

Institut National des Sciences Appliquées
PTP Innovative Smart System

Rapport - Software Defined Radio

Schersach Baptiste - Arens Maxime

Toulouse, le 5 janvier 2020

1 Introduction

Ce rapport reprend notre étude de la radio définie par logiciel (Software-Defined Radio) et plus particulièrement du traitement logiciel post USRP (Universal Software Radio Peripheral). Premièrement nous avons observé à travers le calcul, le comportement d'un USRP comment il permet de démoduler, amplifier et récupérer l'information contenu dans un signal radio. Ensuite nous avons utilisé un logiciel de traitement de signaux radio pour d'abord analyser un signal broadcast FM puis un signal VOLMET sur AM.



FIGURE 1 – Photo d'un USRP

2 Présentation d'un USRP avec quelques calculs

2.1 Question 1

Les ondes radios sont des ondes électromagnétiques possédant donc une amplitude, une fréquence et une phase. Ces ondes sont complexes (composées d'une partie imaginaire et d'une partie réelle), afin de récupérer les informations l'USRP commence par bien séparer la partie imaginaire I de la partie réelle R. Pour cela l'USRP multiplie d'un côté l'onde complexe par un cosinus et de l'autre côté par un sinus. On suppose que le signal reçu et le même que le signal émis :

$$r_{RF}(t) = s_{RF}(t)$$

$$\tilde{r}_R(t) = [s_R * \cos(2\pi f_0 t) - s_I(t) * \sin(2\pi f_0 t)] \cos((2\pi f_0 t))$$

$$\tilde{r}_I(t) = -[s_R * \cos(2\pi f_0 t) - s_I(t) * \sin(2\pi f_0 t)] \sin((2\pi f_0 t))$$

$$\tilde{r}_R(t) = \frac{s_R(t)}{2} [\cos(2\pi(f_0 + f_c)t) + \cos(2\pi(f_0 - f_c)t)] - \frac{s_I(t)}{2} [\sin(2\pi(f_0 + f_c)t) + \sin(2\pi(f_0 - f_c)t)]$$

$$\tilde{r}_I(t) = \frac{s_I(t)}{2} [\cos(2\pi(f_0 - f_c)t) - \cos(2\pi(f_0 + f_c)t)] - \frac{s_R(t)}{2} [\sin(2\pi(f_0 + f_c)t) - \sin(2\pi(f_0 - f_c)t)]$$

si $f_c = f_0$ alors :

$$\tilde{r}_R(t) = \frac{s_R(t)}{2} [\cos(4\pi f_0 t) + 1] - \frac{s_I(t)}{2} \sin(4\pi f_0 t)$$

$$\tilde{r}_I(t) = \frac{s_I(t)}{2} [1 - \cos(4\pi f_0 t)] - \frac{s_R(t)}{2} [\sin(4\pi f_0 t)]$$

2.2 Question 2

Dans les calculs ci-dessus, f_0 représente la fréquence de la porteuse et f_c la fréquence de l'oscillateur de l'USRP. La porteuse est une fréquence qui module le signal et permet de l'envoyer sur de longue distance.

Afin de récupérer le signal, on fixe la fréquence de l'oscillateur à la fréquence de la porteuse : $f_c = f_0$. Cela s'appelle ramener le signal en bande de base. Grâce à une transformée de Fourier on passe les signaux en fréquentielle afin de pouvoir déterminer les caractéristiques du filtre nécessaire pour filtrer la partie du signal désiré : celle qu'on a ramenée en bande de base.

$$\tilde{R}_R(f) = S_R * \frac{1}{2} \delta(f) * [\delta(f) + \frac{1}{2} [\delta(f + 2f_0) + \delta(f - 2f_0)]] - S_I(f) * \frac{1}{2} \delta(f) * [\frac{j}{2} [\delta(f + 2f_0) - \delta(f - 2f_0)]]$$

$$\tilde{R}_I(f) = S_I * \frac{1}{2} \delta(f) * [\delta(f) - \frac{1}{2} [\delta(f + 2f_0) - \delta(f - 2f_0)]] - S_R(f) * \frac{1}{2} \delta(f) * [\frac{j}{2} [\delta(f + 2f_0) - \delta(f - 2f_0)]]$$

$$\tilde{R}_R(f) = \frac{1}{4}[2S_R(f) + S_R(f - 2f_0) + S_R(f + 2f_0) + jS_I(f - 2f_0) - jS_I(f + 2f_0)]$$

$$\tilde{R}_I(f) = \frac{1}{4}[2S_I(f) - S_I(f - 2f_0) - S_I(f + 2f_0) + jS_R(f - 2f_0) - jS_R(f + 2f_0)]$$

