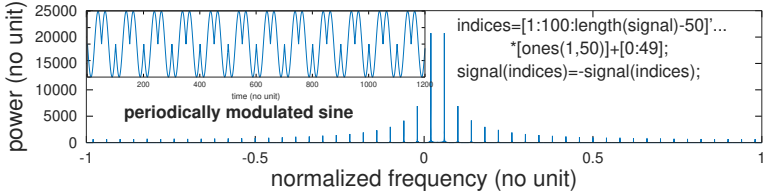
Étalement de spectre

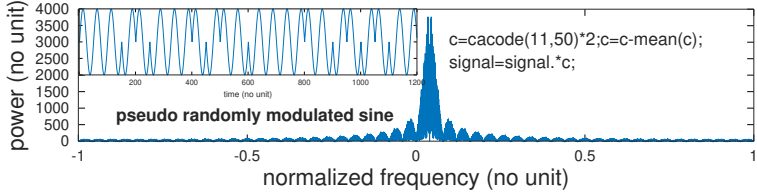
La fréquence porteuse et la bande passante sont deux grandeurs sans relations qui peuvent être manipulées indépendamment pour atteindre un objectif

Modulation de phase binaire : $\varphi \in [0; \pi]$ pour l'étalement de spectre

Premier null du spectre au taux de communication binaire





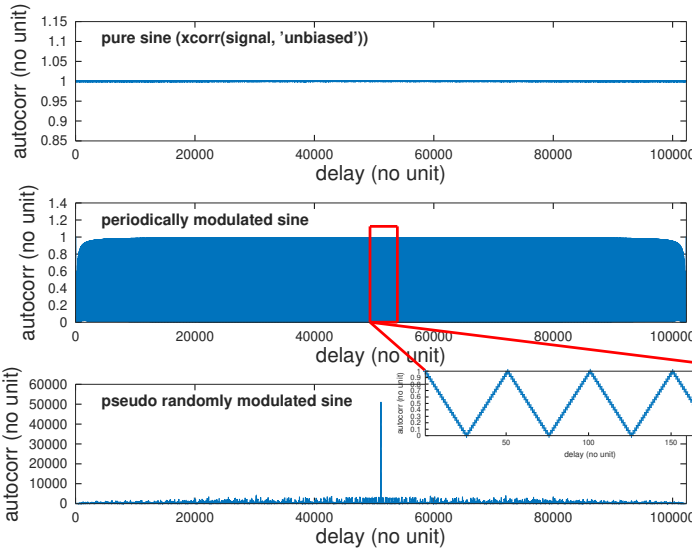


Étalement de spectre

La fréquence porteuse et la bande passante sont deux grandeurs sans relations qui peuvent être manipulées indépendamment pour atteindre un objectif

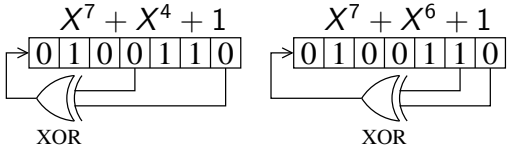
Modulation de phase binaire : $\varphi \in [0; \pi]$ pour l'étalement de spectre

Premier null du spectre au taux de communication binaire



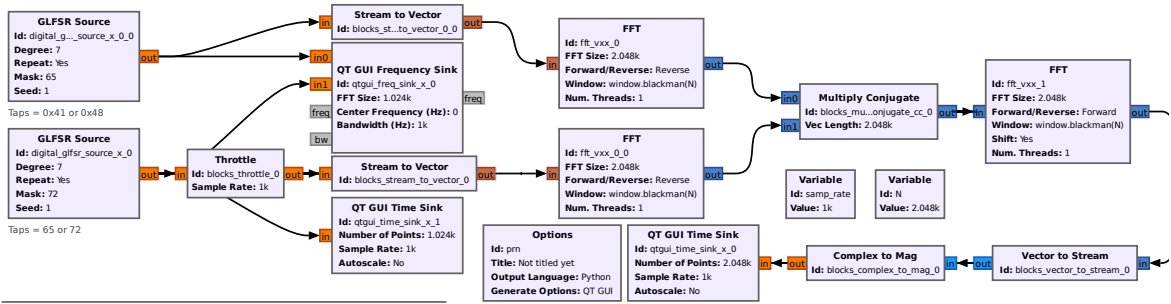
Mise en pratique : PRN sous GNU Radio

Registre à décalage linéaire de Galois (G-LFSR)



Registre à décalage de longueur $N \Rightarrow$ répétition tous les $2^N - 1$

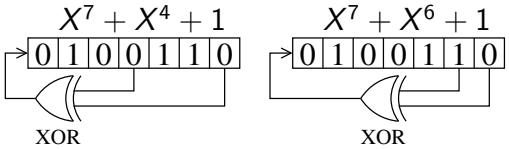
- Expression polynomiale définit la position des connexions (*taps*) des XOR alimentant la rétroaction
- 18 positions possibles des *taps*[3]
- Ici $N = 7 \Rightarrow 2^N - 1 = 127$



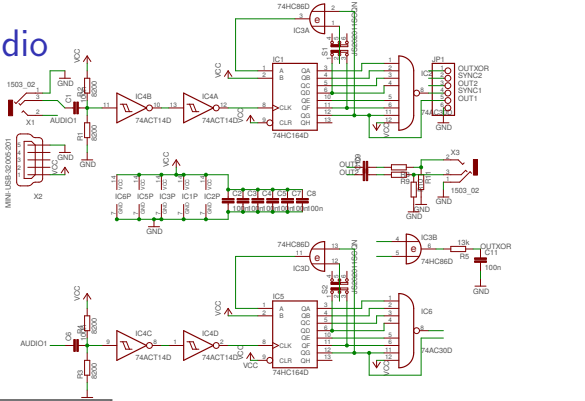
3. https://users.ece.cmu.edu/~koopman/lfsr/index.html

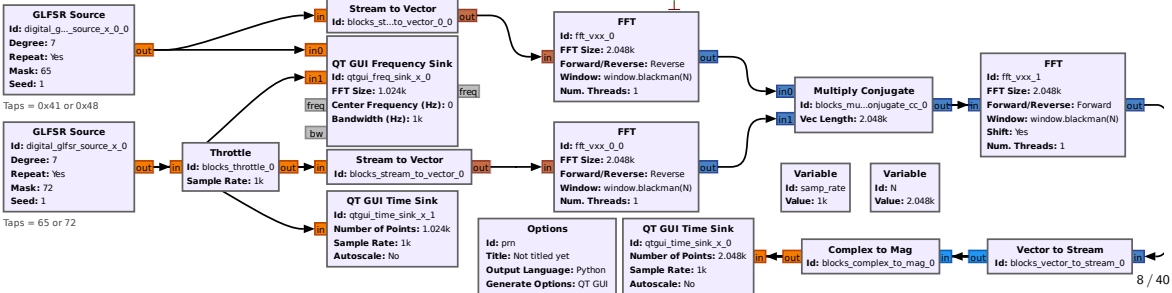
Mise en pratique : PRN sous GNU Radio

Registre à décalage linéaire de Galois (G-LFSR)

