Multiple access channels with non-signaling resources

Samuel ARSAC, sous la direction d'Omar FAWZI,
LIP, équipe MC2, ENS de Lyon

10 juin - 31 juillet 2020

Table des matières

Remerciements

Je remercie chaleureusement Omar Fawzi pour m'avoir pris en stage et m'avoir encadré pendant plusieurs mois malgré des conditions difficiles.

Je remercie également Paul Fermé pour son aide et ses précieux conseils.

1 Introduction

Mon stage portait sur le problème de l'encodage et du décodage de messages pour la transmission au travers d'un canal. Ce canal est bruité, donc est représenté par la probabilité d'obtenir une certaine sortie sachant l'entrée du canal.

Il y a deux façons d'aborder ce problème : le point de vue algorithmique, qui consiste à déterminer la meilleure façon d'encoder et de décoder un message pour un canal donné, et le point de vue asymptotique, étudié en théorie de l'information, pour lequel on s'intéresse au nombre de messages qu'il est possible d'envoyer dans n canaux en parallèle, quand n tend vers l'infini.

On peut de plus faire varier le nombre d'encodeurs en entrée du canal. Je n'ai travaillé que sur les cas à un ou deux encodeurs.

Enfin, en plus du cas classique dans lequel les encodeurs et le décodeur sont indépendants, je me suis intéressé à la possibilité de lier ces éléments entre eux par une ressource commune dite *non-signaling*, c'est-à-dire ne permettant pas la communication entre les différents éléments. Ces ressources peuvent être créées en utilisant l'intrication quantique.

Les cas classiques asymptotiques sont détaillés dans [1], avec le deuxième théorème de Shannon pour le cas simple, et une extension au cas à deux encodeurs. D'autre part, les cas simples algorithmiques sont étudiés dans [2], où il est prouvé que la valeur optimale du cas classique peut être approchée en temps polynomial, et où l'on montre une inégalité entre les probabilités de succès avec et sans ressource *non-signaling*.

On s'intéresse au cas algorithmique classique à deux émetteurs, ainsi qu'aux cas algorithmique et asymptotique *non-signaling* à deux émetteurs. J'ai étudié plus en détail un canal de communication relatif à des jeux *2-prover 1-round*, en me basant sur l'article [3].

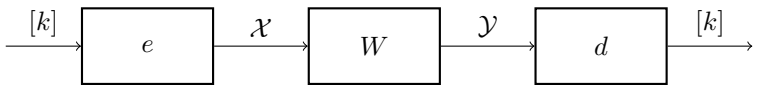

FIGURE 1 – Illustration du cas à un encodeur

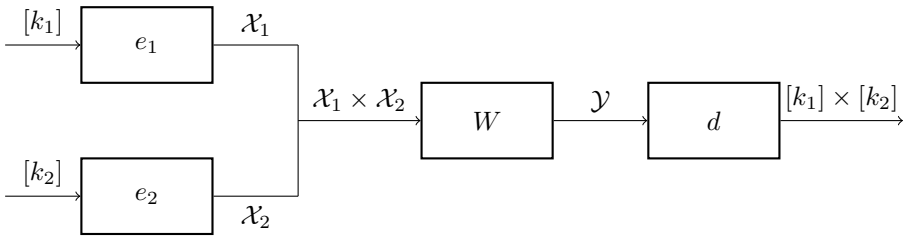

FIGURE 2 – Illustration du cas à deux encodeurs

1.1 Cas classique à un seul encodeur

On se place d'abord dans le cas à un seul encodeur, comme sur la figure 1, avec un encodeur et un décodeur indépendants.

1.1.1 Aspect algorithmique

On se base sur [2]. Prenons k messages et un canal W avec un alphabet d'entrée $\mathcal{X}$ et un alphabet de sortie $\mathcal{Y}$.

Pour un $i \in [k]$ et un $x \in \mathcal{X}$, on note $e(x|i)$ la probabilité pour que l'encodeur envoie x au canal sachant que le message en entrée est i. De même, $d(i'|y)$ est la probabilité pour que le décodeur renvoie $i' \in [k]$ sachant que la sortie du canal est $y \in \mathcal{Y}$. On a enfin $W(y|x)$ la probabilité pour que le canal renvoie y si x est en entrée.

La probabilité de succès maximale associée à W et k est donc la suivante.

Définition 1. *Probabilité de succès maximale classique avec un encodeur*

$$\begin{aligned} S(W,k) \stackrel{\text{def}}{=} \underset{e,d}{\texttt{maximiser}} \; & \frac{1}{k} \sum_{(x,y,i)\in\mathcal{X}\times\mathcal{Y}\times[k]} e(x|i)W(y|x)d(i|y) \\ \texttt{tels que} \; & \sum_{x\in\mathcal{X}} e(x|i) = 1 \quad \forall i \in [k] \\ & \sum_{i\in[k]} d(i|y) = 1 \quad \forall y \in \mathcal{Y} \\ & 0 \leq e(x|i) \quad \forall (x,i) \in \mathcal{X}\times[k] \\ & 0 \leq d(i|y) \quad \forall (i,y) \in [k]\times\mathcal{Y} \end{aligned}$$

Les conditions traduisent le fait que les valeurs de e et de d correspondent à des distributions de probabilités. D'autre part, cette définition correspond au cas dans lequel la loi probabilité régissant les messages en entrée est uniforme, ce qui est une hypothèse conservée tout au long de ce rapport.

De plus, le résultat suivant est prouvé dans [2] :

Théorème 1. *Il existe un algorithme en temps polynomial (l'algorithme glouton convient) renvoyant* $\mathrm{Alg}(W,k)$ *tel que*

$$(1-e^{-1})S(W,k) \leq \mathrm{Alg}(W,k) \leq S(W,k)$$

D'autre part, si un algorithme en temps polynomial donne une meilleure approximation, alors P=NP*.*

1.1.2 Aspect asymptotique

On se place maintenant dans le cas où n copies d'un canal W sont en parallèle, et on s'intéresse au nombre de messages qu'il est possible d'envoyer pour que la probabilité de succès tende vers 1 quand n tend vers l'infini. Dans [1], la capacité d'un canal est définie par une information mutuelle :

Définition 2. *Capacité*

Étant données deux variables aléatoires X et Y à valeurs respectivement dans $\mathcal{X}$ et $\mathcal{Y}$, la capacité C d'un canal W est

$$C = \max_p I(X:Y)$$

Où les p sont les lois possibles pour X (celle pour Y s'en déduisant par W).

En notant W^n le canal correspondant à n canaux W en parallèle, on peut énoncer le théorème suivant :

Théorème 2. *Second théorème de Shannon*
Pour tout canal W, pour tout $R < C$,

$$S(W^n, 2^{nR}) \xrightarrow[n\to\infty]{} 1$$

Réciproquement, si on a un R tel que la condition précédente soit vérifiée, alors

$$R \leq C$$

1.2 Un encodeur avec une ressource *non-signaling*

1.2.1 Ressource *non-signaling*

Plus formellement, on définit les contraintes relatives à cette ressource de la façon suivante.

Supposons que l'on ait des ensembles $\mathcal{X}_1$, $\mathcal{X}_2$, $\mathcal{Y}_1$ et $\mathcal{Y}_2$. Si $x_1 \in \mathcal{X}_1$, $x_2 \in \mathcal{X}_2$, $y_1 \in \mathcal{Y}_1$ et $y_2 \in \mathcal{Y}_2$, on note $p(y_1, y_2|x_1, x_2)$ la probabilité d'obtenir (y_1, y_2) si on a (x_1, x_2). Pour qu'il s'agisse d'une distribution *non-signaling* pour $\mathcal{X}_\infty \times \mathcal{Y}_\infty$ et $\mathcal{X}_\in \times \mathcal{Y}_\in$, il faut que p vérifie les propriétés suivantes :

$$\sum_{y_1 \in \mathcal{Y}_1} p(y_1, y_2|x_1, x_2) = \sum_{y_1 \in \mathcal{Y}_1} p(y_1, y_2|x_1', x_2) \quad \forall (x_1, x_1', x_2, y_2) \in \mathcal{X}_1 \times \mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{Y}_2$$

Et symétriquement

$$\sum_{y_2 \in \mathcal{Y}_2} p(y_1, y_2|x_1, x_2) = \sum_{y_2 \in \mathcal{Y}_2} p(y_1, y_2|x_1, x_2') \quad \forall (x_1, x_2, x_2', y_2) \in \mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{X}_2 \times \mathcal{Y}_2$$

Ce qui correspond intuitivement au fait que x_1 ne peut pas influencer y_2, et x_2 ne peut pas influencer y_1.