Les caractéristiques du filtre passe-bas désiré sont : Gain : $|H(f)| = 2$
Fréquence de coupure : $\frac{BW}{2} \leq f_{cut} \leq 2f_0 - \frac{BW}{2}$

2.3 Question 3

Afin d'avoir le signal en entier nous devons satisfaire $f_c > BW$ et pour éviter d'avoir une superposition avec l'autre bande centrée sur $2f_0$ on doit respecter $f_c < 2f_0$. Dans le cas d'une bande large, on a $f_0 < \frac{BW}{2}$, ce qui entraîne une superposition. C'est pour cela que nous faisons par la suite le choix de considérer le cas des bandes étroites.

Une autre raison empêchant l'utilisation de bandes larges c'est qu'on ne peut pas filtrer analogiquement dans le cas des bandes larges (hautes fréquences).

2.4 Question 4

On applique le théorème Shannon Nyquist pour trouver la fréquence d'échantillonnage :

$$\begin{aligned} F_e &\geq 2f_{max} \\ F_e &\geq 2 * \frac{BW}{2} \\ F_e &\geq BW \end{aligned}$$

La fréquence d'échantillonnage doit être plus grande que la bande passante.

2.5 Question 5

Si on filtre après l'ADC cela signifie qu'on va convertir des hautes fréquences ce qui coûte cher et augmente le risque d'erreurs dues au nombre de digits utilisés dans la conversion.

Même si théoriquement ça marcherait on peut dire qu'il est plus logique de filtrer avant le CAN ainsi on a moins de choses à convertir !

2.6 Question 6

A partir de $S_{RF}(t) = s_R(t)\cos(2\pi f_0 t) - s_I(t)\sin(2\pi f_0 t), \forall t \in R$ on obtient en fréquentiel :

$$S_{RF}(f) = \frac{S_R(f)}{2}[\delta(f - f_0) + \delta(f + f_0)] - \frac{S_I(f)}{2j}[\dots]$$

$$S_{RF}(f) = \frac{1}{2}[S_R(f - f_0) + S_R(f + f_0) + jS_I(f - f_0) - jS_I(f + f_0)]$$

L'expression du signal analytique et de son enveloppe sont :

$$S_a(f) = \begin{cases} 2S_{RF}(f), \forall f \geq 0, \\ 0, \forall f < 0 \end{cases}$$

$$\iff S_a(f) = S_R(f - f_0) + jS_I(f - f_0) = [S_R(f) + jS_I(f)] * \delta(f - f_0), \forall f > 0$$

$$s_A(t) = (s_R(t) + j s_I(t)) e^{j2\pi f_0 t}$$

$$S(f) = S_a(f + f_0) = S_R + jS_I(f)$$

$$s(t) = s_R(t) + j s_I(t)$$

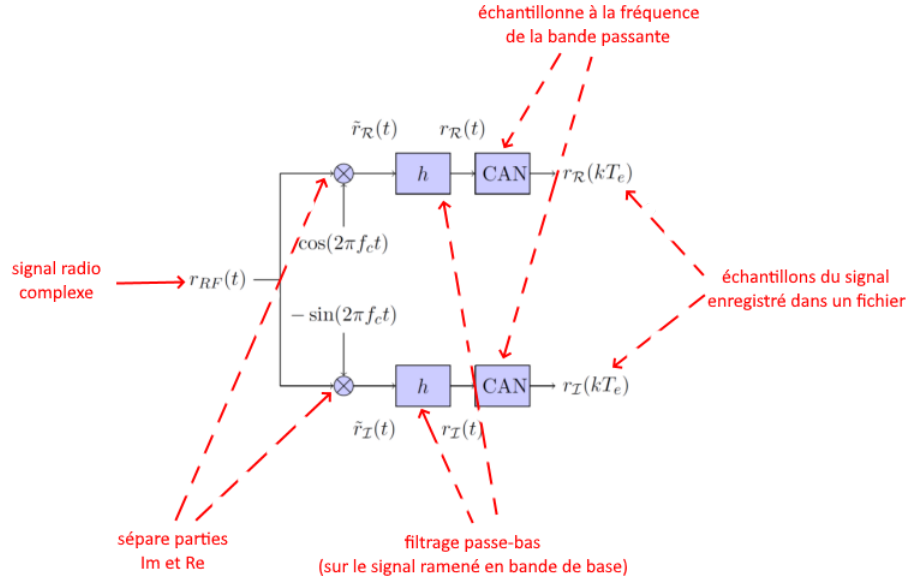


FIGURE 2 – Schéma récapitulatif du traitement par USRP

Il est intéressant de noter que les principes et les calculs sont les mêmes pour tout les USRP mais que ceux-là sont disponibles sur une vaste bande de prix. HackRF est notamment un émetteur/recepteur lowcost (environ 3 fois moins chers que ceux utilisés en cours à 1000 euros) L'intérêt du HackRF en plus de son