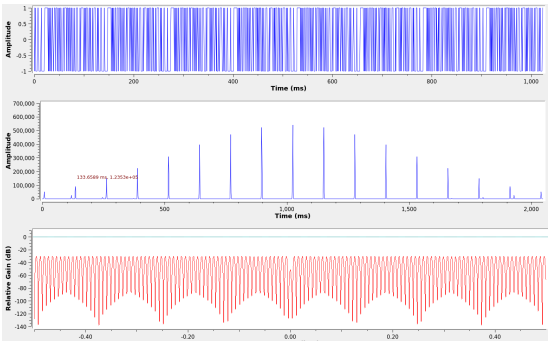


Registre à décalage de longueur $N \Rightarrow$ répétition tous les $2^N - 1$

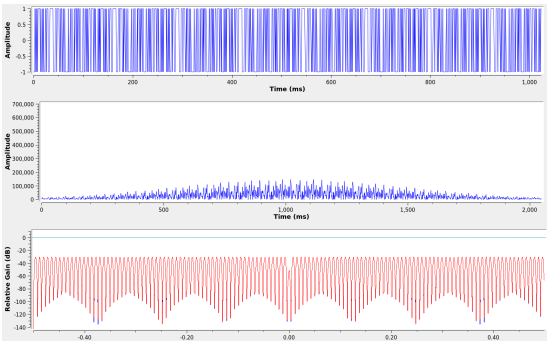




Mise en pratique : PRN sous GNU Radio

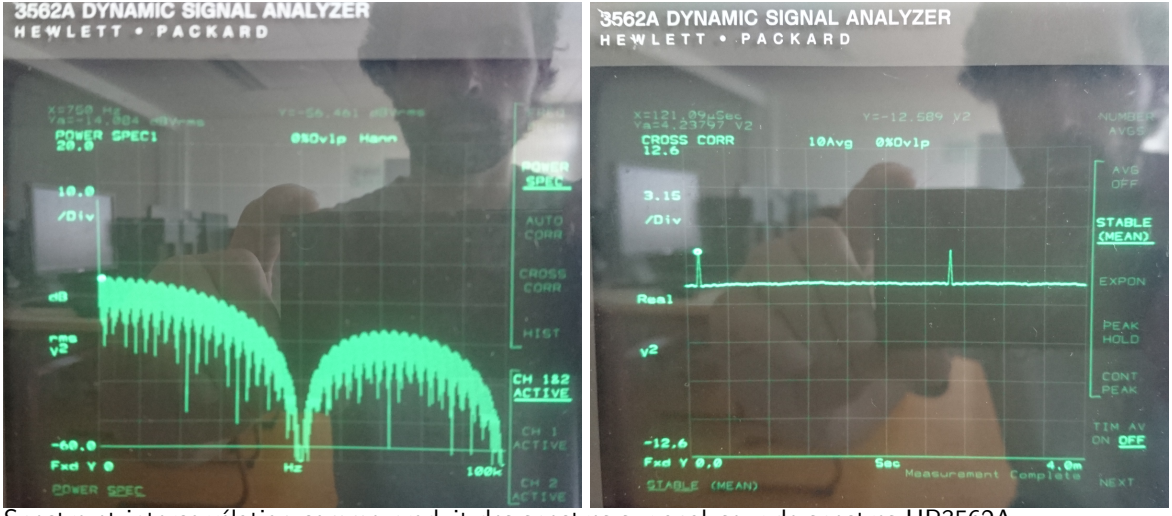


Mêmes PRNs



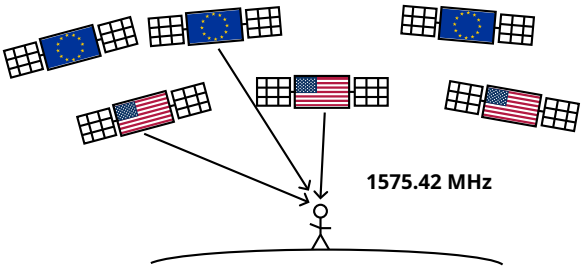
PRNs différents

Mise en pratique (analogique)

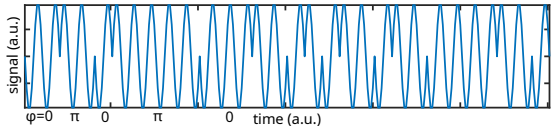


Spectre et intercorrélation comme produit des spectres sur analyseur de spectres HP3562A

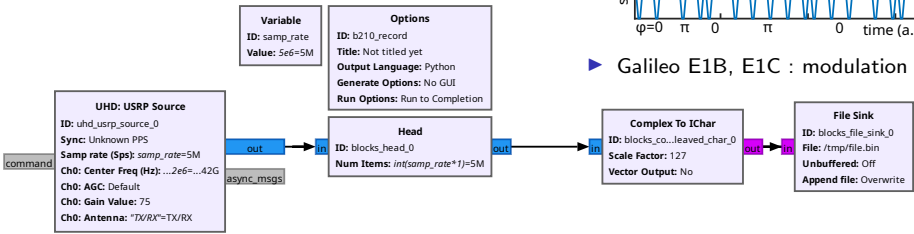
Communication multiplexée en code (CDMA) [3]



- CDMA : chaque bit émis est porté par une séquence pseudo-aléatoire (PRN) après XOR
- Inter-corrélation $\text{xcorr}(x,p)(\tau) = \int x(t) \cdot p^*(t+\tau)dt$
- Linéarité :
  $\text{xcorr}(ax+by,p) = a \cdot \text{xcorr}(x,p) + b \cdot \text{xcorr}(y,p)$
- Dans le domaine de Fourier :
  $\text{FFT}(\text{xcorr}(x,p)) = \text{FFT}(x) \cdot \text{FFT}^*(p)$
- Orthogonalité des codes : $\text{xcorr}(c_i,c_j)=\delta_{i,j}$
- GPS L1 C/A : séquence de Gold modulée en BPSK



- Galileo E1B, E1C : modulation BOC avec sous porteuse



Signal GNSS : GPS L1 C/A et Galileo E1B/E1C

- Modulation BPSK des séquences pseudo-aléatoires de Gold [4]

```
load GNSS-matlab/prn_codes/codes_L1CA.mat;
code=interpolated(codes_L1CA(:,m),fs/1.023e6);
% 0/pi phase at baseband
```

- Modulation BOC des séquences pseudo-aléatoires

```
load GNSS-matlab/prn_codes/codes_E1B.mat
Rsa=1.023e6;
Rsb=6.138e6;
m=1;
code=interpolated(codes_E1B(:,m),fs/1.023e6);
temps=[0:length(code)-1]'/fs;
sce1a=sqrt(10/11)*((sin(2*pi*temps*Rsa)>0)*2-1);
sce1b=sqrt(1/11)*((sin(2*pi*temps*Rsb)>0)*2-1);
signal=(sce1a+sce1b).*code);
```

Voir "Galileo open service signal-in-space interface control document (OS SIS ICD)" à https://www.gsc-europa.eu/sites/default/files/sites/all/files/Galileo_OS_SIS_ICD_v2.1.pdf (remerciement C. Plantard, ESTEC)

. Toutes les séquences PRN à https://github.com/danipascual/GNSS-matlab

E1 Signal

Figure 7 provides a generic view of the E1 CBOC signal generation.