Exemple

Si on prend $p_1(y_1|x_1)$ et $p_2(y_2|x_2)$ respectivement la probabilité d'obtenir y_1 sachant x_1, et y_2 sachant x_2, alors

$$P(y_1, x_2|x_1, x_2) = p_1(y_1|x_1)p_2(y_2|x_2)$$

est bien *non-signaling*.

De plus, si on définit $q_1(y_1|x_1)$ et $q_2(y_2|x_2)$ de la même façon, et si on prend λ tel que $0 \leq \lambda \leq 1$, alors

$$P'(y_1, x_2|x_1, x_2) = \lambda p_1(y_1|x_1)p_2(y_2|x_2) + (1-\lambda)q_1(y_1|x_1)q_2(y_2|x_2)$$

l'est également.

1.2.2 Modification du cas classique

Dans le cas *non-signaling*, on remplace $e(x|i)d(i'|y)$ par $P(x, i'|i, y)$ pour tout (i, i', x, y) dans $[k] \times [k] \times \mathcal{X} \times \mathcal{Y}$. Les contraintes s'appliquant à P sont donc celles définies en 1.2.1, en plus de celles garantissant que ses valeurs correspondent à des probabilités.

Définition 3. *Probabilité de succès maximale* non-signaling *avec un encodeur*

$$
\begin{aligned}
S^{\mathrm{NS}}(W,k) \stackrel{\mathrm{def}}{=} \underset{P}{\texttt{maximiser}}\ & \frac{1}{k} \sum_{(x,y,i)\in\mathcal{X}\times\mathcal{Y}\times[k]} W(y|x)P(x,i|i,y) \\
\texttt{tels que}\ & \sum_{x\in\mathcal{X}} p(x,i'|i,y) = \sum_{x\in\mathcal{X}} p(x,i'|i'',y) \quad \forall (i,i',i'',y) \in [k]\times[k]\times[k]\times\mathcal{Y} \\
& \sum_{i'\in[k]} p(x,i'|i,y) = \sum_{i'\in[k]} p(x,i'|i,y') \quad \forall (i,x,y,y') \in [k]\times\mathcal{X}\times\mathcal{Y}\times\mathcal{Y} \\
& \sum_{(x,i')\in\mathcal{X}\times[k]} P(x,i'|i,y) = 1 \quad \forall (i,y) \in [k]\times\mathcal{Y} \\
& 0 \leq P(x,i'|i,y) \quad \forall (i,i',x,y) \in [k]\times[k]\times\mathcal{X}\times\mathcal{Y}
\end{aligned}
$$

On trouve le résultat suivant dans [2] :

Théorème 3. *Si k et l sont des nombres de messages inférieurs à $|\mathcal{X}|$, alors*

$$S(W,l) \geq \frac{k}{l}\left(1-\left(1-\frac{1}{k}\right)^{l}\right) S^{\mathrm{NS}}(W,k)$$

Et cette inégalité est optimale.

1.3 Cas à deux encodeurs

On passe maintenant au cas classique à deux encodeurs (voir [1]). On a donc maintenant deux paramètres k_1 et k_2, représentant respectivement le nombre de messages possibles en entrée du premier encodeur e_1 et celui du second, e_2. Ces derniers prennent respectivement des messages i et j dans $[k_1]$ et $[k_2]$, et renvoient des élément $x_1 \in \mathcal{X}_1$ et $x_2 \in \mathcal{X}_2$ avec probabilités $e_1(x_1|i)$ et $e_2(x_2|j)$.

L'alphabet d'entrée du canal devient donc $\mathcal{X}_1 \times \mathcal{X}_2$. On note alors $W(y|(x_1,x_2))$ la probabilité pour que W associe $y \in \mathcal{Y}$ à la paire $(x_1,x_2) \in \mathcal{X}_1 \times \mathcal{X}_2$.

Symétriquement, on a un décodeur d qui à un élément $y \in \mathcal{Y}$ associe la paire $(i,j) \in [k_1]\times[k_2]$ avec probabilité $d((i,j)|y)$.

On a donc une définition de S proche de celle à un encodeur :

Définition 4. *Probabilité de succès maximale classique avec deux encodeurs*

$$S(W,k_1,k_2) \stackrel{\text{def}}{=} \underset{e_1,e_2,d}{\texttt{maximiser}} \frac{1}{k_1k_2} \sum_{\substack{(x_1,x_2,y,i,j)\\ \in\mathcal{X}_1\times\mathcal{X}_2\times\mathcal{Y}\times[k_1]\times[k_2]}} e_1(x_1|i)e_2(x_2|j)W(y|(x_1,x_2))d((i,j)|y)$$

$$\begin{aligned}
\texttt{tels que } & \sum_{x_1\in\mathcal{X}_1} e_1(x_1|i) = 1 \quad \forall i \in [k_1] \\
& \sum_{x_2\in\mathcal{X}_2} e_2(x_2|j) = 1 \quad \forall j \in [k_2] \\
& \sum_{(i,j)\in[k_1]\times[k_2]} d((i,j)|y) = 1 \quad \forall y \in \mathcal{Y} \\
& 0 \leq e_1(x_1|i) \leq 1 \quad \forall (x_1,i) \in \mathcal{X}_1 \times [k_1] \\
& 0 \leq e_2(x_2|j) \leq 1 \quad \forall (x_2,j) \in \mathcal{X}_2 \times [k_2] \\
& 0 \leq d((i,j)|y) \leq 1 \quad \forall (i,j,y) \in [k_1]\times[k_2]\times\mathcal{Y}
\end{aligned}$$

D'un point de vue asymptotique, on définit la *zone de capacité* d'un canal W de la façon suivante :

Définition 5. *Zone de capacité*
La zone de capacité est l'adhérence de l'ensemble des paires $(R_1,R_2) \in \mathbf{R}_+^2$ telles que

$$S(W^n, 2^{R_1 n}, 2^{R_2 n}) \underset{n\to\infty}{\to} 1$$

Le théorème suivant donne un moyen de la calculer à l'aide d'informations mutuelles :

Théorème 4. *Si on définit des variables aléatoires X_1, X_2 et Y à valeurs respectivement dans $\mathcal{X}_1$, $\mathcal{X}_2$ et $\mathcal{Y}$, la zone de capacité est égale à l'adhérence de l'enveloppe convexe de l'ensemble des (R_1,R_2) vérifiant*

$$\begin{aligned}
R_1 &< I(X_1;Y|X_2) \\
R_2 &< I(X_2;Y|X_1) \\
R_1+R_2 &< I(X_1,X_2;Y)
\end{aligned}$$

pour des lois produit sur X_1 et X_2 (celle sur Y étant alors donnée par W).

Le point de vue algorithmique sera étudié dans la partie 2.2.

2 Optimisation du cas classique avec deux encodeurs

Si on adopte le même point de vue que pour le cas à un encodeur, c'est à dire un problème de maximisation avec des contraintes, on peut se demander s'il existe dans ce cas un théorème semblable au théorème 1. Ce n'est pas le cas, comme montré après la définition du problème.

2.1 Énoncé équivalent au cas classique à deux encodeurs

Il est possible de simplifier l'énoncé de la façon suivante :

Théorème 5. *Énoncé équivalent*
Si on définit la fonction

$$f_W : \begin{array}{ccc} \mathcal{P}(\mathcal{X}_1 \times \mathcal{X}_2) & \to & \mathbf{R} \\ Z & \mapsto & \sum_{y \in \mathcal{Y}} \max_{(x_1,x_2) \in Z} W(y|(x_1,x_2)) \end{array}$$

On a alors un énoncé équivalent pour le cas classique à deux encodeurs :

$$S(W, k_1, k_2) = \frac{1}{k_1 k_2} \max_{\substack{Z = Z_1 \times Z_2 \\ Z_1 \subseteq \mathcal{X}_1, Z_2 \subseteq \mathcal{X}_2 \\ |Z_1| \leq k_1, |Z_2| \leq k_2}} f_W(Z)$$

Démonstration. La preuve de l'équivalence des deux énoncés est en annexe.