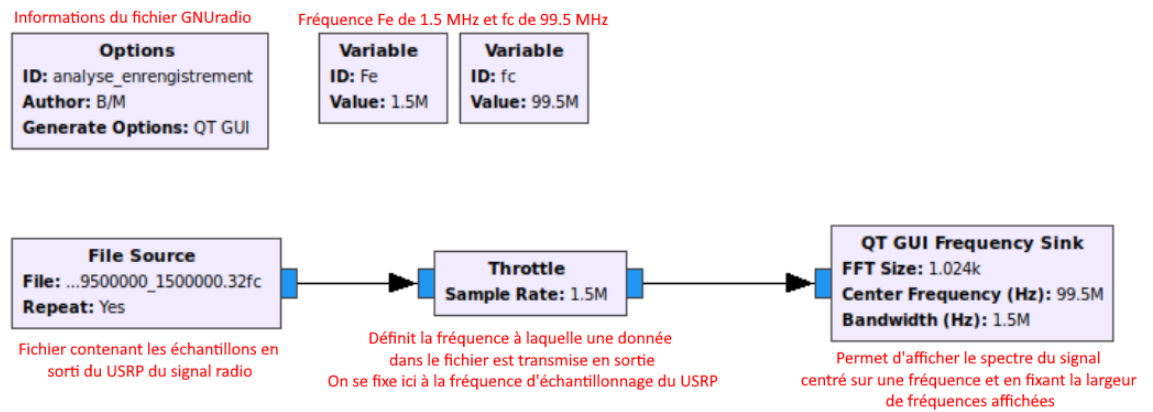
coût est qu'il peut hacker quasiment tout signaux radioélectrique à l'émission et reception (100 MHz et 5,4GHz). Il est donc possible d'émettre et de recevoir selon n'importe quel type de modulation, d'émission, de passer grâce à une commande logiciel d'émetteur à recepteur. Au rappel, un HackRF coûte environ 200 dollars, contre 1 000 euros pour un USRP. Certes les performances ne seront pas aussi hautes qu'avec un USRP mais largement assez pour le commun des mortels.



