Intrication quantique pour la correction du bruit d'un canal de communication

Antoine GROSPELLIER
sous la direction de Omar FAWZI

10 juin 2016

Table des matières

Introduction

On considère un jeu entre deux personnes Alice et Bob qui veulent communiquer via un canal. Ce canal de communication n'est pas parfait ce qui signifie que les messages que reçoit Bob contiennent du bruit. On étudie donc quels sont les moyens pour que Bob puisse retrouver le message initial d'Alice.
Formellement, le but de Alice est de transmettre à Bob un message i choisit uniformément dans un ensemble noté M de cardinal k. En particulier, le cas $k = 2$ correspond à la situation où Alice tente de transmettre un bit ($M = \{0; 1\}$). Leur seul moyen de communication est un canal W. Ce canal est décrit comme la donnée d'un ensemble X de mots d'entrée, d'un ensemble Y de mots de sortie et d'une probabilité conditionnelle notée W (comme le canal). Pour tout $x \in X$ et $y \in Y$, $W(y|x)$ représente la probabilité que la sortie du canal soit y sachant que son entrée est x. C'est à

dire que si Alice envoie x via le canal alors Bob reçoit y avec probabilité $W(y|x)$.
Supposons que Alice veut envoyer $i \in M$ à Bob, le déroulement du protocole est le suivant :

- Alice encode i en un certain $x \in X$
- Alice donne x à l'entrée du canal
- Bob obtient $y \in Y$ à la sortie du canal
- Bob décode y en un certain $j \in M$.

La transmission est un succès lorsque $i = j$.
Alice et Bob doivent ainsi mettre au point une stratégie de codage qui fabrique x à partir de i, et une stratégie de décodage qui fabrique j à partir de y. Ils doivent être capables de faire fonctionner ces deux stratégies sans communication.
L'article [8] a montré expérimentalement que la probabilité de succès peut être augmentée si Alice et Bob partagent un état quantique intriqué. Le but de mon stage est de quantifier le gain maximal que cela apporte. Certains résultats existent déjà : en fait, les stratégies qui consistent à utiliser un état quantique intriqué sont contenues dans un ensemble plus grand, appelé les stratégies non-signaling. Les articles [1] et [4] donnent des bornes (qui sont atteintes) sur le gain apporté par les stratégies non-signaling. Par voix de conséquence, ces bornes sont également valables pour majorer le gain d'une stratégie quantique. Le fait de savoir si ces bornes sont atteites dans le cas quantique est une question ouverte et c'est cela que j'ai étudié pendant mon stage. Le principal canal que j'ai utilisé est le "subset channel".

Durant ce stage, j'ai implémenté certains algorithmes dans le langage sage. J'ai également utilisé un code créé pour l'article [2] écrit en matlab. Pour obtenir ces codes, taper dans un terminal : *git clone https ://github.com/antoine06/Implementation_stage_m2_grospellier.git*

1 Pré-requis

Dans cette section, on présente les outils mathématiques et les postulats de mécanique quantique nécéssaires à la compréhension du problème. On peut trouver les démonstrations des propositions et théorèmes dans [6]

1.1 Généralités mathématiques

Notations 1.1. *On adopte les notations suivantes :*

- $\mathcal{M}_{n,m}(\mathbb{C})$ *désigne les matrices à n lignes et m colonnes à coefficients dans* $\mathbb{C}$ *et* $\mathcal{M}_n(\mathbb{C}) = \mathcal{M}_{n,n}(\mathbb{C})$.
  Parfois on considérera des matrices dont les lignes (resp. colonnes) sont indicées par un ensemble fini quelconque au lieu de $[\![1; n]\!]$ *(resp* $[\![1; m]\!]$*)*
- $\mathcal{S}_n(\mathbb{C})$ *est l'ensemble des matrices* $n \times n$ *hermitiennes*
- $\mathcal{S}_n^+(\mathbb{C})$ *est l'ensemble des matrices* $n \times n$ *hermitiennes semi-définies positives*
- $\preceq$ *: relation d'ordre partiel de Löwner :*
  Soient $A, B \in \mathcal{S}_n(\mathbb{C})$ *alors* $A \preceq B$ *signifie que* $(B - A) \in \mathcal{S}_n^+(\mathbb{C})$.
  Notamment, $0 \preceq A$ *signifie que* $A \in \mathcal{S}_n^+(\mathbb{C})$.
- $\|A\|_1$ *: norme trace de A pour* $A \in \mathcal{S}_n(\mathbb{C})$ *(voir proposition 1.4)*
- A^T, $\bar{A}$, $A^\dagger$ *: transposée, conjuguée (au sens des nombres complexes),* $A^\dagger = (\bar{A})^T$
- $\langle\psi|\,, |\psi\rangle$ *: notations de Dirac (notation bra-ket) :*
  Soit $\mathcal{H}$ *un espace de Hilbert, dans ce rapport on se restreint aux espaces vecoriels de dimension finie. Donc* $\mathcal{H}$ *est isomorphe à* $\mathbb{C}^n$ *muni du produit scalaire usuel. Pour préciser qu'un vecteur*

colonne ψ est un élément de $\mathcal{H}$, on le notera $|\psi\rangle$ ("ket psi").
On pose $\langle\psi| = |\psi\rangle^\dagger$ ("bra psi", c'est donc un vecteur ligne).
Avec ces notations, le produit scalaire entre $|\psi_1\rangle$ et $|\psi_2\rangle$ se note $\langle\psi_1|\,|\psi_2\rangle$ et $|\psi_1\rangle\,\langle\psi_2|$ est une matrice $n \times n$.

- $|i\rangle$ *: soit* $\mathcal{H} = \mathbb{C}^n$ *et* $i \in [\![0; n-1]\!]$. *On note alors* $|i\rangle = \begin{pmatrix} a_0 \\ \vdots \\ a_{n-1} \end{pmatrix}$ *où* $a_i = 1$ *et* $a_j = 0$ *pour* $j \neq i$.
  En particulier, avec cette notation :
  - $|0\rangle$ *n'est pas le vecteur nul*
  - *La matrice* $A = (a_{i,j})_{0 \leq i,j \leq n-1}$ *est égale à* $A = \sum_{0 \leq i,j \leq n-1} a_{i,j}\,|i\rangle\,\langle j|$
  - *Plus généralement, la matrice* $A = \sum_{i \in I}\sum_{j \in J} a_{i,j}\,|i\rangle\,\langle j|$ *est une matrice dont les lignes sont indicées par I et les colonnes par J et dont l'entrée (i,j) est $a_{i,j}$*
- $P_\sigma = \sum_{0 \leq x \leq n-1} |\sigma(x)\rangle\,\langle x|$ *: matrice de permutation associée à* $\sigma \in \mathfrak{S}_n$
- $\otimes$ *désigne le produit tensoriel entre espaces vectoriels, entre vecteurs ou entre matrices (voir définition 1.2).*
  Le vecteur $|\psi_1\rangle \otimes |\psi_2\rangle$ se note aussi $|\psi_1\rangle\,|\psi_2\rangle$ ou $|\psi_1, \psi_2\rangle$
  $A^{\otimes\delta}$ designe $A \otimes \cdots \otimes A$ où la matrice A apparaît δ fois dans le produit.
- $|\phi\rangle = \frac{1}{\sqrt{n}} \sum_{0 \leq i \leq n-1} |i\rangle\,|i\rangle$ *est l'état maximalement intriqué.*
- $\binom{n}{t}$ *est le coefficient binomial et* $\binom{\mathbf{n}}{\mathbf{t}}$ *(en gras) est l'ensemble des sous-ensembles de* $[\![0; n-1]\!]$ *de taille t*

Définition 1.2. *Produit de Kronecker (produit tensoriel en dimension finie) :*

- *Soient* $A \in \mathcal{M}_{n,m}(\mathbb{C})$ *et* $B \in \mathcal{M}_{p,q}(\mathbb{C})$. *Le produit tensoriel entre* $A = (a_{i,j})_{i,j}$ *et* B *est une matrice par blocs définie par :*

$$A \otimes B = \begin{pmatrix} a_{1,1}.B & a_{1,2}.B & \dots & a_{1,n}.B \\ a_{2,1}.B & a_{2,2}.B & \dots & a_{2,n}.B \\ \vdots & \vdots & \vdots & \vdots \\ a_{n,1}.B & a_{n,2}.B & \dots & a_{n,n}.B \end{pmatrix}$$

  On utilisera en particulier le produit tensoriel lorsque A et B sont deux matrices carrées, deux vecteurs lignes ou deux vecteurs colonnes.
- *Soient* $\mathcal{H}_1 = \mathbb{C}^n$ *et* $\mathcal{H}_2 = \mathbb{C}^m$. *On note alors* $\mathcal{H}_1 \otimes \mathcal{H}_2 = \mathbb{C}^{n \times m}$ *qui a pour base* $\{|i\rangle \otimes |j\rangle \mid 0 \leq i \leq n-1, 0 \leq j \leq m-1\}$

Proposition 1.3. *Propriétés du produit tensoriel :*
Soient $A, A' \in \mathcal{M}_{n,m}(\mathbb{C})$ *;* $B, B' \in \mathcal{M}_{p,q}(\mathbb{C})$ *;* $|\psi_1\rangle \in \mathcal{M}_{m,1}(\mathbb{C})$ *;* $|\psi_2\rangle \in \mathcal{M}_{q,1}(\mathbb{C})$ *et* $\lambda \in \mathbb{C}$. *Alors :*

- $(A + A') \otimes B = A \otimes B + A' \otimes B$
- $A \otimes (B + B') = A \otimes B + A \otimes B'$
- $\lambda(A \otimes B) = (\lambda A) \otimes B = A \otimes (\lambda B)$
- $(A \otimes B)(|\psi_1\rangle \otimes |\psi_2\rangle) = A\,|\psi_1\rangle \otimes B\,|\psi_2\rangle$

- $(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$

Proposition 1.4. *Propriétés des matrices hermitiennes :*
Soit $A \in \mathcal{S}_n(\mathbb{C})$. Alors A est diagonalisable en base orthonormée et est à valeurs propres réelles. C'est à dire qu'il existe $(\lambda_1, \cdots, \lambda_n) \in \mathbb{R}^n$ et $(|\psi_1\rangle, \cdots, |\psi_n\rangle)$ une base orthonormée de $\mathbb{C}^n$ tels que : $A = \sum_{1 \leq i \leq n} \lambda_i |\psi_i\rangle \langle\psi_i|$
Avec ces notations :

(a) $A \succeq 0 \Leftrightarrow \forall i, \lambda_i \geq 0$

(b) On définit $\|A\|_1 = \sum_{1 \leq i \leq n} |\lambda_i|$ la norme trace de A.
$\|.\|$ *est une norme sur $\mathcal{S}_n(\mathbb{C})$*

1.2 Postulats de mécanique quantique

Dans cette section, on va donner 4 postulats de physique quantique qui vont nous permettre de décrire mathématiquement ce qu'est une stratégie quantique pour Alice et Bob. Le postulat 2 est donné à titre informatif puisqu'on ne l'utilisera pas dans la suite.

Postulat 1. *À un système physique, on associe un espace de Hilbert $\mathcal{H}$ appelé l'espace des états. L'état du système à un instant donné est décrit par un vecteur $|\psi\rangle \in \mathcal{H}$ de norme 1.*

Dans la suite des postulats, on considère un système physique décrit par l'espace $\mathcal{H}$.

Postulat 2. *On décrit l'évolution d'un système quantique fermé par une transformation unitaire. Ainsi, si l'on considère deux instants t_1 et t_2, il existe une matrice unitaire U agissant sur $\mathcal{H}$ telle que pour tout état $|\psi\rangle$ du système à l'instant t_1, $U.|\psi\rangle$ décrit le système à l'instant t_2.*

Postulat 3. *Une mesure quantique est décrite par une collection $\{M_m\}_{m \in \Sigma}$ de matrices aggisant sur $\mathcal{H}$. Ces matrices sont appelées opérateurs de mesure et vérifient $\sum_{m \in \Sigma} M_m^\dagger M_m = Id_{\mathcal{H}}$.*
De la mesure d'un état quantique $|\psi\rangle \in \mathcal{H}$ par les opérateurs de mesure $\{M_m\}_{m \in \Sigma}$ résulte une sortie $m \in \Sigma$; le système est alors décrit par un nouveau $|\psi'\rangle \in \mathcal{H}$.
La probabilité que la sortie de la mesure soit m est $p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle$.
De plus, si on suppose que la sortie est m alors $|\psi'\rangle = \frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}$

Il arrive lors d'une mesure que seule la sortie nous intéresse (et non pas l'état du système après la mesure). Dans ce cas, on peut décrire la mesure par les matrices $\{E_m\}_{m \in \Sigma}$ où $E_m = M_m^\dagger M_m$. La collection $\{E_m\}_{m \in \Sigma}$ est appelée POVM (positive operator-valued measure).

Définition 1.5. *Un POVM est une collection $\{E_m\}_{m \in \Sigma}$ de matrices hermitiennes positives sur $\mathcal{H}$ qui vérifient $\sum_{m \in \Sigma} E_m = Id_{\mathcal{H}}$. Un POVM permet de mesurer les états quantiques $|\psi\rangle \in \mathcal{H}$ et donne en sortie un $m \in \Sigma$. La probabilité d'obtenir m est $p(m) = \langle\psi| E_m |\psi\rangle$*

Postulat 4. *On suppose que l'on dispose de deux systèmes physiques ayant pour espaces des états $\mathcal{H}_1$ et $\mathcal{H}_2$. Alors le système global a pour espace des états $\mathcal{H}_1 \otimes \mathcal{H}_2$.*
De plus, si $|\psi_1\rangle \in \mathcal{H}_1$ et $|\psi_2\rangle \in \mathcal{H}_2$ décrivent les deux systèmes, le système global est décrit par $|\psi_1\rangle \otimes |\psi_2\rangle$
On suppose que l'on mesure le premier (resp. second) système à l'aide des opérateurs de mesure $\{M_m\}_{m \in \Sigma}$. La mesure sur le système global est décrite par les opérateurs de mesure $\{M_m \otimes Id_{\mathcal{H}_2}\}_{m \in \Sigma}$ (resp. $\{Id_{\mathcal{H}_1} \otimes M_m\}_{m \in \Sigma}$)

Définition 1.6. *Dans les conditions du postulat 4, un état du système global de la forme $|\psi_1\rangle \otimes |\psi_2\rangle$ est dit produit. Sinon, cet état est dit intriqué.*

Le postulat 4 permet en particulier de décrire comment Alice et Bob peuvent partager un état quantique. En théorie, Alice et Bob pourraient préparer le système global en n'importe quel état $|\psi\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$; puis Alice conserve le système décrit par $\mathcal{H}_1$ et Bob conserve le système décrit par $\mathcal{H}_2$. Même si les deux sous-systèmes sont à distance, le système global reste dans l'état $|\psi\rangle$. Or connaître l'état de Alice d'une part et l'état de Bob d'autre part ne permet pas de décrire entièrement $|\psi\rangle$. C'est cela que l'on appelle un état intriqué.
En fait on verra (dans la section 2.4) que partager un état produit ne donne pas d'avantage à Alice et Bob. Ainsi, l'apport du quantique vient des états intriqués.