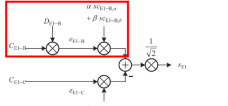


Figure 7: Modulation Scheme for the E1 CBOC Signal

The E1 CBOC signal components are generated as follows:

- $e_{E1\text{-}B}$ from the I/NAV navigation data stream $D_{E1\text{-}B}$ and the ranging code $C_{E1\text{-}B}$ then modulated with the sub-carriers $sc_{E1\text{-}B,a}$ and $sc_{E1\text{-}B,b}$

The E1-B/C composite signal is then generated according to equation Eq. 11 below, with the binary signal components $e_{E1\text{-}B}(t)$ and $e_{E1\text{-}C}(t)$. Note that as for E6, both pilot and data components are modulated onto the same carrier component, with a power sharing of 50 percent.

$$s_{E1}(t) = \frac{1}{\sqrt{2}}\left[e_{E1-B}(t)\left(\alpha\, sc_{E1-B,a}(t) + \beta\, sc_{E1-B,b}(t)\right) - e_{E1-C}(t)\left(\alpha\, sc_{E1-C,a}(t) - \beta\, sc_{E1-C,b}(t)\right)\right]$$

$$\text{with } sc_X(t) = \text{sgn}\left(\sin\left(2\pi\, R_{s,X}\, t\right)\right) \qquad \text{Eq. 11}$$

The parameters α and β are chosen such that the combined power of the $sc_{E1\text{-}B,b}$ and the $sc_{E1\text{-}C,b}$ sub carrier components equals 1/11 of the total power of $e_{E1\text{-}B}$ plus $e_{E1\text{-}C}$, before application of any bandwidth limitation. This yields:

$$e_{E1-B}(t) = \sum_{i=-\infty}^{\infty}\left[C_{E1-B,[i]_{L_{E1-B}}}\, D_{E1-B,[i]_{DC_{E1-B}}}\, \text{rect}_{T_{C,E1-B}}(t - i\,T_{C,E1-B})\right]$$

$$e_{E1-C}(t) = \sum_{i=-\infty}^{\infty}\left[C_{E1-C,[i]_{L_{E1-C}}}\, \text{rect}_{T_{C,E1-C}}(t - i\,T_{C,E1-C})\right] \qquad \text{Eq. 10}$$

Galileo satellites transmit ranging signals for the E1 signal with the chip rates and sub- carrier rates defined in the following Table 9.

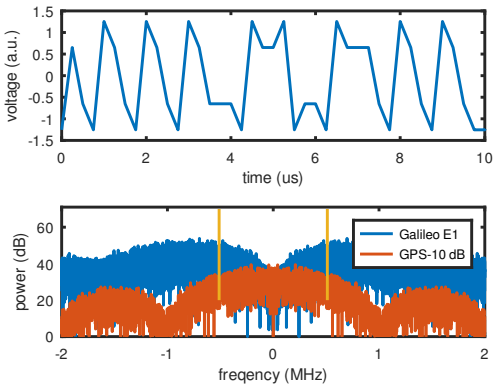
Table 9: E1 CBOC Chip Rates and Sub-carrier Rates

Component (Parameter Y)	Sub-carrier Type	Sub-carrier Rate		Ranging Code Chip-Rate $R_{C,E1\text{-}Y}$ (Mcps)
		$R_{S,E1\text{-}Y,a}$ (MHz)	$R_{S,E1\text{-}Y,b}$ (MHz)	
B	CBOC, in-phase	1.023	6.138	1.023
C	CBOC, anti-phase	1.023	6.138	1.023

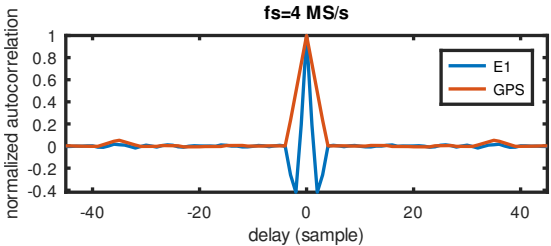
The navigation data message stream, after channel encoding, is transmitted with the symbol rate as stated in Table 10.

Signal Galileo : BOC pour ne pas perturber le lobe principal de BPSK

Haut : signal Galileo E1
Bottom : red=GPS L1 C/A spectrum (1.023 Mchip/s), blue=Galileo E1 spectrum



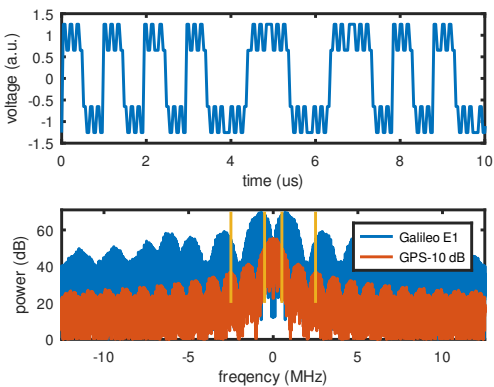
BPSK à X MS/s présente un null à $\pm X$ MHz



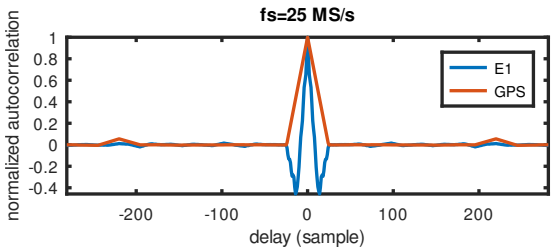
Fonction d'auto-corrélation (corrélation entre signal émis $p(t)$ et reçu $p(t) + n(t)$), rouge=BPSK PRN, bleu=BOC (plus fin mais lobes latéraux)

Signal Galileo : BOC pour ne pas perturber le lobe principal de BPSK

Haut : signal Galileo E1
Bottom : red=GPS L1 C/A spectrum (1.023 Mchip/s), blue=Galileo E1 spectrum



BPSK à X MS/s présente un null à $\pm X$ MHz

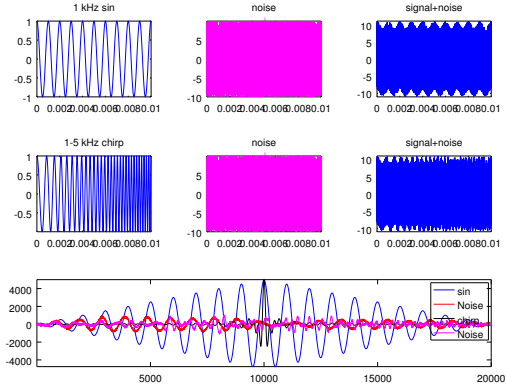


Fonction d'auto-corrélation (corrélation entre signal émis $p(t)$ et reçu $p(t) + n(t)$), rouge=BPSK PRN, bleu=BOC (plus fin mais lobes latéraux)

Compression d'impulsion (*Pulse Compression Ratio* – PCR)

- Plus le code est long (T), plus longue est l'intégrale pendant laquelle l'intercorrélation accumule de l'énergie et **moyenne le bruit**,
- mais une impulsion longue **réduit la résolution temporelle** $\Rightarrow$ large pic d'inter-corrélation
- variation du code dans le temps $\Rightarrow$ bande passante B importante $\Rightarrow$ largeur du pic de corrélation $1/B$
- Rappel : GPS est conçu pour **la datation de signaux** avec mieux que la durée d'un "chip".

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

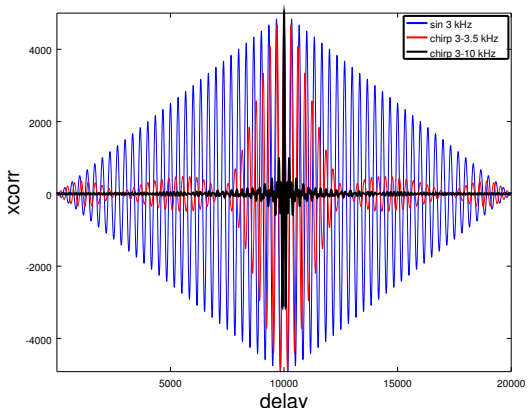



```
time=[0:1e-6:1e-2]; %samp. rate=1 us

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-');
```

Compression d'impulsion (*Pulse Compression Ratio* – PCR)

- Plus le code est long (T), plus longue est l'intégrale pendant laquelle l'intercorrélation accumule de l'énergie et **moyenne le bruit**,
- mais une impulsion longue **réduit la résolution temporelle** $\Rightarrow$ large pic d'inter-corrélation
- variation du code dans le temps $\Rightarrow$ bande passante B importante $\Rightarrow$ largeur du pic de corrélation $1/B$
- Rappel : GPS est conçu pour **la datation de signaux** avec mieux que la durée d'un "chip".

