

# Théorie de l'Information Quantique : Applications à l'Energie

En vue de l'obtention de l'unité de valeur  
**TO52 - TX54**

---

---

Écrit le : 12/01/2017 par :  
**Jaffali Hamza, Nounouh Ismaël**

---

Semestre d'automne 2016

---

---



---

**Établissement :**

Université de Technologie de Belfort-Montbéliard

**Membre du jury :**

GECHTER Franck

**Professeur encadrant :**

HOLWECK Frédéric



# Remerciements

C'est avec un grand plaisir que nous souhaitons adresser ici toute notre reconnaissance à Frédéric Holweck, qui nous permet une fois de plus de développer des sujets intéressants et qui nous tiennent à cœur, et qui prend le temps d'adopter la pédagogie et le suivi nécessaire à notre épanouissement dans ce domaine. Nous le remercions pour nous avoir aiguillé tout au long du semestre et pour nous avoir aidé et fait part de ses idées dans les moments difficiles.

Nous remercions particulièrement Alexandre Ravey d'une part, et Yassine Rui-chek d'autre part, responsables respectifs des unités de valeur TX54 et TO52, d'encadrer ces UV permettant aux élèves de développer des sujets de recherche et des projets de développement en rapport avec leurs intérêts scientifiques.

Nous remercions également Fei Gao et Damien Paire pour nous avoir apporté une explication de leurs travaux, et des pistes et expertises précieuses pour les applications en énergie. Un remerciement distingué se doit d'être adressé à Franck Gechter qui a accepté de faire partie du jury.

Nous vous remercions aussi, vous, lecteur pour le temps que vous prendrez à étudier les notions présentées dans ce rapport, et à éventuellement nous faire part de vos remarques.

Enfin, nous remercions notre famille et nos proches de nous avoir soutenu durant ce semestre, et durant nos études en général.

# Introduction

Depuis l'émergence de cette nouvelle discipline que l'on appelle physique quantique, la communauté scientifique n'a cessé de consacrer une partie de ses efforts à comprendre, investiguer, observer, théoriser, modéliser et implémenter les idées liées à ce domaine d'étude.

De cet effort, et par analogie à la théorie de l'information, est née au fur et à mesure la théorie de l'information quantique, base de ce que l'on appelle parfois informatique quantique. Jusqu'ici, nous n'avons, en tant qu'étudiants, approché cette science que du point de vue mathématique et quelques peu physique, mais en tant que personnes extérieures à cette science. Dans ce projet, nous tentons de nous placer du côté de cette théorie de l'information quantique pour observer le "monde" extérieur de la science, et plus particulièrement celui de l'énergie.

Nous vous présentons alors notre travail effectué dans le cadre de l'Unité de Valeur TO52 pour Hamza JAFFALI, et TX54 pour Ismaël NOUNOUH, sous la forme de ce rapport divisé en deux parties. Dans la première partie, nous nous intéressons à la partie théorique, en présentant tout d'abord les principaux protocoles de communication quantique, et dans un second temps un état de l'art des jeux quantiques existants dans la littérature. Dans la seconde partie, nous tenterons d'entrapercevoir le futur de la gestion d'énergie à travers les Smart Grid et l'information quantique notamment, et nous tenterons de proposer des scénarios d'application des jeux quantiques à une problématique d'allocation de ressources et de gestion de la production. Nous terminerons ce rapport par un bilan personnel, une synthèse ainsi qu'une ouverture sur d'éventuelles pistes à envisager pour la suite.

# Table des matières

|  |           |
|--|-----------|
| <b>Introduction</b>  | <b>3</b>  |
| <b>I Communication et Jeux quantiques</b>                    | <b>9</b>  |
| <b>1 Communication quantique</b>                             | <b>10</b> |
| 1.1 Bases de la théorie de l'information quantique . . . . . | 10        |
| 1.1.1 Postulats quantiques . . . . .                         | 11        |
| 1.1.2 Exemples d'opérations sur les qubits . . . . .         | 12        |
| 1.2 Téléportation quantique . . . . .                        | 13        |
| 1.2.1 Formulation du problème . . . . .                      | 13        |
| 1.2.2 Circuit quantique . . . . .                            | 13        |
| 1.2.3 Protocole quantique . . . . .                          | 13        |
| 1.3 Principe du Superdense coding à 2-qubits . . . . .       | 15        |
| 1.4 Protocole BB84 . . . . .                                 | 16        |
| 1.4.1 Exemple de transmission d'un seul qubit . . . . .      | 17        |
| 1.4.2 Exemple de transmission de plusieurs qubits . . . . .  | 20        |
| 1.5 Multiplexeurs . . . . .                                  | 22        |
| 1.5.1 Fonctionnement classique . . . . .                     | 22        |
| 1.5.2 Portes quantiques sur plusieurs qubits . . . . .       | 23        |
| 1.5.3 Exemple : Multiplexeur quantique 4 : 1 . . . . .       | 26        |
| <b>2 Jeux quantiques</b>                                     | <b>27</b> |
| 2.1 CHSH-Game . . . . .                                      | 27        |
| 2.1.1 Déroulement du jeu . . . . .                           | 27        |
| 2.1.2 Meilleures stratégies classiques . . . . .             | 28        |
| 2.1.3 Stratégie quantique . . . . .                          | 29        |
| 2.1.4 Variante du CHSH-Game . . . . .                        | 31        |
| 2.2 GHZ-Game . . . . .                                       | 32        |
| 2.2.1 Déroulement du jeu . . . . .                           | 32        |
| 2.2.2 Résolution et stratégies classiques . . . . .          | 33        |

|           |   |           |
|-----------|---|-----------|
| 2.2.3     | Stratégie quantique pour le GHZ-Game . . . . .  | 34        |
| 2.2.4     | Questions restantes pour l'arbitre . . . . .  | 35        |
| 2.2.5     | Performance au GHZ-Game avec un état $ W\rangle$ ou $ BiSep\rangle$ partagé . . . . . | 36        |
| 2.2.6     | W-Game . . . . .  | 37        |
| 2.2.7     | Généralisation à $n$ joueurs du GHZ-Game . . . . .                                    | 38        |
| 2.3       | Dilemme du prisonnier . . . . .   | 42        |
| 2.3.1     | Principe du jeu classique . . . . .   | 42        |
| 2.3.2     | Analyse des stratégies classiques . . . . .   | 42        |
| 2.3.3     | Notion de dilemme . . . . .   | 43        |
| 2.3.4     | Déroulement du jeu quantique . . . . .  | 44        |
| 2.4       | Binary Constraint System Game . . . . .   | 47        |
| 2.4.1     | Principe du jeu . . . . .   | 48        |
| 2.4.2     | Stratégie quantique parfaite . . . . .  | 49        |
| 2.4.3     | Condition d'inexistence de stratégie quantique parfaite . . . . .                     | 51        |
| 2.5       | Minority game . . . . .   | 53        |
| 2.5.1     | Origine et énoncé du jeu . . . . .  | 53        |
| 2.5.2     | Mise en place du jeu quantique . . . . .  | 54        |
| 2.5.3     | Cas où $N = 3$ . . . . .  | 56        |
| 2.5.4     | Cas où $N = 4$ . . . . .  | 57        |
| 2.5.5     | Ouvertures . . . . .  | 58        |
| 2.6       | Autres jeux quantiques . . . . .  | 59        |
| 2.6.1     | Paradoxe de Parrondo - Parrondo's game . . . . .                                      | 59        |
| 2.6.2     | Guerre des sexes . . . . .  | 63        |
| 2.6.3     | Spin flip game . . . . .  | 64        |
| 2.6.4     | Jeux quantiques restants . . . . .  | 67        |
| <b>II</b> | <b>Applications au domaine de l'énergie</b>   | <b>68</b> |
| <b>3</b>  | <b>Sécurité et Smart Grid</b>   | <b>69</b> |
| 3.1       | Présentation du réseau intelligent ou Smart Grid . . . . .                            | 69        |
| 3.1.1     | Intérêts principaux d'un nouveau type de réseau . . . . .                             | 69        |
| 3.1.2     | Description du système . . . . .  | 71        |
| 3.1.3     | Différents secteurs affectés . . . . .  | 72        |
| 3.1.4     | Smartgrid en France . . . . .   | 72        |
| 3.1.5     | Prédictions pour le futur . . . . .   | 78        |
| 3.2       | Sécurisation des Smart Grid . . . . .   | 79        |
| 3.3       | Communiquer plus d'informations avec le Superdense Coding . . . . .                   | 80        |
| 3.3.1     | Communication avec 4 choix de messages . . . . .                                      | 81        |
| 3.3.2     | Communication générale dans un système . . . . .                                      | 82        |

|  |            |
|--|------------|
| <b>4 Allocation des ressources</b>   | <b>84</b>  |
| 4.1 Problématique de l'allocation des ressources et théorie des jeux . . . . . | 84         |
| 4.2 Scénario basé sur le Dilemme du Prisonnier . . . . .                       | 85         |
| 4.2.1 Explication du scénario . . . . .  | 85         |
| 4.2.2 Bâtiment intelligent . . . . .   | 85         |
| 4.2.3 Stratégies . . . . .   | 86         |
| 4.2.4 Réalisation du jeu . . . . .   | 87         |
| 4.3 Scénarios basés sur le CHSH et GHZ Game . . . . .                          | 90         |
| 4.3.1 Scénario à deux joueurs - CHSH-Game . . . . .                            | 91         |
| 4.3.2 Premier scénario à 3 joueurs - GHZ-Game . . . . .                        | 101        |
| 4.3.3 Second scénario à 3 joueurs - W-Game . . . . .                           | 109        |
| 4.4 Scénario basé sur le Minority Game . . . . .                               | 110        |
| <b>Conclusion</b>  | <b>114</b> |
| <b>Références - Bibliographie</b>  | <b>117</b> |

# Table des figures

|      |   |    |
|------|---|----|
| 1.1  | Circuit de téléportation . . . . .  | 14 |
| 1.2  | Circuit appliqué par Bob pour décoder . . . . .   | 16 |
| 1.3  | Exemple de MUX 4 :1 . . . . .   | 23 |
| 1.4  | Porte c-NOT . . . . .   | 24 |
| 1.5  | Porte SWAP . . . . .  | 25 |
| 1.6  | Qubit de contrôle $ 1\rangle$ (configuration "High") . . . . .  | 25 |
| 1.7  | Qubit de contrôle $ 0\rangle$ (configuration "Low") . . . . .   | 25 |
| 1.8  | Circuit : Multiplexeur quantique 4 : 1 . . . . .  | 26 |
| 2.1  | Circuit : Dilemme du prisonnier quantique . . . . .   | 44 |
| 2.2  | Carré magique (à gauche) - Pentagramme magique (à droite) . . . . .   | 49 |
| 2.3  | Affectations quantiques valides - Carré magique (à gauche) - Pentagramme magique (à droite) . . . . .   | 51 |
| 2.4  | Schéma du jeu en exemple . . . . .  | 52 |
| 2.5  | Modèles de jeux classiques et quantiques . . . . .  | 55 |
| 2.6  | Jeu A . . . . .   | 60 |
| 2.7  | Jeu B . . . . .   | 60 |
| 2.8  | Simulations de l'associations des jeux A et B. Le couple $[a,b]$ indique que nous jouons a fois le jeu A et ensuite b fois le jeu B et ainsi de suite jusqu'à qu'on ai fait 100 jeux . . . . .    | 61 |
| 2.9  | Jeu A et B' . . . . .   | 62 |
| 2.10 | Simulations de l'associations des jeux A et B'. Le couple $[a,b']$ indique que nous jouons a fois le jeu A et ensuite b' fois le jeu B et ainsi de suite jusqu'à qu'on ai fait 100 jeux . . . . . | 62 |
| 2.11 | Jeu quantique A . . . . .   | 63 |
| 2.12 | Jeu quantique B . . . . .   | 63 |
| 2.13 | Circuit quantique : La guerre des sexes . . . . .   | 64 |
| 2.14 | Portes quantiques finales à appliquer à l'état initial $ u\rangle$ en fonction des stratégies des deux joueurs . . . . .  | 65 |
| 2.15 | Etat final du spin de l'électron mesuré en fonction des stratégies des deux joueurs . . . . .   | 65 |
| 2.16 | Tableau de gain pour le joueur A . . . . .  | 66 |