2 Définition du problème

Passons maintenant au calcul de la probabilité de succès de Alice et Bob. On garde les notations de l'introduction et on désigne par $\mathcal{I}$, $\mathcal{X}$, $\mathcal{Y}$ et $\mathcal{J}$ les variables aléatoires qui correspondent aux valeurs i, x, y et j.
Pour simplifier les notations, dans les formules on ne précisera pas les ensembles de sommation. Si il n'y a pas de précision, on somme pour $i \in M$, $j \in M$, $x \in X$ et $y \in Y$. On a :

$$\begin{aligned}\mathbb{P}(\text{Succès}) &= \sum_{i,x,y} \mathbb{P}(\mathcal{I}=i, \mathcal{X}=x, \mathcal{Y}=y, \mathcal{J}=i) \\ &= \sum_{i,x,y} \mathbb{P}(\mathcal{I}=i) \times \mathbb{P}(\mathcal{X}=x|\mathcal{I}=i) \times \mathbb{P}(\mathcal{Y}=y|\mathcal{X}=x, \mathcal{I}=i) \\ &\qquad \times \mathbb{P}(\mathcal{J}=i|\mathcal{Y}=y, \mathcal{X}=x, \mathcal{I}=i)\end{aligned}$$

Alice choisit le $i \in M$ à transmettre de manière uniforme, donc $\mathbb{P}(\mathcal{I}=i) = \frac{1}{k}$
La transmission via le canal de communication se traduit par :
$\mathbb{P}(\mathcal{Y}=y|\mathcal{X}=x, \mathcal{I}=i) = \mathbb{P}(\mathcal{Y}=y|\mathcal{X}=x) = W(y|x)$
On a donc :

$$\mathbb{P}(\text{Succès}) = \frac{1}{k} \sum_{i,x,y} W(y|x).\mathbb{P}(\mathcal{X}=x|\mathcal{I}=i).\mathbb{P}(\mathcal{J}=i|\mathcal{Y}=y, \mathcal{X}=x, \mathcal{I}=i)$$

Dans la suite on étudie 3 types de stratégies que peuvent adopter Alice et Bob : les stratégies classiques, quantiques et non-signaling. En particulier, on verra pourquoi les stratégies non-signaling sont plus générales que les stratégies quantiques qui sont elles-même plus générales que les stratégies classiques. Pour autant, les stratégies classiques et non-signaling sont mieux comprises que les stratégies quantiques.
Soit W un canal. On va voir dans la suite qu'une stratégie classique se décrit par un couple (e, d). On note alors $Succ^C(W, k, e, d)$ (au lieu de $\mathbb{P}(\text{Succès})$) la probabilité de succès pour cette stratégie. De même la probabilité de succès d'une stratégie quantique $(\mathcal{H}, |\psi\rangle, E, D)$ sera notée $Succ^Q(W, k, \mathcal{H}, |\psi\rangle, E, D)$ et la probabilité de succès d'une stratégie non-signaling P sera notée $Succ^{NS}(W, k, P)$

2.1 Les stratégies classiques

Le premier cas qui nous intéresse est celui d'une stratégie classique. Dans ce cas, Alice et Bob ne partagent pas de ressource et on rappelle qu'ils ne peuvent pas communiquer.
Les stratégies autorisées pour Alice consistent pour chaque $i \in M$ et $x \in X$ à coder i en x avec une certaine probabilité $e(x|i)$. On décrit donc l'encodage de Alice par une probabilité conditionnelle e vérifiant pour tout i, $\sum_x e(x|i) = 1$.
De même $d(j|y)$ sera la probabilité que Bob décode y en j.
Pour résumer, une stratégie classique est un couple (e, d) de probabilités conditionnelles vérifiant $\forall i \in M, \sum_x e(x|i) = 1$ et $\forall y \in Y, \sum_i e(i|y) = 1$
Pour un tel couple (e, d), on a :

$$\begin{cases} \mathbb{P}(\mathcal{X} = x|\mathcal{I} = i) = e(x|i) \\ \mathbb{P}(\mathcal{J} = i|\mathcal{Y} = y, \mathcal{X} = x, \mathcal{I} = i) = \mathbb{P}(\mathcal{J} = i|\mathcal{Y} = y) = d(i|y) \end{cases}$$

Finalement :

$$\textit{Succ}^C(W, k, e, d) = \frac{1}{k} \sum_{i,x,y} e(x|i).W(y|x).d(i|y)$$

2.2 Les stratégies quantiques

Alice possède un système $\mathcal{A}$ décrit par l'espace de Hilbert $\mathcal{H}$ et Bob un système $\mathcal{B}$ décrit par le même espace $\mathcal{H}$. Ils partagent un état quantique $|\psi\rangle \in \mathcal{H} \otimes \mathcal{H}$.
Pour encoder un message i, Alice dispose d'un POVM $\{E(x|i)\}_{x \in X}$ indicé par X. Elle mesure $\mathcal{A}$ (alors que Bob n'agit pas sur $\mathcal{B}$) et donne en entrée du canal le résultat x de la mesure. La probabilité que le résultat de la mesure soit x est donné par $\mathbb{P}(\mathcal{X} = x|\mathcal{I} = i) = \langle\psi| E(x|i) \otimes Id |\psi\rangle$ d'après le postulat 4.
On notera $|\psi_1(x|i)\rangle$ le nouvel état partagé entre Alice et Bob dans le cas où le résultat de la mesure est x. Lorsque Bob reçoit y, il effectue à son tour une mesure sur $\mathcal{B}$ pour déterminer j. Les POVM utilisés par Bob seront notés $\{D(j|y)\}_{j \in M}$.
On a $\mathbb{P}(\mathcal{J} = i|\mathcal{Y} = y, \mathcal{X} = x, \mathcal{I} = i) = \langle\psi_1(x|i)| Id \otimes D(j|y) |\psi_1(x|i)\rangle$

Calculons la probabilité de succès de Alice et Bob. Pour cela, soient $\{M(x|i)\}_{x \in X}$ les opérateurs de mesure associés à $\{E(x|i)\}_{x \in X}$ (on a $E(x|i) = M(x|i)^\dagger.M(x|i)$). Alors :

$$|\psi_1(x|i)\rangle = \frac{M(x|i) \otimes Id |\psi\rangle}{\sqrt{\langle\psi| E(x|i) \otimes Id |\psi\rangle}}$$

Donc

$$\begin{aligned} \mathbb{P}(\mathcal{J} = i|\mathcal{Y} = y, \mathcal{X} = x, \mathcal{I} = i) &= \langle\psi_1(x|i)| Id \otimes D(j|y) |\psi_1(x|i)\rangle \\ &= \frac{\langle\psi| M(x|i)^\dagger.M(x|i) \otimes D(j|y) |\psi\rangle}{\langle\psi| E(x|i) \otimes Id |\psi\rangle} \\ &= \frac{\langle\psi| E(x|i) \otimes D(i|y) |\psi\rangle}{\langle\psi| E(x|i) \otimes Id |\psi\rangle} \end{aligned}$$

La probabilité de succès est donc égale à :

$$\textit{Succ}^Q(W, k, \mathcal{H}, |\psi\rangle, E, D) = \frac{1}{k} \sum_{i,x,y} W(y|x). \langle\psi| E(x|i) \otimes D(i|y) |\psi\rangle$$

2.3 Les stratégies non-signaling

Ce sont une généralisation des stratégies quantiques dans lesquelles Alice et Bob partagent une boite dite "non-signaling". Ce terme fait référence au fait qu'une telle boite ne leur permet pas de communiquer directement (dans un sens que l'on va préciser). On part de l'observation suivante : l'important dans une stratégie quantique (ou classique) est de connnaitre $\mathbb{P}(\mathcal{X} = x|\mathcal{I} = i)$ et $\mathbb{P}(\mathcal{J} = i|\mathcal{Y} = y, \mathcal{X} = x, \mathcal{I} = i)$, c'est à dire la probabilité que Alice encode i en x, et la probabilité que Bob décode y en j sachant que Alice veut transmettre i et qu'elle l'a encodé en x. Plus précisément, c'est le produit de ces deux valeurs qui nous interesse. Dans le cas quantique, ce produit est égal à $\langle\psi| E(x|i) \otimes D(j|y) |\psi\rangle$. Cette quantité que l'on notera $P(x, j|i, y)$ correspond à une mesure simultanée de l'état $|\psi\rangle$ par Alice et Bob.

Une boite non-signaling est un objet (théorique) possèdant une entrée et une sortie du côté de Alice (resp. Bob). Alice (resp. Bob) peut mettre en entrée de la boite un élément $i \in M$ (resp.

$y \in Y$) et la boite renvoie alors en sortie un élément $x \in X$ (resp. $j \in M$).
Pour comprendre les définitions qui suivent, on décrit ce que représentent intuitivement P, P_A, P_B, P_1 et P_2 :

- $P(x, j|i, y)$ est la probabilité que la boite renvoie x et j si elle a reçu en entrée i et y (ici les requêtes de Alice et Bob se font en simultané)
- $P_A(x|i) = P_1(x|i)$ est la probabilité que la boite donne x à Alice si celle-ci a mis i en entrée (le A de P_A fait référence à Alice)
- $P_B(j|y)$ est la probabilité que la boite donne j à Bob si celui-ci a mis y en entrée (le B de P_B fait référence à Bob)
- $P_2(j|i, x, y)$ est la probabilité que la boite donne j à Bob si celui-ci a mis y en entrée, que Alice a mis x en entrée et qu'elle a reçu i en sortie (donc ici, la requête de Bob se fait après celle de Alice).

On donne deux définitions alternatives d'une boite "non-signaling". La définition 2.1 est donnée à titre indicatif car elle est plus intuitive dans notre cas. La définition 2.2 est la définition usuelle.

Définition 2.1. *Une stratégie non-signaling est décrite par un couple (P_1, P_2) tel que :*

- *P_1 et P_2 sont des probabilités conditionnelles :*
  $\forall i, \sum_x P_1(x|i) = 1$, $\forall (i, x, y), \sum_j P_2(j|i, x, y) = 1$ et $0 \leq P_1, P_2 \leq 1$.
- *Si on définit la probabilité conditionnelle $P(x, j|i, y) = P_1(x|i) \times P_2(j|i, x, y)$ alors :*
  $\sum_x P(x, j|i, y)$ ne dépend pas de i. C'est à dire qu'il existe une probabilité conditionnelle P_B telle que $\sum_x P(x, j|i, y) = P_B(j|y)$ pour tout i

Définition 2.2. *Une boite non-signaling est décrite par P où :*

- *P est une probabilité conditionnelle :*
  $\forall (i, y), \sum_{x,j} P(x, j|i, y) = 1$ et $0 \leq P \leq 1$.
- *$\sum_x P(x, j|i, y)$ ne dépend pas de i. C'est à dire qu'il existe une probabilité conditionnelle P_B telle que $\sum_x P(x, j|i, y) = P_B(j|y)$ pour tout i*
- *$\sum_j P(x, j|i, y)$ ne dépend pas de y. C'est à dire qu'il existe une probabilité conditionnelle P_A telle que $\sum_j P(x, j|i, y) = P_A(x|i)$ pour tout y*

Soit P une boite non-signaling. Le protocole que vont adopter Alice et Bob est le suivant :
Lorsque Alice veut envoyer i à Bob :

- Alice fait une requête i à la boite qui renvoie x avec probabilité $P_1(x|i)$
- Alice transmet x à Bob qui reçoit y via le canal
- Bob fait une requête y à la boite qui renvoie j avec probabilité $P_2(j|i, x, y)$.

On peut alors calculer la probabilité de succès :

$$\begin{aligned} \mathit{Succ}^{NS}(W, k, P) &= \frac{1}{k} \sum_{i,x,y} W(y|x) \times \mathbb{P}(\mathcal{X} = x|\mathcal{I} = i) \times \mathbb{P}(\mathcal{J} = i|\mathcal{Y} = y, \mathcal{X} = x, \mathcal{I} = i) \\ &= \frac{1}{k} \sum_{i,x,y} W(y|x) \times P_1(x|i) \times P_2(i|i, x, y) \\ &= \frac{1}{k} \sum_{i,x,y} W(y|x) \times P(x, i|i, y) \end{aligned}$$

2.4 Liens entre les différentes stratégies

Dans ce chapitre, on va voir le lien entre les différentes stratégies. Tout d'abord, on va voir pourquoi les stratégies non-signaling englobent les stratégies classiques et quantiques. On va décrire ces deux dernières à l'aide de la définition 2.2 :

- Soit (e, d) une stratégie classique. La stratégie non-signaling correspondante est définie par $P(x, j|i, y) = e(x|i) \times d(j|y)$. On peut facilement vérifier que P décrit bien une stratégie non-signaling (en particulier $P_A = e$ et $P_B = d$)
- Soit $(\mathcal{H}, |\psi\rangle, E, D)$ une stratégie quantique. La stratégie non-signaling correspondante est définie par $P(x, j|i, y) = \langle\psi| E(x|i) \otimes D(j|y) |\psi\rangle$.
  Ici, $P_A(x|i) = \langle\psi| E(x|i) \otimes Id_{\mathcal{H}} |\psi\rangle$ et $P_B(j|y) = \langle\psi| Id_{\mathcal{H}} \otimes D(j|y) |\psi\rangle$

Le plus simple pour montrer que deux stratégies sont équivalentes est de les exprimer dans le même formalisme (en l'occurence on va utiliser le formalisme non-signaling). Ainsi, deux stratégies sont équivalentes lorsque les stratégies non-signaling correspondantes sont égales. En particulier, on remarque que cela implique que les probabilités de succès des deux stratégies sont les mêmes.