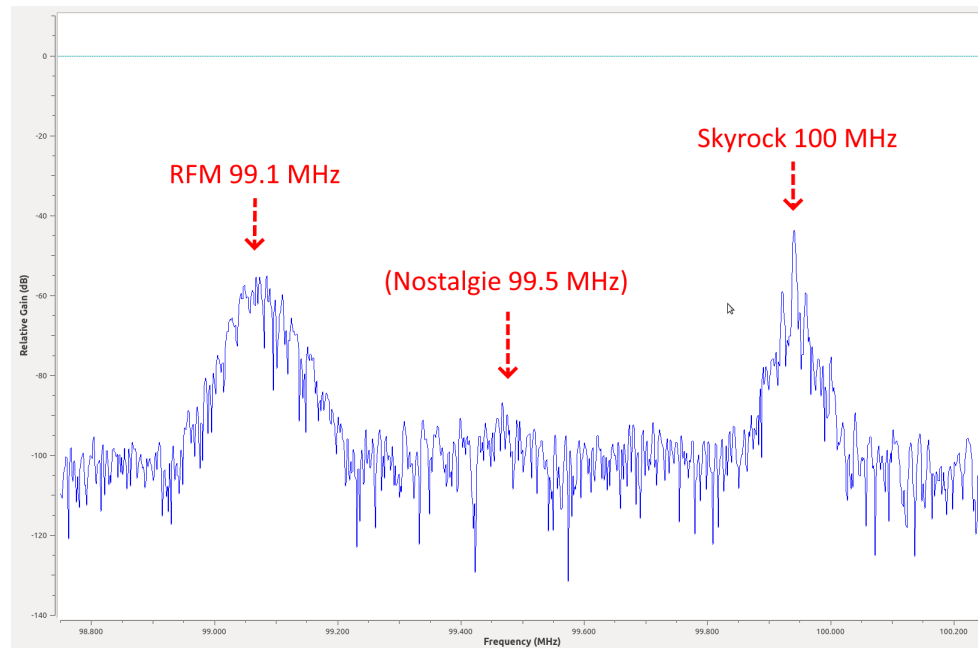
3 Réception d'un broadcast FM

3.1 Analyse fréquentielle de l'enregistrement

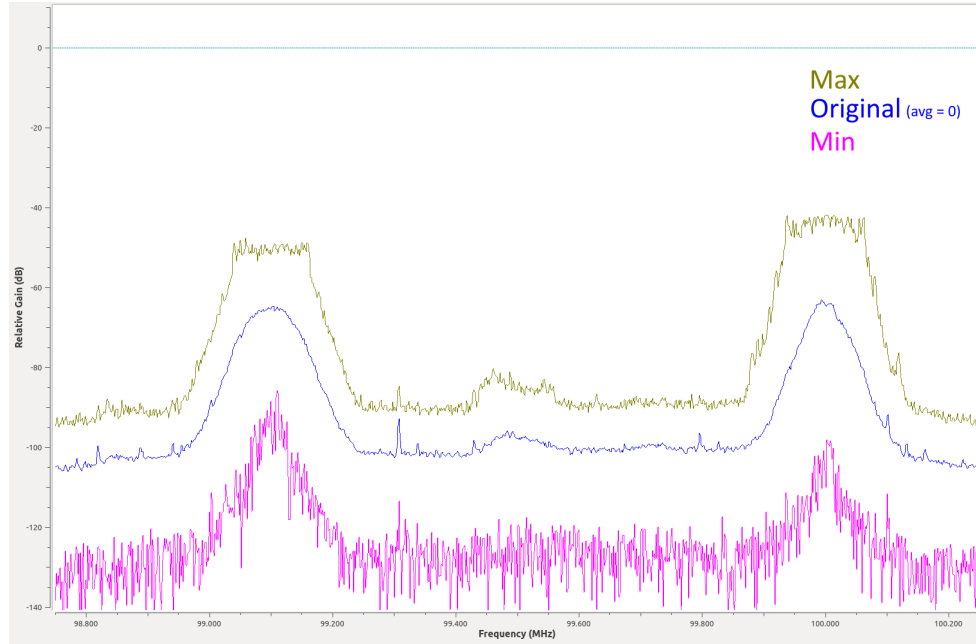
3.1.1 Question 7 et 8



3.1.2 Question 9



3.1.3 Question 10



Pour calculer la rapport signal bruit nous avons utilisé le Max du signal en kaki) de -49dB à -90 dB ça fait une différence de 41 dB ça fait environ un rapport signal sur bruit de 1/10 000 (pour RFM et Skyrock). On pense que c'est très suffisant pour démoduler. Pour Nostalgie le rapport est d'environ 1/30 la démodulation sera donc moins bonne.

3.1.4 Question 11

A partir de la figure ci-dessus on peut calculer la bande passante à -3dB (sur le trait bleu) :

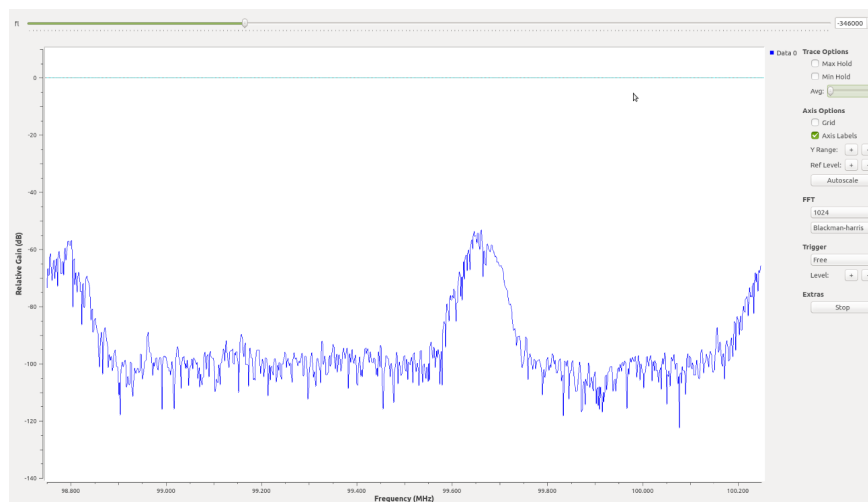
Pour RFM à -64.4dB-3dB on a 99.07 et 99.13 MHz c'est-à-dire une bande passante de 0.06 MHz.