|   |     |
|---|-----|
| 2.17 Tableau regroupant les derniers jeux quantiques présentés dans ce chapitre . . . . .   | 67  |
| 3.1 Flux d'énergie et d'information (Source ERDF) . . . . .   | 71  |
| 3.2 Evolution du réseau électrique . . . . .  | 72  |
| 3.3 Domaines d'applications des technologies des Smartgrids . . . . .   | 73  |
| 3.4 Place du compteur intelligent (Source CRE) . . . . .  | 74  |
| 3.5 Système global . . . . .  | 75  |
| 3.6 Déploiement des technologies . . . . .  | 76  |
| 3.7 Déroulement du projet (Source ENEDIS) . . . . .   | 76  |
| 3.8 Système global (Source ISSY) . . . . .  | 77  |
| 3.9 Etapes clés du projet (Source ENEDIS) . . . . .   | 77  |
| 3.10 Evolution des Smart Grids . . . . .  | 78  |
| 3.11 Schéma du système simplifié de communication . . . . .   | 80  |
| 4.1 Opérateur expérimental J . . . . .  | 88  |
| 4.2 Opérateur expérimental U . . . . .  | 90  |
| 4.3 Schéma explicatif du système complet . . . . .  | 93  |
| 4.4 Evolution de la pénalité de surcharge (gauche) et globale (droite) au fil des itérations pour la stratégie classique optimale . . . . .             | 95  |
| 4.5 Evolution de l'utilisation de l'auxiliaire $P_0$ au fil des itérations pour la stratégie classique optimale . . . . .                               | 96  |
| 4.6 Probabilités d'occurrence de la réponse en fonction de la question, et pénalité associée . . . . .  | 97  |
| 4.7 Evolution de la pénalité de non-production (gauche) et de surproduction (droite) au fil des itérations pour la stratégie quantique . . . . .        | 98  |
| 4.8 Evolution de la pénalité de surcharge (gauche) et globale (droite) au fil des itérations pour la stratégie quantique . . . . .                      | 99  |
| 4.9 Evolution de l'utilisation de l'auxiliaire $P_0$ au fil des itérations pour la stratégie quantique . . . . .  | 100 |
| 4.10 Evolution de la pénalité de surcharge (gauche) et globale (droite) au fil des itérations pour la stratégie classique optimale . . . . .            | 104 |
| 4.11 Evolution de l'utilisation de l'auxiliaire $P_0$ au fil des itérations pour la stratégie classique optimale . . . . .                              | 105 |
| 4.12 Evolution de la pénalité de non-production (gauche) et de surcharge (droite) au fil des itérations pour la stratégie quantique . . . . .           | 107 |
| 4.13 Evolution de la pénalité de globale (gauche) et de l'utilisation de l'auxiliaire $P_0$ au fil des itérations pour la stratégie quantique . . . . . | 108 |

# Première partie

## Communication et Jeux quantiques

# Chapitre 1

## Communication quantique

Cette section a pour principal but d'apporter quelques notions élémentaires concernant la théorie de l'information quantique. Pour ce faire, nous définirons, tout d'abord, les principales différences qui résident entre l'informatique classique et quantique. Nous présenterons par la suite un certain nombre de protocoles quantiques célèbres. Pour plus d'approfondissement, vous pouvez consulter notre rapport consacré aux bases de la théorie de l'information quantique [11].

### 1.1 Bases de la théorie de l'information quantique

Comme chacun d'entre nous le sait, en informatique classique, l'information la plus simple transmise par un ordinateur est le bit (Binary digit). Ce dernier correspond à la quantité minimale d'information d'un message et est l'unité de mesure de base en informatique. Celui-ci ne peut valoir que 0 ou 1. La manipulation des bits s'effectue par nos ordinateurs au moyen de processus physiques simples et véhiculants des informations binaires : vrai/faux, on/off, 0/1,...etc.

Cependant, la théorie de l'information quantique introduit un nouveau "concept". En effet, le bit classique va être remplacé par un bit quantique (nommé qubit). L'information porté par cette entité pourrait correspondre à la polarisation d'un photon ou encore à l'orientation du spin d'un électron. Le qubit représente un système quantique à 2 états de base :  $|0\rangle$  et  $|1\rangle$ . Pour distinguer les états quantiques des états classiques, une convention a été introduite dans les années 1930 par le physicien Paul Dirac <sup>1</sup>.

---

1. 1902-1984 Il est considéré comme l'un des "pères" de la mécanique quantique et il a aussi prévu l'existence de l'antimatière.

Pour un qubit  $|\psi\rangle$ , on notera :

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$\alpha$  et  $\beta$  étant des nombres complexes,  $\alpha, \beta \in \mathbb{C}$ . Ainsi  $|\alpha|^2$  et  $|\beta|^2$  correspondent, respectivement, aux probabilités pour  $|\psi\rangle$  de se trouver dans les états  $|0\rangle$  ou  $|1\rangle$  avant d'avoir été mesurés. De plus,  $|\alpha|^2 + |\beta|^2 = 1$ .

De fait, la principale différence avec un bit classique est que le qubit a la capacité de se trouver dans une infinité d'états entre  $|0\rangle$  et  $|1\rangle$ .

### 1.1.1 Postulats quantiques

Pour plus de clarté, nous allons exposer les 3 postulats principaux de l'informatique quantique, à savoir :

□ **Postulat de l'état d'un système :** Les états d'un système quantique sont des éléments d'un espace vectoriel aussi appelé espace de Hilbert noté  $\mathbb{H}$ . Les états du système quantique d'un qubit sont les éléments d'un espace à deux dimensions, engendrés par les états de base  $|0\rangle$  et  $|1\rangle$ . Notre espace est ici fini, il est donc plus simple d'utiliser une représentation matricielle :

$$|0\rangle \rightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix}; |1\rangle \rightarrow \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

et ainsi :

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \rightarrow \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

De plus, la norme d'un vecteur peut être défini par :

$$\|\psi\| = \sqrt{\langle\psi|\psi\rangle} = \sqrt{\alpha^2 + \beta^2}$$

$$\text{Avec } \langle\psi|\psi\rangle = (\alpha \ \beta) \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

□ **Postulat de la mesure :** Le point important à retenir est qu'effectuer une mesure transforme le qubit. Si nous avons un état  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$  et que l'on effectue une mesure sur celui-ci alors dans ce cas  $|\psi\rangle = |0\rangle$  ou  $|1\rangle$ , autrement dit le qubit  $|\psi\rangle$  a été projeté dans la base  $\{|0\rangle, |1\rangle\}$ . Imaginons que la mesure nous donne le résultat  $|0\rangle$  et bien il est maintenant impossible d'effectuer la moindre opération sur l'état  $|\psi\rangle$  car la mesure a modifié notre état et l'a transformé en  $|\psi\rangle = |0\rangle$ . Il est alors impossible de retirer des informations supplémentaires sur ce qubit.

- **Postulat de l'évolution :** L'évolution d'un système quantique fermé, c'est à dire sans interaction extérieure, est décrit par une transformation unitaire. Cette évolution de l'état provient de l'application d'un opérateur linéaire, nommé l'opérateur d'évolution, qui est un opérateur unitaire (préservant la norme). Prenons un état  $|\psi\rangle$  d'un système quelconque au temps  $t_1$ , et bien cet état est lié à l'état  $|\psi'\rangle$  du système au temps  $t_2$  par l'opérateur d'évolution  $U$  qui dépend seulement du temps entre  $t_1$  et  $t_2$ .

$$|\psi'\rangle = U|\psi\rangle$$

### 1.1.2 Exemples d'opérations sur les qubits

La manipulation de qubits se fait à l'aide d'opérateurs unitaires, en tant qu'opérateurs d'évolution, pouvant être représentés par leur matrice unitaire, qui est une généralisation des matrices orthogonales aux complexes. Nous présentons alors ci-dessous les principales matrices unitaires permettant de manipuler les qubits. Ces portes seront réutilisées tout au long du rapport.

**Porte quantique X ou NON (NOT) :** La matrice de l'application NOT dans la base  $|0\rangle, |1\rangle$  est :

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Cette matrice permet d'effectuer les transformations suivantes :

$$X|0\rangle = |1\rangle \text{ et } X|1\rangle = |0\rangle$$

**Porte quantique Y :** La porte Y est définie par la matrice :  $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$  dont la table de vérité est :

$$\begin{aligned} |0\rangle &\rightarrow i|1\rangle \\ |1\rangle &\rightarrow -i|0\rangle \end{aligned}$$

**Porte quantique Z :** La porte Z est définie par la matrice :  $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$  ou opérateur de *flip* dont la table de vérité est :

$$\begin{aligned} |0\rangle &\rightarrow |0\rangle \\ |1\rangle &\rightarrow -|1\rangle \end{aligned}$$

**Porte quantique de Hadmard ou H :** La porte de Hadamard est définie par la matrice :  $H = \frac{1}{\sqrt{2}}(X + Z) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$  dont la table de vérité est :

$$\begin{aligned} |0\rangle &\rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |1\rangle &\rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned}$$

**Porte quantique  $U_\theta$  :** La porte  $U_\theta$  est définie par la matrice :  $U_\theta = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$ , rotation d'angle  $\theta$ , dont la table de vérité est :

$$\begin{aligned} |0\rangle &\rightarrow \cos(\theta)|0\rangle + \sin(\theta)|1\rangle \\ |1\rangle &\rightarrow \cos(\theta)|1\rangle - \sin(\theta)|0\rangle \end{aligned}$$

## 1.2 Téléportation quantique

Nous allons voir, dans cette partie, un exemple d'application possible en utilisant les concepts de la théorie de l'information quantique.

### 1.2.1 Formulation du problème

*Un agent secret (ou pas) remet à Anne une enveloppe (ici, le qubit) qui contient un message (l'état du qubit) très important destiné à un autre agent, Benoît situé à quelques kilomètres de là (mais cela pourrait être des milliards de kilomètres). L'agent demande à Anne de ne pas prendre connaissance du message (état inconnu du qubit) et, n'ayant pas confiance dans les services postaux, de ne pas envoyer l'enveloppe à Benoît (c'est-à-dire ici, de ne pas envoyer le qubit en lui-même, mais seulement l'information qu'il contient). Dans ces conditions comment Anne parviendra-t-elle à transmettre le message à Benoît ?*

**Remarque 1.2.1.** *Nous pouvons remarquer que la notion de téléportation abordée ici est un transfert d'information et non pas de matière.*

### 1.2.2 Circuit quantique

### 1.2.3 Protocole quantique

Dans tout ce protocole, nous supposons qu'Anne et Benoît se sont rencontrés précédemment et se sont partagé à l'amiable un système à deux qubits intriqué, plus exactement l'état de Bell (qui nous le rappelons est défini par  $|\psi_{Bell}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ ). De plus, Anne détient un deuxième qubit dont l'état lui est inconnu  $|\psi_{A_1}\rangle =$

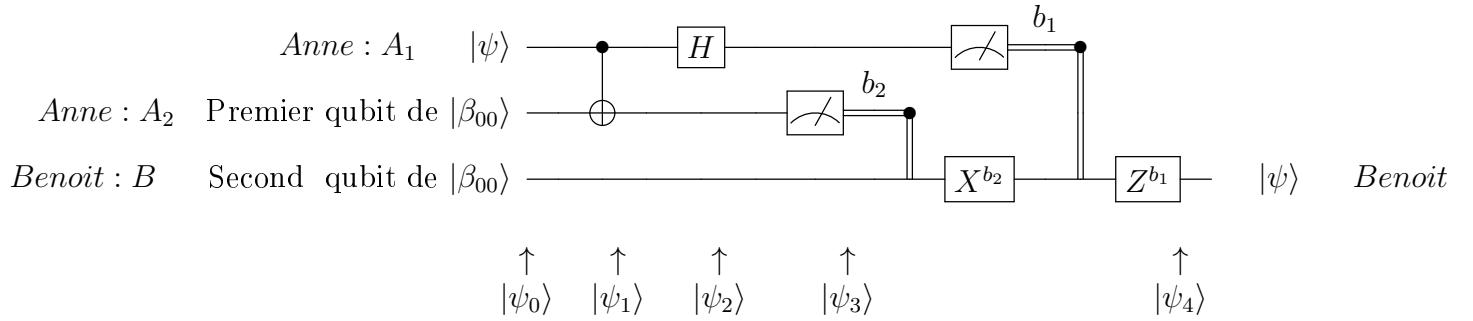


FIGURE 1.1 – Circuit de téléportation

$\alpha|0\rangle + \beta|1\rangle$ , qui par ailleurs veut être transmis à Benoît (nous parlons bien, ici, de l'état du qubit). Nous obtenons donc un système à 3 qubits dont l'état est décrit par :

$$\begin{aligned}
 |\psi_0\rangle &= |\psi_{Bell}\rangle \otimes |\psi_{A_1}\rangle = \frac{1}{\sqrt{2}} \underbrace{(\alpha|0\rangle + \beta|1\rangle)}_{|A_1\rangle} \underbrace{(|00\rangle + |11\rangle)}_{|A_2B\rangle} \\
 &= \frac{1}{\sqrt{2}} \{ \alpha(|000\rangle + |011\rangle) + \beta(|100\rangle + |111\rangle) \} \text{ avec } \underbrace{|\dots\rangle}_{|A_1A_2B\rangle}
 \end{aligned}$$

1. La première étape de la téléportation consiste à appliquer la porte C-Not sur le système à 2 qubits constitué par la paire des qubits que détient Anne :  $A_1$  et  $A_2$ . Ainsi, Anne obtient :

$$|\psi_1\rangle = \frac{1}{\sqrt{2}} \{ \alpha(|000\rangle + |011\rangle) + \beta(|110\rangle + |101\rangle) \}$$

2. Ensuite, la deuxième étape consiste à envoyer le premier qubit d'Anne, noté  $A_1$ , sur une porte de Hadamard. De fait, l'état  $|\psi_1\rangle$  devient :

$$\begin{aligned}
 |\psi_2\rangle &= \frac{1}{2} \{ \alpha(|000\rangle + |100\rangle + |011\rangle + |111\rangle) + \beta(|010\rangle - |110\rangle + |011\rangle - |101\rangle) \} \\
 &= \frac{1}{2} \{ |00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle + \beta|0\rangle) \}
 \end{aligned}$$

Ici, nous pouvons voir que l'état du qubit inconnu est complètement déterminé par l'état du système à 2 qubits défini par  $|A_1A_2\rangle$ . Ce phénomène est dû à l'intrication quantique.

