UMONS
Université de Mons

Faculté des Sciences

Rapport du projet d'optimisation

Envoi d'un message crypté sur un canal avec du bruit creux

Réalisé par Roméo IBRAIMOVSKI & Nicolas SOURNAC

Faculté
des Sciences

Supervisé par Nicolas GILLIS

Année 2020-2021

ACADÉMIE
UNIVERSITAIRE
WALLONIE-
BRUXELLES

Résumé

Dans le cadre du cours d'optimisation linéaire, nous avons du former des groupes de 2 pour ce projet.
Ce projet a pour objectif de nous faire mettre en pratique ce que nous avons appris en cours dans une situation " réelle " ainsi que nous apprendre à utiliser de nouveaux outils tel que Matlab ou Octave.
Nous avons choisi d'utiliser Octave étant l'alternative open source de Matlab et contenant la fonction " GNU Linear Programming Kit" (GLPK).

Table des matières

Description du problème

Alice et Bob souhaient s'envoyer des messages cryptés via un canal contenant du bruit creux, c'est-à-dire un canal ne perturbant qu'un petit nombre des entrées du message, mais les entrées perturbées le sont très fortement. Plus précisément, Alice veut envoyer un message binaire $x \in \{0,1\}^p$ à Bob.

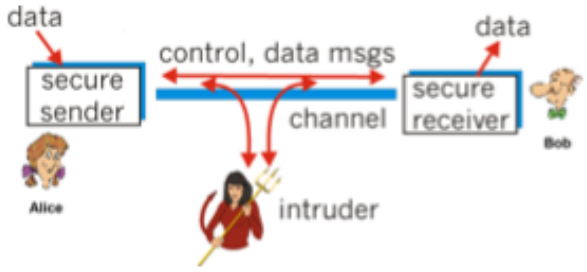

FIGURE 1 – Illustration du problème.

Avant de commencer leur communication, Alice et Bob se sont rencontrés et se sont mis d'accord sur le choix d'une matrice d'encodage $A \in \mathbb{R}^{m \times p}$ où $m \geq p$ (on utilisera pour ce projet m = 4p). Ainsi, Alice encode le message en utilisant la matrice A et envoie le message $y = Ax \in \mathbb{R}^m$ sur le canal. Le canal va transmettre le message bruité $y' = Ax + n$ à Bob où le vecteur de bruit n ne contient qu'un petit nombre d'entrées non nulle (par exemple, 10%). En présence de ce type de bruit, une bonne approche est de minimiser la norme 1 de l'erreur. En termes mathématiques, afin de récupérer le message d'Alice, Bob aurait intéret à résoudre le problème d'optimisation suivant :

$$\min_{x' \in \mathbb{R}^p} \quad \|Ax' - y'\|_1 \quad \text{tel que} \quad x' \in \{0,1\}^p,$$

$$\text{où} \quad \|z\|_1 = \sum_{i=1}^{m} |z_i| \text{ pour } z \in \mathbb{R}^m$$

Modélisation du problème comme un problème d'optimisation linéaire

Le problème précédent est combinatoire et difficile à résoudre. En pratique, il est courant d'utiliser la relaxation continue suivante :

$$\min_{x' \in \mathbb{R}^p} \quad \|Ax' - y'\|_1 \quad \text{tel que} \quad 0 \leq x' \leq 1, \qquad (1)$$

et d'arrondir la solution obtenue. Si le bruit n'est pas trop important, $x' \approx x$, ce qui permet à Bob de récupérer le message d'Alice.
Par définition de la norme 1, notre problème (1) devient le problème équivalent suivant :

$$\min_{x' \in \mathbb{R}^p} \quad \sum_{i=1}^{m} |(Ax' - y')_i| \quad \text{tel que} \quad 0 \leq x' \leq 1, \qquad (2)$$

Malheureusement, le problème d'optimisation (2) n'est pas linéaire parce que la valeur absolue est une fonction linéaire par morceau. Nous avons vu au cours qu'il est possible de linéariser un problème comportant des expressions linéaires en valeur absolue en posant $t_i = |(Ax' - y')_i|$ et en imposant $t_i \geq (Ax' - y')_i$ et $t_i \geq -(Ax' - y')_i$ comme nouvelles contraintes, on obtient le problème d'optimisation suivant :

$$\begin{aligned} \min_{t \in \mathbb{R}^m_+, x' \in \mathbb{R}^p} \quad & \sum_{i=1}^{m} t_i & (3) \\ \text{tel que} \quad & \forall i \in \{1, \ldots, m\}, \quad t_i \geq (Ax' - y')_i, \\ & \forall i \in \{1, \ldots, m\}, \quad t_i \geq -(Ax' - y')_i, \\ & -x' \geq -1, \\ & x' \geq 0 \end{aligned}$$