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



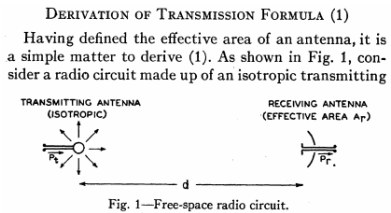

```
time=[0:1e-6:1e-2]; %samp. rate=1 us

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-');
```

Bilan de liaison et conséquence du PCR

- Un satellite GNSS émet 50 W (47 dBm) sur des antennes de gain 13 dBi à 20000 km
- Conservation de l'énergie (Friis [5]) : $\mathrm{FSPL} = 20\log_{10}(d^2) + 20\log_{10}(f^2) - \underbrace{147.55}_{20\log_{10}(c/4\pi)} = 182$ dB
- antenne de réception active avec 35 dB de gain
- plancher de bruit thermique$=-174$ dBm/Hz$+10\log_{10}(5\cdot 10^6) = -107$ dBm
- GNSS est $(\underbrace{47}_{TX_{pow}} + \underbrace{13}_{TX_{gain}} + \underbrace{35}_{RX_{gain}} - \underbrace{182}_{FSPL}) + 107 = 20$ dB **sous le bruit thermique**
- nécessité de moyenner ... tout en conservant la capacité de dater
- séquence pseudo-aléatoire de N-bits de long améliore le rapport signal à bruit de $B \times T = N$

$$\boxed{\Rightarrow PCR = N = 30 \text{ dB de gain pour GPS L1 C/A } (N = 1023)}$$

$\Rightarrow$ le SNR après corrélation par un PRN **connu** croît à 10 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.

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

Avons nous un signal ?

Analyse sans code (*codeless*) : le signal reçu a subi un décallage Doppler δf et est modulé en phase avec le motif $\varphi(t)$:

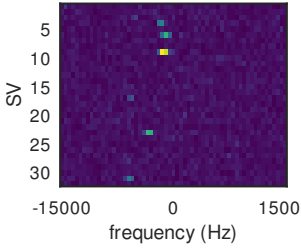
$$s(t) = \exp\left(j2\pi\delta f \cdot t + j\varphi(t)\right) + \underbrace{n(t)}_{noise}$$

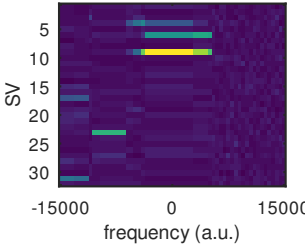
- Autocorrélation : $\int s(t)s^*(t+\tau)dt = \int \exp(\cancel{j2\pi\delta f \cdot t} + j\varphi(t)) \cdot \exp(\cancel{-j2\pi\delta f \cdot (t+\tau)} - j\varphi(t+\tau))dt$ devient $\exp(j2\pi\delta f\tau) \int \exp(j\varphi)\exp(-j\varphi(t+\tau))dt = \underbrace{\exp(j2\pi\delta f\tau)}_{|\cdot|=1} xcorr(\varphi,\varphi)$

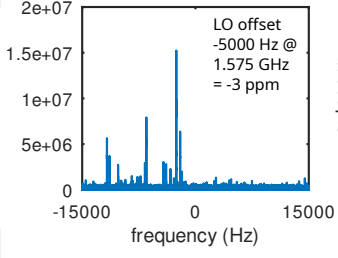
```
f=fopen(myfile); fs=1.023e6; freq0=[-1.5e4:500:1.5e4];
d=fread(f,fs*4,'int8'); d=d(1:2:end)+j*d(2:2:end);fclose(f)→
      ↪;
plot([-length(d)+1:length(d)-1],abs(xcorr(d,d)))
```

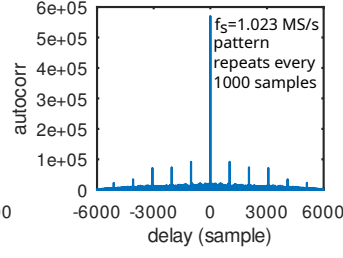
- Mettre au carré I+jQ :
  $s(t) = \exp(j2\pi\delta f \cdot t + j\underbrace{\varphi}_{\in[0;\pi]})$
  $\Rightarrow s^2(t) = \exp(j2\pi \cdot 2\delta f \cdot t + j\underbrace{\cancel{2\varphi}}_{0[2\pi]})$
  $s^2(t) = \exp(j2\pi 2\delta f \cdot t)$ porteuse pure au double de la fréquence **mais** bruit au carré

```
f=linspace(-fs/2,fs/2-fs/length(d),length(d));
p=find((f>min(freq0))&(f<max(freq0))); f=f(p);
df=abs(fftshift(fft(d.^2))); df=df(p); plot(f,df)
```



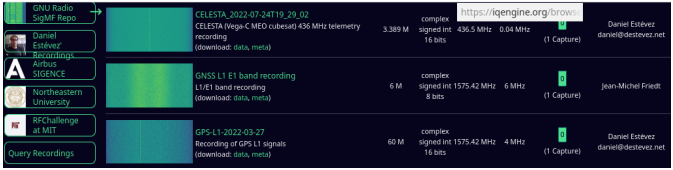






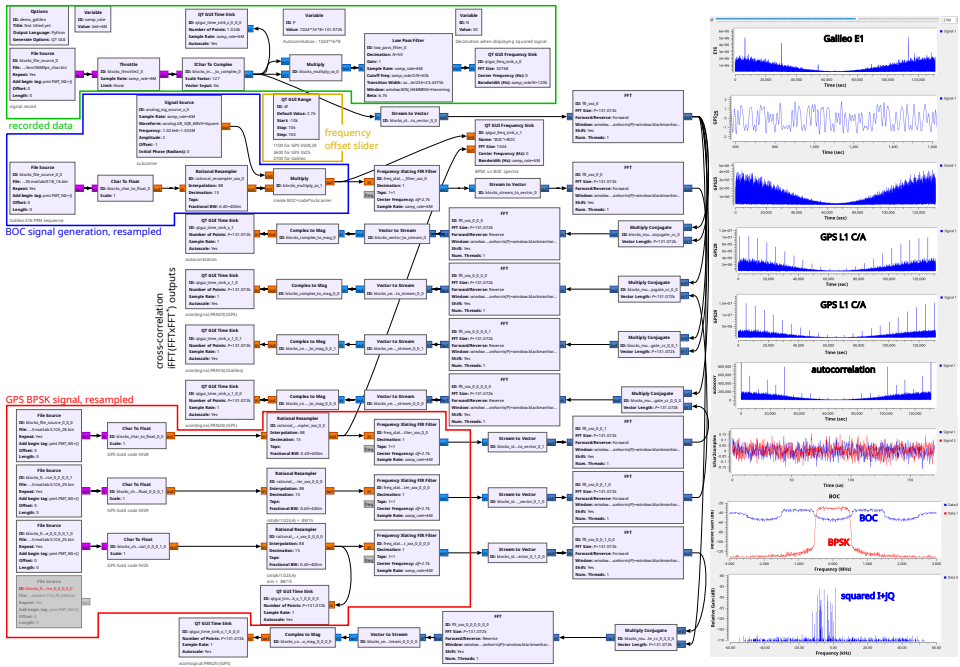
Comment un signal a-t-il été stocké ? sigMF