- Par exemple, on peut simuler une stratégie classique avec une stratégie quantique. Soit (e, d) une stratégie classique et $P^C(x, j|i, y) = e(x|i) \times d(j|y)$ la stratégie non-signaling correspondante. En utilisant un état quantique $|\psi\rangle$ quelconque, Alice et Bob peuvent créer un générateur aléatoire qui leur permet de mettre en place la stratégie (e, d).
  Il suffit de considérer la stratégie quantique (E, D) où $E(x|i) = e(x|i).Id_{\mathcal{H}}$ et $D(x|i) = d(x|i).Id_{\mathcal{H}}$. On note P^Q la stratégie non-signaling correspondante. Alors :

$$\begin{aligned} P^Q(x, j|i, y) &= \langle\psi| E(x|i) \otimes D(j|y) |\psi\rangle \\ &= e(x|i) \times d(i|y) \times \langle\psi| Id_{\mathcal{H}} \otimes Id_{\mathcal{H}} |\psi\rangle \\ &= e(x|i) \times d(i|y) \\ &= P^C(x, j|i, y) \end{aligned}$$

  Donc $P^Q = P^C$ et les deux stratégies sont équivalentes. Ainsi toute stratégie classique peut être simulée par une stratégie quantique.

- Dans ce point, on va montrer que l'apport des stratégies quantique est dû à l'utilisation des état intriqués. C'est à dire qu'utiliser un état produit correspond à une stratégie classique. Soit $(\mathcal{H}, |\psi_A\rangle \otimes |\psi_B\rangle, E, D)$ une stratégie quantique dans laquelle l'état utilisé par Alice et Bob est un état produit. On note P^Q la stratégie non-signaling correspondante. On définit (e, d) une stratégie classique par $e(x|i) = \langle\psi_A| E(x|i) |\psi_A\rangle$ et $d(j|y) = \langle\psi_B| D(j|y) |\psi_B\rangle$. Soit P^C la stratégie non-signaling correspondante :

$$\begin{aligned} P^Q(x, j|i, y) &= \langle\psi_A, \psi_B| E(x|i) \otimes D(j|y) |\psi_A, \psi_B\rangle \\ &= \langle\psi_A| E(x|i) |\psi_A\rangle \times \langle\psi_B| D(j|y) |\psi_B\rangle \\ &= e(x|i) \times d(i|y) \\ &= P^C(x, j|i, y) \end{aligned}$$

Pour résumer ce chapitre, Alice et Bob ont accès à trois types de stratégies. Les stratégies classiques correspondent à l'utilisation d'un générateur aléatoire ; les stratégies quantique supposent que Alice et Bob sont capables de maintenir des états quantiques intactes (ce qui n'est pas le cas en pratique à cause de la décorrélation) ; enfin les stratégies non-signaling sont un outil pratique d'un point de vue mathématique mais que l'on ne peut pas implémenter en pratique.
Le chapitre suivant, regroupe quelques propriétés de ces stratégies.

3 Résultats connus

Pour les 3 types de stratégies, le but est de trouver la stratégie qui maximise la probabilité de succès. On notera $S^C(W,k)$ cette probabilité maximale pour les stratégies classiques, $S^Q(W,k)$ pour les stratégies quantiques et $S^{NS}(W,k)$ pour les stratégies non-signaling. On exprime ces trois valeurs sous la forme de problèmes de maximisation.

Définition 3.1.

$$
\begin{aligned}
S^C(W,k) = \underset{e,d}{\textit{Maximize}} \quad & \frac{1}{k}\sum_{i,x,y} e(x|i).W(y|x).d(i|y) \\
\textit{Subject to} \quad & \sum_x e(x|i) = 1 \qquad \forall i \\
& \sum_j d(j|y) = 1 \qquad \forall y \\
& 0 \leq e(x|i) \leq 1 \qquad \forall (i,x) \\
& 0 \leq d(j|y) \leq 1 \qquad \forall (y,j)
\end{aligned}
$$

Définition 3.2.

$$
\begin{aligned}
S^Q(W,k) = \underset{\mathcal{H},\psi,E,D}{\textit{Maximize}} \quad & \frac{1}{k}\sum_{i,x,y} W(y|x).\left\langle \psi \right| E(x|i) \otimes D(i|y) \left| \psi \right\rangle \\
\textit{Subject to} \quad & \sum_x E(x|i) = Id_{\mathcal{H}} \qquad \forall i \\
& \sum_j D(j|y) = Id_{\mathcal{H}} \qquad \forall y \\
& 0 \preceq E(x|i) \preceq Id_{\mathcal{H}} \qquad \forall (i,x) \\
& 0 \preceq D(j|y) \preceq Id_{\mathcal{H}} \qquad \forall (y,j)
\end{aligned}
$$

Définition 3.3.

$$
\begin{aligned}
S^{NS}(W,k) = \underset{P,P_A,P_B}{\textit{Maximize}} \quad & \frac{1}{k}\sum_{i,x,y} W(y|x).P(x,i|i,y) \\
\textit{Subject to} \quad & \sum_x P(x,j|i,y) = P_B(j|y) \qquad \forall (i,y,j) \\
& \sum_j P(x,j|i,y) = P_A(x|i) \qquad \forall (i,x,y) \\
& \sum_{x,j} P(x,j|i,y) = 1 \qquad \forall (i,y) \\
& 0 \leq P(x,j|i,y) \qquad \forall (i,x,y,j)
\end{aligned}
$$

3.1 Caractérisations des probabilités de succès

La proposition suivante exprime trois propriétés intéressantes concernant les stratégies classiques. On peut en trouver la preuve dans [1].

Proposition 3.4.

(i) On pose $l = Min(k, |X|)$*, alors :*

$$S^C(W,k) = \frac{1}{k} \quad \underset{S\subseteq X,|S|=l}{Max} \sum_y \underset{x\in S}{Max}\, W(y|x)$$

(ii) Il existe un algorithme polynomial glouton qui calcule un stratégie classique (e,d) *telle que* $(1-e^{-1})S^C(W,k) \leq Succ^C(W,k,e,d)$

(iii) Si $P \neq NP$*, il n'existe pas d'algorithme polynomial donnant une* $(1-e^{-1}+\epsilon)$ *approximation pour* $\epsilon > 0$

Le point (i) exprime le fait qu'il existe une stratégie classique optimale qui est déterministe. Pour la construire, on choisit un S optimal dans la formule de (i) puis on fait correspondre à chaque $i \in M$ un élément $x_i \in S$. Alice encode alors i en x_i et Bob décode y par le i tel que x_i maximise $x \mapsto W(y|x)$.
Les points (ii) et (iii) signifient que de manière polynomiale, on peut au mieux créer une $(1-e^{-1})$ approximation de la stratégie optimale. Un algorithme glouton qui y parvient construit S de la manière suivante :

- On part de $S_0 = \emptyset$
- $S_{i+1} = S_i \cup \{x_{i+1}\}$ où x_{i+1} maximise $x \mapsto \sum_y \underset{x\in(S_i\cup\{x\})}{Max} W(y|x)$
- On prend $S = S_l$ et on construit (e,d) suivant l'explication précédente.

Passons maintenant aux stratégies non-signaling.
Leur intéret est qu'elles contiennent les stratégies quantiques mais sont plus simples à étudier. Pour le problème qui nous intéresse dans ce rapport, $S^{NS}(W,k)$ est la valeur d'un programme d'optimisation linéaire. En particulier, on peut le calculer de manière efficace. La proposition suivante a été montrée dans [5].

Proposition 3.5.

$$\begin{aligned} S^{NS}(W,k) = \underset{r_{x,y},p_x}{\textit{Maximize}} \quad & \frac{1}{k}\sum_{x,y} W(y|x).r_{x,y} & \\ \textit{Subject to} \quad & \sum_x r_{x,y} \leq 1 & \forall y \\ & \sum_x p_x = k & \\ & r_{x,y} \leq p_x & \forall (x,y) \\ & 0 \leq r_{x,y}, p_x \leq 1 & \forall (x,y) \end{aligned}$$

Ce programme linéaire est connu comme le "Polyanskiy-Poor-Verdu meta-converse"

L'étude du cas quantique est plus compliquée, on va suivre le raisonnement de [2] et [7]. Une des caractérisations possible de $S^Q(W,k)$ est de l'exprimer comme la limite d'une suite réelle dont chaque élément est la valeur d'un sdp (semi-definite programm). Les sdp sont une généralisation des programmes d'optimisation linéaire (on peut notamment les résoudre en temps polynomial). Pour exprimer ces sdp, on va considérer des matrices indicées sur des mots.

Notations 3.6.

- *On pose $N = k.n$ et $M = k.m$*
- *On identifie le couple (x, i) à un élément de $[\![1; N]\!]$ noté $\boldsymbol{(x, i)}$ (en gras) et le couple (i, y) à un élément de $[\![1; M]\!]$ noté $\boldsymbol{(i, y)}$*
- *$\Sigma = \{z_1, \cdots, z_N, y_1, \cdots, y_M\}$ un alphabet de $(N + M)$ lettres ; Σ^* les mots sur l'alphabet Σ et ϵ le mot vide*
- *On pose $w_0 = \epsilon$, $w_i = z_i$ pour $i \in [\![1, N]\!]$ et $w_{j+N} = y_j$ pour $i \in [\![1, M]\!]$.*
- *$\circ$ est la concatenation de mots*

De manière informelle on peut caractériser $S^Q(W, k)$ comme la valeur d'un sdp ayant une infinité de contraintes :

$$
\begin{aligned}
S^Q(W,k) = \underset{\Omega}{\text{Maximize}} \quad & \frac{1}{k}\sum_{i,x,y} W(y|x).\Omega_{w_{(\boldsymbol{x},\boldsymbol{i})},w_{(\boldsymbol{i},\boldsymbol{y})}} \\
\text{Subject to} \quad & \Omega \succeq 0 \\
& \Omega_{\epsilon,\epsilon} = 1 \\
& \Omega_{r\circ s,w} = \sum_{x\in X} \Omega_{r\circ w_{(\boldsymbol{x},\boldsymbol{i})}\circ s,w} \qquad \forall i \in [\![1;k]\!], \forall r,s,w \in \Sigma^* \\
& \Omega_{r\circ s,w} = \sum_{i\in[\![1;k]\!]} \Omega_{r\circ w_{(\boldsymbol{i},\boldsymbol{y})}\circ s,w} \qquad \forall y \in Y, \forall r,s,w \in \Sigma^* \\
& 0 \preceq \sum_{r,s,u,v\in\Sigma^*} \Omega_{r^*\circ w_{\gamma_1}\circ s,u^*\circ w_{\gamma_2}\circ v} \quad \forall \gamma_1,\gamma_2 \in [\![1; N+M]\!]
\end{aligned}
$$

Ce problème d'optimisation a un nombre infini de contraintes d'une part car la matrice Ω est une matrice infinie et d'autre part à cause des conditions $\forall r, s, w \in \Sigma^*$.
On créé donc une hiérarchie de sdp. C'est à dire que l'on va considérer des ensembles I_n finis tels que $(\{\epsilon\} \cup \Sigma) \subseteq I_n \subseteq I_{n+1} \subseteq \Sigma^*$ et $\bigcup_n I_n = \Sigma^*$ (par exemple prendre I_n l'ensemble des mots de taille inférieure à n).
On définit alors pour tout n un sdp noté sdp_n comme suit :
On maximise sur une matrice Ω^n dont les lignes et les colonnes sont indicées par I_n (Ω^n correspond en fait à la restriction de Ω à I_n). On remplace alors dans le problème d'optimisation Ω par Ω^n et dans les trois dernières lignes, on ne garde que les conditions qui ont un sens (par exemple on doit avoir $w \in I_n$ au lieu de $w \in \Sigma^*$ pour que w soit un indice de la matrice Ω^n).
Si on note S_n la valeur de sdp_n, la suite $(S_n)_n$ est décroissante et tend vers $S^Q(W, k)$. En particulier, pour tout n, $S_n \geq S^Q(W, k)$ ce qui permet de calculer des bornes supérieures pour $S^Q(W, k)$.

3.2 Majoration des probabilités de succès

Le gain apporté par l'utilisation des stratégies non-signaling (et donc quantiques) par rapport aux stratégies classiques peut être borné (voir [1] et [4]).

Proposition 3.7.

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

Le deuxième point concerne le gain de biais qu'apporte les stratégies non-signaling. Le biais se défini comme l'écart entre la probabilité de succès de la stratégie et celle de la stratégie triviale (une stratégie triviale a pour probabilité de succès $1/k$, par exemple Bob décode tout y en 0). Une fois ces deux bornes établies, on se demande si elles sont atteintes. Le "subset channel" est un canal de communication qui y parvient.

3.3 Le "subset channel"

On s'interresse ici à un canal particulier : le "subset channel" que l'on notera W_t^n où $1 \leq t \leq n$. Il est caractérisé par $X = [\![0; n-1]\!]$ et $Y = \binom{\mathbf{n}}{\mathbf{t}}$. Le cardinal de Y est donc $m = \binom{n}{t}$. Pour une entrée x, la sortie de W_t^n est un élement choisi uniformément dans $\{y \in Y | x \in y\}$. Ainsi :

$$\begin{cases} W(y|x) = \frac{1}{\binom{n-1}{t-1}} \text{ si } x \in y \\ W(y|x) = 0 \text{ sinon} \end{cases}$$

Lorsque Bob reçoit $y = \{x_1, \cdots, x_t\}$ via le canal, il sait que Alice a voulu lui transmettre l'un des x_i. Le paramètre t représente donc la quantité de bruit du canal. En particulier, il est facile de montrer que pour toute stratégie non-signaling P, $Succ^{NS}(W_n^n, P) = 1/2$ et que si $n \geq k$ alors $S^C(W_1^n, k) = 1$

L'un des intérêts du subset channel est que c'est un exemple concret de canal pour lequel $S^C(W, k) < S^Q(W, k) < S^{NS}(W, k)$. Il permet également de montrer que les bornes de la proposition 3.7 sont atteintes.

Proposition 3.8. *Soient n, t alors :*

(i) Avec $l = Min(k, n)$:

$$S^C(W_t^n, k) = \frac{n}{k.t} \cdot \left(1 - \frac{\binom{n-l}{t}}{\binom{n}{t}}\right)$$

(ii) Si $n \geq 2$:

$$S^C(W_t^n, 2) = \frac{1}{2} + \frac{\binom{n-2}{t-1}}{2\binom{n-1}{t-1}}$$

(iii) Si $k.t \leq n$:

$$S^{NS}(W_t^n, k) = 1$$

Pour montrer ces valeurs, on utilise les caractérisations de $S^C(W_t^n, k)$ et $S^{NS}(W_t^n, k)$ des propositions 3.4 et 3.5.