3. Anne mesure l'état du système  $|A_1A_2\rangle$  et transmet le résultat de cette mesure, appelé mesures de Bell, à Benoît par n'importe quel moyen de communication (ex : telephone,...) : cette étape montre bien que la relativité n'est pas remise en question dans le principe de téléportation.

4. Benoît reçoit le résultat d'Anne noté  $|a_1a_2\rangle$ . Il effectue enfin l'opération  $Z^{a_1}X^{a_2}$ , avec "Z" et "X" les sortes logiques quantiques définies précédemment, sur son qubit. Le résultat de cette manipulation donnera, avec certitude, l'état du qubit inconnu noté  $|A_1\rangle$ .

### 1.3 Principe du Superdense coding à 2-qubits

Notre second exemple d'application de l'intrication pour la communication sera le Superdense coding. Ce moyen de communication introduit pour la première fois en 1992<sup>2</sup>, permet de mettre en place un codage et une transmission des informations plus "dense" que les protocoles classiques. En effet, le principe est le suivant :

*Alice et Bob partagent initialement l'état de Bell  $\beta_{00}$  : chacun d'entre eux possède un qubit de cet état intriqué. Comment Alice peut elle transmettre deux bits classiques d'information à Bob, en ne lui envoyant qu'un seul qubit ?*

Alice voudrait donc transmettre à Bob l'un des état basiques suivant :  $|00\rangle$ ,  $|01\rangle$ ,  $|10\rangle$  et  $|11\rangle$ . Les étapes du protocole de Superdense coding sont les suivantes :

- Alice choisit les 2 bits qu'elle veut transmettre
- En fonction de ces derniers, elle agit sur son qubit appartenant à l'état de Bell partagé
  - Alice envoie son qubit de l'état de Bell après manipulation
  - Bob réceptionne ce qubit, et applique alors une porte à tout le système intriqué
  - L'état de base à 2 qubits ainsi récupéré correspond aux 2 bits choisis par Anne

En fonction de l'état de base à 2 qubits choisi par Alice, la manipulation sur le premier qubit de  $\beta_{00} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$  sera différente :

| Choix de Anne | Manipulation associée sur $\beta_{00}$ |
|---------------|--|
| $ 00\rangle$  | $I$                                    |
| $ 01\rangle$  | $X_1$                                  |
| $ 10\rangle$  | $Z_1$                                  |
| $ 11\rangle$  | $(ZX)_1$                               |

Il en résulte donc la transformation suivante, en fonction de chacun des choix de Alice.

---

2. C. H. Bennett and Stephen J. Wiesner, Phys. Rev. Lett. 69, 2881 (1992)

$$\begin{aligned}
|00\rangle &: \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \xrightarrow{I} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\omega_1\rangle \\
|01\rangle &: \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \xrightarrow{X_1} \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) = |\omega_2\rangle \\
|10\rangle &: \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \xrightarrow{Z_1} \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = |\omega_3\rangle \\
|11\rangle &: \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \xrightarrow{(ZX)_1} \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = |\omega_4\rangle
\end{aligned}$$

Une fois son qubit manipulé, elle l'envoie à Bob. Il possède donc désormais l'état intriqué dans son intégralité. Il applique alors la porte inverse de la porte génératrice des états de Bell à savoir : une porte c-NOT contrôlée par le premier qubit, suivie d'une porte de Hadamard sur le premier qubit également.

Bob applique donc ce circuit-ci :

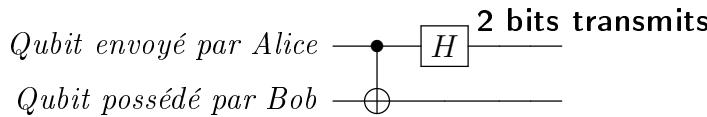


FIGURE 1.2 – Circuit appliqué par Bob pour décoder

C'est à la sortie de ce circuit que l'on retrouve l'état initialement choisi pour être transmis par Alice. Vérifions cela pour chacun des cas de figure :

$$\begin{aligned}
|\omega_1\rangle &\xrightarrow{c-NOT} \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \xrightarrow{H} \frac{1}{2}[ (|0\rangle + |1\rangle)|0\rangle + (|0\rangle - |1\rangle)|0\rangle ] = |\mathbf{00}\rangle \\
|\omega_2\rangle &\xrightarrow{\text{---}} \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle) \xrightarrow{\text{---}} \frac{1}{2}[ (|0\rangle + |1\rangle)|1\rangle + (|0\rangle - |1\rangle)|1\rangle ] = |\mathbf{01}\rangle \\
|\omega_3\rangle &\xrightarrow{\text{---}} \frac{1}{\sqrt{2}}(|00\rangle - |10\rangle) \xrightarrow{\text{---}} \frac{1}{2}[ (|0\rangle + |1\rangle)|0\rangle - (|0\rangle - |1\rangle)|0\rangle ] = |\mathbf{10}\rangle \\
|\omega_4\rangle &\xrightarrow{\text{---}} \frac{1}{\sqrt{2}}(|01\rangle - |11\rangle) \xrightarrow{\text{---}} \frac{1}{2}[ (|0\rangle + |1\rangle)|1\rangle - (|0\rangle - |1\rangle)|1\rangle ] = |\mathbf{11}\rangle
\end{aligned}$$

Ainsi, Alice peut en effet transmettre deux bits d'information qu'elle doit avoir préalablement choisi, en n'envoyant qu'un seul qubit au destinataire Bob. Il y a donc un réel "gain" d'information en utilisant ce processus.

## 1.4 Protocole BB84

Afin d'étudier la protocole BB84<sup>3</sup>, nous nous plaçons ici dans le cadre d'un codage à clé privée.

L'information transmise par Alice vers Bob prendra la forme de photons, dont la polarisation sert de support au codage de l'information. On introduit donc les

3. C. H. Bennett et G. Brassard en 1984

états de base de polarisation d'un photon, en leur associant chacun la valeur d'un qubit :

$$\begin{aligned} |\rightarrow\rangle &\equiv |0\rangle \\ |\uparrow\rangle &\equiv |1\rangle \end{aligned}$$

Alice dispose en fait d'un émetteur, "un par un", de photons, muni d'un polariseur lui permettant de polariser horizontalement ou verticalement ce photon, codant ainsi le  $|0\rangle$  ou le  $|1\rangle$ . Bennett et Brassard proposent alors d'introduire une nouvelle base de polarisation dans laquelle les polariseurs sont inclinés de  $-45^\circ$  par rapport à la base précédente. Les états possibles du photons seront donc :

$$\begin{aligned} |\nwarrow\rangle &= \frac{1}{\sqrt{2}}(|\rightarrow\rangle - |\uparrow\rangle) \equiv |0\rangle \\ |\nearrow\rangle &= \frac{1}{\sqrt{2}}(|\rightarrow\rangle + |\uparrow\rangle) \equiv |1\rangle \end{aligned}$$

De ce fait, le qubit  $|1\rangle$  pourra être codé de 2 manières différentes : soit par la polarisation  $|\uparrow\rangle$ , soit par la polarisation  $|\nearrow\rangle$ . Pour savoir dans quelle base de polarisation on travaille, on introduit la notation  $\oplus$  pour la base de polarisation horizontale/verticale, et  $\otimes$  pour la base de polarisation à  $45^\circ$ .

Ainsi, un photon polarisé  $|\nearrow\rangle$  aura une probabilité de 1 d'être le résultat de la mesure du photon dans la base  $\otimes$ , mais une probabilité de  $\frac{1}{2}$  dans la base  $\oplus$ , car  $|\frac{1}{\sqrt{2}}|^2 = \frac{1}{2}$ .

#### 1.4.1 Exemple de transmission d'un seul qubit

Supposons qu'Alice veuille transmettre un qubit  $|0\rangle$  en polarisant un photon avec un polariseur orienté au hasard  $\oplus$  ou  $\otimes$ . Ce même photon est intercepté par un espion, que l'on nommera Eve, qui en mesure la polarisation dans la base  $\oplus$ . On cherche à savoir qu'elle est la probabilité pour qu'il mesure bien  $|0\rangle$ .

Eve utilise donc la base  $\oplus$  pour la mesure.

- Si Alice utilise la base  $\oplus$  pour polariser son photon, alors Eve mesurera  $|0\rangle$  avec une probabilité de 1.
- Si Alice utilise la base  $\otimes$  pour polariser son photon, elle enverra donc le photon polarisé  $|\nwarrow\rangle$ . Comme  $|\nwarrow\rangle = \frac{1}{\sqrt{2}}(|\rightarrow\rangle - |\uparrow\rangle)$ , le qubit a une chance sur deux d'être projeté sur l'un des vecteurs de base de la base de mesure  $\oplus$ . Eve mesurera alors  $|0\rangle$  avec une probabilité de  $\frac{1}{2}$ .

En supposant qu'Alice ait autant de chance de choisir l'une ou l'autre des deux bases de polarisation, c'est à dire une chance sur deux de choisir  $\oplus$  ou  $\otimes$ , on peut

calculer la probabilité qu'Eve mesure  $|0\rangle$  sur le photon intercepté.

Soient les évènements A : “Eve mesure  $|0\rangle$ ”, B : “Alice choisit la base  $\oplus$ ” et C : “Alice choisit la base  $\otimes$ ”. Comme les évènements B et C forment un système complet d'évènements, d'après la formule des probabilités totales, nous avons donc :

$$p(A) = p(A \cap B) + p(A \cap C)$$

D'où d'après les formules des probabilités conditionnelles :

$$p(A) = p(B) \times p_B(A) + p(C) \times p_C(A)$$

Or on sait que  $p(B) = p(C) = p_C(A) = \frac{1}{2}$  et que  $p_B(A) = 1$ . On obtient alors le résultat suivant :

$$p(A) = \frac{1}{2} \times \frac{1}{2} + 1 \times \frac{1}{2} = \frac{3}{4}$$

**L'espion Eve a donc 75% de chances de mesurer  $|0\rangle$  pour un photon codé initialement  $|0\rangle$  par Alice dans une base choisie au hasard.**

Introduisons maintenant, encore un fois, une nouvelle base de polarisation. Au lieu cette fois ci de tourner la base  $\oplus$  d'un angle de  $45^\circ$ , nous effectuerons une rotation de cette même base  $\oplus$  mais d'un angle  $\theta$ . On définit ainsi les deux vecteurs de base,  $|\theta\rangle$  et  $|\theta_\perp\rangle$  de cette nouvelle base vérifient :

$$\begin{aligned} |\theta\rangle &= \cos(\theta)|\rightarrow\rangle + \sin(\theta)|\uparrow\rangle \equiv |0\rangle \\ |\theta_\perp\rangle &= \sin(\theta)|\rightarrow\rangle - \cos(\theta)|\uparrow\rangle \equiv |1\rangle \end{aligned}$$

Il sera utile pour la suite de relier dès à présent les vecteurs de cette nouvelle base que l'on appellera  $\Theta$ . En utilisant les relations déjà établies entre les 2 bases  $\oplus$  et  $\otimes$  on obtient :

$$\begin{aligned} |\rightarrow\rangle &= \cos(\theta)|\theta\rangle + \sin(\theta)|\theta_\perp\rangle \\ |\uparrow\rangle &= \sin(\theta)|\theta\rangle - \cos(\theta)|\theta_\perp\rangle \\ |\nwarrow\rangle &= \frac{\cos(\theta) - \sin(\theta)}{\sqrt{2}}|\theta\rangle + \frac{\cos(\theta) + \sin(\theta)}{\sqrt{2}}|\theta_\perp\rangle \\ |\nearrow\rangle &= \frac{\sin(\theta) + \cos(\theta)}{\sqrt{2}}|\theta\rangle + \frac{\sin(\theta) - \cos(\theta)}{\sqrt{2}}|\theta_\perp\rangle \end{aligned}$$

On sait qu'à présent Eve utilise donc la base  $\Theta$  pour la mesure.