2.2 Inexistence d'une solution approchée en temps polynomial avec facteur constant

Contrairement au cas à un encodeur, sous l'hypothèse 1.1 de [4] sur les formules k-AND, on a le résultat suivant :

Théorème 6. *Inexistence d'une solution approchée*
Sous l'hypothèse 1.1 de [4], pour tout W, k_1 et k_2, il n'existe pas d'algorithme en temps polynomial calculant une valeur approchée de $S(W, k_1, k_2) - 1$ avec un facteur 1/2.

Démonstration. La preuve complète est en annexe. Dans l'article [4], on trouve une démonstration de l'impossibilité (toujours sous l'hypothèse mentionnée) de trouver une approximation en temps polynomial pour le problème du sous-graphe le plus dense dans un graphe biparti.

En définissant les alphabets d'entrée à partir des deux parties du graphe, et la probabilité d'obtenir un symbole en sortie à partir des arêtes, on peut réduire ce problème à notre problème d'encodage.

3 Cas *non-signaling* avec deux encodeurs

On passe maintenant au cas dans lequel les deux encodeurs et le décodeur ont accès à une ressource commune, mais qui ne leur permet pas de communiquer entre eux.

3.1 Énoncé du problème

3.1.1 Transformation du cas classique

On enlève l'indépendance entre les deux encodeurs et le décodeur. $P(x_1, x_2, (i', j')|y, i, j)$ représente la probabilité pour que, sachant que les messages d'entrée sont i et j, et que le symbole en sortie du canal est y, on ait x_1 et x_2 en entrée du canal, et (i', j') en sortie du décodeur.
On doit toujours avoir des distributions de probabilités, mais à cette contrainte on rajoute l'absence de possibilité de communication par la ressource NS.

Définition 6. *Probabilité de succès maximale* non-signaling *avec deux encodeurs*

$$
\begin{aligned}
&S^{\mathrm{NS}}(W,k_1,k_2) \stackrel{\text{def}}{=} \\
&\underset{P(x_1,x_2,(i',j')|i,j,y)}{\texttt{maximise}} \\
&\qquad\qquad \frac{1}{k_1k_2}\sum_{x_1,x_2,y,i,j} P(x_1,x_2,(i,j)|i,j,y)W(y|(x_1,x_2)) \\
&\qquad \texttt{tel que}\ \ P \text{ probabilité} \\
&\qquad\qquad\ \ P \textit{ non-signaling}
\end{aligned}
$$

Les conditions détaillées sont en annexe dans la preuve du théorème suivant.

3.1.2 Un énoncé équivalent

Théorème 7. *Énoncé équivalent*
On peut également définir S^{NS} de la façon suivante.

$$
\begin{aligned}
&S^{\mathrm{NS}}(W,k_1,k_2) \stackrel{\text{def}}{=} \\
&\underset{r_{x_1,x_2,y},r^1_{x_1,x_2,y},r^2_{x_1,x_2,y},p_{x_1,x_2}}{\texttt{maximiser}} \ \frac{1}{k_1k_2}\sum_{x_1,x_2,y} W(y|x_1x_2)r_{x_1,x_2,y} \\
&\qquad\qquad \texttt{tels que} \sum_{x_1,x_2} r_{x_1,x_2,y} = 1 \\
&\qquad\qquad\qquad \sum_{x_1} r^1_{x_1,x_2,y} = k_1 \sum_{x_1} r_{x_1,x_2,y} \\
&\qquad\qquad\qquad \sum_{x_2} r^2_{x_1,x_2,y} = k_2 \sum_{x_2} r_{x_1,x_2,y} \\
&\qquad\qquad\qquad \sum_{x_1} p_{x_1,x_2} = k_1 \sum_{x_1} r^2_{x_1,x_2,y} \\
&\qquad\qquad\qquad \sum_{x_2} p_{x_1,x_2} = k_2 \sum_{x_2} r^1_{x_1,x_2,y} \\
&\qquad\qquad\qquad 0 \le r_{x_1,x_2,y} \le r^1_{x_1,x_2,y} \le p_{x_1,x_2} \\
&\qquad\qquad\qquad 0 \le r_{x_1,x_2,y} \le r^2_{x_1,x_2,y} \le p_{x_1,x_2} \\
&\qquad\qquad\qquad 0 \le p_{x_1,x_2} - r^1_{x_1,x_2,y} - r^2_{x_1,x_2,y} + r_{x_1,x_2,y}
\end{aligned}
$$

Démonstration. La preuve de l'équivalence est en annexe, les relations entre les variables des deux énoncés sont les suivantes :

$$
\begin{aligned}
r_{x_1,x_2,y} &= \sum_{i,j} P(x_1,x_2,(i,j)|i,j,y) \\
r^1_{x_1,x_2,y} &= \sum_{i,i',j} P(x_1,x_2,(i',j)|i,j,y) \\
r^2_{x_1,x_2,y} &= \sum_{i,j,j'} P(x_1,x_2,(i,j')|i,j,y) \\
p_{x_1,x_2} &= \sum_{i,i',j,j'} P(x_1,x_2,(i',j')|i,j,y)
\end{aligned}
$$

$$
P(x_1,x_2,(i',j')|i,j,y) = \begin{cases}
\dfrac{r_{x_1,x_2,y}}{k_1,k_2} & \text{si } i,j = i',j' \\
\dfrac{r^1_{x_1,x_2,y} - r_{x_1,x_2,y}}{k_1k_2(k_1-1)} & \text{si } i \neq i', j = j' \\
\dfrac{r^2_{x_1,x_2,y} - r_{x_1,x_2,y}}{k_1k_2(k_2-1)} & \text{si } i = i', j \neq j' \\
\dfrac{p_{x_1,x_2} - r^1_{x_1,x_2,y} - r^2_{x_1,x_2,y} + r_{x_1,x_2,y}}{k_1k_2(k_1-1)(k_2-1)} & \text{si } i \neq i', j \neq j'
\end{cases}
$$

3.2 Un lemme utile

On peut démontrer le lemme suivant, qui traduit le fait que le non-signaling est plus puissant que l'indépendance :

Lemme 1. *Pour tout W, n, k_1, k_2, on a $S^{\mathrm{NS}}(W^n,k_1,k_2) \geq S(W^n,k_1,k_2)$*

Démonstration. Si on a les e_1, e_2 et d du cas classique, alors on définit P comme leur produit. On vérifie facilement que P vérifie alors les conditions *non-signaling* (ce qui est naturel, puisqu'il s'agit même du cas où tous les éléments sont indépendants). Ce qui donne également le corollaire suivant.

Corollaire 1. *La zone de capacité dans le cas* non-signaling *est toujours plus grande que dans le cas classique.*

Démonstration. Par passage à la limite des inégalités.

3.3 Un exemple : l'additionneur

Appliquons les définitions précédentes sur un exemple. On considère le cas d'un canal prenant deux bits en entrée et renvoyant leur somme. On définit W_{add} tel que

$$
W_{\mathrm{add}}(y|(x_1,x_2)) = \delta_{y,x_1+x_2} \qquad \forall y \in \{0,1,2\}, \forall (x_1,x_2) \in \{0,1\}^2
$$

Cas classique

On calcule la zone de capacité à l'aide des informations mutuelles, en notant p_1 la probabilité pour que e_1 renvoie 1 et on note p_2 de même pour e_2.

$$\begin{aligned} I(X_1; Y|X_2) &= H(X_1|X_2) - H(X_1|Y, X_2) \\ &= H(X_1) \\ &= -(p_1 \log_2(p_1) + (1-p_1)\log_2(1-p_1)) \end{aligned}$$

On a un maximum de 1 pour $p_1 = 1/2$, donc $R_1 < 1$. La situation étant symétrique, on a de même $R_2 < 1$.

D'autre part,

$$I(X_1, X_2; Y) = H(X_1, X_2) - H(X_1, X_2|Y)$$

On obtient numériquement (détails sur le code en annexe) que le maximum est obtenu pour des lois uniformes, et est de $3/2$, donc $R_1 + R_2 < 3/2$.