Si on évalue la probabilité de (i) dans le cas particulier où $n = k.t$, on obtient une expression qui tend vers $\left(1 - \left(1 - \frac{1}{k}\right)^k\right)$ quand t tend vers $+\infty$. En combinant avec (ii), on montre que les bornes de la proposition 3.7 sont atteintes.

Pour résumer, on est capable de donner une borne sur le gain des stratégies non-signaling et cette borne est atteinte pour le subset channel. Ainsi cette borne est optimale pour les stratégies non-signaling. Le but de mon stage est de voir si on peut montrer des propriétés similaires pour les stratégies quantiques.

4 Mon travail

Durant mon stage j'ai étudié le subset-channel W_t^n en détail. Dans toute la suite, on fixe $k = 2$ (c'est à dire que Alice veut envoyer un bit à Bob). Plutôt que d'étudier directement $S^Q(W_t^n, k)$,

on va fixer $\mathcal{H}$ et $|\psi\rangle \in \mathcal{H}$ et s'intérésser à deux valeurs : $Succ_B^Q(W_t^n, E)$ et $Succ_{A,B}^Q(W_t^n)$. $Succ_{A,B}^Q(W_t^n)$ est défini comme la probabilité de succès maximale lorsque Alice et Bob partagent l'état $|\psi\rangle$ (le A, B en indice fait référence au fait que l'on optimise les stratégies de Alice et de Bob). $Succ_B^Q(W_t^n, E)$ est la probabilité de succès maximale lorsque l'on a fixé une stratégie E pour Alice (le B en indice fait référence au fait que l'on optimise la stratégie de Bob).
Dans un premier temps, j'ai étudié la dépendance de ces valeurs en n et t. Elles sont en fait décroissantes en t et croissantes en n. Le gain du biais par rapport aux stratégies classiques est également intéressant à étudier. Intuitivement, le gain de biais quantifie l'intérêt d'utiliser la stratégie quantique par rapport à la stratégie classique optimale.
Dans un deuxième temps, j'ai étudié $Succ_B^Q(W_t^n, E_U)$ dans le cas où $\mathcal{H}$ est de dimension n, $|\psi\rangle = |\phi\rangle$ est l'état maximalement intriqué et E_U est déterminé par une matrice unitaire U. $Succ_B^Q(W_t^n, E_U)$ peut alors s'exprimer à l'aide de la norme trace $\|.\|_1$ et de plus, $Succ_{A,B}^Q(W_t^n)$ revient à une maximisation sur l'ensemble des matrices unitaires. Ainsi, j'ai pu m'aider de l'outil informatique pour essayer de comprendre la situation. De plus, il est intéréssant de noté qu'il existe une stratégie E_U qui est optimale parmi les stratégies quantiques pour $n = 4$ et $t = 2$.
Dans un soucis de formalisme, on rappelle les stratégies autorisées pour Alice et Bob :

Notations 4.1.

- *On note $\mathcal{E}_n$ les stratégies d'encodage de Alice, qui est l'ensemble des fonctions $E : [\![0; n-1]\!] \times [\![0; 1]\!] \to \mathcal{M}_{dim(\mathcal{H})}(\mathbb{C})$ telles que :*

$$\begin{cases} E(x|i) \text{ est hermitienne} & \forall (i,x) \in [\![0;1]\!] \times [\![0;n-1]\!] \\ \sum_{x=0}^{n-1} E(x|i) = Id_{\mathcal{H}} & \forall i \in [\![0;1]\!] \\ 0_{\mathcal{H}} \preceq E(x|i) \preceq Id_{\mathcal{H}} & \forall (i,x) \in [\![0;1]\!] \times [\![0;n-1]\!] \end{cases}$$

- *On note $\mathcal{D}_{n,t}$ les stratégies de décodage de Bob, qui est l'ensemble des fonctions $D : [\![0; 1]\!] \times \binom{\mathbf{n}}{\mathbf{t}} \to \mathcal{M}_{dim(\mathcal{H})}(\mathbb{C})$ telles que :*

$$\begin{cases} D(j|y) \text{ est hermitienne} & \forall (y,j) \in \binom{\mathbf{n}}{\mathbf{t}} \times [\![0;1]\!] \\ \sum_{j=0}^{1} D(j|y) = Id_{\mathcal{H}} & \forall y \in \binom{\mathbf{n}}{\mathbf{t}} \\ 0_{\mathcal{H}} \preceq D(j|y) \preceq Id_{\mathcal{H}} & \forall (y,j) \in \binom{\mathbf{n}}{\mathbf{t}} \times [\![0;1]\!] \end{cases}$$

- *Pour $E \in \mathcal{E}_n$ et $D \in \mathcal{D}_{n,t}$, on notera $Succ^Q(W_t^n, E, D)$ pour $Succ^Q(W_t^n, 2, \mathcal{H}, |\psi\rangle, E, D)$*

Les démonstrations des propositions qui suivent sont laissées en annexe.

4.1 Influence des paramètres du subset channel

Définition 4.2. *On pose :*

(i) $Succ_B^Q(W_t^n, E) = \underset{D \in \mathcal{D}_{n,t}}{Max} \left(Succ^Q(W_t^n, E, D) \right)$

(ii) $Succ_{A,B}^Q(W_t^n) = \underset{E \in \mathcal{E}_n}{Max} \left(Succ_B^Q(W_t^n, E) \right)$

(iii) On suppose que p est la probabilité de succès de Alice et Bob pour une certaine stratégie. On définit alors le gain du biais de cette stratégie par rapport à une stratégie classique par :
$biais(W_t^n, p) = \dfrac{p - 1/2}{S^C_{A,B}(W_t^n) - 1/2}$

(iv) Pour simplifier les notations :
$biais^Q(W, E, D) = biais(W, Succ^Q(W, E, D))$
$biais^Q_B(W, E) = biais(W, Succ^Q_B(W, E))$
$biais^Q_{A,B}(W) = biais(W, Succ^Q_{A,B}(W))$

Proposition 4.3. *Soient $n \in \mathbb{N}^*$ et $t \in [\![1; n]\!]$. Alors :*

(i) $t \mapsto Succ_B(W_t^n, E)$ *et* $t \mapsto Succ_{A,B}(W_t^n)$ *sont décroissants*

(ii) $n \mapsto Succ_{A,B}(W_t^n)$ *est croissant*

(iii) $biais^Q_B(W^n_{n-t}, E) = biais^Q_B(W_t^n, E)$ *et* $biais^Q_{A,B}(W^n_{n-t}) = biais^Q_{A,B}(W_t^n)$

Démonstration. On donne ici une preuve informelle. La preuve détaillée est donnée en annexe.

(i) Ce point traduit simplement le fait que plus le paramètre t est grand, plus la sortie du canal est bruitée. Il est donc plus dur pour Bob de retrouver le message qu'a voulu lui envoyer Alice.
Pour le démontrer, on part d'une stratégie E de Bob pour le canal W_n^t et on en créé une pour le canal W_n^{t+1} :
dans le cas $t + 1$, Bob reçoit en sortie du canal un ensemble $y \in \binom{\mathbf{n}}{\mathbf{t+1}}$. Il lui suffit alors de supprimer l'un des éléments $x \in y$ de l'ensemble y et d'appliquer la stratégie E à $y \setminus \{x\}$. Choisir l'élément à supprimer de manière uniforme permet de montrer le point (i).

(ii) Cela vient du fait que plus n est grand, plus Alice a de choix pour coder le bit qu'elle veut envoyer. La différence entre W_t^n et W_t^{n+1} est que Alice peut envoyer le message n via le canal W_t^{n+1} et pas via le canal W_t^n.
À partir d'une stratégie (E, D) pour le canal W_t^n, on en créé une pour le canal W_t^{n+1} de la manière suivante :
Alice ne change pas de stratégie dans le sens où elle encode ses messages de la même façon que pour le canal W_t^n et n'utilise jamais le message n. Lorsque Bob reçoit la sortie y du canal, si $n \in y$ alors il sait que Alice n'a pas voulu lui transmettre n et peut donc considérer qu'il a reçu $y \setminus \{n\}$ (qui est plus facile à décoder que y d'après le point (i)). Dans le cas où $n \notin y$, il applique la stratégie D directement.

□

L'étude de certaines stratégies particulières (notamment le (iv) de la proposition 4.12) laisse penser que, en plus de la propriété de symétrie exprimée par (iii), $biais^Q_B(W_n^t, E)$ est croissante sur $[\![0; \lfloor \frac{n}{2} \rfloor]\!]$ et décroissante sur $[\![\lfloor \frac{n}{2} \rfloor ; n]\!]$ (un peu à la manière de $t \mapsto \binom{n}{t}$). Cela voudrait dire que l'apport des stratégies quantiques est maximal pour $t = \lfloor \frac{n}{2} \rfloor$
Si Bob se comporte comme dans le point (i), cela ne suffit pas pour montrer cette conjecture. Une façon plus efficace serait que Bob choisisse le x à supprimer de y non pas uniformément mais de manière déterministe (il supprime le x qui augmente le plus la probabilité de succès). Je n'ai pas réussi à montrer cette propriété.

4.2 Étude d'une stratégie quantique particulière

Dans cette section, on étudie un type particulier de stratégies pour le canal W_t^n. On garde $k = 2$, on prend $\mathcal{H}$ de dim n et $|\psi\rangle = |\phi\rangle = \frac{1}{\sqrt{n}} . \sum_{i \in [\![0;n-1]\!]} |i\rangle \otimes |i\rangle$ l'état maximalement

intriqué.
Pour une matrice unitaire U, on définit la stratégie E_U suivante pour Alice :

$$\forall x \in [\![0; n-1]\!] \qquad \begin{cases} E_U(x|0) = |x\rangle \langle x| \\ E_U(x|1) = U |x\rangle \langle x| U^\dagger \end{cases}$$

Pour simplifier les notations, on pose $\mathit{Succ}_B^Q(W_t^n, U) = \mathit{Succ}_B^Q(W_t^n, \mathcal{H}, |\phi\rangle, E_U)$ et $\mathit{biais}_B^Q(W_t^n, U) = \mathit{biais}_B^Q(W_t^n, \mathcal{H}, |\phi\rangle, E_U)$
$\mathit{Succ}_B^Q(W_t^n, U)$ représente donc la probabilité de succès maximale lorsque Alice utilise la stratégie E_U.
L'idée dans la suite est que l'on va être capable dans certains cas de donner explicitement la probabilité de succès. On traite notamment le cas de matrices avec beaucoup de 0.

Proposition 4.4. *Si on pose* $\Gamma_y = \sum_{x \in y} |x\rangle \langle x|$ *alors :*

$$\mathit{Succ}_B^Q(W_t^n, U) = \frac{1}{2} + \frac{1}{4.n.\binom{n-1}{t-1}} \sum_{y \in \binom{\mathbf{n}}{\mathbf{t}}} \left\| \Gamma_y - U \Gamma_y U^\dagger \right\|_1$$

L'intérêt de cette expression est que la norme trace peut se calculer dans des cas particuliers (numériquement ou de manière exacte). On peut de plus implémenter un algorithme d'optimisation qui recherche pour n et t fixés la matrice unitaire qui maximise $\mathit{Succ}_B^Q(W_t^n, U)$. C'est ce qui est fait dans le fichier matlab issu de [1].

Exemple 4.5. *Pour* $n \in \{4, 6, 8\}$ *et* $t = \frac{n}{2}$*, l'algorithme matlab renvoie comme matrices optimales les matrices* U_n^* *suivantes :*

$$U_4^* = \frac{1}{\sqrt{3}} \begin{pmatrix} 0 & -1 & 1 & 1 \\ -1 & 0 & 1 & -1 \\ -1 & 1 & 0 & 1 \\ 1 & -1 & -1 & 0 \end{pmatrix} \quad U_6^* = \frac{1}{\sqrt{5}} \begin{pmatrix} 0 & 1 & 1 & 1 & -1 & 1 \\ -1 & 0 & -1 & -1 & -1 & 1 \\ 1 & 1 & 0 & -1 & -1 & -1 \\ -1 & -1 & 1 & 0 & -1 & -1 \\ -1 & 1 & -1 & 1 & 0 & -1 \\ 1 & -1 & -1 & 1 & -1 & 0 \end{pmatrix}$$

$$U_8^* = \frac{1}{\sqrt{7}} \begin{pmatrix} 0 & -1 & -1 & 1 & -1 & -1 & 1 & 1 \\ -1 & 0 & 1 & 1 & -1 & 1 & -1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 0 & 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & -1 & 0 & 1 & -1 & 1 \\ -1 & -1 & 1 & -1 & 1 & 0 & 1 & 1 \\ -1 & -1 & -1 & 1 & 1 & 1 & 0 & -1 \\ 1 & -1 & 1 & 1 & 1 & -1 & -1 & 0 \end{pmatrix}$$

Le cas $n = 4$ *est particulièrement intéressant. En effet* $\mathit{Succ}_B^Q(W_t^n, U_4^*)$ *correspond exactement à la valeur de* sdp_1 *(défini dans la section 3.1). Cela signifie que cette stratégie est optimale parmi toutes les stratégies quantiques (et pas seulement celles décrites par une matrice unitaire et l'état* $|\phi\rangle$*).*

Pour une matrice U, plusieurs opérations élémentaires sur la matrice ne changent pas la probabilité de succès :

Appliquer une permutation σ simultanément aux lignes et aux colonnes de U, multiplier des lignes et/ou des colonnes par -1, transposer U, en prendre la matrice conjuguée.

Proposition 4.6. *On a les invariances suivantes :*

(i) $Succ_B^Q(W_t^n, U) = Succ_B^Q(W_t^n, P_{\sigma^{-1}}.U.P_\sigma)$ *pour* σ *une permutation*

(ii) $Succ_B^Q(W_t^n, J_1.U.J_2) = Succ_B^Q(W_t^n, U)$ *où* J_1 *et* J_2 *sont des matrices diagonales avec des* 1 *et des* -1 *sur la diagonale.*

(iii) $Succ_B^Q(W_t^n, U^T) = Succ_B^Q(W_t^n, \bar{U}) = Succ_B^Q(W_t^n, U)$

Les matrices unitaires les plus simples auquelles on peut penser sont les matrices n'ayant qu'une entrée non nulle par colonne. Ce sont en fait des matrices de permutations dans lesquelles on a remplacé des 1 par des -1. Par (ii) de la proposition 4.6, ce cas se ramène à étudier les matrices de permutation.