- Si Alice utilise la base  $\oplus$  pour polariser son photon, alors Eve mesurera  $|0\rangle$  avec une probabilité de  $\cos^2(\theta)$ .
- Si Alice utilise la base  $\otimes$  pour polariser son photon, alors Eve mesurera  $|0\rangle$  avec une probabilité de  $(\frac{\cos(\theta)-\sin(\theta)}{\sqrt{2}})^2 = \frac{1}{2} - \sin(\theta)\cos(\theta)$ .

En supposant qu’Alice ait toujours autant de chance de choisir l’une ou l’autre des deux bases de polarisation  $\oplus$  ou  $\otimes$ , on peut calculer la probabilité  $p(\theta)$  qu’Eve mesure  $|0\rangle$  sur le photon intercepté :

$$p(\theta) = \frac{1}{2} \times \cos^2(\theta) + \frac{1}{2} \times \left(\frac{1}{2} - \sin(\theta)\cos(\theta)\right)$$

On linéarise cette expression à l’aide des formules de trigonométrie usuelles :

$$p(\theta) = \frac{1}{4} \times (\cos(2\theta) + 1) + \frac{1}{2} \times \left(\frac{1}{2} - \frac{1}{2}\sin(2\theta)\right)$$

Après simplification, on trouve :

$$p(\theta) = \frac{1}{4}(2 + \cos(2\theta) - \sin(2\theta))$$

Il serait maintenant intéressant de chercher pour quel angle optimal  $\theta$  tel que la probabilité pour Eve de mesurer  $|0\rangle$  est la plus élevée. Il suffit en effet de trouver pour quelle valeur de  $\theta$  on atteint la maximum de la fonction  $p(\theta)$ . Après étude de la fonction, on trouve que pour un angle  $\theta = \frac{7\pi}{8}$  la fonction atteint son maximum  $p(\frac{7\pi}{8}) = \frac{2+\sqrt{2}}{4} \simeq 85\%$ .

**L’espion Eve a donc 85% de chance au maximum de mesurer  $|0\rangle$  dans la base  $\Theta$  pour un photon codé initialement  $|0\rangle$  par Alice dans une base choisie au hasard parmi  $\oplus$  et  $\otimes$ .**

Supposons maintenant qu’Alice et Bob aient leur polariseurs orientés dans la même direction, mais que le photon, émis initialement par Alice dans l’état  $|0\rangle$  soit intercepté par l’espion Eve. Celui-ci mesure la polarisation avec un choix aléatoire d’orientation entre  $\oplus$  et  $\otimes$  : quelle la probabilité qu’Eve altère l’information de départ, c’est à dire, **quelle est la probabilité que Bob reçoive le photon dans l’état  $|1\rangle$  ?**

Pour répondre à cette question, dans le fond promordiale en cryptographie quantique, il apparait important dans un premier temps de lister toutes les combinaisons de choix de base pour Alice, Bob et Eve :

|    | Alice     | Eve       | Bob       |
|----|-----------|-----------|-----------|
| 1. | $\oplus$  | $\oplus$  | $\oplus$  |
| 2. | $\oplus$  | $\otimes$ | $\oplus$  |
| 3. | $\otimes$ | $\otimes$ | $\otimes$ |
| 4. | $\otimes$ | $\oplus$  | $\otimes$ |

Soit l'évènement D : "Bob reçoit la photon dans l'état  $|1\rangle$ ". On se propose de calculer la probabilité de l'évènement D en fonction de chaque cas de figure figurants ci-dessus.

– Si la base utilisée par Alice et Bob et la même que celle utilisée par Eve, alors la polarisation du photon ne sera pas altérée. Ceci se manifeste dans les cas 1 et 3, d'où :

$$p_1(D) = p_3(D) = 0$$

– Si la base utilisée par Alice et Bob diffère de celle utilisée par Eve, il y a une probabilité d' $\frac{1}{2}$  qu'Eve mesure et modifie l'état du qubit  $|0\rangle$  en  $|1\rangle$ , du fait de la différence de base entre Alice et Eve. Ensuite, Bob a lui aussi une probabilité d' $\frac{1}{2}$  de modifier le qubit, du fait de la différence entre sa base et celle d'Eve. On retrouve ce cas de figure dans les cas 2 et 4, d'où :

$$p_2(D) = p_4(D) = \frac{1}{2} \times \frac{1}{2} + \frac{1}{2} \times \frac{1}{2} = \frac{1}{2}$$

Au final, en supposant que chacun de ces 4 cas ait la même probabilité de se réaliser, on trouve :

$$p(D) = \frac{1}{4}(p_1(D) + p_2(D) + p_3(D) + p_4(D))$$

D'où

$$p(D) = \frac{1}{4}$$

**Bob a donc 1 chance sur 4 de mesurer le mauvais qubit transmit, sachant qu'un espion à antérieurement intercepté ce dernier.**

#### 1.4.2 Exemple de transmission de plusieurs qubits

On s'intéresse maintenant au cas où Alice tente de transmettre plus qu'un seul qubit d'information à Bob. Pour transmettre plusieurs qubits à Bob on supposera

qu'Alice les transmet un par un. De plus, pour chaque qubit, Alice choisit aléatoirement la base de polarisation, toujours entre  $\oplus$  et  $\otimes$ . Alice transmet alors les photons polarisés en fonction du message binaire, et de la base choisie pour chaque bit.

Lorsque Bob reçoit les photons, il procède de son côté à la même opération qu'Alice : il choisit aléatoirement, pour chaque qubit, la base de mesure entre  $\oplus$  et  $\otimes$ . Une fois les différents choix effectués, il communique publiquement la liste de ses choix à Alice. Alice compare alors les deux listes de choix de bases de polarisation.

Alice transmet alors, toujours publiquement, quelles sont les positions des qubits de la séquence pour lesquels la base de polarisation est la même. Pour ces positions là, Alice et Bob auront bien les même valeurs de qubits, puisque pour ces qubits là, ils auront utilisés le même choix de codage.

Ainsi Alice et Bob peuvent utiliser ces qubits "sûrs" pour constituer une clé privée de codage.

La théorie étant énoncée, voyons un exemple pratique de transmission de 6 qubits entre Alice et Bob :

|              |                      |                    |                    |                       |                    |                       |                       |
|--------------|----------------------|--------------------|--------------------|-----------------------|--------------------|-----------------------|-----------------------|
| Alice        | Bits à transmettre   | 1                  | 0                  | 0                     | 1                  | 1                     | 0                     |
|              | Choix de base        | $\oplus$           | $\otimes$          | $\oplus$              | $\otimes$          | $\otimes$             | $\oplus$              |
|              | Polarisation envoyée | $ \uparrow\rangle$ | $ \nwarrow\rangle$ | $ \rightarrow\rangle$ | $ \nearrow\rangle$ | $ \nearrow\rangle$    | $ \rightarrow\rangle$ |
| Bob          | Choix de base        | $\oplus$           | $\oplus$           | $\otimes$             | $\otimes$          | $\oplus$              | $\oplus$              |
|              | Polarisation mesurée | $ \uparrow\rangle$ | $ \uparrow\rangle$ | $ \nwarrow\rangle$    | $ \nearrow\rangle$ | $ \rightarrow\rangle$ | $ \rightarrow\rangle$ |
|              | Bits lus             | 1                  | 1                  | 0                     | 1                  | 0                     | 0                     |
| Alice et Bob | Bits acceptés ?      | ✓                  | ✗                  | ✗                     | ✓                  | ✗                     | ✓                     |
|              | Message secret       | 1                  |                    |                       | 1                  |                       | 0                     |

La clé de codage secrète ainsi générée et partagée par Alice et Bob sera donc : **110**. Ainsi, dans cet exemple, Alice et Bob ont engendré 3 bits. Ils peuvent en fait engendrer autant qu'ils veulent en utilisant ce système. En moyenne, Bob devinera le bon positionnement de la base dans 50% des cas. Alice devra donc envoyer en moyenne  $2n$  photons pour générer un code à  $n$  bits.

Mais, à présent, comment s'assurer que ce message n'a pas été intercepté par un espion ?

Si un espion intercepte un photon, et que Bob a choisi la même base qu'Alice : l'espion a donc 25% de chance de modifier la valeur du qubit, et donc 75% de chances de ne pas modifier cette valeur<sup>4</sup>.

---

4. voir *Exemple de transmission d'un seul qubit*

On prélève alors 700 bits pour être comparés entre Alice et Bob. Attardons-nous sur 2 questions intéressantes

*Quelle est la probabilité que, si un espion mesure tous les qubits transmis, aucun des 700 bits ne soit modifié par cette interception ?*

Pour un qubit, la probabilité que l'espion ne le modifie pas après interception est de  $\frac{3}{4}$ . Ainsi, si on transmet 700 qubits, la probabilité d'en modifier aucun tout en espionnant est de  $(\frac{3}{4})^{700} \simeq 3,5 \cdot 10^{-88}$ .

*La ligne a un taux d'erreur physique de 3%. Quel pourcentage de qubit l'espion peut-il intercepter pour le taux d'erreurs dû à l'interception ne soit pas supérieur au taux physique ?*

S'il y a un taux d'erreur physique sur la ligne, Alice et Bob peuvent accepter que  $700 \times 3\% = 21$  qubits soient mal transmis. Sachant que l'espion a 25% (1 chance sur 4) de modifier un qubit intercepté, si il ne veut pas créer plus de 21 erreurs, il doit se limiter à observer  $21 \times 4 = 84$  qubits. Donc Eve ne pourra regarder que  $\frac{84}{700} = 12\%$  du message.

Ainsi, pour s'assurer que le canal de transmission n'est pas “écouté”, il suffit à Alice et Bob de prendre un échantillon de bits acceptés par Bob et Alice, et donc pour lesquels Alice et Bob possèdent exactement les bases de polarisation. Alice et Bob se communiquent cet échantillon là, et ils comparent chacuns le résultat de la transmission par rapport à la l'échantillon initial : *tous les bits doivent être identiques*. Une seule différence signe la présence d'un intrus ou d'une erreur physique sur la ligne. L'intrusion n'est avérée que si le taux de bits qui diffèrent dans le processus de reconnaissance est supérieur au taux d'erreur physique. Si le nombre de bits échangés est suffisamment grand, le fait qu'ils soient tous identiques correspond à la quasi-certitude de n'avoir pas été écouté.

Si une erreur est détectée sur cette transmission de vérification, Alice et Bob devront recommencer un nouveau processus et retester la sécurité de la ligne.

## 1.5 Multiplexeurs

### 1.5.1 Fonctionnement classique

Les multiplexeurs (ou plus connu sous le nom de MUX) font partie intégrante des moyens de communication en électronique. Ils permettent effectivement de sélectionner, sur un ensemble d'informations récoltées (en entrée du MUX), un ou plusieurs types de données à transmettre (en sortie du MUX). Ceci est réalisé à

l'aide notamment d'un auxiliaire de contrôle (par exemple un ou plusieurs bits de contrôle dont l'état est 0 ou 1) qui permet de définir les données d'entrées à transferer en sortie du MUX. Il faut noter que cette manipulation est effectuée afin de condenser l'information pour n'obtenir plus qu'une seule voie en sortie.