La zone de capacité est donc la suivante :

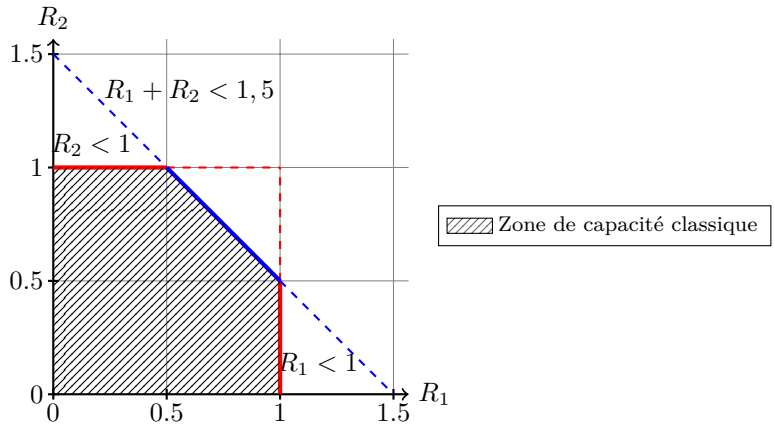

FIGURE 3 – Zone de capacité de l'additionneur dans le cas classique

Cas NS

Si on utilise un solveur LP pour résoudre le problème, on obtient les valeurs suivantes pour le point $(1, 1)$.

n	1	2	3	4
$S^{\mathrm{NS}}_{\mathrm{add}}(2^n, 2^n, n)$	0,7500	0,5625	0,4219	0,3164

On peut donc supposer que $(1, 1)$ n'appartient pas à la zone de capacité.

4 Canaux correspondant à des jeux

On s'intéresse maintenant à des canaux définis comme dans [3], à partir de jeux *2-prover 1-round*. On définit ces jeux de la façon suivante :

Définition 7. *Jeu* 2-prover 1-round

Étant donnés un vérifieur, deux joueurs et des ensembles Q_1, Q_2, A_1 et A_2, le jeu se déroule de la façon suivante :

- *Le vérifieur envoie une question $q_1 \in Q_1$ au joueur 1, et $q_2 \in Q_2$ au joueur 2.*
- *Chacun des deux joueurs renvoie une réponse, respectivement $a_1 \in A_1$ et $a_2 \in A_2$.*
- *Le vérifieur accepte si $(q_1, q_2, a_1, a_2) \in V$, avec $V \subseteq Q_1 \times Q_2 \times A_1 \times A_2$.*

Définition 8. *Stratégie*

On définie une stratégie pour un jeu G comme une paire de fonctions (Π_1, Π_2), respectivement de Q_1 dans A_1 et de Q_2 dans A_2.

Définition 9. *Probabilité de succès maximale*

On définit la probabilité maximale ω pour un jeu G :

$$\omega(G) = \frac{1}{|Q_1||Q_2|} \max_{(\Pi_1,\Pi_2)} |\{(q_1, q_2, \Pi_1(q_1), \Pi_2(q_2))|q_1 \in Q_1, q_2 \in Q_2\} \cap V|$$

Les (Π_1, Π_2) étant des stratégies. Il s'agit de la définition supposant une distribution uniforme sur les questions.

On définit un canal ayant pour alphabet d'entrée $(Q_1 \times A_1) \times (Q_2 \times A_2)$ et pour alphabet de sortie $Q_1 \times Q_2$, avec Q_1 et Q_2 les questions du jeu et A_1 et A_2 les réponses.

$$W((q_1', q_2')|(q_1, a_1), (q_2, a_2)) = \begin{cases} \delta_{q_1,q_1'}\delta_{q_2,q_2'} & \text{si } (q_1, q_2, a_1, a_2) \in V \\ 1/(|Q_1||Q_2|) & \text{sinon} \end{cases}$$

Pour tout $(q_1, q_1', q_2, q_2', a_1, a_2) \in Q_1 \times Q_1 \times Q_2 \times Q_2 \times A_1 \times A_2$.

4.1 CHSH

On prend par exemple le jeu CHSH, dans lequel les questions et les réponses sont des bits, et qui possède un ensemble de configurations de victoire

$$V = \{(q_1, q_2, a_1, a_2) \in \{0, 1\}^4 | q_1 \wedge q_2 = a_1 \oplus a_2\}$$

4.1.1 Cas classique

On recherche encore une fois numériquement le maximum des informations mutuelles, et on obtient approximativement

$$R_1, R_2 < 1$$
$$R_1 + R_2 < 1,5$$

Ce qui donne donc une zone de capacité identique à celle de l'additionneur.

4.1.2 Cas *non-signaling*

On est ici dans un cas où la ressource *non-signaling* apporte un avantage certain, puisque l'on a

$$S^{\mathrm{NS}}(W_{\mathrm{CHSH}}, 2, 2) = 1$$

(le détail des valeurs permettant d'atteindre cette probabilité de succès sont en annexe). Il en découle que pour tout $n \in \mathbf{N}$,

$$S^{\mathrm{NS}}(W_{\mathrm{CHSH}}^n, 2^n, 2^n) = 1$$

puisqu'il suffit alors de traiter indépendemment chaque canal. Donc $(1, 1)$ appartient à la zone de capacité.

On peut de plus démontrer le lemme suivant :

Lemme 2. *Si (R_1, R_2) est dans la zone de capacité, et si $(R'_1, R'_2) \leq_{\text{lex}} (R_1, R_2)$, alors (R'_1, R'_2) est dans la zone de capacité.*

Démonstration. Il suffit de montrer que pour tout W, n, k_1, k_2, $k'_1 \leq k_1$ et $k'_2 \leq k_2$, on a

$$S(W^n, k_1, k_2) \leq S(W^n, k'_1, k'_2)$$

Notons e_1, e_2 et d les deux encodeurs et le décodeur correspondant à $S_n(W, k_1, k_2)$. On note $I_1 \subseteq [k_1]$ et $I_2 \subseteq [k_2]$ tels que $[I_1| = k'_1$ et $|I_2| = k'_2$ des ensembles tels que la probabilité de succès soit maximale pour les éléments de $I_1 \times I_2$ parmi tous les ensembles de ce type possibles.

On a alors une probabilité de succès plus élevée sur les messages de $I_1 \times I_2$. On définit donc une nouvelle fonction correspondant à la restriction à $I_1 \times I_2$ du cas original, en augmentant si nécessaire certaines valeurs pour conserver des sommes égales à 1.

On en déduit donc que la zone de capacité contient le carré ayant (1,1) et (0,0) comme angles.

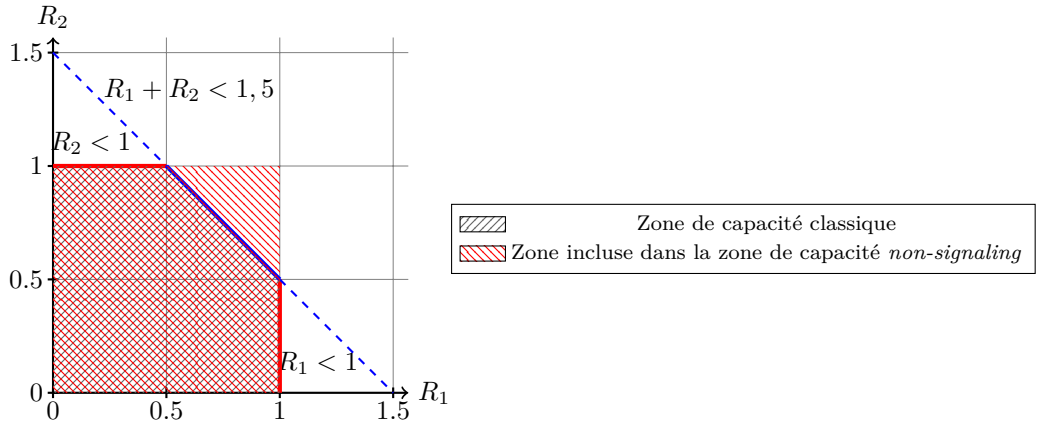

FIGURE 4 – Zones de capacité du canal correspondant à CHSH

4.2 Correspondance avec les stratégies

Puisque les canaux sont définis à partir de jeux, on peut se demander si une stratégie optimale pour un jeu peut correspondre à des émetteurs et des décodeurs donnant une probabilité de succès maximale.