Proposition 4.7. *On note* f_σ *le nombre de points fixes de la permutation* σ*. Alors :*

$$Succ_B^Q(W_t^n, P_\sigma) = \frac{1}{2} + \frac{\binom{n-2}{t-1}}{2.n.\binom{n-1}{t-1}}(n - f_\sigma)$$

Cette probabilité est maximisée lorsque $f_\sigma = 0$, c'est à dire lorsque σ n'a pas de point fixe. Dans ce cas :

$$Succ_B^Q(W_t^n, P_\sigma) = \frac{1}{2} + \frac{\binom{n-2}{t-1}}{2.\binom{n-1}{t-1}} = S^C(W_t^n, 2)$$

Des matrices un peu plus compliquées sont des matrices unitaires qui ont deux entrées non nulles par colonne.

Notations 4.8. *On note* $\mathcal{Z}_n$ *l'ensemble des matrices de* $\mathcal{M}_n(\mathbb{C})$ *unitaires de la forme* $\frac{1}{\sqrt{2}}M_1$ *où* M_1 *est une matrice avec des* 0*,* 1 *et* -1 *et exactement deux coefficients non nuls par colonne.*

Exemple 4.9.

- *La matrice de Hadamard :* $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \in \mathcal{Z}_2$
- $U_{\mathcal{Z}_{2n}} = \begin{pmatrix} \boxed{H} & & & \\ & \boxed{H} & 0 & \\ & & \ddots & \\ & 0 & & \boxed{H} \\ & & & & \boxed{H} \end{pmatrix} \in \mathcal{Z}_{2n}$

En fait, toutes les matrices de $\mathcal{Z}_n$ peuvent être obtenues à partir de la matrice $U_{\mathcal{Z}_n}$ de l'exemple précédent en lui appliquant une permutation sur les lignes, une permutation sur les colonnes et en multipliant certaines lignes et colonnes par -1. C'est ce qu'exprime la proposition suivante.

Proposition 4.10. *Soit* $U \in \mathcal{Z}_n$ *alors* n *est pair et :*
$U = L.P_{\sigma_1}.U_0.P_{\sigma_2}.C$*. Avec* L *et* C *des matrices diagonales avec des 1 et* -1 *sur la diagonale ;* σ_1*,* σ_2 *des permutations et* $U_{\mathcal{Z}_n}$ *la matrice de l'exemple 4.9.*
De plus, $Succ_B^Q(W_t^n, U) = Succ_B^Q(W_t^n, P_\sigma.U_{\mathcal{Z}_n})$ *avec* $\sigma = \sigma_2^{-1} \circ \sigma_1$

La matrice $U_{\mathcal{Z}_n}$ est diagonale par blocs avec des blocs de taille 2×2. On va revenir à cet exemple plus loin, mais pour l'instant on considère un cas plus général. Soit $U_d \in \mathcal{M}_d(\mathbb{C})$ et $U_0 = Id_{\frac{n}{d}} \otimes U_d \in \mathcal{M}_n(\mathbb{C})$ qui est une matrice diagonale par blocs avec tous les blocs égaux à U_d. On va donner un moyen de calculer la probabilité de succès d'une matrice $P_\sigma U_0$. On dira qu'une matrice $M \in \mathcal{M}_n(\mathbb{C})$ est diagonale par blocs $d \times d$ si c'est une matrice diagonale par blocs et que chacun de ses blocs est une matrice de $\mathcal{M}_d(\mathbb{C})$.

Remarque 4.11.

- *Dans ces conditions, $d \mid n$ et M possède $\dfrac{n}{d}$ blocs.*
- *Soit H la matrice de Hadamard, alors la matrice $U_{\mathcal{Z}_{2n}} = Id_n \otimes H$ est la matrice de l'exemple 4.9.*
- *Plus généralement, si $U_d \in \mathcal{M}_d(\mathbb{C})$ alors $(Id_{\frac{n}{d}} \otimes U_d) \in \mathcal{M}_n(\mathbb{C})$ est diagonale par blocs $d \times d$ et tous ses blocs sont égaux à U_d.*
- *Dans la suite, on s'intéresse à des matrices de la forme $P_\sigma.(Id_{\frac{n}{d}} \otimes U_d)$*

La proposition qui suit montre que si on connait les 4^d valeurs $\left\|\Gamma_{y_1} - U_d.\Gamma_{y_2}.U_d^\dagger\right\|_1$ pour $y_1, y_2 \subseteq [\![0; d-1]\!]$, alors on peut calculer assez facilement $Succ_B^Q(W_t^n, P_\sigma.(Id_{\frac{n}{d}} \otimes U_d))$ pour toute permutation σ et n multiple de d.

Proposition 4.12. *Soit $U = P_\sigma.(Id_{\frac{n}{d}} \otimes U_d)$. On pose $\Gamma_y = \sum_{x \in y} |x\rangle \langle x|$ alors :*

(i) $Succ_B^Q(W_t^n, U) = \dfrac{1}{2} + \dfrac{1}{4.n.\binom{n-1}{t-1}} \sum_{q=0}^{\frac{n}{d}-1} \sum_{y_1, y_2 \subset [\![0;d-1]\!]} \left\|\Gamma_{y_1} - U_d.\Gamma_{y_2}.U_d^\dagger\right\|_1 .c^\sigma_{q,y_1,y_2}$

Pour définir c^σ_{q,y_1,y_2}, on définit d'abord les ensembles I, z_1 et z_2 :

- $I = [\![dq; dq + d - 1]\!] \cap \sigma^{-1}([\![dq; dq + d - 1]\!])$
- $z_1 = \sigma^{-1}(dq + y_1)$
- $z_2 = dq + y_2$

Alors :

- *Si $z_1 \cap I \neq z_2 \cap I$ alors $c^\sigma_{q,y_1,y_2} = 0$.*
- *Sinon* $c^\sigma_{q,y_1,y_2} = \binom{n - 2d + Card(I)}{t - Card(y_1) - Card(y_2) + Card(z_1 \cap z_2)}$

(ii) Pour $\sigma = \tau$ avec $\tau(x) = x + d \pmod n$ et $n \geq 2d$:

Il existe $(\alpha_1, \cdots, \alpha_d)$ tels que $Succ_B^Q(W_t^n, U) = \dfrac{1}{2} + \dfrac{1}{\binom{n-1}{t-1}} \sum_{j=1}^{d} \alpha_j \binom{n-2j}{t-j}$

(iii) Pour $\sigma = id$:

Il existe $(\alpha_1, \cdots, \alpha_{\lfloor \frac{d}{2} \rfloor})$ tels que $Succ_B^Q(W_t^n, U) = \dfrac{1}{2} + \dfrac{1}{\binom{n-1}{t-1}} \sum_{j=1}^{\lfloor \frac{d}{2} \rfloor} \alpha_j \binom{n-2j}{t-j}$

(iv) Si $Succ_B^Q(W_t^n, U) = \dfrac{1}{2} + \dfrac{1}{\binom{n-1}{t-1}} \sum_{j=1}^{f} \alpha_j \binom{n-2j}{t-j}$ *avec $\alpha_j \geq 0$ alors* $biais_B^Q(W_t^n, U)$ *est maximisé pour n minimum et $t = \lfloor \frac{n}{2} \rfloor$*

4.3 Exemples numériques

Remarque 4.13. *On reprend les notations de la proposition 4.12.*
On fixe $q \in [\![0; \frac{n}{d} - 1]\!]$ *et on pose* $v_\sigma = \sum_{y_1, y_2 \subset [\![0;d-1]\!]} \left\| \Gamma_{y_1} - U_d.\Gamma_{y_2}.U_d^\dagger \right\|_1 .c^\sigma_{q,y_1,y_2}$
v_σ *ne dépend que de* σ *mais on peut regarder plus précisément quelles sont les propriétés de* σ *auquelles* v_σ *est sensible.*
Soit $F_\sigma = \{x \in [\![dq; dq+d-1]\!] \mid \sigma^{-1}(x) \in [\![dq; dq+d-1]\!]\}$ *alors on voit à partir de la définition de* c^σ_{q,y_1,y_2} *que* v_σ *dépend de l'ensemble* F_σ *et des valeurs* $\sigma^{-1}(x)$ *pour* $x \in F_\sigma$

Cette remarque va nous permettre de calculer la probabilité de succès pour les stratégies associées aux matrices de $\mathcal{Z}_n$.
On applique donc la proposition 4.12 pour $d = 2$ et $U_0 = H$. Ce tableau donne la valeur de $\left\| \Gamma_{y_1} - H.\Gamma_{y_2}.H^\dagger \right\|_1$ pour tout $y_1, y_2 \subseteq [\![0; 1]\!]$:

y_1 \ y_2	{}	{0}	{1}	{0,1}
{}	0	1	1	2
{0}	1	$\sqrt{2}$	$\sqrt{2}$	1
{1}	1	$\sqrt{2}$	$\sqrt{2}$	1
{0,1}	2	1	1	0

Soit $v_\sigma = \sum_{y_1, y_2 \subset [\![0;1]\!]} \left\| \Gamma_{y_1} - U_d.\Gamma_{y_2}.U_d^\dagger \right\|_1 .c^\sigma_{q,y_1,y_2}$.
Pour $q \in [\![0; \frac{n}{2} - 1]\!]$ fixé, la remarque 4.13 nous dit que v_σ ne dépend que de $\sigma^{-1}(2q)$ et $\sigma^{-1}(2q+1)$. Ce tableau donne v_σ en fonction de ces deux valeurs :

$\sigma^{-1}(2q)$ \ $\sigma^{-1}(2q+1)$	$2q$	$2q+1$	Autre
$2q$	X	a	b
$2q+1$	a	X	b
Autre	b	b	c

$a = 2\sqrt{2}\binom{n-2}{t-1}$
$b = \sqrt{2}\binom{n-3}{t-1} + \sqrt{2}\binom{n-3}{t-2} + 2\binom{n-3}{t-1} + 2\binom{n-3}{t-2} = (2+\sqrt{2})\binom{n-2}{t-1}$
$c = 4\sqrt{2}\binom{n-4}{t-2} + 4\binom{n-4}{t-1} + 4\binom{n-4}{t-2} + 4\binom{n-4}{t-3} = 4\binom{n-2}{t-1} + (4\sqrt{2}-4)\binom{n-4}{t-2}$
On a $a \leq b \leq c$. En particulier, $Succ^Q_B(W^n_t, P_\sigma.U_{\mathcal{Z}_n})$ serait maximisé si pour tout $q \in [\![0; \frac{n}{2} - 1]\!]$, $\{\sigma^{-1}(2q), \sigma^{-1}(2q+1)\} \cap \{2q, 2q+1\} = \emptyset$.
C'est possible pour $\sigma = \tau$ où $\tau(x) = x + d \pmod n$ Dans ce cas on a

$$\begin{aligned} Succ^Q_B(W^n_t, P_\tau.U_{\mathcal{Z}_n}) &= \frac{1}{2} + \frac{1}{2}.\frac{\binom{n-2}{t-1}}{\binom{n-1}{t-1}} + \frac{(\sqrt{2}-1)}{2}.\frac{\binom{n-4}{t-2}}{\binom{n-1}{t-1}} \\ &= S^C(W^n_t) + \frac{(\sqrt{2}-1)}{2}.\frac{\binom{n-4}{t-2}}{\binom{n-1}{t-1}} \end{aligned}$$

Plus généralement, on va appliquer les points (ii) et (iii) de la proposition 4.12. Le tableau suivant donne pour chaque couple (U_d, σ) de la première colonne, les valeurs approchées des α_j et du

biais maximum définis dans les points (ii), (iii) et (iv) de la proposition 4.12. Le cas $k = 2$ de la proposition 3.7 nous donne que le biais est majoré par 2 :

(U_d, σ) \ j	1	2	3	4	5	6	7	8	biais
$(H^{\otimes 0}, \tau)$	0.5	0	0	0	0	0	0	0	1
$(H^{\otimes 1}, \tau)$	0.5	0.207	0	0	0	0	0	0	1.207
$(H^{\otimes 2}, \tau)$	0.5	0.232	0.314	0.221	0	0	0	0	1.224
$(H^{\otimes 3}, \tau)$	0.5	0.241	0.348	0.680	1.474	2.401	3.421	4.062	1.241
(U_4^*, id)	0.5	0.224	0	0	0	0	0	0	1.224
(U_6^*, id)	0.5	0.236	0.254	0	0	0	0	0	1.242
(U_8^*, id)	0.5	0.240	0.330	0.522	0	0	0	0	1.262

Les valeurs exactes de ce tableau peuvent être calculées (et affichées) par le logiciel sage en tapant la commande :
sage main/main_example_alpha.sage à partir de répertoire *sage* du dépot git.

4.4 Implémentation

Afin de vérifier certains de mes résultats j'ai utilisé le langage sage. Les fonctions principales se trouvent dans le repertoire "main". Il y a 5 fichiers dans ce répertoire :

- Le fichier "main/main_example_alpha.sage" qui m'a permis de créer le dernier tableau du rapport
- Le fichier "main/main_generation.sage" est un algorithme pour rechercher une matrice unitaire qui optimise la probabilité de succès
- Le fichier "main/main_sdp.sage" implémente les sdp définis dans la section 3 pour trouver une borne supérieure pour $S^Q(W_t^n, k)$.
- Le fichier "main/main_test_dependency.sage" vérifie numériquement la proposition 4.3
- Le fichier "main/main_test_val.sage" vérifie numériquement la proposition 4.12

Pour obtenir ces fichiers, taper dans un terminal :
git clone https ://github.com/antoine06/Implementation_stage_m2_grospellier.git
Pour lancer l'un de ces 5 fichiers : dans un terminal se positionner dans le répertoire "sage" puis lancer la commande "sage main/nom_du_fichier.sage"

Le programme matlab "subset_channel.m" a été écrit pour l'article [1]. Je m'en suis servi pour trouver les matrices U_4^*,U_6^* et U_8^*.