Voici un exemple de MUX qui passe de 4 entrées à une seule sortie [71] :

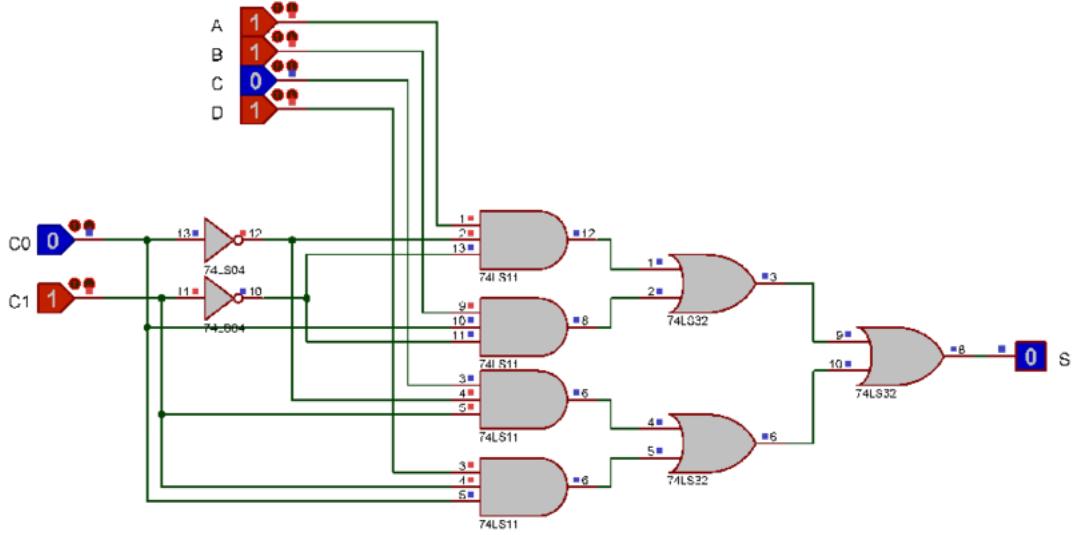


FIGURE 1.3 – Exemple de MUX 4 :1

Sur cet exemple, nous pouvons constater que les portes classiques NON, ET et OU sont utilisées. Nous avons en entrée  $(A, B, C, D) = (1, 1, 0, 1)$  et les bits de contrôle sont à l'état  $(C_0, C_1) = (0, 1)$ . Ceci nous permet d'obtenir l'information détenue par le bit C en sortie. Il nous suffit de changer l'état des bits de contrôle afin de déterminer l'entrée à sélectionner.

### 1.5.2 Portes quantiques sur plusieurs qubits

Il nous paraît utile de rappeler les principales portes quantiques agissant sur 2 qubits dont la porte c-NOT, SWAP et CSAWP (plus connu sous le nom Fredkin).

## Porte c-NOT

La porte c-NOT, ou *controlled NOT* est souvent utilisée pour remplacer la porte NOT. Elle fonctionne de la manière suivante :

| Etat d'entrée | Etat de sortie |
|---------------|----------------|
| $ 00\rangle$  | $ 00\rangle$   |
| $ 01\rangle$  | $ 01\rangle$   |
| $ 10\rangle$  | $ 11\rangle$   |
| $ 11\rangle$  | $ 10\rangle$   |

La porte c-NOT agit en effet sur un système à deux qubits. Le premier bit sert de contrôle (bit de *contrôle*) et le second bit (bit *cible*) subit ou pas une négation, en fonction de l'état du bit de *contrôle*. Sachant comment l'opérateur c-NOT transforme les vecteurs de la base  $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ , on peut alors le représenter par une matrice, dans cette même base :

$$\text{c-NOT : } \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Ainsi, la valeur du bit *cible* est inchangée, si le bit de *contrôle* vaut 0 et la valeur du bit *cible* est changée, si le bit de *contrôle* vaut 1. En fait, le bit *cible* vaut à la sortie la somme, modulo 2, des deux bits d'entrée, tandis que le bit de *contrôle* reste inchangé. On note alors, c-NOT :  $(x, y) \rightarrow (x, x \oplus y)$ .

En plus de la notation matricielle, on peut introduire la représentation sous forme de circuit des opérateurs :

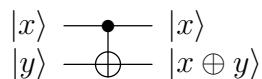


FIGURE 1.4 – Porte c-NOT

On voit donc ici que la porte c-NOT prend en entrée deux qubits simples :  $|x\rangle$  et  $|y\rangle$  formant à eux deux un système à deux qubits. Le système passe donc la porte c-NOT et cette dernière retourne le résultat attendu, à savoir : on retourne l'identité du premier qubit d'entrée sur le premier qubit de sortie, et on retourne une somme binaire entre les deux premiers qubits sur le second qubit de sortie.

## Porte SWAP

La porte SWAP, comme son nom l'indique, échange la place les deux qubits passés en paramètre : SWAP :  $(x, y) \rightarrow (y, x)$ . La porte SWAP se compose d'une succession de 3 portes c-NOT, avec alternance du bit de *contrôle* :

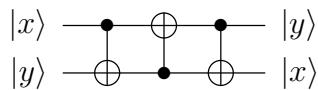


FIGURE 1.5 – Porte SWAP

## Porte Fredkin (CSWAP)

Cette porte est une extension de la porte SWAP. En effet, elle permet, comme la porte c-NOT, d'avoir un bit de contrôle. Le circuit et les matrices représentant cette porte (pour les deux cas où le qubit de contrôle vaut  $|0\rangle$  ou  $|1\rangle$ ) est défini ci-dessous [63] :

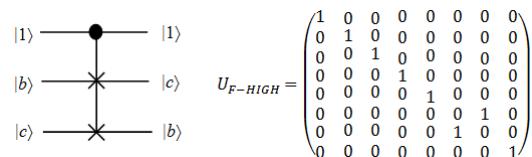


FIGURE 1.6 – Qubit de contrôle  $|1\rangle$  (configuration "High")

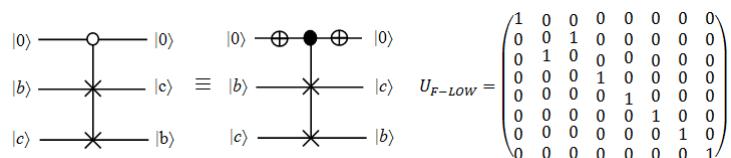


FIGURE 1.7 – Qubit de contrôle  $|0\rangle$  (configuration "Low")

Nous pouvons noter que cette porte peut disposer de plusieurs qubits de contrôle (par exemple, pour 2 qubits de contrôle nous disposerons de 4 configurations possibles).

### 1.5.3 Exemple : Multiplexeur quantique 4 : 1

Pour expliquer le fonctionnement d'un multiplexeur quantique, nous avons choisi d'étudier le cas particulier où l'on a 4 entrées et 1 sortie ( QMUX 4 : 1) avec 2 qubits de contrôle [63].

Le circuit représentant ce multiplexeur quantique est défini de la manière suivante :

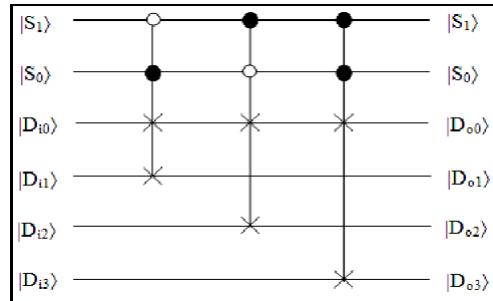


FIGURE 1.8 – Circuit : Multiplexeur quantique 4 : 1

Sur celui-ci, nous avons  $|S\rangle_0$  et  $|S\rangle_1$  qui sont les qubits de contrôle,  $|D\rangle_{i0}$  et  $|D\rangle_{i3}$  les qubits d'entrées et  $|D\rangle_{i0}$  le qubit de sortie. Ce dernier fait parti des circuits réversibles.

Ainsi, ce type de multiplexeur quantique pourrait servir à des fins de communication. De plus, il serait également possible de montrer que l'intrication des états quantique pourrait être transmise.

# Chapitre 2

## Jeux quantiques

La théorie de jeux est un domaine de science qui est très répandu de nos jours, et connaît des applications diverses, allant de la biologie à l'économie, en passant par l'énergie et les mathématiques. Nous nous proposons dans ce chapitre de présenter un certain nombre de jeux issus de la théorie des jeux quantiques. Cette théorie quantique des jeux vise à introduire les formalismes présents en théorie de l'information quantique afin de développer de nouvelles stratégies et de nouveaux jeux, dont la performance serait basée sur l'utilisation de la superposition et de l'intrication comme facteur d'amélioration des résultats. Les jeux qui seront réutilisés dans la seconde partie du rapport, c'est à dire ceux qui seront mis en scène dans une application énergétique seront plus amplement détaillés, par rapport aux autres jeux quantiques traités. La liste des jeux quantiques présentés n'est pas exaustive, mais comprend les jeux les plus connus dans la littérature associée.

### 2.1 CHSH-Game

Le CHSH Game est un jeu à 2 joueurs. Son nom est tiré des CHSH Inequalities introduites par Clauser, Horne, Shimony et Holt [3, 4]. Ceci vient tout d'abord du paradoxe EPR introduit en 1935 par Einstein, Podolsky et Rosen. En 1964, John Bell leur apportera une réponse en établissant sa célèbre "inégalité de Bell". De même, la "CHSH Inequality" sera introduite pour répondre à la théorie des variables cachées. Le CHSH Game sera alors présenté comme protocole à cette occasion, et c'est ce protocole en tant que jeu que nous allons étudier.

#### 2.1.1 Déroulement du jeu

Soient deux joueurs  $A$  et  $B$ , ne pouvant pas communiquer mutuellement, et  $R$  l'arbitre du jeu.  $R$  envoie une question biniaire, 0 ou 1, à chacun des joueurs de la

partie. On dénote par  $r$  la question envoyée à  $A$  et  $s$  la question envoyée à  $B$ . On dénote par  $rs$  la question globale envoyée aux joueurs. On note  $Q$  l'ensemble des questions possibles. L'arbitre posera alors la question  $rs \in Q$  avec :

$$Q = \{00, 01, 10, 11\}$$

Dans un second temps, les deux joueurs doivent donner une réponse suite à la réception de leur question. Leur réponse est également binaire, 0 ou 1, pour chacun des joueurs. On dénote par  $a$  la réponse du joueur  $A$  et par  $b$  la réponse du joueur  $B$ . On dit que le jeu est gagné si et seulement si :

$$r \vee s = a \oplus b$$

Le cœur du jeu est donc, pour les joueurs  $A$  et  $B$ , de trouver une stratégie qui maximise la probabilité de gagner au CHSH game.

### 2.1.2 Meilleures stratégies classiques

On peut imaginer différentes manières à  $A$  et  $B$  de s'accorder en avance pour répondre d'une manière précise en fonction de leur question respective. Mais certaines stratégies permettent d'atteindre la probabilité maximale de gagner qui est de  $\frac{3}{4}$ .

En effet, aucune stratégie classique ne permet de gagner le jeu de manière sûre. Pour le démontrer, on note respectivement  $a(r)$  et  $b(s)$  la réponse des joueurs  $A$  et  $B$  à leurs questions respectives  $r$  et  $s$ . Résoudre totalement le jeu reviendrait à trouver une stratégie, c'est-à-dire une réponse pour chacun des joueurs, en fonction de leurs questions, qui satisfait la condition de gain. En d'autres termes, cela reviendrait à trouver une solution aux équations suivantes :

$$\begin{aligned} 0 \vee 0 &= 0 = a(0) \oplus b(0) \\ 0 \vee 1 &= 1 = a(0) \oplus b(1) \\ 1 \vee 0 &= 1 = a(1) \oplus b(0) \\ 1 \vee 1 &= 1 = a(1) \oplus b(1) \end{aligned}$$

En sommant ces équations, on en déduit la condition suivante :

$$a(0) \oplus a(0) \oplus a(1) \oplus a(1) \oplus b(0) \oplus b(1) \oplus b(0) \oplus b(1) = 0 \oplus 1 \oplus 1 \oplus 1$$

Ceci nous amène à une absurdité ( $0 = 1$ ), ce qui montre que le système d'équation n'est pas résolvable, donc que ne peut trouver de solution qui résoud le jeu

totalelement. Les scientifiques du domaine on montré que l'on ne peut excéder une probabilité de  $\frac{3}{4}$  en faisant varier les stratégies. Cela peut se comprendre aussi de la manière suivante : si l'on retire une équation du système, le système devient résolvable, et il existe plusieurs solutions.

Ainsi, une des stratégies possible pour  $A$  et  $B$  est de répondre le complément de la question posée par l'arbitre. La stratégie se résume alors par ces équations :

$$a(0) = 1, a(1) = 0, b(0) = 1, b(1) = 0$$

Si l'on remplace ces valeurs dans le système on obtient alors :

$$0 = 1 \oplus 1$$

$$1 = 1 \oplus 0$$

$$1 = 0 \oplus 1$$

$$1 = 0 \oplus 0$$

On voit bien que 3 sur 4 équations sont correctes, et donc que l'on résoud le jeu dans 3 des 4 cas possibles : seule la question  $\{11\}$  posée par l'arbitre les fera échouer.