Théorème 8. *Étant donné une stratégie optimale (Π_1, Π_2) pour un jeu G, on peut obtenir des encodeurs et un décodeur, avec $k_1 = |Q_1|$ et $k_2 = |Q_2|$, donnant une probabilité de succès égale à*

$$\omega(G) + \frac{1 - \omega(G)}{k_1 k_2}$$

Démonstration. On associe chaque question à un message, et l'encodeur associe alors à ce message la paire contenant la question et la réponse apportée par la stratégie. Le décodeur associe réciproquement la paire des messages auxquels les questions qu'il reçoit en entrée sont associées. La preuve détaillée est en annexe.

Malheureusement, la réciproque n'est pas vraie :

Théorème 9. *Étant donné des e_1, e_2 et d optimaux, il n'est pas toujours possible de donner une stratégie optimale, et telle que $\omega(G) + \frac{1-\omega(G)}{k_1 k_2}$ soit la probabilité de succès du problème d'encodage.*

Démonstration. On a l'exemple suivant :

$$Q_1 = Q_2 = A_1 = A_2 = \{0, 1\}$$

$$V = \{(0, 0, 0, 0), (0, 1, 1, 0)\}$$

Si on utilise le deuxième énoncé, on s'aperçoit en étudiant les cas que prendre $Z_1 = \{(0, 0), (0, 1)\}$ et $Z_2 = \{(0, 0), (1, 0)\}$ donne une probabilité de succès égale à $1/2$, qui n'est atteinte par aucun autre Z.

Or l'ensemble Z_1 contient deux fois 0 comme question, ce qui ne correspond pas à une stratégie. Un ensemble Z correspondant à une stratégie est donc nécessairement différent de l'ensemble optimal énoncé précédemment, or la probabilité de succès maximale n'est atteinte que pour ce dernier.

On a donc

$$S(W, |Q_1|, |Q_2|) \geq \omega(G) + \frac{1 - \omega(G)}{|Q_1||Q_2|}$$

5 Une hypothèse sur la zone de capacité dans le cas *non-signaling*

Hypothèse 1. *Si on définit des variables aléatoires X_1, X_2 et Y à valeurs respectivement dans $\mathcal{X}_1$, $\mathcal{X}_2$ et $\mathcal{Y}$, la zone de capacité* non-signaling *est égale à l'adhérence de l'enveloppe convexe de l'ensemble des (R_1, R_2) vérifiant*

$$R_1 < I(X_1; Y|X_2)$$
$$R_2 < I(X_2; Y|X_1)$$
$$R_1 + R_2 < I(X_1, X_2; Y)$$

pour des lois ***quelconques*** *sur (X_1, X_2) (celle sur Y étant alors donnée par W).*

Cette hypothèse se base sur un affaiblissement de la contrainte sur les lois de probabilités par rapport au cas classique. On trouve par exemple en annexe la majoration de la somme $R_1 + R_2$ dans le cas *non-signaling* pour CHSH.

6 Conclusion

On a un résultat sur la possibilité de calculer une solution approchée en temps polynomial pour le cas classique à deux encodeurs. Les résultats démontrés sur le cas *non-signaling* sont en revanche plus anecdotiques, et concernent notamment le cas particulier des canaux correspondant aux jeux *2-prover 1-round*, pour lesquels on a une minoration de la probabilité de succès. On a toutefois une hypothèse générale sur la forme des zones de capacité *non-signaling*.

La principale piste future serait donc de chercher à démontrer cette hypothèse, si celle-ci est vraie.

Références

[1] Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory, 2nd Edition*. Wiley, 2006.

[2] Siddharth Barman and Omar Fawzi. Algorithmic aspects of optimal channel coding. *IEEE Transactions on Information Theory*, PP, 08 2015.

[3] Felix Leditzky, Mohammad A. Alhejji, Joshua Levin, and Graeme Smith. Playing games with multiple access channels. *Nature Communications*, march 2020. https ://www.nature.com/articles/s41467-020-15240-w.pdf.

[4] Noga Alon, Sanjeev Arora, Rajsekar Manokaran, Dana Moshkovitz, and Omri Weinstein. Inapproximability of densest κ-subgraph from average case hardness, dec 2011. www.tau.ac.il/~nogaa/PDFS/dks8.pdf.

Annexes

Preuve du théorème 5

On rappelle les deux énoncés :

$$S(W,k_1,k_2) \stackrel{\text{def}}{=} \underset{e_1,e_2,d}{\texttt{maximiser}} \frac{1}{k_1k_2} \sum_{\substack{(x_1,x_2,y,i,j)\\ \in \mathcal{X}_1\times\mathcal{X}_2\times\mathcal{Y}\times[k_1]\times[k_2]}} e_1(x_1|i)e_2(x_2|j)W(y|(x_1,x_2))d((i,j)|y)$$

$$\texttt{tels que} \sum_{x_1\in\mathcal{X}_1} e_1(x_1|i) = 1 \quad \forall i \in [k_1] \tag{6.0.1}$$

$$\sum_{x_2\in\mathcal{X}_2} e_2(x_2|j) = 1 \quad \forall j \in [k_2] \tag{6.0.2}$$

$$\sum_{(i,j)\in[k_1]\times[k_2]} d((i,j)|y) = 1 \quad \forall y \in \mathcal{Y} \tag{6.0.3}$$

$$0 \le e_1(x_1|i) \le 1 \quad \forall (x_1,i) \in \mathcal{X}_1 \times [k_1] \tag{6.0.4}$$

$$0 \le e_2(x_2|j) \le 1 \quad \forall (x_2,j) \in \mathcal{X}_2 \times [k_2] \tag{6.0.5}$$

$$0 \le d((i,j)|y) \le 1 \quad \forall (i,j,y) \in [k_1]\times[k_2]\times\mathcal{Y} \tag{6.0.6}$$

Et

$$S(W,k_1,k_2) = \frac{1}{k_1k_2} \max_{\substack{Z=Z_1\times Z_2\\ Z_1\subseteq\mathcal{X}_1, Z_2\subseteq\mathcal{X}_2\\ |Z_1|\le k_1, |Z_2|\le k_2}} f_W(Z)$$

avec

$$f_W : \begin{array}{ccc} \mathcal{P}(\mathcal{X}_1\times\mathcal{X}_2) & \to & \mathbf{R} \\ Z & \mapsto & \sum_{y\in\mathcal{Y}} \max_{(x_1,x_2)\in Z} W(y|(x_1,x_2)) \end{array}$$

— Montrons que si on définit $S(W,k_1,k_2)$ selon le premier énoncé, alors

$$S(W,k_1,k_2) \ge \frac{1}{k_1k_2} \max_{\substack{Z=Z_1\times Z_2\\ Z_1\subseteq\mathcal{X}_1, Z_2\subseteq\mathcal{X}_2\\ |Z_1|\le k_1, |Z_2|\le k_2}} f_W(Z)$$

Prenons $Z_1 \subseteq \mathcal{X}_1, Z_2 \subseteq \mathcal{X}_2$ de taille $l_1 \le k_1$ et $l_2 \le k_2$, et $Z = Z_1 \times Z_2$. On note ses éléments $\{(x_{1,1},x_{2,1}),\dots,(x_{1,l_1},x_{2,l_2})\}$.
On définit

$$e_1(x_{1,i'}|i) = \delta_{i,i'} \quad \forall (i,i') \in [l_1]\times[k_1] \tag{6.0.7}$$

et de même pour e_2.
Pour $i \in \{l_1+1,\dots,k_1\}$ et $j \in \{l_2+1,\dots,k_2\}$, on choisit des valeurs arbitraires vérifiant les conditions du premier énoncé.
Pour tout $y \in \mathcal{Y}$ on définit $m(y) = (m_1(y), m_2(y))$ le plus petit $(i,j) \in [l_1]\times[l_2]$ tel que

$$W(y|(x_{1,i},x_{2,j})) = \max_{i'\in[l_1],j'\in[l_2]} W(y|(x_{1,i'},x_{2,j'})) \tag{6.0.8}$$

On définit alors

$$d(p|y) = \delta_{p,m(y)} \tag{6.0.9}$$

e_1, e_2 et d satisfont bien les contraintes du premier énoncé.
De plus, on a

$$\begin{aligned}
&\frac{1}{k_1 k_2} \sum_{\substack{(i,j,x_1,x_2,y)\\ \in [k_1]\times[k_2]\times\mathcal{X}_1\times\mathcal{X}_2\times\mathcal{Y}}} e_1(x_1|i)e_2(x_2|j)W(y|(x_1,x_2))d((i,j)|y) \\
&\geq \frac{1}{k_1 k_2} \sum_{(i,j,y)\in[l_1]\times[l_2]\times\mathcal{Y}} W(y|(x_{1,i},x_{2,j}))d((i,j)|y) && \text{Par (6.0.7)} \\
&= \frac{1}{k_1 k_2} \sum_{y\in\mathcal{Y}} W(y|(x_{1,m_1(y)},x_{2,m_2(y)})) && \text{Par (6.0.9)} \\
&= \frac{1}{k_1 k_2} \sum_{y\in\mathcal{Y}} \max_{x\in Z} W(y|x) && \text{Par (6.0.8)} \\
&= \frac{1}{k_1 k_2} f_W(Z)
\end{aligned}$$

Ce qui nous donne bien l'inégalité présentée plus haut.