Pour Skyrock à -63dB-3dB on a 99.98 MHz et 100.02MHz c'est-à-dire une bande passante de 0.04MHz.

On peut donc dire que la bande passante à -3 dB est autour de 50kHz, la plupart des autres groupes ont trouvées des valeurs supérieures à 100 kHz ce qui montre que l'hypothèse de départ de prendre 100kHz était optimiste (pas pour nous!).

3.2 Extraction de la chaine : transposition fréquentielle et filtrage passe-bas

3.2.1 Question 12



Avec GNUradio on a rajouté la possibilité de shifté fréquemment notre signal. On règle ce shift manuellement à travers le curseur qu'on peut voir sur l'image ci-dessus. Pour centrer les signaux radios il faut shifter respectivement de -500000 et +400000.

3.2.2 Question 13

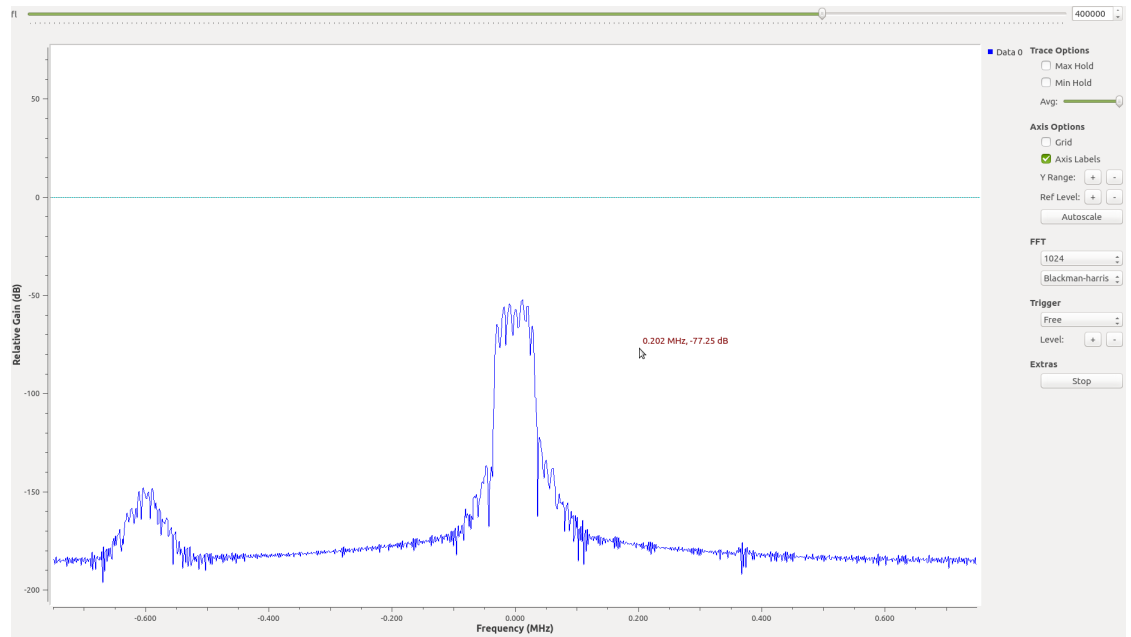
Lorsque l'on met un offset (ce que nous appelons shifter à la question précédente) égale à la fréquence d'échantillonnage on revient à notre signal de base (avec un offset de 0). Cela est dû au cosinus présent dans le signal, le cosinus est égal à un F_c prêt.

3.2.3 Question 14

Pour le filtre passe-bas on met une décimation de 6 (on prend une valeur sur 6, pour limiter le temps de calcul), une fréquence d'échantillonnage de 1.5MHz une fréquence de coupure de 30000 kHz et une largeur de transition de 1500 Hz.

On note que pour la suite, comme nous avons décimer le signal, il faut adapter en paramètre des prochains composants la fréquence d'échantillonnage (ici la diviser par 6 donc 250 kHz).