### 2.1.3 Stratégie quantique

La stratégie quantique pour résoudre le CHSH-Game est basée sur le fait que les joueurs  $A$  et  $B$  disposent d'une préparation supplémentaire avant le début du jeu. En effet, les 2 joueurs vont partager un état de Bell. Chacun des joueurs possèdera donc un qubit de l'état intriqué noté  $|\beta_{ell}\rangle$  définit par :

$$|\beta_{ell}\rangle = \frac{1}{\sqrt{2}} \left( |0_A 0_B\rangle + |1_A 1_B\rangle \right)$$

La stratégie à adopter pour le joueur  $A$  consiste donc en 2 cas :

- Si  $A$  reçoit la question  $\{0\}$  de la part de l'arbitre, il mesure son qubit dans la base classique  $\{|0\rangle, |1\rangle\}$  (base de  $Z$  de Pauli).  $A$  envoie ensuite le résultat de la mesure comme réponse à l'arbitre. Autrement dit, si  $A$  mesure  $|0\rangle$  pour son qubit, elle renvoie la réponse  $\{0\}$  à l'arbitre, et inversement.
- Si  $A$  reçoit la question  $\{1\}$  de la part de l'arbitre, il mesure son qubit dans la base  $\{|+\rangle, |-\rangle\}$  avec  $|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$  et  $|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$  (base de  $X$  de Pauli, ou base de Hadamard). Cela revient à appliquer la porte Hadamard à son qubit, puis de le mesure dans la base classique. Si  $A$  mesure  $|+\rangle$  elle répond  $\{0\}$  à l'arbitre ; si il mesure  $|-\rangle$  elle répond  $\{1\}$  à l'arbitre.

Le joueur  $B$  quant à lui, possède une base qu'il peut roter autour de l'origine selon un angle  $\alpha$  qu'il choisi. Les deux vecteurs de base  $\{|\phi\rangle, |\phi^\perp\rangle\}$ , vecteur orthogonaux dans la sphère de Bloch, se définissent alors de manière générique comme suit :

$$|\phi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)|1\rangle \quad |\phi^\perp\rangle = -\sin\left(\frac{\theta}{2}\right)|0\rangle + \cos\left(\frac{\theta}{2}\right)|1\rangle$$

La stratégie à adopter pour le joueur alors  $B$  consiste donc en 2 cas :

- Si  $B$  reçoit la question  $\{0\}$  de la part de l'arbitre, il mesure son qubit dans la base dont la direction dans la sphère de Bloch est entre celles des bases  $X$  et  $Z$  de Pauli, ce qui correspond à un angle de  $\frac{\pi}{4}$ .  $B$  envoie ensuite le résultat de la mesure comme réponse à l'arbitre. Autrement dit, si  $A$  mesure  $|\phi\rangle$  pour son qubit, il renvoie la réponse  $\{0\}$  à l'arbitre ; si il mesure  $|\phi^\perp\rangle$  il répond  $\{1\}$  à l'arbitre.
- Si  $B$  reçoit la question  $\{1\}$  de la part de l'arbitre, il mesure son qubit dans la base dont la direction dans la sphère de Bloch est entre l'opposé de la direction de la base  $X$  et l'opposé de la direction de la base  $Z$  de Pauli, ce qui correspond à un angle de  $\frac{3\pi}{4}$ .  $B$  envoie ensuite de la même manière que précédemment le résultat de la mesure comme réponse à l'arbitre.

En utilisant la sphère de Bloch comme représentation, on peut plus facilement s'apercevoir que c'est la stratégie la plus intéressante du point de vue du joueur  $B$ .

Intéressons nous maintenant à la probabilité de gain pour cette stratégie quantique. Avant cela, on rappelle les relations liant la base classique à la base de  $B$  :

$$|0\rangle = \cos\left(\frac{\theta}{2}\right)|\phi\rangle - \sin\left(\frac{\theta}{2}\right)|\phi^\perp\rangle \quad |1\rangle = \sin\left(\frac{\theta}{2}\right)|\phi\rangle + \cos\left(\frac{\theta}{2}\right)|\phi^\perp\rangle$$

Supposons que  $\{rs\} = \{00\}$ .  $A$  va donc mesurer son qubit dans la base classique : elle a autant de chance de mesurer  $|0\rangle$  que de mesurer  $|1\rangle$ . Dans les deux cas, le qubit de  $B$  se retrouve projeté dans le même état que celui de  $A$ . Pour gagner, les deux joueurs devront avoir la même réponse, car la question est  $\{00\}$  et que  $0 \oplus 0 = 1 \oplus 1 = 0 \vee 0 = 0$ . Si  $A$  mesure  $|0\rangle$ , le qubit de  $B$  en sera de même, et pour gagner  $B$  va devoir mesurer  $|\phi\rangle$  pour renvoyer la réponse  $\{0\}$ . Comme on le voit sur l'équation ci-dessus, la probabilité d'être projeté sur l'état  $|\phi\rangle$  en mesurant  $|0\rangle$  dans la base  $\{|\phi\rangle, |\phi^\perp\rangle\}$  est de  $|\cos(\frac{\theta}{2})|^2$  qui est dans notre cas actuel  $|\cos(\frac{\pi}{8})|^2$  car  $B$  a reçu la question  $\{0\}$ .

De la même manière, si  $A$  mesure  $|1\rangle$ ,  $B$  aura son qubit projeté vers  $|1\rangle$ , mais sans le savoir, car il ne l'a toujours pas mesuré. Voulant répondre  $\{1\}$  et étant donné que la probabilité de mesurer  $|\phi^\perp\rangle$  à partir de l'état  $|1\rangle$  est de  $|\cos(\frac{\pi}{8})|^2$ , on retrouve bien le même résultat que dans le cas précédent. Ceci se vérifie de la même manière pour les questions restantes  $\{01\}$ ,  $\{10\}$  et  $\{11\}$ , en considérant que  $|\sin(\frac{3\pi}{8})|^2 = |\cos(\frac{\pi}{8})|^2$ .

Ainsi la probabilité pour  $A$  et  $B$  de gagner le jeu avec la stratégie quantique est de  $\cos^2(\frac{\pi}{8}) \approx 0.85355339$ . On surpasse alors la stratégie classique dans ce cas grâce au partage d'un état intriqué.

#### 2.1.4 Variante du CHSH-Game

Cette variante proposée par Alan Bojić [5] possède globalement le même principe de jeu que le CHSH original, hormis la condition de gain du jeu qui est modifiée en inversant les opérateurs de part et d'autre de l'égalité, ce qui nous donne, avec les mêmes notations :

$$r \otimes s = a \vee b$$

Dans cette configuration, on montre, en suivant le même raisonnement que précédemment, que les joueurs  $A$  et  $B$  ne peuvent gagner que dans 50% des cas, au maximum, s'ils adoptent une stratégie classique. En posant les équations du jeu, le lecteur pourra s'assurer que l'on ne peut trouver de stratégie qui gagne à chaque fois, et qu'au maximum, quelque soit la stratégie, on ne peut vérifier que la moitié des équations du jeu simultanément au maximum.

En outre, si l'on suppose que les joueurs  $A$  et  $B$  décident de mettre en place leur stratégie quantique utilisée pour le CHSH Game original, afin de solutionner le jeu proposé par Bojić, on montre que la probabilité totale de gagner le jeu est d'environ 0.526, ce qui est meilleur que la stratégie classique.

Ce qui est intéressant, c'est que l'auteur propose également une nouvelle stratégie afin d'augmenter la probabilité de gagner. Succinctement, voici les étapes de la nouvelle stratégie quantique :

- Les joueurs  $A$  et  $B$  partagent un système à 2-qubit maximallement intriqué, initialisé avec l'état de Bell suivant  $\frac{1}{\sqrt{2}}(|0_A1_B\rangle - |1_A0_B\rangle)$

- Si le joueur  $A$  reçoit la question  $\{0\}$ , il applique l'identité sur son qubit (ou n'agit pas dessus). S'il reçoit la question  $\{1\}$  le joueur  $A$  applique la porte d'Hadamard sur son qubit. Le joueur  $B$  agira de la même manière que le joueur  $A$ , c'est à dire l'idenité si sa question est  $\{0\}$ , la porte d'Hadamard sinon.
- Les joueurs  $A$  et  $B$  mesurent leur qubit et renvoient leurs réponses respectives  $a$  et  $b$ , résultats de la mesure de leur qubit.

Avec cette nouvelle stratégie, si l'on détaille les différents cas, on s'aperçoit que l'on gagne avec une probabilité de 1, pour les questions  $\{00\}$  et  $\{11\}$ , et avec une probabilité de 25% pour les questions  $\{01\}$  et  $\{10\}$ . La probabilité totale de gagner s'élève donc à 0.625, ce qui surpasse les stratégies précédentes appliquées à ce jeu. On pourrait s'intéresser à trouver une stratégie plus performante, si elle existe.

## 2.2 GHZ-Game

Dans cette partie nous nous intéresserons au GHZ-game, variante à 3 joueurs du CHSH game. Le GHZ-game, contrairement au CHSH game, propose une probabilité de gain de 1, mais restreint le nombre de questions possibles de moitié pour l'arbitre.

### 2.2.1 Déroulement du jeu

Soit  $R$  l'arbitre du jeu. Soient  $A$ ,  $B$  et  $C$  les trois joueurs. Le jeu se déroule en deux temps. Dans un premier temps, l'aribtre sollicite respectivement chacun des joueurs en lui posant une question. Dans un second temps, les joueurs répondent à leurs questions respectives de manière à gagner le jeu, c'est à dire de manière à remplir une condition dépendant des questions posées et réponses données. La difficulté du jeu réside dans le fait que les trois joueurs sont isolés et ne peuvent en aucun cas communiquer entre eux une fois le jeu commencé (une fois la question posée). Le résultat au jeu dépendra de la préparation et des stratégies mis en place par les joueurs avant le début du jeu.

L'arbitre envoie donc une question à chaque joueur. Chaque question prend la forme d'un bit : 0 ou 1. On note respectivement  $r$ ,  $s$  et  $t$  la question posée à  $A$ ,  $B$  et  $C$ . Une manière de noter la question globale posée aux joueurs par l'arbitre est de concaténer les questions en un seul nombre binaire  $rst$ .

L'ensemble des question possibles est noté  $Q$  :

$$Q = \{000, 001, 010, 011, 100, 101, 110, 111\}$$

Le GHZ Game restreint de moitié le nombre de question pour l'arbitre, nous donnant l'ensemble  $\tilde{Q}$  :

$$\tilde{Q} = \{000, 011, 101, 110\}$$

On note ensuite respectivement  $a$ ,  $b$  et  $c$  les réponses données par les joueurs  $A$ ,  $B$  et  $C$ . Afin de gagner le jeu, les joueurs doivent remplir la condition suivante :

$$r \vee s \vee t = a \oplus b \oplus c$$

### 2.2.2 Résolution et stratégies classiques

Une fois le jeu défini, il apparaît intéressant de s'intéresser à sa résolution. On note respectivement  $a(r)$ ,  $b(s)$  et  $c(t)$  la réponse des joueurs  $A$ ,  $B$  et  $C$  à leur question respective  $r$ ,  $s$  et  $t$ . Résoudre totalement le jeu reviendrait à trouver une stratégie, c'est à dire une réponse pour chacun des joueurs, en fonction de sa question, qui satisfait la condition de gain. En d'autres termes, cela reviendrait à trouver une solution aux équations suivantes :

$$\begin{aligned} 0 \vee 0 \vee 0 &= 0 = a(0) \oplus b(0) \oplus c(0) \\ 0 \vee 1 \vee 1 &= 1 = a(0) \oplus b(1) \oplus c(1) \\ 1 \vee 0 \vee 1 &= 1 = a(1) \oplus b(0) \oplus c(1) \\ 1 \vee 1 \vee 0 &= 1 = a(1) \oplus b(1) \oplus c(0) \end{aligned}$$

En sommant ces équations, on en déduit la condition suivante :

$$a(0) \oplus a(0) \oplus b(0) \oplus b(1) \oplus b(0) \oplus b(1) \oplus c(0) \oplus c(1) \oplus c(1) \oplus c(0) = 0 \oplus 1 \oplus 1 \oplus 1$$

Autrement dit, on en arrive à  $0 = 1$ , ce qui est bien entendu une contradiction. On peut alors en conclure qu'il n'existe pas une configuration ou stratégie générale permettant de gagner de manière sûre le jeu.