- Enregistrements de fichiers **binaires** (stockage efficace) mais quelle organisation des échantillons ? Interlacés ? Entiers ou flottants ? réels ou complexes ? fréquence d'échantillonnage ? Boutisme (*endianness*) ?
- SigMF méta format : `https://github.com/sigmf/SigMF`
- Description détaillée à `https://sigmf.org/index.html`
- Chaque enregistrement `sigmf-data` est associé à un fichier de format lisible `sigmf-meta`



- Voir données à `iqengine.org` et `http://jmfriedt.free.fr/fosdem_galileo.tar.gz`

```
{
 "global": {
  "antenna:gain": 35,
  "antenna:type": "none",
  "core:version": "1.0.0",
  "core:datatype": "ci8",
  "core:description": "L1/E1 band recording",
  "core:sample_rate": 6E6,
  "core:author": "Jean-Michel Friedt",
  "core:recorder": "GNU Radio",
  "core:hw": "Ettus Research B210",
  "core:license": "CC BY-SA"
  },
  "captures": [
    {
     "core:sample_start": 0,
     "core:frequency": 1575.42E6
    }
  ],
  "annotations": []
}
```



Haut en bas : inter-corrélation du motif Galileo

interpolation BPSK

intercorrélation PRN GPS (mauvais décallage de fréquence)

intercorrélation GPS PRN

intercorrélation GPS PRN

auto-corrélation

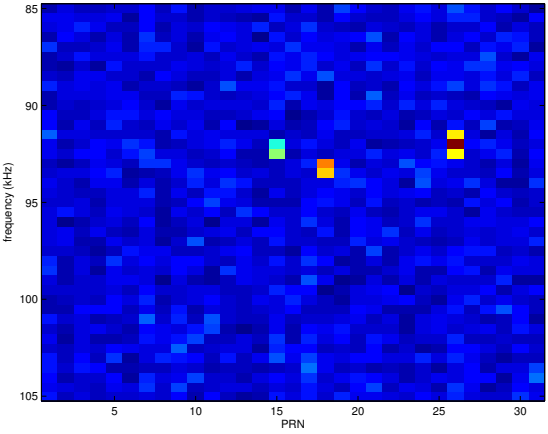
signal (± 8 ou 3 bits)

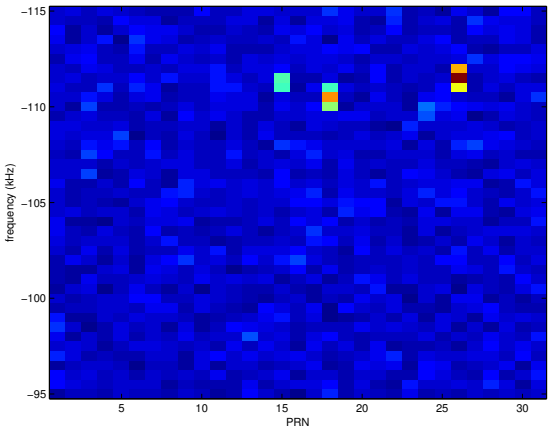
spectres BPSK v.s BOC

mise au carré (porteuses)

CDMA : acquisition GPS

De la nécessité d'oscillateurs exacts :





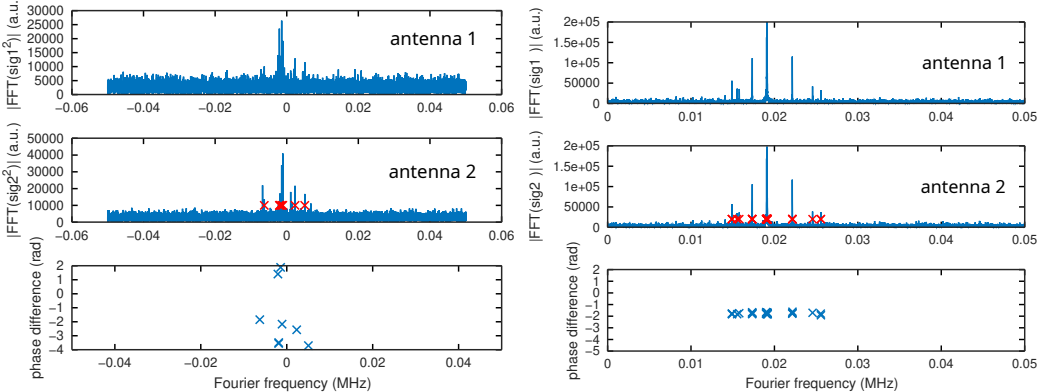
E4000 DVB-T
biais $+59$ ppm$= +91$ kHz à 1575,42 MHz

R820T DVB-T
biais -68 ppm$= -107$ kHz à 1575,42 MHz

Au lieu de rechercher une gamme ± 5 kHz (Doppler) avec un pas de 500 Hz, il faut explorer ± 150 kHz $\Rightarrow$ temps de calcul (bande de 20 kHz par pas de 500 Hz sur $2 \cdot 10^5$ échantillons : 302 secondes avec Matlab R2010, 342 secondes avec GNU/Octave 3.8.2, i.e. $\times 30$!)

Détection de leurrage GNSS

- Utilisation de la direction d'arrivée pour identifier une distribution incohérente
- Les satellites sont distribués sur des azimuth/élévations variables alors que la source unique de leurrage ne présente qu'une unique différence de phases entre antennes pour tous les satellites.
- Éviter de décoder en mettant le signal au carré et analyser la phase des porteuses pures résultantes



- P récepteurs peuvent annuler $P-1$ sources de leurrage/brouillage par ajustement de la position du null, mais dynamique limitée par nombre de bits d'ADC (6.02 dB/bit)

Réception en temps réel de GPS L1 avec gnss-sdr [6]

```
Tracking of GPS L1 C/A signal started on channel 0 for satellite GPS PRN 01 (Block IIF)
Current receiver time: 1 min 49 s
New GPS NAV message received in channel 9: subframe 1 from satellite GPS PRN 21 (Block IIR) with CN0=42 dB-Hz
New GPS NAV message received in channel 5: subframe 1 from satellite GPS PRN 02 (Block IIR) with CN0=43 dB-Hz
New GPS NAV message received in channel 6: subframe 1 from satellite GPS PRN 08 (Block IIF) with CN0=44 dB-Hz
New GPS NAV message received in channel 4: subframe 1 from satellite GPS PRN 32 (Block IIF) with CN0=43 dB-Hz
First position fix at 2024-Jul-26 09:31:48.120000 UTC is Lat = 47 [deg], Long = 6 [deg], Height= 3.8e+02 [m]
Current receiver time: 1 min 50 s
The RINEX Navigation file header has been updated with UTC and IONO info.
Position at 2024-Jul-26 09:31:49.000000 UTC using 4 observations is Lat = 47.251620 [deg], Long = 5.993221 [deg],
Height = 366.06 [m]
Velocity: East: 0.91 [m/s], North: 0.65 [m/s], Up = 3.82 [m/s]
Current receiver time: 1 min 51 s
Loss of lock in channel 11!
Tracking of GPS L1 C/A signal started on channel 11 for satellite GPS PRN 19 (Block IIR)
Position at 2024-Jul-26 09:31:49.989988 UTC using 4 observations is Lat = 47.251560 [deg], Long = 5.993090 [deg],
Height = 311.77 [m]
Velocity: East: -0.83 [m/s], North: -1.32 [m/s], Up = -2.92 [m/s]
```