On obtient :



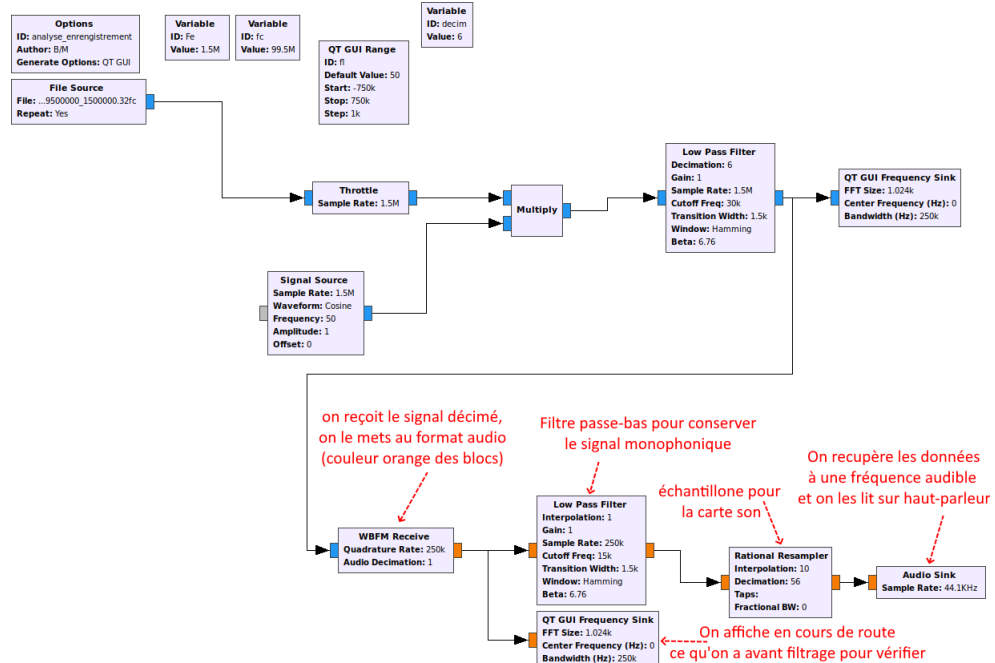
3.3 Fréquence de démodulation et restitution du signal

3.3.1 Question 15

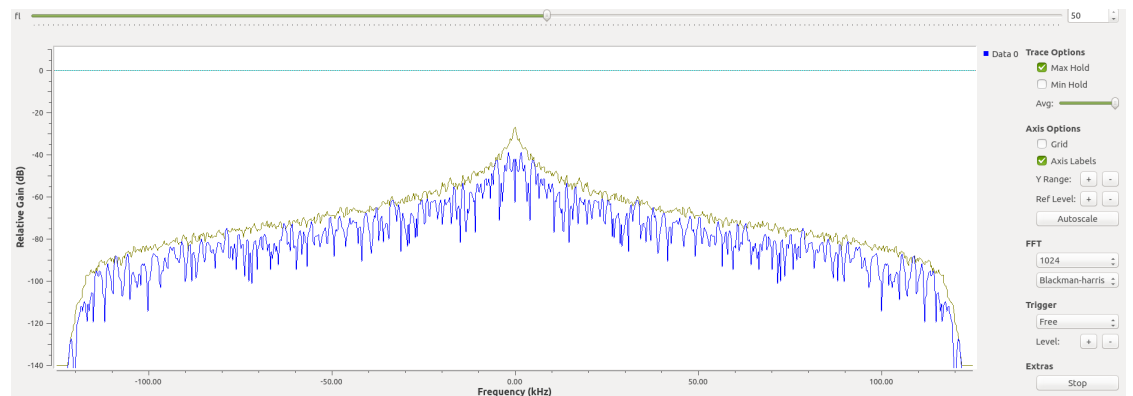
En appliquant la règle de Carson on a la bande passante $BP = 2 \cdot (75 + 53) = 250 \text{ kHz}$

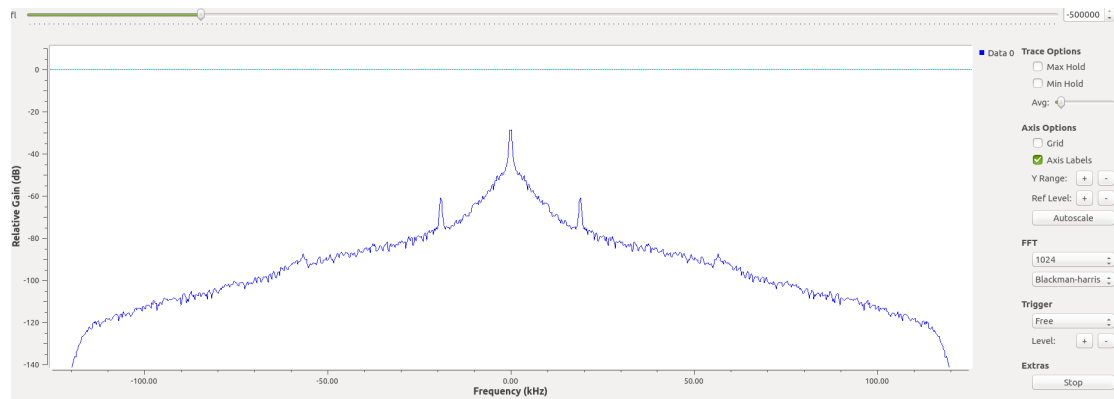
La plupart des groupes ont effectivement trouver des valeurs de bande passante à -3 dB s'approchant de cette valeur théorique.