— Montrons maintenant l'inégalité inverse.
On prend e_1, e_2 et d vérifiant les contraintes du premier énoncé. Notons $x_{(i,j)}$ une paire telle que

$$\sum_{y\in\mathcal{Y}} W(y|x_{(i,j)})d((i,j)|y) = \max_{(x_1,x_2)\in\mathcal{X}_1\times\mathcal{X}_2} \sum_{y\in\mathcal{Y}} W(y|(x_1,x_2))d((i,j)|y) \tag{6.0.10}$$

On a alors

$$\begin{aligned}
&\sum_{\substack{(i,j,x_1,x_2)\\ \in[k_1]\times[k_2]\times\mathcal{X}_1\times\mathcal{X}_2}} e_1(x_1|i)e_2(x_2|j) \sum_{y\in\mathcal{Y}} W(y|(x_1,x_2))d((i,j)|y) \\
&\leq \sum_{(i,j)\in[k_1]\times[k_2]} \max_{(x_1,x_2)\in\mathcal{X}_1\times\mathcal{X}_2} \sum_{y\in\mathcal{Y}} W(y|(x_1,x_2))d((i,j)|y) \\
&\text{Par (6.0.1), (6.0.2), (6.0.4), (6.0.5)} \\
&= \sum_{(i,j,y)\in[k_1]\times[k_2]\times\mathcal{Y}} W(y|x_{(i,j)})d((i,j)|y) && \text{Par (6.0.10)} \\
&\leq \sum_{y\in\mathcal{Y}} \max_{(i,j)\in[k_1]\times[k_2]} W(y|x_{(i,j)}) && \text{Par (6.0.3), (6.0.6)} \\
&\leq \max_{\substack{Z=Z_1\times Z_2\\ Z_1\subseteq\mathcal{X}_1, Z_2\subseteq\mathcal{X}_2\\ |Z_1|\leq k_1, |Z_2|\leq k_2}} \sum_{y\in\mathcal{Y}} \max_{x\in Z} W(y|x)
\end{aligned}$$

On a donc bien cette seconde inégalité.

Preuve du théorème 6

On a le problème suivant, que l'on note P_1 :

Données : un graphe biparti $G = (V_1 \cup V_2, E)$, deux paramètres κ_1 et κ_2

Question : Trouver $S_1 \subseteq V_1$ et $S_2 \subseteq V_2$ tels que :

$|S_1| = \kappa_1$

$|S_2| = \kappa_2$

Le nombre d'arêtes de $S_1 \cup S_2$ est maximal parmi tous les S_1 et S_2 possibles.

Pour lequel on sait d'après [4] qu'il ne possède pas d'algorithme polynomial donnant une solution approchée avec un facteur 1/2.

On le réduit au problème P_2 :

Données : un canal W, des alphabets d'entrée $\mathcal{X}_1$ et $\mathcal{X}_2$,
un alphabet de sortie $\mathcal{Y}$, deux paramètres k_1 et k_2.

Question : Trouver $Z_1 \subseteq \mathcal{X}_1$ et $Z_2 \subseteq \mathcal{X}_2$ tels que :
$|Z_1| = k_1$
$|Z_2| = k_2$
$f_W(Z_1 \times Z_2) - 1$ est maximal parmi tous les Z_1 et Z_2 possibles.

Instance de P_2 à partir de P_1

Prenons une instance $(G = (V_1 \cup V_2, E), \kappa_1, \kappa_2)$ de P_1. On suppose que pour chaque arête (x, y), $x \in V_1$ et $y \in V_2$, sans perte de généralité. On définit $k_1 = \kappa_1$, $k_2 = \kappa_2$, $\mathcal{X}_1 = V_1$, $\mathcal{X}_2 = V_2$ et $\mathcal{Y} = V_1 \times V_2$.

Pour tout $(x_1, x_2) \in \mathcal{X}_1 \times \mathcal{X}_2$, $(x'_1, x'_2) \in \mathcal{Y}$, on définit $W((x'_1, x'_2)|(x_1, x_2))$ de la façon suivante.

$$W((x'_1, x'_2)|(x_1, x_2)) = \begin{cases} \delta_{x'_1, x_1}\delta_{x'_2, x_2} & \text{si } (x_1, x_2) \in E \\ 1/|\mathcal{Y}| & \text{sinon} \end{cases}$$

On a alors bien $\sum_{y \in \mathcal{Y}} W(y|(x_1, x_2)) = 1$ pour tout $x_1 \in \mathcal{X}_1$ et $x_2 \in \mathcal{X}_2$.

Solution de P_2 vers solution de P_1

On définit une bijection des solutions de P_2, que l'on note $\mathrm{sol}(P_2)$ dans les solutions de P_1 ($\mathrm{sol}(P_1)$) :

$$g : \left\{ \begin{array}{ccc} \mathrm{sol}(P_2) & \to & \mathrm{sol}(P_1) \\ Z_1 \times Z_2 & \mapsto & Z_1 \cup Z_2 \end{array} \right.$$

On prend $S = S_1 \cup S_2$ une solution de l'instance du premier problème et on note E_S ses arêtes. On note $Z = g^{-1}(S)$. On a alors

$$\begin{aligned} f_W(Z) &= \sum_{y \in E_S} \max_{(x_1,x_2) \in Z} W(y|(x_1, x_2)) + \sum_{y \in \mathcal{Y} \setminus E_S} \max_{(x_1,x_2) \in Z} W(y|(x_1, x_2)) \\ &= |E_S| + \frac{|\mathcal{Y}| - |E_S|}{|\mathcal{Y}|} \\ &= 1 + |E_S| \left(1 - \frac{1}{|\mathcal{Y}|}\right) \end{aligned}$$

Réciproquement, si $Z = Z_1 \times Z_2$, on prend $S = g(Z)$ et on a

$$|E_S| = \frac{f_W(Z) - 1}{1 - \frac{1}{|\mathcal{Y}|}}$$

On remarque que maximiser $|E_S|$ est équivalent à maximiser $f_W(Z) - 1$, donc si $Z = Z_1 \times Z_2$ est une solution optimale de l'instance de P_2, alors $S = g(Z)$ est une solution optimale de l'instance de P_1.

Supposons que l'on ait Z une solution optimale pour P_1, et Z' une approximation de cette solution avec un facteur 1/2. À partir de ces solutions, on définit $S = g(Z)$ et $S' = g(Z')$.

Si $f_W(Z) - 1 > 0$:

$$\begin{aligned}\frac{|E_{S'}|}{|E_S|} &= \frac{f_W(Z') - 1}{f_W(Z) - 1} \\ &= 1/2\end{aligned}$$

Si $f_W(Z) - 1 = 0$, on a également $E_{|S|} = 0$, donc le facteur d'approximation reste le même. D'autre part, f_W est toujours supérieure à 1, étant la somme de $|\mathcal{Y}|$ valeurs supérieures à $\frac{1}{|\mathcal{Y}|}$. On a donc bien le résultat attendu.