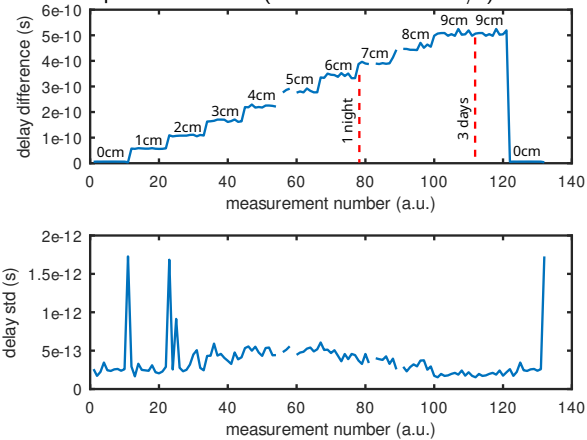
Séquences de la machine à états de GNSS-SDR

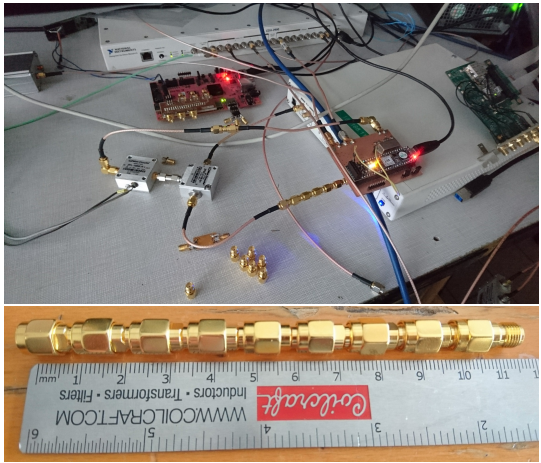
1. **Tracking** : un satellite a été associé à un canal de traitement, recherche en cours
2. **GPS L1 C/A tracking bit synchronization locked** : un signal est trouvé !
3. **New GPS NAV message received** : message de navigation, bientôt la solution PVT

6. film de la séquence de traitements à `https://www.youtube.com/watch?v=B5UcFnkbXIk`

Étalement de spectre pour la mesure fine de retards

- Ajustement parabolique du pic de corrélation
- Gain en résolution temporelle = SNR
- Bande passante 5 MHz (mesure SDR à 5 MS/s) ou 200 ns période d'échantillonnage



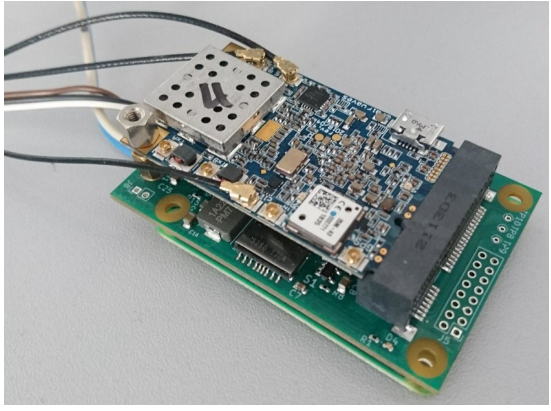


Mesure avec résolution sub-ps (1 cm=50 ps @ 20 cm/ns)

6. J.-M Friedt, *Time of flight measurement with sub-sampling period resolution using SDR* (SDRA2023) at https://www.youtube.com/watch?v=B_fs9fWPTWw

Conclusion : traitements sécurisés GNSS par SDR

- Grande vulnérabilité des signaux de navigation par satellite (brouillage, leurrage)
- SDR donne accès au plus bas niveau (physique) du signal, avant tout traitement irrémédiable de leurrage
- Études à l'intersection de la SDR, systèmes embarqués, HPC (FPGA) pour le traitement temps-réel
- Problème de bande passante : traiter E1+E5 nécessite deux récepteurs SDR [a]
- Recherche de solutions alternatives : satellites en orbites basses, émissions terrestres VLF, signaux d'opportunité : NASIO (ASTRID) – Navigation avec signaux d'opportunités (ONERA/dept Traitement de l'information et systèmes) [b]

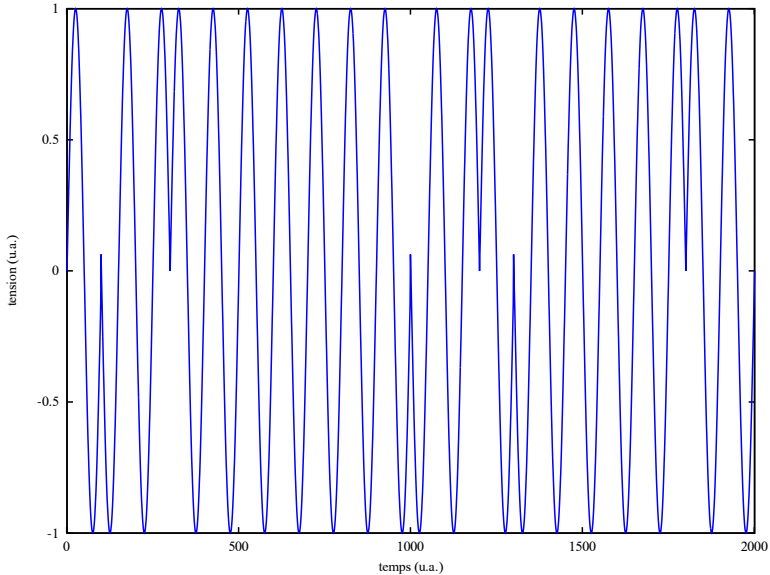


a. https://github.com/jmfriedt/max2771_fx2lp/

b. https://www.onera.fr/fr/actualites/onera-laureat-ou-co-laureat-de-21-financements-anr-en-2024

Phase modulation

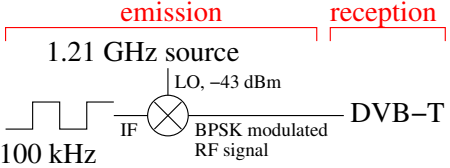
- PSK : Phase Shift Keying
- $\varphi = \arctan(Q/I)$: output of the I/Q demodulator
- local oscillator stability – constellation diagram
- GPS : BPSK (Binary Phase Shift Keying) – demonstration using a saturated mixer controlled by the bits to be transmitted