3.3.2 Question 16



3.3.3 Question 17





Sur le second graphique la présence des 3 pics est caractéristique de la présence du signal contenant l'information. Cela tombe bien car nous sommes en train de regarder le signal autour d'une chaîne de radio (celle à l'offset de -500kHz).

3.3.4 Question 18

Jordi est l'heureux gagnant de l'album de Sam Smith, la chance. Sur l'autre chaîne on peut écouter Counting Stars de One Republic, moins la chance...

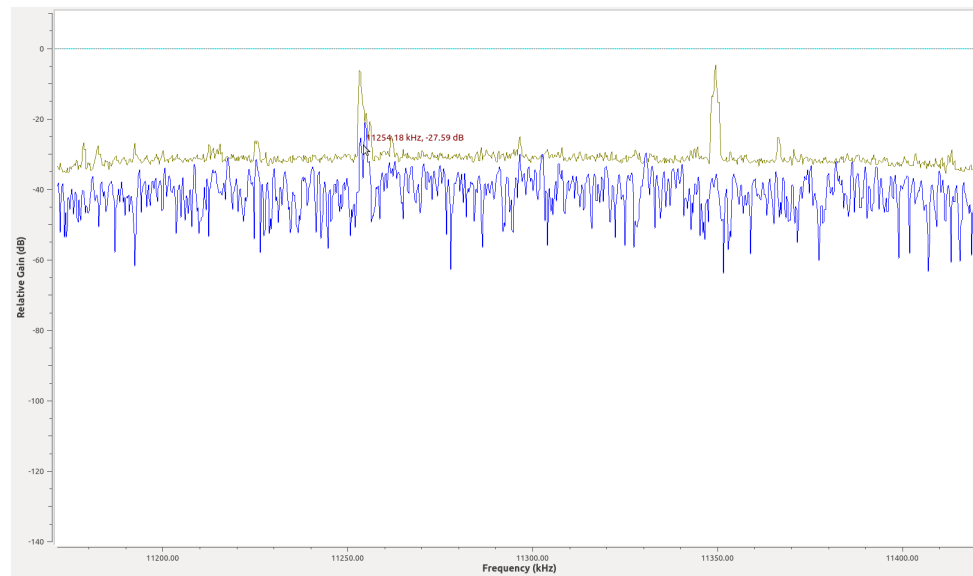
3.4 Implémentation en temps réel avec un vrai USRP

Tout les groupes n'ont pas eu le temps de pouvoir implémenter le lien entre GNUradio et un USRP en temps réel. Nous avons cependant pu manipuler un USRP sur la paillasse de nos collègues. Nous nous sommes rendu compte que les antennes de l'USRP étaient extrêmement directionnelles et sensibles aux obstacles (murs fenêtres). A noter avec surprise que c'est la station Nostalgie qui fut supportée le plus longtemps par nos collègues.

4 Reception de messages VOLMET sur AM-SSB

4.1 Analyse fréquentielle de l'enregistrement

4.1.1 Question 19



La station que nous cherchons à écouter émet à la fréquence 11.253 MHz, on peut voir sur l'image ci-dessus qu'il y a bien un pic de réception à cette fréquence.