Cependant, si l'on ne peut pas gagner le jeu avec une probabilité de 1 avec une stratégie classique, on peut se demander quelle est la probabilité maximale de gagner au GHZ-Game possible avec une stratégie classique. Cela se comprend également des équations établies plus haut. En effet, on ne peut valider les 4 équations simultanément et gagner à chaque fois le jeu, mais on montre que l'on peut au maximum valider 3 sur 4 des équations en choisissant certaines stratégies

(assignations de  $a(0), a(1), \dots, b(1)$ ). Par exemple, si on choisit la stratégie qui est de répondre la question qui nous est posée, donc  $a(0) = b(0) = 0$  et  $a(1) = b(1) = 1$ , alors on peut gagner avec une chance de  $\frac{3}{4} = 75\%$  car 3 des équations du systèmes seront toujours résolues. Bien entendu, tout ceci suppose que l'arbitre choisit de manière uniforme la probabilité de poser l'un ou l'autre des questions pour chaque joueur.

C'est un assez bon résultat à première vue, mais on ne peut malheureusement faire mieux pour les deux joueurs sans introduire de communication entre eux. Un moyen d'améliorer ce résultat est l'introduction d'une corrélation entre les joueurs, et c'est ce que nous allons voir avec la présentation de la stratégie quantique suivante

### 2.2.3 Stratégie quantique pour le GHZ-Game

La règle impose aux joueurs de ne pas communiquer entre eux durant le jeu, et donc d'éventuellement se préparer en amont pour maximiser les chances de gain. Un des manières de se préparer serait de partager un état intriqué et d'utiliser cette intrication afin de mettre en place un stratégie permettant encore une fois de maximiser les chances de gain, et si possible qu'elles soient supérieures à celles des stratégies classiques.

Supposons que les joueurs partagent un système quantique intriqués, un 3-qubit notamment. On choisit un état maximalement intriqué, c'est à dire un état équivalent à  $|GHZ\rangle$  noté  $|GHZ'\rangle$ , construit comme suit :

$$|GHZ'\rangle = P^{\otimes 3} H^{\otimes 3} |GHZ\rangle = \frac{1}{2} \left( |000\rangle - |011\rangle - |101\rangle - |110\rangle \right)$$

avec

$$H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \text{ et } P = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2}} \end{pmatrix}$$

La stratégie quantique pour chaque joueur est la suivante :

- Si le joueur reçoit la question  $\{0\}$  de la part de l'arbitre, il mesure sa particule dans la base classique  $\{|000\rangle, \dots, |111\rangle\}$  ( $Z$ -basis), et renvoie à l'arbitre le résultat de sa mesure comme réponse
- Si le joueur reçoit la question  $\{1\}$  de la part de l'arbitre, il mesure sa particule dans la base  $X$  de Pauli, ce qui revient à appliquer la porte Hadamard puis de mesure dans la base classique  $Z$ , et renvoie à l'arbitre le résultat de sa mesure comme réponse

Cette stratégie permet aux joueurs de gagner avec une probabilité de 1, pour une question appartenant à  $\tilde{Q}$ .

*Démonstration.* Si la question posée est  $\{000\}$ , alors chacun des joueurs n'agit pas (ou applique l'identité à sa particule) et mesure. L'état partagé par les 3 joueurs demeure toujours  $|GHZ'\rangle = \frac{1}{2}(|000\rangle - |011\rangle - |101\rangle - |110\rangle)$  et donc quelque soit l'état de base mesuré et envoyé par les joueurs, il répond bien à la condition de victoire du jeu :

$$0 \vee 0 \vee 0 = 0 \oplus 0 \oplus 0 = 0 \oplus 1 \oplus 1 = 1 \oplus 0 \oplus 1 = 1 \oplus 1 \oplus 0$$

Si la question posée est  $\{011\}$ , les joueurs  $B$  et  $C$  appliquent Hadamard à leur qubit avant la mesure. L'état partagé par les 3 joueurs devient donc :

$$|GHZ''\rangle = I \otimes H \otimes H |GHZ'\rangle = \frac{1}{2}(|001\rangle + |010\rangle - |100\rangle + |111\rangle)$$

On voit également ici que quelque soit l'état de base mesuré et la réponse envoyée par les joueurs, cela répond bien à la condition de victoire du jeu :

$$0 \vee 1 \vee 1 = 0 \oplus 0 \oplus 1 = 0 \oplus 1 \oplus 0 = 1 \oplus 0 \oplus 0 = 1 \oplus 1 \oplus 1$$

Par permutation, l'état obtenu avec les questions  $\{101\}$  et  $\{110\}$  est équivalent à celui obtenu avec la question  $\{011\}$ . On montre alors bien que pour les questions  $\{00\}$ ,  $\{011\}$ ,  $\{101\}$  et  $\{110\}$ , la stratégie quantique est gagnante à 100%.  $\square$

#### 2.2.4 Questions restantes pour l'arbitre

Dans cette sous partie, nous nous intéresserons rapidement aux performances de la stratégie quantique pour répondre aux questions restantes, non prises en compte dans le GHZ-Game ( $Q \setminus \tilde{Q}$ ).

Pour la question  $\{001\}$ , par permutation équivalente à  $\{010\}$  et  $\{100\}$ , le troisième joueur  $C$  applique la porte d'Hadamard à son qubit. L'état partagé par les trois joueurs devient :

$$|GHZ''\rangle = I \otimes I \otimes H |GHZ'\rangle = \frac{1}{2\sqrt{2}}(|000\rangle + |001\rangle - |010\rangle + |011\rangle - |100\rangle + |101\rangle - |110\rangle - |111\rangle)$$

On remarque alors que seulement la moitié des états de base composant le système répondent à la condition de victoire. La probabilité de victoire dans ce cas est de 50%, et de même pour les questions  $\{010\}$  et  $\{100\}$  de ce fait.

La question  $\{111\}$  reçue par les joueurs implique l'application de la porte Hadamard à chacun des qubits du système. L'état qui en résulte s'exprime alors comme suit :

$$|GHZ''\rangle = H \otimes H \otimes H |GHZ'\rangle = \frac{1}{2\sqrt{2}} \left( -|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle - |111\rangle \right)$$

On remarque de la même manière que l'on ne gagne que dans 50% des cas. On comprend alors qu'introduire ces 4 questions dans le jeu réduirait la probabilité moyenne de gagner à 75% au lieu de 100%, ce qui n'avantage pas le jeu et ne le rend plus aussi efficace.

### 2.2.5 Performance au GHZ-Game avec un état $|W\rangle$ ou $|BiSep\rangle$ partagé

Une autre configuration à laquelle nous pouvons réfléchir est celle où l'on choisirait, à la place d'un état intriqué équivalent à  $|GHZ\rangle$ , un état intriqué équivalent à  $|W\rangle$ . On pourrait alors étudier la différence de performance entre les deux types d'intrication pour la même stratégie quantique.

On suppose alors que les 3 joueurs partagent un état équivalent à  $|W\rangle$ , tel que :

$$|W'\rangle = X^{\otimes 3} |W\rangle = \frac{1}{\sqrt{3}} \left( |011\rangle + |101\rangle + |110\rangle \right)$$

Si la question  $\{000\}$  est posée, on observe que l'on gagne le jeu quelque soit la mesure effectuée.

Si la question  $\{011\}$  est posée, les joueurs  $B$  et  $C$  appliquent Hadamard à leur qubit, ce qui donne l'état suivant :

$$|W''\rangle = I \otimes H \otimes H |W'\rangle = \frac{1}{2\sqrt{3}} \left( |000\rangle - |001\rangle - |010\rangle + |011\rangle + 2|100\rangle - 2|111\rangle \right)$$

On remarque que l'on perd si l'on mesure les états de base  $|000\rangle$  et  $|011\rangle$ . La probabilité de perdre est donc la probabilité d'obtenir ces états :

$$p_{perdre}(\{011\}) = 2 \times \left(\frac{1}{2\sqrt{3}}\right)^2 = 2 \times \frac{1}{4} \times \frac{1}{3} = \frac{1}{6}$$

Donc la probabilité de gagner dans ce cas est de  $\frac{5}{6}$ . Ainsi, la probabilité générale en moyenne de gagner est de  $\frac{7}{8} = 0.875$  avec un état  $|W\rangle$  partagé.

On remarque alors que l'on ne peut gagner avec une probabilité de 1, et on le montre même si l'on change de stratégie [2]. La différence de nature de l'intrication joue ici un rôle important pour la performance du joueur. De la même manière, si l'on prend un état bi-séparable comme état partagé par les 3 joueurs, un état du type :

$$|BiSep\rangle = \frac{1}{\sqrt{2}}(|000\rangle - |011\rangle) = \frac{1}{\sqrt{2}}|0\rangle \otimes (|00\rangle - |11\rangle)$$

Dans ce cas, le qubit de  $A$  est totalement séparé, tandis que  $B$  et  $C$  partagent un état maximalement intriqué (état de Bell). On montre alors que dans cette situation, si les joueurs utilisent la même stratégie quantique, la probabilité générale de gagner au jeu est égale à 75%, c'est à dire la même qu'en classique. On peut vérifier pour cela que les questions  $\{000\}$  et  $\{011\}$  amènent vers un gain certain, tandis que les questions  $\{101\}$  et  $\{110\}$  ne permettent de gagner que la moitié du temps. Si les joueurs  $B$  et  $C$  décident d'employer la même stratégie que celle vue pour le CHSH-Game, alors le gain devient de 0.8536 comme attendu, ce qui est toujours inférieur à 1.

Ainsi, la nature de l'intrication joue bien un rôle dans la performance de ce jeu quantique, et peut être dans d'autres. Il serait intéressant d'investiguer d'autres jeux quantiques similaires et d'étudier les performances de systèmes quantiques d'autre nature (4-qubits, 3-qutrits, etc.) en fonction de leur intrication. Néanmoins, il est toujours possible de modifier ce jeu afin que les performances soient supérieures pour un type d'intrication donné. Ceci est l'objet de la prochaine sous-section.

### 2.2.6 W-Game

Si l'on veut obtenir une meilleure performance avec un état partagé de type  $|W\rangle$ , il convient de modifier la nature du jeu pour que la nature de l'intrication de cet état soit un avantage par rapport aux autres classes d'intrications.

Il est intéressant de remarquer, tout d'abord, qu'un état de type  $|W\rangle$  fait intervenir une intrication maximale mais du point de vue individuel d'une paire à 2-qubits constituant l'état, tandis qu'un état de type  $|GHZ\rangle$  fait intervenir une

intrication "pure" entre les trois qubits de l'état, et de ce fait devient séparable si on mesure un des qubits, ce qui n'est pas le cas pour un état  $|W\rangle$  où l'on obtiendrait un état maximalement intriqué, à une opération filtrage locale près.

Ceci nous amène à comprendre qu'un jeu, où l'arbitre pose les mêmes questions que dans le jeu GHZ,  $\tilde{Q} = \{000, 011, 101, 110\}$ , mais qu'il choisit d'ignorer aléatoirement un des joueurs, pourra être gagné si les joueurs partagent un état de type  $|W\rangle$ . Ceci revient en fait à jouer au CHSH-Game avec les 2 des 3 joueurs choisis aléatoirement, et donc la probabilité de gagner sera identique pour les deux jeux, qui sera de 0.8536, ce qui est meilleur que la performance classique (0.75) et celle avec un état GHZ partagé (0.75).

### 2.2.7 Généralisation à $n$ joueurs du GHZ-Game

Dans cette sous-section, nous proposons une généralisation à  $n$ -joueurs du GHZ-Game précédemment présenté. Pour ce faire, on essaye de se placer dans la même configuration que pour le jeu à trois joueur.

Les paramètres à considérer pour le GHZ-Game à trois joueurs sont les suivants : l'état équivalent à  $|GHZ\rangle$  que les joueurs partagent, les questions posées par l'arbitre, et les stratégies appliquées à chaque cas. On souhaite trouver une généralisation de ces paramètres pour  $n$  joueurs, tout en gardant une probabilité de 1 de gain. L'énoncé du jeu est donc le suivant.