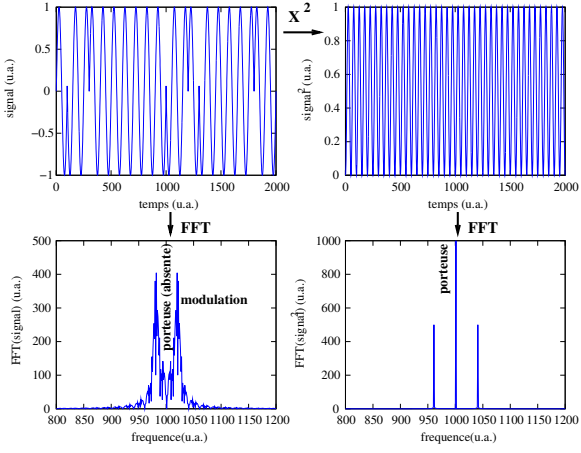


Phase demodulation

Requires accurate reproduction of the unmodulated carrier

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



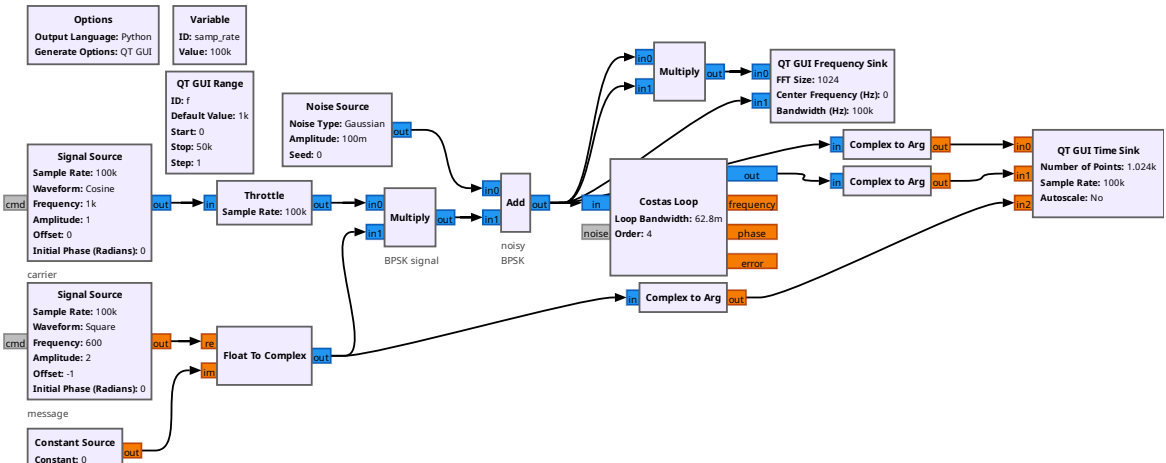


Carrier recovery by squaring BPSK

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

Phase demodulation

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

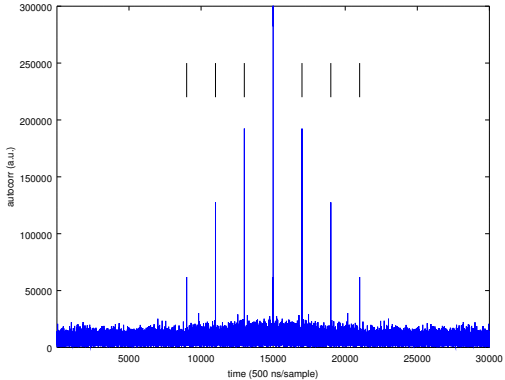


Carrier offset : $\Delta\omega$ + Modulation : $\varphi = [0; \pi] \rightarrow \sin(\underbrace{\Delta\omega \cdot t + \varphi}_{separate})$

CDMA code repetition interval

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 : **autocorrelation**

```
f=fopen('file.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
```

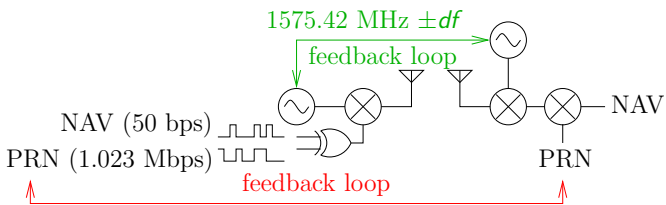


Repetition every 1 ms at 2 MS/s $\Rightarrow$ max(autocorr) every 2000 samples

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

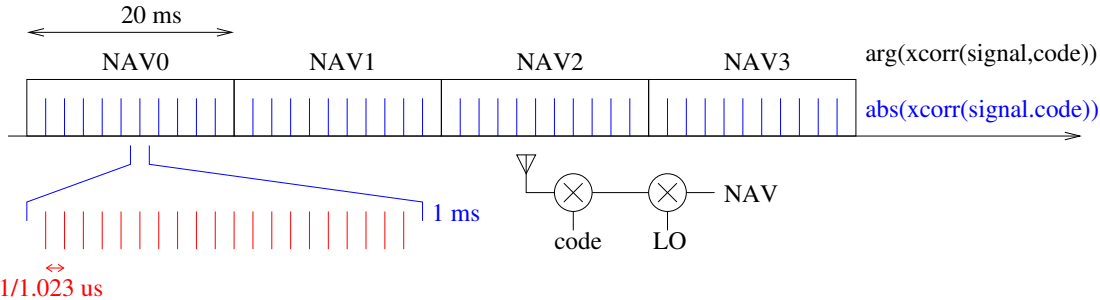
$\Rightarrow$ carrier recovery and code position (delay) recovery



CDMA : decoding GPS

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)

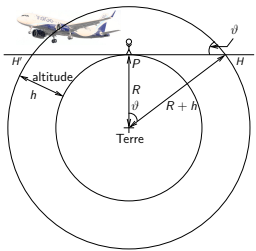


- when demodulating ; first eliminate the code, ...
- ... to identify and eliminate the carrier,
- in order to recover the message.

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

CDMA : decoding GPS

- 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 ?



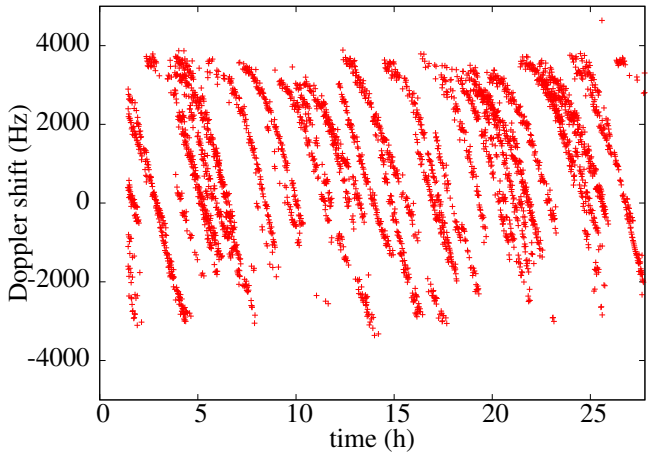
Doppler shift : $(R+r) = 20000+6400$ km in 12 h ($T^2/R^3 = \text{cst}$)
$\Rightarrow |\vec{v}| = 3830$ m/s
Since $\sin(\theta) = \frac{R}{r+R}$ or $R \simeq 6400$ km
$\Rightarrow |\vec{v}_{//}| = |\vec{v}| \cos(90-\theta) = |\vec{v}| \sin(\theta) = |\vec{v}| \frac{R}{r+R}$

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

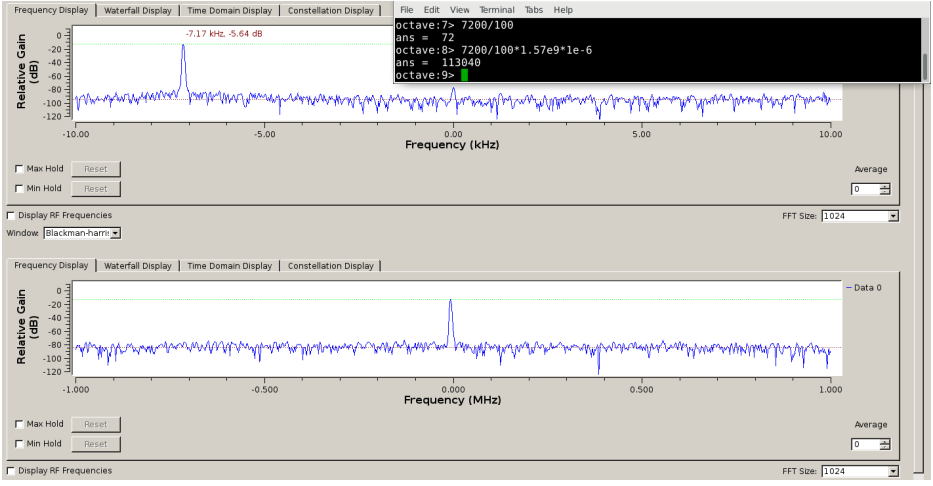
Record Doppler offset provided by `gnss-sdr` as a function of time for all visible satellites