Preuve du théorème 7

On rappelle les énoncés :

$$S^{\mathrm{NS}}(W, k_1, k_2) \stackrel{\mathrm{def}}{=}$$

$$\underset{P(x_1,x_2,(i',j')|i,j,y)}{\texttt{maximiser}} \ \frac{1}{k_1 k_2} \sum_{x_1,x_2,y,i,j} P(x_1, x_2, (i,j)|i,j,y) W(y|(x_1,x_2))$$

$$\texttt{tel que} \quad \sum_{x_1 \in \mathcal{X}_1} P(x_1, x_2, (i',j')|i,j,y) = \sum_{x_1 \in \mathcal{X}_1} P(x_1, x_2, (i',j')|k,j,y) \quad \forall i, i', j, j', k, x_2, y \tag{6.0.11}$$

$$\sum_{x_2 \in \mathcal{X}_2} P(x_1, x_2, (i',j')|i,j,y) = \sum_{x_2 \in \mathcal{X}_2} P(x_1, x_2, (i',j')|i,k,y) \quad \forall i, i', j, j', k, x_1, y \tag{6.0.12}$$

$$\sum_{i',j'} P(x_1, x_2, (i',j')|i,j,y) = \sum_{i',j'} P(x_1, x_2, (i',j')|i,j,y') \quad \forall i, j, x_1, x_2, y, y' \tag{6.0.13}$$

$$\sum_{i',j',x_1,x_2} P(x_1 x_2, (i',j')|i,j,y) = 1 \tag{6.0.14}$$

$$0 \leq P(x_1, x_2, (i',j')|i,j,y) \leq 1 \quad \forall x_1, x_2, i, i', j, j', y \tag{6.0.15}$$

Et

$$S^{\mathrm{NS}}(W,k_1,k_2) \stackrel{\mathrm{def}}{=}$$

$$\underset{r_{x_1,x_2,y},r^1_{x_1,x_2,y},r^2_{x_1,x_2,y},p_{x_1,x_2}}{\texttt{maximiser}} \quad \frac{1}{k_1k_2}\sum_{x_1,x_2,y} W(y|x_1x_2)r_{x_1,x_2,y}$$

$$\texttt{tels que} \sum_{x_1,x_2} r_{x_1,x_2,y} = 1 \tag{6.0.16}$$

$$\sum_{x_1} r^1_{x_1,x_2,y} = k_1 \sum_{x_1} r_{x_1,x_2,y} \tag{6.0.17}$$

$$\sum_{x_2} r^2_{x_1,x_2,y} = k_2 \sum_{x_2} r_{x_1,x_2,y} \tag{6.0.18}$$

$$\sum_{x_1} p_{x_1,x_2} = k_1 \sum_{x_1} r^2_{x_1,x_2,y} \tag{6.0.19}$$

$$\sum_{x_2} p_{x_1,x_2} = k_2 \sum_{x_2} r^1_{x_1,x_2,y} \tag{6.0.20}$$

$$0 \leq r_{x_1,x_2,y} \leq r^1_{x_1,x_2,y} \leq p_{x_1,x_2} \tag{6.0.21}$$

$$0 \leq r_{x_1,x_2,y} \leq r^2_{x_1,x_2,y} \leq p_{x_1,x_2} \tag{6.0.22}$$

$$0 \leq p_{x_1,x_2} - r^1_{x_1,x_2,y} - r^2_{x_1,x_2,y} + r_{x_1,x_2,y} \tag{6.0.23}$$

Montrons d'abord que si on a $P(x_1,x_2,(i',j')|i,j,y)$ vérifiant les conditions du premier énoncé, alors si on prend

$$\begin{aligned}
r_{x_1,x_2,y} &= \sum_{i,j} P(x_1,x_2,(i,j)|i,j,y) \\
r^1_{x_1,x_2,y} &= \sum_{i,i',j} P(x_1,x_2,(i',j)|i,j,y) \\
r^2_{x_1,x_2,y} &= \sum_{i,j,j'} P(x_1,x_2,(i,j')|i,j,y) \\
p_{x_1,x_2} &= \sum_{i,i',j,j'} P(x_1,x_2,(i',j')|i,j,y)
\end{aligned}$$

ces valeurs vérifient les conditions de l'énoncé 2 :

$$\begin{aligned}
\sum_{x_1,x_2} r_{x_1,x_2,y} &= \sum_{x_1,x_2,i,j} P(x_1,x_2,(i,j)|i,j,y) \\
&= \sum_{x_1,x_2,i,j} P(x_1,x_2,(i,j)|i',j',y) \\
&= 1
\end{aligned}$$

$$\begin{aligned}\sum_{x_1} r^1_{x_1,x_2,y} &= \sum_{i,i',j}\sum_{x_1} P(x_1,x_2,(i',j)|i,j,y)\\ &= \sum_{i,i',j}\sum_{x_1} P(x_1,x_2,(i',j)|i',j,y)\\ &= \sum_{x_1,i} r_{x_1,x_2,y}\\ &= k_1\sum_{x_1} r_{x_1,x_2,y}\end{aligned}$$

De la même façon :

$$\sum_{x_2} r^2_{x_1,x_2,y} = k_2\sum_{x_2} r_{x_1,x_2,y}$$

$$\begin{aligned}\sum_{x_1} p_{x_1,x_2} &= \sum_{i,i',j,j'}\sum_{x_1} P(x_1,x_2,(i',j')|i,j,y)\\ &= \sum_{i,i',j,j'}\sum_{x_1} P(x_1,x_2,(i,j')|i,j,y)\\ &= \sum_{x_1,i'} r^2_{x_1,x_2,y}\\ &= k_1\sum_{x_1} r^2_{x_1,x_2,y}\end{aligned}$$

De même,

$$\sum_{x_2} p_{x_1,x_2} = k_2\sum_{x_2} r^1_{x_1,x_2,y}$$

Les conditions

$$0 \le r_{x_1,x_2,y} \le r^1_{x_1,x_2,y} \le p_{x_1,x_2}$$

et

$$0 \le r_{x_1,x_2,y} \le r^2_{x_1,x_2,y} \le p_{x_1,x_2}$$

proviennent du fait que tous les $P(x_1,x_2,(i',j')|i,j,y)$ sont positifs.
Enfin,

$$\begin{aligned}&p_{x_1,x_2} - r^1_{x_1,x_2,y} - r^2_{x_1,x_2,y} + r_{x_1,x_2,y}\\ =&\sum_{i,j}(P(x_1,x_2,(i,j)|i,j,y) - (\sum_{i'} P(x_1,x_2,(i',j)|i,j,y))\\ &- (\sum_{j'} P(x_1,x_2,(i,j')|i,j,y)) + \sum_{i',j'} P(x_1,x_2,(i',j')|i,j,y))\\ =&\sum_{i,j}(P(x_1,x_2,(i,j)|i,j,y) + \sum_{i'\neq i,j'\neq j} P(x_1,x_2,(i',j')|i,j,y)\\ \ge&0\end{aligned}$$

Réciproquement, prenons

$$P(x_1,x_2,(i',j')|i,j,y)=\begin{cases}\dfrac{r_{x_1,x_2,y}}{k_1,k_2} & \text{si } i,j=i',j'\\ \dfrac{r^1_{x_1,x_2,y}-r_{x_1,x_2,y}}{k_1k_2(k_1-1)} & \text{si } i\neq i',j=j'\\ \dfrac{r^2_{x_1,x_2,y}-r_{x_1,x_2,y}}{k_1k_2(k_2-1)} & \text{si } i=i',j\neq j'\\ \dfrac{p_{x_1,x_2}-r^1_{x_1,x_2,y}-r^2_{x_1,x_2,y}+r_{x_1,x_2,y}}{k_1k_2(k_1-1)(k_2-1)} & \text{si } i\neq i',j\neq j'\end{cases}$$

et montrons que les conditions de l'énoncé 1 sont vérifiées :