Conclusion

L'étude qui précède permet d'affirmer que les stratégies quantiques représentent une amélioration par rapport aux stratégies classiques. Toutefois, la question de quantifier cet avantage (comme dans le cas non-signaling) reste ouvert. On sait qu'une stratégie non-signaling peut apporter au maximum un gain de $1 - \frac{1}{e}$ et que cette borne est atteinte. La situation du cas quantique reste ouverte et différentes pistes peuvent être explorées dans ce sens :

- La forme des matrices U_4^*,U_6^* et U_8^* de l'exemple 4.5 semble suggérer d'étudier les matrices avec des 0 sur la digonales et des $1, -1$ ailleurs. L'article [3] étudie l'existance de telles matrices en fonction de leur dimension.
- On peut étudier d'autres canaux que le subset channel W_t^n.
- On peut étudier en détails les sdp qui caractérisent la probabilité de succès quantique dans le but de montrer des propriétés sur $S^Q(W, k)$.

Références

[1] Siddharth Barman and Omar Fawzi. Algorithmic aspects of optimal channel coding. *arXiv preprint arXiv :1508.04095*, 2015.

[2] Mario Berta, Omar Fawzi, and Volkher B Scholz. Quantum bilinear optimization. *arXiv preprint arXiv :1506.08810*, 2015.

[3] JM Goethals and JJ Seidel. Orthogonal matrices with zero diagonal. *Geometry and Combinatorics*, page 257, 2014.

[4] Brett Hemenway, Carl A Miller, Yaoyun Shi, and Mary Wootters. Optimal entanglement-assisted one-shot classical communication. *Physical Review A*, 87(6) :062301, 2013.

[5] William Matthews. A linear program for the finite block length converse of polyanskiy–poor–verdú via nonsignaling codes. *Information Theory, IEEE Transactions on*, 58(12) :7036–7044, 2012.

[6] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.

[7] Stefano Pironio, Miguel Navascués, and Antonio Acin. Convergent relaxations of polynomial optimization problems with noncommuting variables. *SIAM Journal on Optimization*, 20(5) :2157–2180, 2010.

[8] Robert Prevedel, Yang Lu, William Matthews, Rainer Kaltenbaek, and Kevin J Resch. Entanglement-enhanced classical communication over a noisy classical channel. *Physical review letters*, 106(11) :110505, 2011.

5 Annexe

Proposition 4.3

La proposition 4.3 correspond aux points (v), (vii), (ix), (iv), et (vi) du lemme 5.5

Notations 5.1. *Pour $y \subseteq [\![0; n-1]\!]$, on pose* $\widetilde{E}(y) = \sum_{x \in y} E(x|0) - E(x|1)$

Lemme 5.2.

$$Succ^{Q}(W_t^n, E, D) = \frac{1}{2} + \frac{1}{2.\binom{n-1}{t-1}} \sum_{y \in \binom{\mathbf{n}}{\mathbf{t}}} \left[\langle \psi | \, \widetilde{E}(y) \otimes D(0|y) \, | \psi \rangle \right]$$

Démonstration.

$$\begin{aligned}
Succ^{Q}(W_t^n, E, D) &= \frac{1}{2} \sum_{i,x,y} W_t^n(y|x). \langle \psi | \, E(x|i) \otimes D(i|y) \, | \psi \rangle \\
&= \frac{1}{2.\binom{n-1}{t-1}} \sum_{\substack{y \in \binom{\mathbf{n}}{\mathbf{t}} \\ x \in y}} [\langle \psi | \, E(x|0) \otimes D(0|y) \, | \psi \rangle \\
&\qquad - \langle \psi | \, E(x|1) \otimes (Id_{\mathcal{H}} - D(0|y)) \, | \psi \rangle] \\
&= \frac{1}{2} + \frac{1}{2.\binom{n-1}{t-1}} \sum_{y \in \binom{\mathbf{n}}{\mathbf{t}}} \left[\langle \psi | \left(\sum_{x \in y} E(x|0) - E(x|1) \right) \otimes D(0|y) \, | \psi \rangle \right] \\
&= \frac{1}{2} + \frac{1}{2.\binom{n-1}{t-1}} \sum_{y \in \binom{\mathbf{n}}{\mathbf{t}}} \left[\langle \psi | \, \widetilde{E}(y) \otimes D(0|y) \, | \psi \rangle \right]
\end{aligned}$$

□

Notations 5.3. *On pose :*

(i) $val'(W_t^n, E, D) = \sum_{y \in \binom{\mathbf{n}}{\mathbf{t}}} \langle \psi | \, \widetilde{E}(y) \otimes D(0|y) \, | \psi \rangle$

(ii) $val'_B(W_t^n, E) = \underset{D \in \mathcal{D}_{n,t}}{Max} \left(val'(W_t^n, E, D) \right)$

(iii) $val'_{A,B}(W_t^n) = \underset{E \in \mathcal{E}_n}{Max} \left(val'_B(W_t^n, E) \right)$

Lemme 5.4. *Soit $E \in \mathcal{E}_n$ alors :*

(i) $\widetilde{E}(\bar{y}) = -\widetilde{E}(y)$

(ii) Si $t = Card(y) - 1 > 0$ alors $\widetilde{E}(y) = \frac{1}{t} \sum_{x \in y} \widetilde{E}(y \setminus \{x\})$

Lemme 5.5. *Soient $n \in \mathbb{N}^*$ et $t \in [\![0; n]\!]$. Alors :*

(i) $val'_B(W_t^n, E) = \sum_{y \in \binom{\mathbf{n}}{\mathbf{t}}} \underset{0 \preceq D \preceq Id_{\mathcal{H}}}{Max} \langle \psi | \, \widetilde{E}(y) \otimes D \, | \psi \rangle$

(ii) $val'_B(W_{n-t}^n, E) = val'_B(W_t^n, E)$

(iii) Pour $t < n$: $\frac{n-t-1}{t+1} val'_B(W_t^n, E) \leq val'_B(W_{t+1}^n, E) \leq \frac{n-t}{t} val'_B(W_t^n, E)$

(iv) $biais_B(W_{n-t}^n, E) = biais_B(W_t^n, E)$

(v) $t \mapsto Succ_B(W_t^n, E)$ *est décroissant*

(vi) $biais_{A,B}(W_{n-t}^n) = biais_{A,B}(W_t^n)$

(vii) $t \mapsto Succ_{A,B}(W_t^n)$ *est décroissant*

(viii) $val'_{A,B}(n+1,t) \geq \frac{n}{n-t+1} val'_{A,B}(W_t^n)$

(ix) $n \mapsto Succ_{A,B}(W_t^n)$ *est croissant*

Preuve.

(i) OK

(ii) Soit $D_1 \in \mathcal{D}_{n,t}$ qui maximise $D \mapsto val'_B(W_t^n, E, D)$.

Pour $x \in [\![0; n-1]\!]$, $y \in \binom{\mathbf{n}}{\mathbf{n-t}}$, on pose : $\begin{cases} D_2(0|y) = D_1(1|\bar{y}) \\ D_2(1|y) = D_1(0|\bar{y}) \end{cases}$

On a bien $D_2 \in \mathcal{D}_{n,n-t}$

$$\begin{aligned} val'_B(W_{n-t}^n, E) &\geq val'(W_{n-t}^n, E, D_2) \\ &= \sum_{y \in \binom{\mathbf{n}}{\mathbf{n-t}}} \langle\psi| \widetilde{E}(y) \otimes D_2(0|y) |\psi\rangle \\ &= \sum_{y \in \binom{\mathbf{n}}{\mathbf{t}}} \langle\psi| \widetilde{E}(\bar{y}) \otimes D_2(0|\bar{y}) |\psi\rangle \\ &= \sum_{y \in \binom{\mathbf{n}}{\mathbf{t}}} \langle\psi| (-\widetilde{E}(y)) \otimes D_1(1|y) |\psi\rangle \\ &= -\sum_{y \in \binom{\mathbf{n}}{\mathbf{t}}} \langle\psi| \widetilde{E}(y) \otimes (Id_{\mathcal{H}} - D_1(0|y)) |\psi\rangle \\ &= val'(W_t^n, E, D_1) - \langle\psi| \left(\sum_{y \in \binom{\mathbf{n}}{\mathbf{t}}} \widetilde{E}(y) \right) \otimes Id_{\mathcal{H}} |\psi\rangle \end{aligned}$$

Mais :

$$\begin{aligned} \sum_{y \in \binom{\mathbf{n}}{\mathbf{t}}} \widetilde{E}(y) &= \sum_{y \in \binom{\mathbf{n}}{\mathbf{t}}} \sum_{x \in y} E(x|0) - E(x|1) \\ &= \binom{n-1}{t-1} \sum_{x=0}^{n-1} E(x|0) - E(x|1) \\ &= \binom{n-1}{t-1} (Id_{\mathcal{H}} - Id_{\mathcal{H}}) \\ &= 0_{\mathcal{H}} \end{aligned}$$

Donc $val'_B(W_{n-t}^n, E) \geq val'(W_t^n, E, D_1) = val'_B(W_t^n, E)$

Par symétrie, $val'_B(W_t^n, E) = val'_B(n, n-(n-t), E) \geq val'_B(W_{n-t}^n, E)$

Donc $val'_B(W_{n-t}^n, E) = val'_B(W_t^n, E)$

(iii) On utilise (i) du lemme 5.5 et (ii) du lemme 5.4 :

$$\begin{aligned} val'_B(W_{t+1}^n, E) &= \sum_{y \in \binom{\mathbf{n}}{\mathbf{t+1}}} \operatorname*{Max}_{0 \preceq D \preceq Id_{\mathcal{H}}} \langle\psi| \widetilde{E}(y) \otimes D |\psi\rangle \\ &= \frac{1}{t} \sum_{y \in \binom{\mathbf{n}}{\mathbf{t+1}}} \operatorname*{Max}_{0 \preceq D \preceq Id_{\mathcal{H}}} \sum_{x \in y} \langle\psi| \widetilde{E}(y \setminus \{x\}) \otimes D |\psi\rangle \\ &\leq \frac{n-t}{t} \sum_{y \in \binom{\mathbf{n}}{\mathbf{t}}} \operatorname*{Max}_{0 \preceq D \preceq Id_{\mathcal{H}}} \langle\psi| \widetilde{E}(y) \otimes D |\psi\rangle \end{aligned}$$

$$val'_B(W_{t+1}^n, E) \leq \frac{n-t}{t} val'_B(W_t^n, E)$$

Par symétrie,

$$\begin{aligned} \mathit{val}'_B(W^n_{t+1}, E) &= \mathit{val}'_B(W^n_{n-t} - 1, E) \\ &\geq \frac{n-t-1}{n-(n-t-1)} \mathit{val}'_B(W^n_{n-t}, E) \\ &\geq \frac{n-t-1}{t+1} \mathit{val}'_B(W^n_t, E) \end{aligned}$$

Donc $\frac{n-t-1}{t+1} \mathit{val}'_B(W^n_t, E) \leq \mathit{val}'_B(W^n_{t+1}, E) \leq \frac{n-t}{t} \mathit{val}'_B(W^n_t, E)$

(iv) On a :

$$\begin{aligned} \mathit{biais}_B(W^n_{n-t}, E) &= \frac{1}{\binom{n-2}{n-t-1}} \mathit{val}'_B(W^n_{n-t}, E) \\ &= \frac{1}{\binom{n-2}{n-2-(n-t-1)}} \mathit{val}'_B(n, n, E) \qquad \text{Par (ii)} \\ &= \mathit{biais}_B(W^n_t, E) \end{aligned}$$

(v) On a :

$$\begin{aligned} Succ_B(W^n_{t+1}, E) &= \frac{1}{2} + \frac{1}{2\binom{n-1}{t}} \mathit{val}'_B(W^n_{t+1}, E) \\ &\leq \frac{1}{2} + \frac{1}{2} \frac{t!(n-1-t)!}{(n-1)!} \frac{n-t}{t} \mathit{val}'_B(W^n_t, E) \qquad \text{Par (iii)} \\ &\leq \frac{1}{2} + \frac{1}{2} \frac{(t-1)!(n-t)!}{(n-1)!} \mathit{val}'_B(W^n_t, E) \\ &\leq \frac{1}{2} + \frac{1}{2\binom{n-1}{t-1}} \mathit{val}'_B(W^n_t, E) \\ &\leq Succ_B(W^n_t, E) \end{aligned}$$

(vi) Conséquence directe de (iv)

(vii) Conséquence directe de (v)

(viii) Soit $E_1 \in \mathcal{E}_n$ qui maximise $E \mapsto \mathit{val}'_B(W^n_t, E)$. On pose pour tout $i \in [\![0; 1]\!]$: $\begin{cases} E_2(x|i) = E_1(x|i) & \forall x \in [\![0 \\ E_2(n|i) = 0_{\mathcal{H}} \end{cases}$

On a alors $E_2 \in \mathcal{E}_{n+1}$ et donc :

$$
\begin{aligned}
val'_{A,B}(n+1,t) &= \underset{E\in\mathcal{E}_{n+1}}{\text{Max}} \left(val'_B(n+1,t,E)\right) \\
&\geq val'_B(n+1,t,E_2) \\
&\geq \sum_{y\in\binom{\mathbf{n+1}}{\mathbf{t}}} \underset{0\preceq D\preceq Id_{\mathcal{H}}}{\text{Max}} \langle\psi|\, \widetilde{E_2}(y)\otimes D\,|\psi\rangle \qquad \text{par (i)} \\
&\geq \sum_{\{y\in\binom{\mathbf{n+1}}{\mathbf{t}}|n\in y\}} \underset{0\preceq D\preceq Id_{\mathcal{H}}}{\text{Max}} \langle\psi|\, \widetilde{E_2}(y)\otimes D\,|\psi\rangle \\
&\quad + \sum_{\{y\in\binom{\mathbf{n+1}}{\mathbf{t}}|n\notin y\}} \underset{0\preceq D\preceq Id_{\mathcal{H}}}{\text{Max}} \langle\psi|\, \widetilde{E_2}(y)\otimes D\,|\psi\rangle \\
&\geq \sum_{y\in\binom{\mathbf{n}}{\mathbf{t-1}}} \underset{0\preceq D\preceq Id_{\mathcal{H}}}{\text{Max}} \langle\psi|\, \widetilde{E_2}(y\cup\{x\})\otimes D\,|\psi\rangle \\
&\quad + \sum_{y\in\binom{\mathbf{n}}{\mathbf{t}}} \underset{0\preceq D\preceq Id_{\mathcal{H}}}{\text{Max}} \langle\psi|\, \widetilde{E_2}(y)\otimes D\,|\psi\rangle \\
&\geq \sum_{y\in\binom{\mathbf{n}}{\mathbf{t-1}}} \underset{0\preceq D\preceq Id_{\mathcal{H}}}{\text{Max}} \langle\psi|\, (\widetilde{E_2}(y)+E_2(n|0)-E_2(n|1))\otimes D\,|\psi\rangle \\
&\quad + \sum_{y\in\binom{\mathbf{n}}{\mathbf{t}}} \underset{0\preceq D\preceq Id_{\mathcal{H}}}{\text{Max}} \langle\psi|\, \widetilde{E_2}(y)\otimes D\,|\psi\rangle \\
&\geq \sum_{y\in\binom{\mathbf{n}}{\mathbf{t-1}}} \underset{0\preceq D\preceq Id_{\mathcal{H}}}{\text{Max}} \langle\psi|\, \widetilde{E_1}(y)\otimes D\,|\psi\rangle \\
&\quad + \sum_{y\in\binom{\mathbf{n}}{\mathbf{t}}} \underset{0\preceq D\preceq Id_{\mathcal{H}}}{\text{Max}} \langle\psi|\, \widetilde{E_1}(y)\otimes D\,|\psi\rangle \\
&\geq val'_B(W^n_{t-1},E_1) + val'_B(W^n_t,E_1) \\
&\geq \left[1+\frac{t-1}{n-t+1}\right] val'_B(W^n_t,E_1) \qquad \text{par (iii)} \\
&\geq \frac{n}{n-t+1} val'_{A,B}(W^n_t)
\end{aligned}
$$