4.2 Transposition fréquentielle

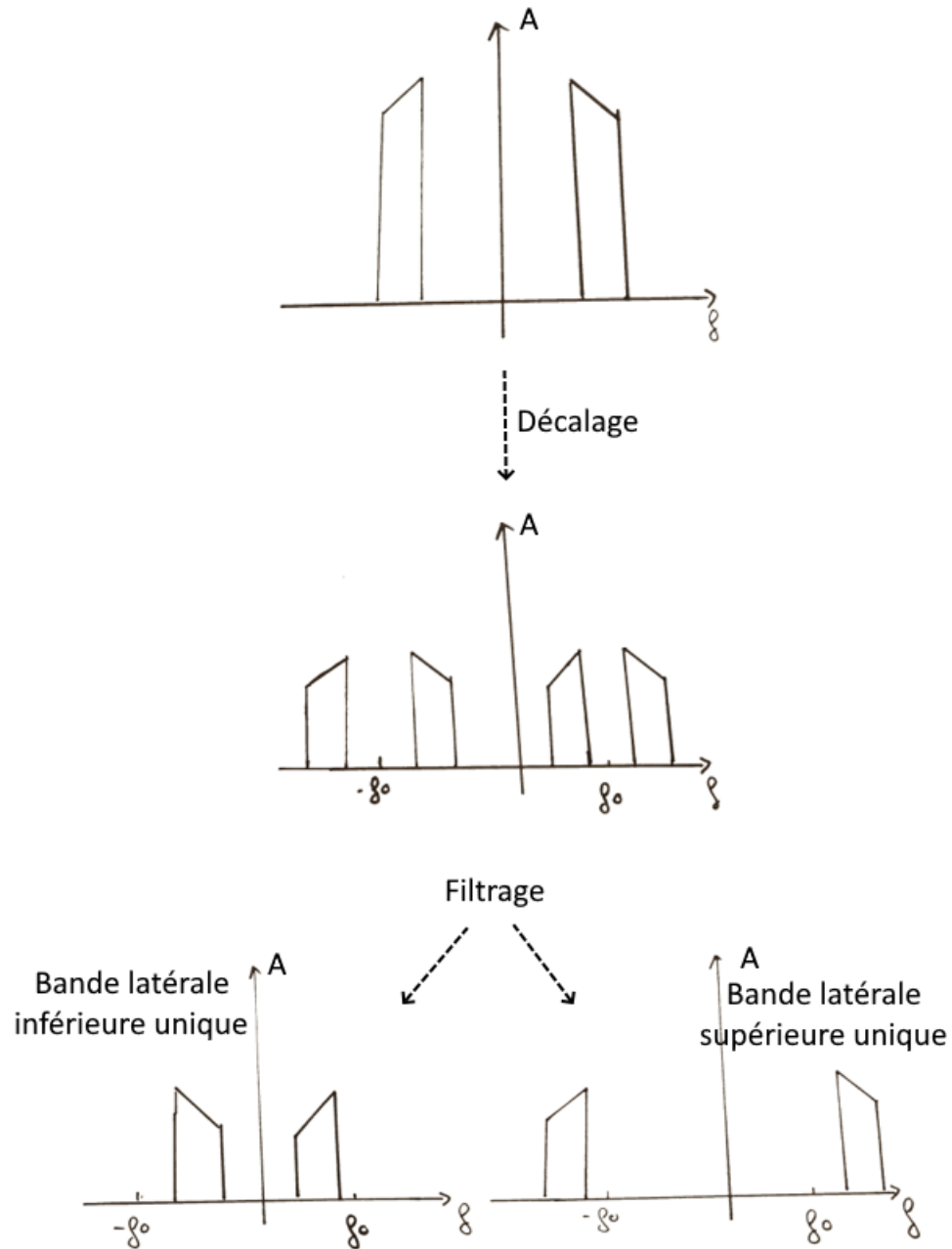
4.2.1 Question 20

On a besoin d'une fréquence d'offset de 43 kHz pour centrer le signal de la chaîne sur la fréquence nulle.



4.3 Démodulation par amplitude d'une bande unique

4.3.1 Question 21 et 22



Etant donné la forme des pics des questions 19 et 20 on peut affirmer que

4.3.2 Question 23



5 Conclusion

Lors de ces travaux pratiques les séances deux et trois furent intéressantes car les résultats étaient très concrets : de la musique ou un message clair. Nous avons pu manipuler des appareils réels ce qui a permis d'appliquer la théorie.

La première partie, plus mathématique a été compliquée pour l'un des membres du binôme (provenant de TBS) qui n'avait pas les bases pour comprendre le déroulé des questions.

Il était intéressant de remplir le même objectif que certaines anciennes technologies (autoradio) mais avec des nouvelles technologies (radio logicielle) permettant l'intégration dans des solutions actuelles.

L'ouverture de la matière sur les questions de sécurité était intéressante. Les discussions étaient intéressantes, que ce soit sur le piratage (des clés de voiture par exemple) ou le fait que l'écoute passive soit compliquée à détecter mais qu'encore aujourd'hui, l'émission radio soit très surveillée.