Par habitude, nous avons mis le problème (3) sous forme géométrique :

$$\begin{aligned} \min_{t \in \mathbb{R}^m_+, x' \in \mathbb{R}^p} \quad & \sum_{i=1}^{m} t_i & (4) \\ \text{tel que} \quad & \forall i \in \{1, \ldots, m\}, \quad t_i - (Ax')_i \geq -y'_i, \\ & \forall i \in \{1, \ldots, m\}, \quad t_i + (Ax')_i \geq y'_i, \\ & -x' \geq -1, \\ & x' \geq 0 \end{aligned}$$

Mise sous forme standard

Pour passer de la forme géométrique (4) à la forme standard, nous allons devoir éliminer les contraintes d'inégalités en introduisant des variables d'écarts s_i et éliminer les variables libres x_i en les remplaçant par $x_i = x_i^+ - x_i^-$ où x_i^+ et $-x_i^-$ sont de nouvelles variables pour lesquelles nous imposons $x_i^+ \geq 0$ et $x_i^- \geq 0$.

Commençons par introduire des variables d'écarts :

$$\begin{aligned}
\min_{t\in\mathbb{R}_+^m, x'\in\mathbb{R}^p} \quad & \sum_{i=1}^{m} t_i \\
\text{tel que} \quad & \forall i \in \{1,\dots,m\}, \quad t_i - (Ax')_i - s_{1i} = -y'_i, \\
& \forall i \in \{1,\dots,m\}, \quad t_i + (Ax')_i - s_{2i} = \quad y'_i, \\
& -x' - s_3 = -1, \\
& x', s_{1i}, s_{2i}, s_3 \geq 0
\end{aligned}$$

Éliminons les variables libres. Ici, nous n'avons que t_i de libre.
On pose $t_i = t_i^+ - t_i^-$ où $t_i^+ \geq 0$ et $-t_i^- \geq 0$,

$$\begin{aligned}
\min_{t\in\mathbb{R}_+^m, x'\in\mathbb{R}^p} \quad & \sum_{i=1}^{m} t_i^+ - t_i^- \qquad (5) \\
\text{tel que} \quad & \forall i \in \{1,\dots,m\}, \quad t_i^+ - t_i^- - (Ax')_i - s_{1i} = -y'_i, \\
& \forall i \in \{1,\dots,m\}, \quad t_i^+ - t_i^- + (Ax')_i - s_{2i} = \quad y'_i, \\
& -x' - s_3 = -1, \\
& x', s_{1i}, s_{2i}, s_3, t_i^+, -t_i^- \geq 0
\end{aligned}$$

Message envoyé par Alice

Pour déchiffrer le message envoyé par Alice, nous avons entré le problème (5) dans Octave. Voir code en annexe. Et à l'aide de la fonction " glpk ", nous avons trouvé " Alice vous flicite ! ", on devine bien que les caractères accentués peuvent poser problèmes et donc que le message qu'Alice a envoyé à Bob est " Alice vous félicite ! ".

Correspondance avec le sommet du polyèdre

Glpk résoud des programmes linéaires à l'aide d'un des plus célèbres algorithmes connus : la méthode du simplexe. Ce qui nous garantit que la solution optimale obtenue est un sommet du polyèdre.

Comme expliqué dans la modélisation, nous arrondissons la solution optimal du problème relaxé (1) ce qui implique que la solution que nous obtenons au final n'est pas forcément la solution du problème.

En effet, si le sommet en nombres entiers le plus proches se trouve à l'extérieur du polyèdre des contraintes, certaines de ses contraintes pourraient ne plus être respectées et donc sa solution pourraient ne pas être un sommet du polyèdre.

Par contre, si la solution arrondi est égale à la solution du problème relaxé, ce qui veut dire que la solution relaxé est entière, alors la solution est un sommet du polyèdre.

Limite du bruit

Nous remarquons que lorsque nous pertubons 40% des entrées de notre message, celui-ci devient impossible à déchiffrer. Cela n'est pas surprenant car au delà de 40% de perturbation, le taux d'entrée pertubée est trop élevée et l'arrondi de notre solution devient incorrect.

Variables binaires

En imposant des variables binaires, le message reste déchiffrable jusqu'à un niveau de bruit de plus ou moins 42%. Nous pouvons donc déchiffrer notre message avec un niveau de bruit supérieur de plus ou moins 2%.

Conclusion

En conclusion, ce travail nous a permis de mettre en pratique ce que nous avons appris en cours face à un problème proche de la réalité, le décryptage. Il nous a aussi permis d'approfondir nos connaissances en optimisation linéaire, de prendre en main des outils tel qu'Octave ainsi qu'améliorer nos facultés à travailler en groupe.