Projet d’optimisation linéaire

Activité d’Apprentissage I-MARO-035

Membre du groupe :
DOM Eduardo Massamesso
Matricule : 161974

Année Académique : 2018 - 2019
BAC 2 en Sciences Informatiques

Faculté des Sciences, Université de Mons

23 novembre 2018

Résumé

Ce *rapport* est rendu dans le cadre de l’AA I-MARO-035 ”Optimisation linéaire”, dispensé par le Prof. *Nicolas Gillis* en année académique 2018-2019. Le but de ce rapport est de présenter la réalisation de mon projet.

1 Description du problème

1.1 Objectifs

L'objectif est de déchiffrer un message binaire crypté qu'Alice souhaite envoyer à Bob via un canal perturbant très fortement un petit nombre des entrées du message.

2 Questions

2.1 Modélisation du problème

Il faut d'abord minimiser la norme 1 de l'erreur. Pour récupérer le message d'Alice, il faut résoudre le problème d'optimisation suivant :

$$\underset{x' \in \mathbb{R}^p}{min} \sum_{i=1}^{m} |Ax'_i - y'_i| \quad tel\ que \quad x' \in \{0,1\}^p, \tag{1}$$

(1) est un problème difficile à résoudre en pratique, il faut donc utiliser la relaxation continue suivante :

$$\underset{x' \in \mathbb{R}^p}{min} \sum_{i=1}^{m} |Ax'_i - y'_i| \quad tel\ que \quad 0 \leq x' \leq 1, \tag{2}$$

et d'arrondir la solution obtenue. Si le bruit n'est pas trop important , $x \approx x'$, ce qui permet de récupérer le message d'Alice.

2.2 Forme standard

Je cherche à le mettre sous forme standard, de ce fait, les contraintes sont les suivantes :

$$\forall i \ \in \ \{1, ..., p\},\ x'_i \geq \ 0 \tag{3}$$

$$\forall i \ \ \{1, ..., p\},\ -x'_i \geq \ -1 \tag{4}$$

(3) est une contrainte déjà remplie sous forme standard, car les variables y sont toutes positives, elle est donc redondante. Les valeurs absolues ne faisant pas partie de la forme standard, je dois m'en débarrasser. Par le cours, je sais que je peux remplacer $|x|$ par une nouvelle variable t_i en imposant les contraintes $t_i \ \geq \ x$ et $t_i \ \geq \ -x$, ce qui est équivalent à $max\{x, -x\}$. J'obtiens donc le nouveau problème suivant :

$$\underset{x' \in \mathbb{R}^p}{min} \sum_{i=1}^{m} t_i \tag{5}$$

Il a les contraintes suivantes :

$$\forall i \ \ \{1, ..., p\},\ -x'_i \geq \ -1 \tag{6}$$

$$\forall i \ \ \{1, ..., p\},\ t_i - Ax' \ \geq \ -y' \tag{7}$$

$$\forall i \ \ \{1, ..., p\},\ t_i + Ax' \ \geq \ y' \tag{8}$$

Il me faut maintenant introduire des variables d'écarts positives a_i,b_i et c_i afin de transformer les inégalités en égalité. De plus, les variables positives n'étant pas supportées par la forme standard, il faut substituer t_i par les deux nouvelles variables positives $t_i^+ - t_i^-$. Le nouveau problème est le suivant :

$$\underset{x' \in \mathbb{R}^p}{min} \sum_{i=1}^{m} t_i^+ - t_i^- \quad tel\ que, \tag{9}$$

$$\forall i \ \ \{1, ..., p\},\ -x'_i - a_i = \ -1 \tag{10}$$

$$\forall i \ \ \{1, ..., p\},\ t_i^+ - t_i^- - Ax' - b_i = \ -y' \tag{11}$$

$$\forall i \ \ \{1, ..., p\},\ t_i^+ - t_i^- + Ax' - c_i = \ y' \tag{12}$$

2.3 Déchiffrage

J'utilise Octave et la fonction **glpk** en y entrant les contraintes mentionnées ci-dessus afin de déchiffrer le message d'Alice contenu dans le fichier *messagedAlice.mat* . L'implémentation de l'algorithme est fournie en annexe. Le message déchiffré d'Alice est le suivant : *Alice vous félicite !*

2.4 Sommet du polyèdre

L'algorithme implémenté n'utilise pas la solution optimale du problème relaxé mais une solution arrondie. Dans le cas où le sommet en nombres entiers le plus proche se trouve en dehors du polyèdre des contraintes,certaines contraintes pourraient probablement ne plus être respectées après l'arrondi de la solution.Celle-ci pourrait donc ne pas être une solution du problème initial.En conclusion, la solution pourrait ne pas être un sommet du polyèdre.

2.5 Génération de message

Après génération du message, je constate qu'au delà de 40% de bruit, il devient très difficile de déchiffrer le message étant donné qu'a partir de 40% , la réussite du déchiffrage est arbitraire. Si la solution du problème relaxé est différente de la solution arrondie, alors je peux utiliser l'arrondi de la solution mais je n'ai pas de certitude sur l'optimalité de cette solution.

2.6 Variables binaires

Si la valeur de l'argument **isIntOptimal** de *votralgorithme* est vraie, **glpk** me renvoie une valeur en nombres entiers. L'arrondi de la solution n'est donc plus nécessaire. La résolution peut être rapide si l'algorithme du simplexe retourne une valeur en nombres entiers. Mais si cette solution est en nombres réels , il faut utiliser l'algorithme du *Branch and Bound*. Celui-ci est plus lent que le simplexe, mais il permet de déchiffrer un message contenant plus de bruit.