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

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

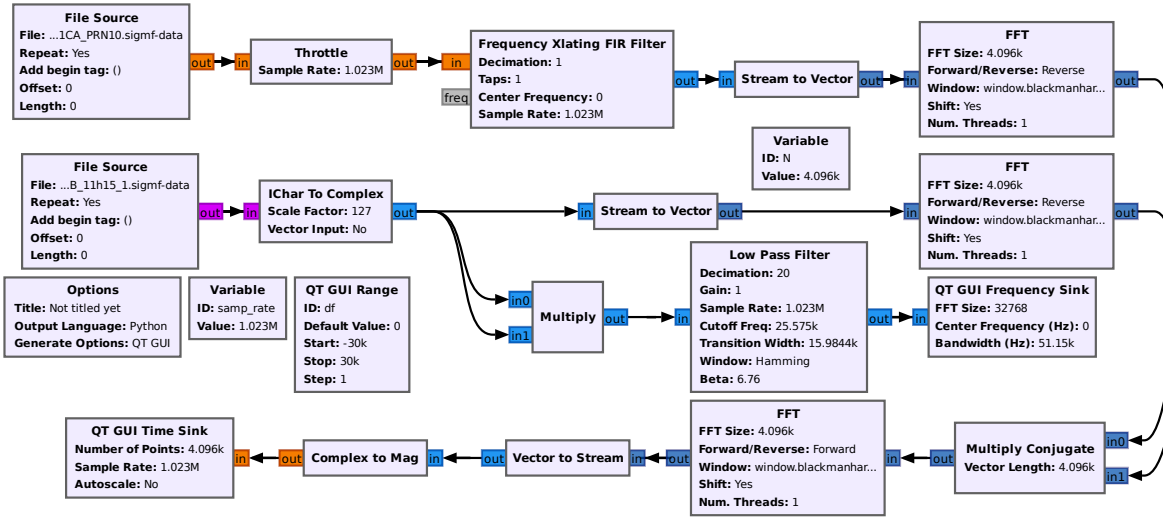
Recording a 100 MHz carrier referenced to a Cs clock :



-75 ppm offset or 120 kHz at 1.57 GHz

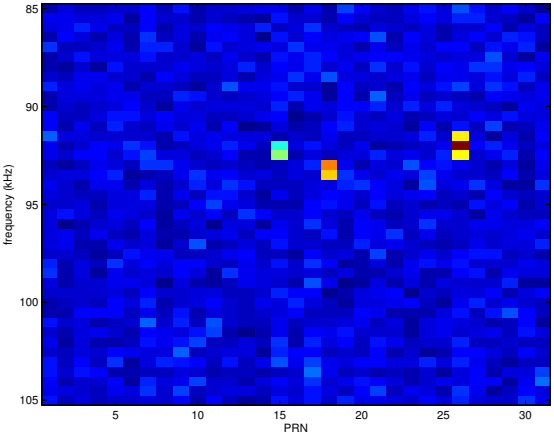
$\Rightarrow$ rather than **20** Doppler frequencies ($\pm$5 kHz with 500 Hz steps), probe $\geq$ **500** Doppler

Code-Doppler maps



CDMA : decoding GPS

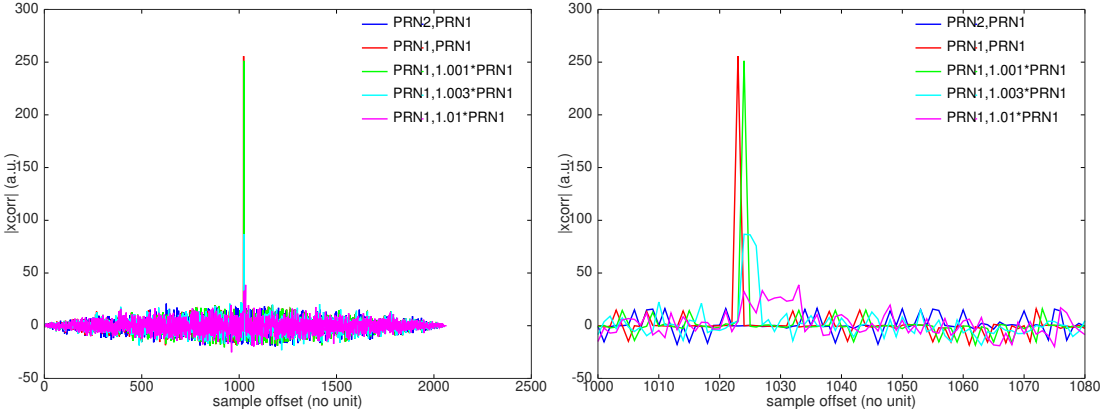
- CDMA basics : each useful bit (*navigation data*) is transmitted with its associated satellite identifier (SV PRN).
- All satellites transmit on the same carrier (1575.42 MHz), only their unique identifier allows differentiating each source.
- Each identifier is repeated every millisecond, NAV is at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



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

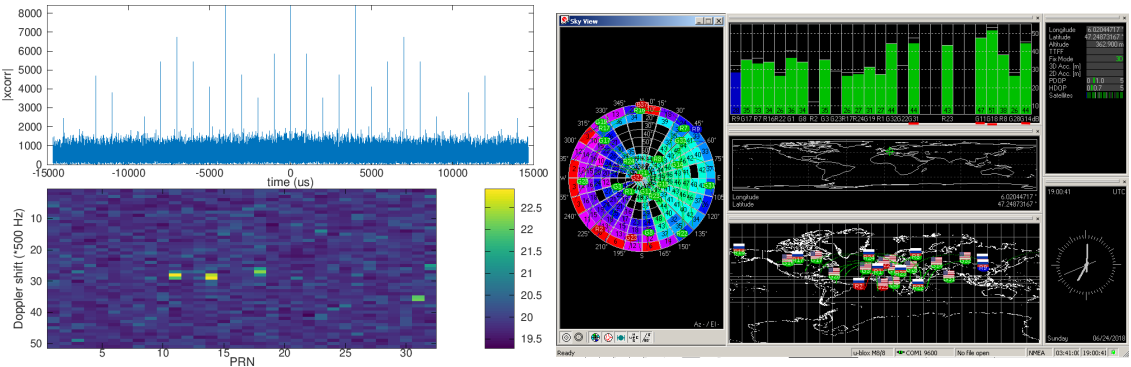
Doppler analysis frequency step

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

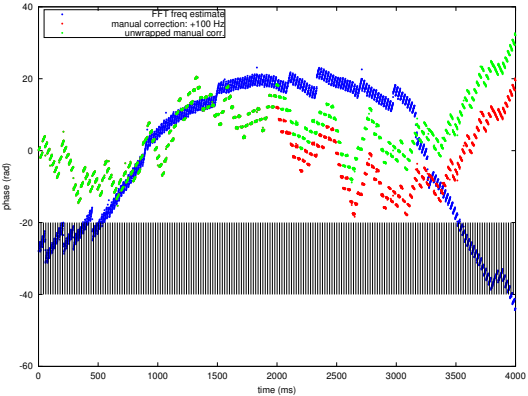
SDR v.s U-Blox

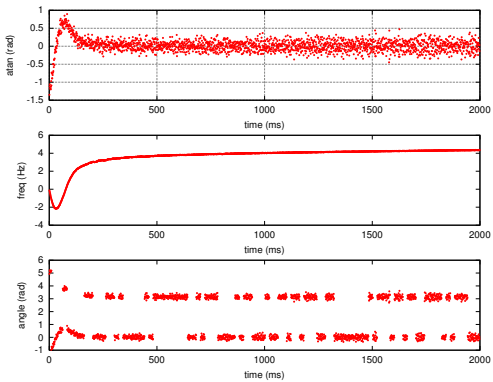


SV 11, 14, 18, 31 best visible with both receivers recording at the same time

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..