$$\begin{aligned}&\sum_{x_1}P(x_1,x_2,(i',j')|i,j,y)\\ &=\begin{cases}\displaystyle\sum_{x_1}\frac{r_{x_1,x_2,y}}{k_1,k_2} & \text{si } i,j=i',j'\\ \displaystyle\sum_{x_1}\frac{r^1_{x_1,x_2,y}-r_{x_1,x_2,y}}{k_1k_2(k_1-1)} & \text{si } i\neq i',j=j'\\ \displaystyle\sum_{x_1}\frac{r^2_{x_1,x_2,y}-r_{x_1,x_2,y}}{k_1k_2(k_2-1)} & \text{si } i=i',j\neq j'\\ \displaystyle\sum_{x_1}\frac{p_{x_1,x_2}-r^1_{x_1,x_2,y}-r^2_{x_1,x_2,y}+r_{x_1,x_2,y}}{k_1k_2(k_1-1)(k_2-1)} & \text{si } i\neq i',j\neq j'\end{cases}\\ &=\begin{cases}\displaystyle\sum_{x_1}\frac{r_{x_1,x_2,y}}{k_1,k_2}\\ \dfrac{k_1(\sum_{x_1}r_{x_1,x_2,y})-\sum_{x_1}r_{x_1,x_2,y}}{k_1k_2(k_1-1)}\\ \displaystyle\sum_{x_1}\frac{r^2_{x_1,x_2,y}-r_{x_1,x_2,y}}{k_1k_2(k_2-1)}\\ \dfrac{k_1(\sum_{x_1}r^2_{x_1,x_2,y})-k_1(\sum_{x_1}r_{x_1,x_2,y})-(\sum_{x_1}r^2_{x_1,x_2,y})+\sum_{x_1}(r_{x_1,x_2,y})}{k_1k_2(k_1-1)(k_2-1)}\end{cases}\\ &=\begin{cases}\displaystyle\sum_{x_1}\frac{r_{x_1,x_2,y}}{k_1,k_2}\\ \displaystyle\sum_{x_1}\frac{r_{x_1,x_2,y}}{k_1k_2}\\ \displaystyle\sum_{x_1}\frac{r^2_{x_1,x_2,y}-r_{x_1,x_2,y}}{k_1k_2(k_2-1)}\\ \displaystyle\sum_{x_1}\frac{r^2_{x_1,x_2,y}-r_{x_1,x_2,y}}{k_1k_2(k_2-1)}\end{cases}\\ &=\sum_{x_1}P(x_1,x_2,(i',j')|k,j,y)\end{aligned}$$

De même pour la somme sur x_2.

$$\begin{aligned}
&\sum_{i',j'} P(x_1, x_2, (i', j')|i, j, y) \\
=&\frac{r_{x_1,x_2,y}}{k_1 k_2} + (k_1 - 1)\frac{r^1_{x_1,x_2,y} - r_{x_1,x_2,y}}{k_1 k_2 (k_1 - 1)} + (k_2 - 1)\frac{r^2_{x_1,x_2,y} - r_{x_1,x_2,y}}{k_1 k_2 (k_2 - 1)} \\
&+ (k_1 - 1)(k_2 - 1)\frac{p_{x_1,x_2} - r^1_{x_1,x_2,y} - r^2_{x_1 x_2,y} + r_{x_1,x_2,y}}{k_1 k_2 (k_1 - 1)(k_2 - 1)} \\
=&\frac{p_{x_1,x_2}}{k_1 k_2} \\
=&\sum_{i',j'} P(x_1, x_2, (i', j')|i, j, y')
\end{aligned}$$

$$\begin{aligned}
\sum_{x_1,x_2,i',j'} P(x_1, x_2, (i', j')|i, j, y) &= \sum_{x_1,x_2} \frac{p_{x_1,x_2}}{k_1 k_2} \\
&= \sum_{x_1,x_2} \frac{r^2_{x_1,x_2,y}}{k_2} \\
&= \sum_{x_1,x_2} r_{x_1,x_2,y} \\
&= 1
\end{aligned}$$

On a enfin bien $P(x_1, x_2, (i', j')|i, j, y) \geq 0$.

Solution pour le cas $k_1 = k_2 = 2$ de CHSH

On utilise le second énoncé du problème. Ces valeurs ont été calculées par un solveur LP (détails dans l'annexe réservée au code).

r :

(q'_1, q'_2)	(q_1, a_1) \ (q_2, a_2)	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	1/2	0	0	0
	(0,1)	0	1/2	0	0
	(1,0)	0	0	0	0
	(1,1)	0	0	0	0
(0,1)	(0,0)	0	0	1/2	0
	(0,1)	0	0	0	1/2
	(1,0)	0	0	0	0
	(1,1)	0	0	0	0
(1,0)	(0,0)	0	0	0	0
	(0,1)	0	0	0	0
	(1,0)	1/2	0	0	0
	(1,1)	0	1/2	0	0
(1,1)	(0,0)	0	0	0	0
	(0,1)	0	0	0	0
	(1,0)	0	0	0	1/2
	(1,1)	0	0	1/2	0

r^1 :

(q'_1, q'_2)	(q_1, a_1) \ (q_2, a_2)	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	1/2	0	0	0
	(0,1)	0	1/2	0	0
	(1,0)	1/2	0	0	0
	(1,1)	0	1/2	0	0
(0,1)	(0,0)	0	0	1/2	0
	(0,1)	0	0	0	1/2
	(1,0)	0	0	0	1/2
	(1,1)	0	0	1/2	0
(1,0)	(0,0)	1/2	0	0	0
	(0,1)	0	1/2	0	0
	(1,0)	1/2	0	0	0
	(1,1)	0	1/2	0	0
(1,1)	(0,0)	0	0	1/2	0
	(0,1)	0	0	0	1/2
	(1,0)	0	0	0	1/2
	(1,1)	0	0	1/2	0

r^2 :

(q_1', q_2')	(q_2, a_2) / (q_1, a_1)	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	1/2	0	1/2	0
	(0,1)	0	1/2	0	1/2
	(1,0)	0	0	0	0
	(1,1)	0	0	0	0
(0,1)	(0,0)	1/2	0	1/2	0
	(0,1)	0	1/2	0	1/2
	(1,0)	0	0	0	0
	(1,1)	0	0	0	0
(1,0)	(0,0)	0	0	0	0
	(0,1)	0	0	0	0
	(1,0)	1/2	0	0	1/2
	(1,1)	0	1/2	1/2	0
(1,1)	(0,0)	0	0	0	0
	(0,1)	0	0	0	0
	(1,0)	1/2	0	0	1/2
	(1,1)	0	1/2	1/2	0

p :

(q_2, a_2) / (q_1, a_1)	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	1/2	0	1/2	0
(0,1)	0	1/2	0	1/2
(1,0)	1/2	0	0	1/2
(1,1)	0	1/2	1/2	0

Preuve du théorème 8

Supposons que l'on dispose d'une stratégie (Π_1, Π_2) pour un jeu G. On numérote arbitrairement les éléments de $\mathcal{X}_1$ et $\mathcal{X}_2$, et on note $x_{1,i}$ le i^e élément de $\mathcal{X}_1$ et $y_{1,i}$ l'image par Π_1 de $x_{1,i}$, et semblablement pour $\mathcal{X}_2$.

On définit alors

$$e_1((x_{1,i'}, y_{1,i'})|i) = \delta_{i,i'}$$

Et symétriquement pour e_2. On définit de plus

$$d((i', j')|(x_{1,i}, x_{2,j})) = \delta_{i,i'}\delta_{j,j'}$$

Dans un cas où configuration est gagnante, les messages sont bien transmis. Si elle ne l'est pas, il reste toujours la possibilité que la sortie aléatoire du canal convienne. On a donc bien une probabilité de succès égale à

$$\omega(G) + \frac{1 - \omega(G)}{k_1 k_2}$$

Majoration de $R_1 + R_2$ pour CHSH sous l'hypothèse 1

On remarque d'abord que $I(X_1, X_2; Y) \leq H(Y) \leq 2$ (Y ayant quatre valeurs possibles).

D'autre part, pour chaque élément (q_1, q_2) de $\mathcal{Y}$, on prend $a_1 \in A_1$ et $a_2 \in A_2$ tels que $q_1 \wedge q_2 = a_1 \oplus a_2$ (on peut remarquer que de telles valeurs réponses existent dans tous les cas). On affecte alors la probabilité $1/4$ à $((q_1, a_1), (q_2, a_2))$.

Ces quadruplets étant nécessairement tous distincts (les (q_1, q_2) le sont), connaître la valeur de Y implique connaître la valeur de (X_1, X_2), et réciproquement. On a donc $I(X_1, X_2; Y) = H(Y) = 2$.

On a donc $R_1 + R_2 < 2$ comme borne la plus serrée, ce qui correspond à l'appartenance de (1,1) à la zone de débits.

Détails sur le code utilisé

Tout le code utilisé dans le cadre de ce stage a été rédigé en Python 3. Ont été réalisés :

— Un solveur pour les problèmes linéaires (le cas *non-signaling*) à l'aide de la bibliothèque PuLP. C'est grâce à ce code que j'ai obtenu rapidement une solution pour le cas *non-signaling* de CHSH.

— Une fonction de recherche de maximum pour les informations mutuelles, avec les bibliothèques SciPy optimize et NumPy.

Au total, le code compte environ 270 lignes.