(ix) On a :

$$
\begin{aligned}
Succ_{A,B}(n+1,t) &= \frac{1}{2} + \frac{1}{2\binom{n-1}{t-1}} val'_{A,B}(n+1,t) \\
&\geq \frac{1}{2} + \frac{1}{2}\frac{(t-1)!(n-t+1)!}{n!}\frac{n}{n-t+1} val'_{A,B}(W^n_t) \qquad \text{par (viii)} \\
&\geq \frac{1}{2} + \frac{1}{2}\frac{(t-1)!(n-t)!}{(n-1)!} val'_{A,B}(W^n_t) \\
&\geq Succ_{A,B}(W^n_t)
\end{aligned}
$$

□

Proposition 4.4

Proposition 5.6. *Si on pose* $\Gamma_y = \sum_{x\in y} |x\rangle\langle x|$ *alors :*

$$
Succ^Q_B(W^n_t,U) = \frac{1}{2} + \frac{1}{4.n.\binom{n-1}{t-1}} \sum_{y\in\binom{\mathbf{n}}{\mathbf{t}}} \left\| \Gamma_y - U\Gamma_y U^\dagger \right\|_1
$$

Démonstration. On utilise :

- Le lemme 5.2
- Le point (i) du lemme 5.5
- Le "Transpose trick" : si $|\phi\rangle$ est l'état maximalement intriqué, alors pour tout $A, B \in \mathcal{M}_n(\mathbb{C})$, $\langle\phi| A \otimes B |\phi\rangle = \frac{1}{n} Tr(A.B^T)$
- Si $Tr(A) = 0$ alors $\frac{1}{2}\|A\|_1 = \underset{0 \preceq \Lambda \preceq Id_n}{\text{Max}} Tr(\Lambda A)$

□

Proposition 4.6

Proposition 5.7. *On a les invariances suivantes :*

(i) $Succ_B^Q(W_t^n, U) = Succ_B^Q(W_t^n, P_{\sigma^{-1}}.U.P_\sigma)$ *pour* σ *une permutation*

(ii) $Succ_B^Q(W_t^n, J_1.U.J_2) = Succ_B^Q(W_t^n, U)$ *où* J_1 *et* J_2 *sont des matrices diagonales avec des* 1 *et des* -1 *sur la diagonale.*

(iii) $Succ_B^Q(W_t^n, U^T) = Succ_B^Q(W_t^n, \bar{U}) = Succ_B^Q(W_t^n, U)$

Démonstration.

(i) Il suffit de montrer que $val_B^Q(W_t^n, U) = val_B^Q(W_t^n, P_{\sigma^{-1}}.U.P_\sigma)$.
On a $P_\sigma \Gamma_y P_{\sigma^{-1}} = \Gamma_{\sigma(y)}$
Donc :

$$\begin{aligned} val_B^Q(W_t^n, P_{\sigma^{-1}}.U.P_\sigma) &= \sum_{y \in \binom{\mathbf{n}}{\mathbf{t}}} \left\| \Gamma_y - P_{\sigma^{-1}}.U.P_\sigma \Gamma_y P_{\sigma^{-1}}.U^\dagger.P_\sigma \right\|_1 \\ &= \sum_{y \in \binom{\mathbf{n}}{\mathbf{t}}} \left\| P_{\sigma^{-1}} \left(P_\sigma.\Gamma_y.P_{\sigma^{-1}} - U.P_\sigma.\Gamma_y P_{\sigma^{-1}}.U^\dagger \right) P_\sigma \right\|_1 \\ &= \sum_{y \in \binom{\mathbf{n}}{\mathbf{t}}} \left\| \Gamma_{\sigma(y)} - U\Gamma_{\sigma(y)}.U^\dagger \right\|_1 \\ &= \sum_{y \in \binom{\mathbf{n}}{\mathbf{t}}} \left\| \Gamma_y - U\Gamma_y.U^\dagger \right\|_1 \\ &= val_B^Q(W_t^n, U) \end{aligned}$$

(ii) On remarque que $J^\dagger = J^{-1} = J$

$$\begin{aligned} val_B^Q(W_t^n, J_1.U.J_2) &= \sum_{y \in \binom{\mathbf{n}}{\mathbf{t}}} \left\| \Gamma_y - J_1.U.J_2^\dagger \Gamma_y J_2.U^\dagger.J_1 \right\|_1 \\ &= \sum_{y \in \binom{\mathbf{n}}{\mathbf{t}}} \left\| J_1 \left(J_1.\Gamma_y.J_1 - U.J_2 \Gamma_y J_2.U^\dagger \right) J_1 \right\|_1 \\ &= \sum_{y \in \binom{\mathbf{n}}{\mathbf{t}}} \left\| \Gamma_y - U\Gamma_y U^\dagger \right\|_1 \text{ car } J.\Gamma_y.J = \Gamma_y \\ &= val_B^Q(W_t^n, U) \end{aligned}$$

(iii) Cela vient du fait que les matrices $(\Gamma_y - U\Gamma_y U^\dagger)$ sont hermitiennes.

□

Proposition 4.7

Proposition 5.8. *On note f_σ le nombre de points fixes de la permutation σ. Alors :*

$$Succ_B^Q(W_t^n, P_\sigma) = \frac{1}{2} + \frac{\binom{n-2}{t-1}}{2.n.\binom{n-1}{t-1}}(n - f_\sigma)$$

Démonstration. On va utiliser le fait que $\left\| \sum_{i=0}^{n-1} \lambda_i |i\rangle \langle i| \right\|_1 = \sum_{i=0}^{n-1} |\lambda_i|$:

$$\begin{aligned}
val_B^Q(W_t^n, P_\sigma) &= \sum_{y \in \binom{\mathbf{n}}{\mathbf{t}}} \|\Gamma_y - P_\sigma \Gamma_y P_{\sigma^{-1}}\|_1 \\
&= \sum_{y \in \binom{\mathbf{n}}{\mathbf{t}}} \left\|\Gamma_y - \Gamma_{\sigma(y)}\right\|_1 \\
&= \sum_{y \in \binom{\mathbf{n}}{\mathbf{t}}} Card(y \Delta \sigma(y)) \\
&= \sum_{y \in \binom{\mathbf{n}}{\mathbf{t}}} (2t - 2.Card(y \cap \sigma(y))) \\
&= 2t\binom{n}{t} - 2 \sum_{y \in \binom{\mathbf{n}}{\mathbf{t}}} \sum_{x \in y} Card(\{x\} \cap \sigma(y)) \\
&= 2t\binom{n}{t} - 2 \sum_{x=0}^{n-1} \sum_{\{y \in \binom{\mathbf{n}}{\mathbf{t}} | x \in y\}} Card(\{x\} \cap \sigma(y))
\end{aligned}$$

On décompose la somme sur x en fonction de si x est point fixe de σ. On note f_σ le nombre de points fixes de σ :

$$\begin{aligned}
S_2 &= \sum_{x=0}^{n-1} \sum_{\{y \in \binom{\mathbf{n}}{\mathbf{t}} | x \in y\}} Card(\{x\} \cap \sigma(y)) \\
&= \sum_{\sigma(x)=x} \binom{n-1}{t-1} + \sum_{\sigma(x) \neq x} \binom{n-2}{t-2} \\
&= f_\sigma . \binom{n-1}{t-1} + (n - f_\sigma) . \binom{n-2}{t-2} \\
&= f_\sigma . \binom{n-2}{t-1} + n . \binom{n-2}{t-2} \\
Succ_B^Q(W_t^n, P_\sigma) &= \frac{1}{2} + \frac{1}{4.n.\binom{n-1}{t-1}} \left[2t\binom{n}{t} - 2\left(f_\sigma . \binom{n-2}{t-1} + n . \binom{n-2}{t-2} \right) \right] \\
&= \frac{1}{2} + \frac{1}{2.n.\binom{n-1}{t-1}} \left[n\binom{n-1}{t-1} - \left(f_\sigma . \binom{n-2}{t-1} + n . \binom{n-1}{t-1} - n . \binom{n-2}{t-1} \right) \right] \\
&= \frac{1}{2} + \frac{\binom{n-2}{t-1}}{2.n.\binom{n-1}{t-1}}(n - f_\sigma)
\end{aligned}$$

□

Proposition 4.10

Proposition 5.9. *Soit $U \in \mathcal{Z}_n$ alors n est pair et :*
$U = L.P_{\sigma_1}.U_0.P_{\sigma_2}.C$. Avec L et C des matrices diagonales avec des 1 et -1 sur la diagonale ;

σ_1, σ_2 des permutations et $U_{\mathcal{Z}_n}$ la matrice de l'exemple 4.9.
De plus, $Succ_B^Q(W_t^n, U) = Succ_B^Q(W_t^n, P_\sigma.U_{\mathcal{Z}_n})$ avec $\sigma = \sigma_2^{-1} \circ \sigma_1$

Démonstration.

Soit $U \in \mathcal{Z}_n$. On pose $M_1 = \sqrt{2}.U$.
$U^\dagger$ est également unitaire, donc les lignes de U sont des vecteurs unitaires. Ainsi, M_1 a exactement deux coefficients non nuls par ligne.
On s'interresse d'abord à la première colonne. Modulo le fait de multiplier les lignes par -1 et d'en faire une permutation, on a :

$$M_1 = \left(\begin{array}{c|c} 1 & \\ 1 & \\ 0 & \ast \\ \vdots & \\ 0 & \end{array}\right)$$

La matrice M_1 a deux coefficients non nuls par ligne. Ainsi modulo permutation et multiplication par -1 des colonnes, le coefficient en première ligne et deuxième colonne de la matrice M_1 est 1. Par orthogonalité de la première et de la deuxième colonne, le coefficient de la deuxième colonne et de la deuxième ligne est un -1.

On a donc : $M_1 = \left(\begin{array}{cc} \boxed{\begin{array}{cc} 1 & 1 \\ 1 & -1 \end{array}} & 0 \\ 0 & \boxed{M_2} \end{array}\right)$ Avec $M_2 \in \mathcal{Z}_{n-2}$.

Par récurrence on obtient le résultat.
La formule vient de la proposition 4.6.

□

Proposition 4.12

C'est la proposition 5.12.

Lemme 5.10.

(i) $\forall a, b, c \in \mathbb{N}$, $\binom{a}{b} = \sum_{j=0}^{c} \binom{a-c}{b-j}\binom{c}{j}$

(ii) Soient $n, j \in \mathbb{N}^*$ tels que $n \geq 2j$, alors $t \mapsto \frac{\binom{n-2j}{t-j}}{\binom{n-2}{t-1}}$ est maximisé pour $t = \lfloor \frac{n}{2} \rfloor$

(iii) Soit $j \in \mathbb{N}^*$ alors $n \mapsto \frac{\binom{n-2j}{\lfloor \frac{n}{2} \rfloor - j}}{\binom{n-2}{\lfloor \frac{n}{2} \rfloor - 1}}$ est décroissant sur $[\![2j; +\infty[\![$

(iv) Si $Succ_B^Q(W_t^n, P_\sigma.U_0) = \frac{1}{2} + \frac{1}{\binom{n-1}{t-1}} \sum_j^f \alpha_j \binom{n-2j}{t-j}$ avec $\alpha_j \geq 0$ alors $biais_B^Q(W_t^n, P_\sigma.U_0)$ est maximisé pour n minimum et $t = \lfloor \frac{n}{2} \rfloor$

Démonstration.

(i) Se prouve par récurence sur c.

(ii) Soient $n, j \in \mathbb{N}^*$ avec $n \geq 2j$. Pour tout $t \in [\![j, n-j]\!]$:
$\frac{\binom{n-2j}{t-j}}{\binom{n-2}{t-1}} = \prod_{a=1}^{j-1} \frac{\binom{n-2a-2}{t-a-1}}{\binom{n-2a}{t-a}} = \prod_{a=1}^{j-1} \frac{(t-a)(n-t-a)}{(n-2a)(n-2a-1)}$
Or, pour $a \in [\![1; j-1]\!]$, $t \mapsto (t-a)(n-t-a)$ est maximisé en $t = \left\lfloor \frac{n}{2} \right\rfloor$. Comme $\frac{(t-a)(n-t-a)}{(n-2a)(n-2a-1)} \geq 0$, on a le résultat.

(iii) Soit $j \in \mathbb{N}^*$. On considère $f : n \mapsto \frac{\binom{n-2j}{\lfloor \frac{n}{2} \rfloor - j}}{\binom{n-2}{\lfloor \frac{n}{2} \rfloor - 1}}$ pour $n \geq 2j$. Il s'agit de montrer que f est décroissante.
Tout d'abord, si n est impair, il est facile de montrer que $f(n) = f(n+1)$. Il suffit donc de montrer que pour n pair, $f(n) \geq f(n+2)$. Pour n pair, on a :
$f(n) = \frac{\binom{n-2j}{\frac{n}{2}-j}}{\binom{n-2}{\frac{n}{2}-1}} = \prod_{a=1}^{j-1} \frac{\binom{n-2a-2}{\frac{n}{2}-a-1}}{\binom{n-2a}{\frac{n}{2}-a}} = \prod_{a=1}^{j-1} \frac{1}{4}\left(1 + \frac{1}{n-2a-1}\right)$
Tout est positif, et chaque terme du produit est décroissant en n donc $f(n) \geq f(n+2)$ d'où le résultat.

(iv) C'est une conséquence directe de ce qui précède

□

Lemme 5.11. *Soient $e \geq 2$ et $\beta_1, \cdots, \beta_{e-1} \in \mathbb{R}$ tels que $\forall i, \beta_i = \beta_{e-i}$.*

$$\textit{On pose} \quad \begin{cases} f = \left\lfloor \frac{e}{2} \right\rfloor \\ A \in \mathcal{M}_f(\mathbb{R}) \textit{définit par} A_{i,j} = \binom{e-2j}{i-j} \\ \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_f \end{pmatrix} = A^{-1} \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_f \end{pmatrix} \end{cases}$$

Alors : $\forall n, t \in \mathbb{N}, \sum_{i=1}^{e-1} \beta_i \binom{n-e}{t-i} = \sum_{j=1}^{f} \alpha_j \binom{n-2j}{t-j}$

Preuve. Soient $e \geq 2$ et $\beta_1, \cdots, \beta_{e-1} \in \mathbb{R}$ tels que $\forall j, \beta_j = \beta_{e-j}$. On pose $f = \left\lfloor \frac{e}{2} \right\rfloor$
On considère $A \in \mathcal{M}_f(\mathbb{R})$ définit par $A_{i,j} = \binom{e-2j}{i-j}$. A est une matrice triangulaire supérieure avec des 1 sur la diagonale donc elle est inversible.
On pose $\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_f \end{pmatrix} = A^{-1} \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_f \end{pmatrix}$. On a donc $\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_f \end{pmatrix} = A \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_f \end{pmatrix}$
Ainsi, $\forall i \in [\![1; f]\!] : \beta_i = \sum_{j=1}^{f} \alpha_j \binom{e-2j}{i-j}$
De plus, par une disjonction de cas en fonction de la parité de e,
si $f+1 \leq i \leq e-1$ alors $1 \leq e-i \leq f$
Ainsi, $\forall i \in [\![f+1; e-1]\!]$:
$\beta_i = \beta_{e-i} = \sum_{j=1}^{f} \alpha_j \binom{e-2j}{e-i-j} = \sum_{j=1}^{f} \alpha_j \binom{e-2j}{i-j}$

Donc, $\forall i \in [\![1; e-1]\!]$, $\beta_i = \sum_{j=1}^{f} \alpha_j \binom{e-2j}{i-j}$

$$\begin{aligned}
\sum_{j=1}^{f} \alpha_j \binom{n-2j}{t-j} &= \sum_{j=1}^{f} \alpha_j \sum_{i=0}^{e-2j} \binom{n-e}{t-i-j}\binom{e-2j}{i} \qquad \text{par (i) de lemme 5.10} \\
&= \sum_{j=1}^{f} \alpha_j \sum_{i=j}^{e-j} \binom{n-e}{t-i}\binom{e-2j}{i-j} \\
&= \sum_{j=1}^{f} \alpha_j \sum_{i=1}^{e-1} \binom{n-e}{t-i}\binom{e-2j}{i-j} \\
&= \sum_{i=1}^{e-1} \sum_{j=1}^{f} \alpha_j \binom{n-e}{t-i}\binom{e-2j}{i-j} \\
&= \sum_{i=1}^{e-1} \binom{n-e}{t-i} \left[\sum_{j=1}^{f} \alpha_j \binom{e-2j}{i-j}\right] \\
&= \sum_{i=1}^{e-1} \beta_i \binom{n-e}{t-i}
\end{aligned}$$

□

Proposition 5.12. *Soit $U = P_\sigma.(Id_{\frac{n}{d}} \otimes U_d)$. On pose $\Gamma_y = \sum_{x \in y} |x\rangle \langle x|$ alors :*

(i) $Succ_B^Q(W_t^n, U) = \frac{1}{2} + \frac{1}{4.n.\binom{n-1}{t-1}} \sum_{q=0}^{\frac{n}{d}-1} \sum_{y_1,y_2 \subset [\![0;d-1]\!]} \left\| \Gamma_{y_1} - U_d.\Gamma_{y_2}.U_d^\dagger \right\|_1 .c^\sigma_{q,y_1,y_2}$

Pour définir c^σ_{q,y_1,y_2}, on définit d'abord les ensembles I, z_1 et z_2 :

- $I = [\![dq; dq+d-1]\!] \cap \sigma^{-1}([\![dq; dq+d-1]\!])$
- $z_1 = \sigma^{-1}(dq + y_1)$
- $z_2 = dq + y_2$

Alors :

- *Si $z_1 \cap I \neq z_2 \cap I$ alors $c^\sigma_{q,y_1,y_2} = 0$.*
- *Sinon* $c^\sigma_{q,y_1,y_2} = \binom{n - 2d + Card(I)}{t - Card(y_1) - Card(y_2) + Card(z_1 \cap z_2)}$

(ii) Pour $\sigma = \tau$ avec $\tau(x) = x + d \pmod n$ et $n \geq 2d$:

Il existe $(\alpha_1, \cdots, \alpha_d)$ tels que $Succ_B^Q(W_t^n, U) = \frac{1}{2} + \frac{1}{\binom{n-1}{t-1}} \sum_{j=1}^{d} \alpha_j \binom{n-2j}{t-j}$

(iii) Pour $\sigma = id$:

Il existe $(\alpha_1, \cdots, \alpha_{\lfloor \frac{d}{2} \rfloor})$ tels que $Succ_B^Q(W_t^n, U) = \frac{1}{2} + \frac{1}{\binom{n-1}{t-1}} \sum_{j=1}^{\lfloor \frac{d}{2} \rfloor} \alpha_j \binom{n-2j}{t-j}$

(iv) Si $Succ_B^Q(W_t^n, U) = \frac{1}{2} + \frac{1}{\binom{n-1}{t-1}} \sum_{j=1}^{f} \alpha_j \binom{n-2j}{t-j}$ *avec $\alpha_j \geq 0$ alors* $biais_B^Q(W_t^n, U)$ *est maximisé pour n minimum et $t = \lfloor \frac{n}{2} \rfloor$*

Démonstration.

(i) On note q_x et r_x le quotient et le reste dans la division euclidienne de x par d. On peut donc en décomposer la norme trace :

$$\begin{aligned} val_B^Q(W_t^n, P_\sigma.U) &= \sum_{y\in\binom{\mathbf{n}}{\mathbf{t}}} \left\| \sum_{x\in\sigma(y)} |x\rangle\langle x| - \sum_{x\in y} U.|x\rangle\langle x|.U^\dagger \right\|_1 \\ &= \sum_{y\in\binom{\mathbf{n}}{\mathbf{t}}} \left\| \sum_{q=0}^{\frac{n}{d}-1} \left(\sum_{\substack{x\in\sigma(y)\\ q_x=q}} |x\rangle\langle x| - \sum_{\substack{x\in y\\ q_x=q}} U.|x\rangle\langle x|.U^\dagger \right) \right\|_1 \\ &= \sum_{y\in\binom{\mathbf{n}}{\mathbf{t}}} \sum_{q=0}^{\frac{n}{d}-1} \left\| \sum_{\substack{x\in y\\ q_{\sigma(x)}=q}} |\sigma(x)\rangle\langle\sigma(x)| - \sum_{\substack{x\in y\\ q_x=q}} U.|x\rangle\langle x|.U^\dagger \right\|_1 \\ &= \sum_{y\in\binom{\mathbf{n}}{\mathbf{t}}} \sum_{q=0}^{\frac{n}{d}-1} \left\| \sum_{\substack{x\in y\\ q_{\sigma(x)}=q}} |r_{\sigma(x)}\rangle\langle r_{\sigma(x)}| - \sum_{\substack{x\in y\\ q_x=q}} U_0.|r_x\rangle\langle r_x|.U_0^\dagger \right\|_1 \end{aligned}$$

Dans la dernière ligne, les vecteurs ne sont plus de taille n mais de taille d.

$$\begin{aligned} val_B^Q(W_t^n, P_\sigma.U) &= \sum_{q=0}^{\frac{n}{d}-1} \sum_{y\in\binom{\mathbf{n}}{\mathbf{t}}} \left\| \Gamma_{\{r_{\sigma(x)}|x\in y, q_{\sigma(x)}=q\}} - U_0.\Gamma_{\{r_x|x\in y, q_x=q\}}.U_0^\dagger \right\|_1 \\ &= \sum_{q=0}^{\frac{n}{d}-1} \sum_{\substack{y_1\subset[\![0;d-1]\!]\\ y_2\subset[\![0;d-1]\!]}} \left\| \Gamma_{y_1} - U_0.\Gamma_{y_2}.U_0^\dagger \right\|_1 .Card(Y^\sigma_{q,y_1,y_2}) \end{aligned}$$

où

$$\begin{aligned} Y^\sigma_{q,y_1,y_2} = \{y \subset [\![0; n-1]\!] \mid Card(y) = t,& \\ y_2 = \{r_x | x \in y, q_x = q\},& \\ y_1 = \{r_{\sigma(x)} | x \in y, q_{\sigma(x)} = q\}\}& \end{aligned}$$

On fixe $q \in [\![0; \frac{n}{d} - 1]\!]$, $y_1 \subset [\![0; d-1]\!]$, $y_2 \subset [\![0; d-1]\!]$.
On considère les sous-ensembles de $[\![0; n-1]\!]$ suivants :

- $A_q = [\![dq; dq + d - 1]\!]$
- $B_q = \sigma^{-1}([\![dq; dq + d - 1]\!])$
- $C_q = [\![0; n-1]\!] \setminus (A_q \cup B_q)$
- $I_q = A_q \cap B_q$

Soit $y \subset [\![0; n-1]\!]$ avec $Card(y) = t$, alors :

$$y \in Y^\sigma_{q,y_1,y_2} \Leftrightarrow \begin{cases} y \cap A_q = dq + y_2 \triangleq z_2 \\ y \cap B_q = \sigma^{-1}(dq + y_1) \triangleq z_1 \end{cases}$$

Si on pose $z_1 = \sigma^{-1}(dq + y_1)$ et $z_2 = dq + y_2$, alors $y \in Y^\sigma_{q,y_1,y_2}$ signifie que y coincide avec z_2 sur A_q et que y coincide avec z_1 sur B_q. Ce y peut être quelconque sur C_q.
Calculons $Card(Y^\sigma_{q,y_1,y_2})$:

- Si $z_1 \cap I_q \neq z_2 \cap I_q$ alors $Card(Y^\sigma_{q,y_1,y_2}) = 0$.
  En effet, pour tout $y \in Y^\sigma_{q,y_1,y_2}$, on a $z_1 \cap I_q = y \cap I_q = z_2 \cap I_q$.
  Donc $Y^\sigma_{q,y_1,y_2} \neq \emptyset \Rightarrow z_1 \cap I_q = z_2 \cap I_q$,

- Si $z_1 \cap I_q = z_2 \cap I_q$ alors pour caractériser y, il suffit d'en donner les éléments sur C_q.

$$Card(Y^{\sigma}_{q,y_1,y_2}) = \binom{Card(C_q)}{Card(y \cap C_q)}$$

$$Card(C_q) = n - Card(A_q \cup B_q) = n - 2d + Card(I_q)$$

$$y \cap C_q = y \setminus [y \cap (A_q \cup B_q)] = y \setminus [(y \cap A_q) \cup (y \cap B_q)] = y \setminus [z_2 \cup z_1]$$

$$Card(y \cap C_q) = t - Card(z_1) - Card(z_2) + Card(z_1 \cap z_2)$$

$$Card(y \cap C_q) = t - Card(y_1) - Card(y_2) + Card(z_1 \cap z_2)$$

$$Card(Y^{\sigma}_{q,y_1,y_2}) = \binom{n - 2d + Card(I_q)}{t - Card(y_1) - Card(y_2) + Card(z_1 \cap z_2)}$$

(ii) Dans le cas où $\tau(x) = x + d \pmod n$, pour tout $q \in [\![0; \frac{n}{d} - 1]\!]$, $y_1 \subset [\![0; d-1]\!]$, $y_2 \subset [\![0; d-1]\!]$ on a :

- $A_q = [\![dq; dq + d - 1]\!]$
- $B_q = [\![dq - d \pmod n; dq - 1 \pmod n]\!]$
- $I_q = \emptyset$
- $z_1 \cap z_2 = \emptyset$ car $z_1 \subseteq A_q$ et $z_2 \subseteq B_q$

On peut alors calculer $Card(Y^{\tau}_{q,y_1,y_2})$.
Puisque $z_1 \cap I_q = \emptyset = z_2 \cap I_q$, que $I_q = \emptyset$ et que $z_1 \cap z_2 = \emptyset$, on a :

$$Card(Y^{\tau}_{q,y_1,y_2}) = \binom{n - 2d}{t - Card(y_1) - Card(y_2)}$$

On a donc la forme $Succ^Q_B(W^n_t, U) = \frac{1}{2} + \frac{1}{\binom{n-1}{t-1}} \sum_{i=1}^{2d-1} \beta_i \binom{n-2d}{t-i}$ d'où la proposition grâce au lemme 5.11.

(iii) Dans le cas où $\sigma = id$, pour tout $q \in [\![0; \frac{n}{d} - 1]\!]$, on a : $I_q = [\![dq; dq + d - 1]\!]$. Soient $y_1 \subset [\![0; d-1]\!]$, $y_2 \subset [\![0; d-1]\!]$.
$z_1 \cap I_q = z_1$, $z_2 \cap I_q = z_2$ et $z_1 \cap I_q = z_2 \cap I_q \Leftrightarrow y_1 = y_2$.
De plus, pour $y_1 = y_2$, $Card(Y^{id}_{q,y_1,y_2}) = \binom{n-d}{t-Card(y_1)}$
Donc, $val(U) = \frac{n}{d} \sum_{y \subset [\![0;d-1]\!]} \left\| \Gamma_y - U.\Gamma_y.U^{\dagger} \right\|_1 . \binom{n-d}{t-Card(y)}$

On a donc la forme $Succ^Q_B(W^n_t, U) = \frac{1}{2} + \frac{1}{\binom{n-1}{t-1}} \sum_{i=1}^{d-1} \beta_i \binom{n-d}{t-i}$ d'où la proposition grâce au lemme 5.11.

□