#### Définition du jeu

Soit  $J$  l'ensemble  $\{J_1, J_2, \dots, J_n\}$  de cardinal  $n$  des joueurs au GHZ <sub>$n$</sub> -Game. On dénote par  $R$  l'arbitre. On note  $\{q_1 q_2 \dots q_n\}$  la question envoyée par l'arbitre, avec chaque  $q_i$  étant la question envoyée au joueur  $J_i$ . On note  $r_i$  la réponse du joueur  $J_i$ . La condition de gain est toujours de la même forme :

$$\bigvee_{i=0}^n q_i = \bigoplus_{i=0}^n r_i$$

Soit  $|GHZ_n\rangle$  l'état  $|GHZ\rangle$  généralisé à  $n$ -qubit, s'écrivant :

$$|GHZ_n\rangle = \frac{1}{\sqrt{2}} (|0\rangle^{\otimes n} + |1\rangle^{\otimes n})$$

On définit ensuite  $|GHZ'_n\rangle$  tel que :

$$|GHZ'_n\rangle = H^{\otimes n} |GHZ_n\rangle = \frac{1}{\sqrt{2}} (H^{\otimes n} |0\rangle^{\otimes n} + H^{\otimes n} |1\rangle^{\otimes n})$$

Or on sait que :

$$H^{\otimes n}|0\rangle^{\otimes n} = \sum_{x=0}^{2^n-1} \frac{1}{\sqrt{2^n}}|x\rangle$$

De plus :

$$H^{\otimes n}|1\rangle^{\otimes n} = \sum_{x=0}^{2^n-1} \frac{(-1)^{\varphi(x)}}{\sqrt{2^n}}|x\rangle$$

avec  $\varphi(x)$  désignant le nombre de 1 dans l'écriture binaire de  $x$ .

Ainsi, on obtient un état  $|GHZ'_n\rangle$  comme somme de  $2^{n-1}$  état de base de  $\mathcal{H} = (\mathbb{C}^2)^{\otimes n}$ . Les états de base présents sont tous le sétais de base dont l'écriture binaire comprend un nombre pair de 1. Ainsi, on peut ré-écrire l'état comme suit :

$$|GHZ'_n\rangle = \sum_{x=0}^{2^n-1} \frac{\varphi(x) + 1 \pmod{2}}{\sqrt{2^{n-1}}}|x\rangle$$

On définit ensuite l'état  $|GHZ''_n\rangle$  tel que :

$$|GHZ''_n\rangle = P^{\otimes n}|GHZ'_n\rangle \quad \text{avec } P = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2}} \end{pmatrix}$$

Cet état  $|GHZ''_n\rangle$ , équivalent à  $|GHZ\rangle$ , sera partagé par les  $n$ -joueurs du GHZ-Game.

L'arbitre sélectionne ensuite les questions à poser. Pour être sur d'avoir un gain de 1, les questions sont restreintes à la question  $\{00\dots 0\}$ , ainsi qu'à toutes les questions comprenant exactement deux digits à 1 dans leur écriture binaire. On dénombre alors  $1 + \binom{n}{2}$  questions, soit  $\frac{n^2-n+2}{2}$ .

Si on prend le cas  $n = 3$ , on retrouve bien que les  $1 + \binom{3}{2} = 4$  questions choisies par l'arbitre sont bien la question  $\{000\}$ , ainsi que toutes les questions possédant 2 digits à 1 exactement soit  $\{011\}$ ,  $\{101\}$  et  $\{110\}$ .

Enfin, la stratégie à appliquer est la même que pour le jeu à 3 joueurs. Si un joueur reçoit la question  $\{0\}$ , il mesure son qubit dans la base classique, sinon il applique la porte d'Hadamard à son qubit et ensuite il mesure dans la base classique.

## Exemple avec 4 joueurs

Supposons que nous voulions généraliser le GHZ-Game pour 4 joueurs. On commence par déterminer l'état quantique partagé par les 4 joueurs. On part de l'état  $|GHZ_4\rangle$  afin de construire l'état  $|GHZ'_4\rangle$ , tel que :

$$|GHZ'_4\rangle = H^{\otimes 4}|GHZ_4\rangle = \frac{1}{\sqrt{8}}(|0000\rangle + |0011\rangle + |0101\rangle + |1001\rangle + |0110\rangle + |1010\rangle + |1100\rangle + |1111\rangle)$$

On détermine ensuite  $|GHZ''_4\rangle$  l'état partagé par les 4 joueurs :

$$\begin{aligned} |GHZ''_4\rangle = P^{\otimes 4}|GHZ'_4\rangle = \frac{1}{\sqrt{8}}\Big(&|0000\rangle + i^2|0011\rangle + i^2|0101\rangle + i^2|1001\rangle + i^2|0110\rangle \\ &+ i^2|1010\rangle + i^2|1100\rangle + i^4|1111\rangle\Big) \end{aligned}$$

Après simplification, on obtient alors :

$$|GHZ''_4\rangle = \frac{1}{\sqrt{8}}(|0000\rangle - |0011\rangle - |0101\rangle - |1001\rangle - |0110\rangle - |1010\rangle - |1100\rangle + |1111\rangle)$$

L'ensemble des questions disponibles pour l'arbitre sera

$$\tilde{Q} = \{0000, 0011, 0101, 1001, 0110, 1010, 1100\}$$

conformément à la définition du jeu. Nous verrons plus tard pourquoi la question  $\{1111\}$  doit être enlevée du jeu.

Supposons alors que la question posée est  $\{0000\}$ . Chacun des joueurs va alors appliquer l'identité sur son qubit et ensuite le mesurer, ce qui revient à ne pas agir du tout sur leur état partagé  $|GHZ''_4\rangle$ . On remarque alors que quelque soit l'état de base mesuré à partir de l'état partagé, tous sont solutions du jeu. Ainsi, les joueurs gagnent le jeu avec une probabilité de 1 pour cette question.

Supposons à présent que la question posée est  $\{0011\}$ . Par permutation, l'étude de cette question est équivalente à l'étude de toutes les questions restantes (hormis  $\{0000\}$ ). Les deux premiers joueurs ne vont donc pas agir sur leur qubit (ou appliquer l'identité), tandis que les deux derniers vont appliquer la porte d'Hadamard. L'état partagé résultant est donc :

$$I \otimes I \otimes H \otimes H |GHZ''_4\rangle = \frac{1}{\sqrt{8}\sqrt{2}\sqrt{2}} \Big[$$

$$\begin{aligned}
& |00\rangle(|0\rangle + |1\rangle)(|0\rangle + |1\rangle) - |00\rangle(|0\rangle - |1\rangle)(|0\rangle - |1\rangle) - |01\rangle(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) \\
& - |10\rangle(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) - |01\rangle(|0\rangle - |1\rangle)(|0\rangle + |1\rangle) - |10\rangle(|0\rangle - |1\rangle)(|0\rangle + |1\rangle) \\
& - |11\rangle(|0\rangle + |1\rangle)(|0\rangle + |1\rangle) + |00\rangle(|0\rangle - |1\rangle)(|0\rangle - |1\rangle)
\end{aligned}$$

En développant les produits tensoriels, on obtient :

$$\begin{aligned}
I \otimes I \otimes H \otimes H |GHZ''_4\rangle = \frac{1}{2\sqrt{8}} \Big[ & \\
& |0000\rangle + |0001\rangle + |0010\rangle + |0011\rangle - |0000\rangle + |0001\rangle + |0010\rangle - |0011\rangle - |0100\rangle + |0101\rangle - |0110\rangle + |0111\rangle \\
& - |1000\rangle + |1001\rangle - |1010\rangle + |1011\rangle - |0100\rangle - |0101\rangle + |0110\rangle + |0111\rangle - |1000\rangle - |1001\rangle + |1010\rangle + |1011\rangle \\
& - |1100\rangle - |1101\rangle - |1110\rangle - |1111\rangle + |1100\rangle - |1101\rangle - |1110\rangle + |1111\rangle \Big]
\end{aligned}$$

Après simplifications des termes doubles et ceux qui s'annulent, on obtient l'état final :

$$I \otimes I \otimes H \otimes H |GHZ''_4\rangle = \frac{1}{\sqrt{8}} \left( |0001\rangle + |0010\rangle - |0100\rangle + |0111\rangle - |1000\rangle + |1011\rangle - |1101\rangle - |1110\rangle \right)$$

Si on regarde chacun des états de base, on se rend compte qu'ils font tous office de réponse gagnante pour le jeu. Les joueurs ont donc une probabilité de 1 de gagner pour ce type de question, et donc, au final, une probabilité totale de gagner au jeu de 1, comme voulu.

Concernant le délaissement question {1111} qui apparaît en fait dans l'écriture de l'état  $|GHZ''_4\rangle$ , on peut se demander pourquoi ne pas tout simplement prendre comme questions la séquence binaires de tous les états de l'état intriqué partagé par les joueurs, comme c'est le cas pour le jeu GHZ-Game à trois joueurs. Et bien, on se rend compte en posant les calculs que la stratégie ne marche pas pour la question {1111} car le nombre de fois où l'on applique Hadamard n'est pas convenable pour éliminer dans la simplification finale les états de base qui ne font pas gagner le jeu. On peut s'attendre au même genre de phénomène pour un nombre de joueurs plus grand. En restreignant les questions à celles qui ont deux digits à 1 exactement dans l'écriture binaire, on s'assure d'écartier ce problème, mais l'on peut dans le même temps omettre certaines questions qui permettent de gagner tout de même. Une étude approfondie, et une démonstration rigoureuse des résultats présentés se doit d'être menée dans la suite.

## 2.3 Dilemme du prisonnier

### 2.3.1 Principe du jeu classique

Le dilemme du prisonnier est une jeu dans lequel deux prisonniers, qui sont arrêtés pour l'infraction d'un petit délit, doivent faire face aux questions d'un inspecteur de police. En effet, ils sont, tout deux, soupçonnés d'avoir commis un délit plus grave. Cependant, l'inspecteur ne dispose d'aucunes preuves plausibles contre ces deux "malfrats" concernant le deuxième délit. Par conséquent, ce dernier va les séparer et les couper de toutes communications entre eux afin d'obtenir des aveux. Ce jeu fait donc partie des jeux non coopératif puisque chaque joueur doit prendre sa décision sans connaître la décision prise par l'autre joueur.

Afin d'obtenir des aveux, l'inspecteur de police propose, aux deux prisonniers, la possibilité de dénoncer l'autre prisonnier afin d'écopier d'une peine de prison moins importante. Chaque prisonnier peut également refuser cette option. Ainsi, différents résultats, exactement 4 dans notre cas, peuvent avoir lieu. Ces derniers sont résumés dans le tableau suivant :

|              |          | Prisonnier 2 |          |
|--------------|----------|--------------|----------|
|              |          | Se taire     | Dénoncer |
| Prisonnier 1 | Se taire | (3 ; 3)      | (0 ; 5)  |
|              | Dénoncer | (5 ; 0)      | (1 ; 1)  |

Dans notre étude de cas, nous avons choisi des gains qui pourraient correspondre à des allégements de peine de 0, 1, 3 ou 5 ans. Il faut noter que dans la notation choisie pour le tableau (à savoir (Gain 1 ; Gain2)), le gain 1 et le gain 2 correspondent respectivement au gain du prisonnier 1 et du prisonnier 2. L'objectif de chaque joueur est de maximiser son gain individuel.

### 2.3.2 Analyse des stratégies classiques

#### 1. Coopération des 2 prisonniers (Loyauté)

Dans ce cas où les deux prisonniers choisissent de ne pas se dénoncer et faire preuve de solidarité, nous pouvons constater que l'allègement de la peine de prison est de 3 ans. Le gain est maximal pour l'ensemble des deux joueurs mais ne l'est pas si l'on prend chaque joueur individuellement. Cette situation est très fructueuse pour les deux partis mais nécessite une certaine confiance l'un en vers l'autre.

On peut remarquer que si l'on fixe la stratégie du premier prisonnier et que l'on fait varier la stratégie de l'autre, le gain du premier prisonnier est augmenté en dépit du gain de l'autre prisonnier. Ici, le proverbe "le malheur des uns fait le bonheur des autres" est mis à l'honneur. On appelle ce type de stratégie un "Pareto optimal".

### 2. L'un dénonce l'autre (Individualisme)

Cette configuration est envisageable pour les deux joueurs. Il est ainsi possible de faire preuve d'égoïsme en dénonçant son collègue afin d'obtenir un allègement de peine. Dans notre cas, le dénonciateur obtiendra un allègement de peine de 5 ans, ce qui correspond au gain maximal individuel, alors que l'autre joueur sera accusé coupable et ne bénéficiera d'aucune indulgence, c'est-à-dire un allègement de peine nul (gain minimal individuel). Cette stratégie amène donc à une trahison de l'un en vers l'autre en vue d'obtenir un gain maximal individuel.

### 3. Dénonciation des 2 prisonniers (Lâcheté mutuelle)

La dernière stratégie possible consiste à une dénonciation "inter" prisonnier. Les deux vont tenter d'obtenir le gain maximal individuel. Cependant, les aveux des deux prisonniers ne vont pas permettre l'obtention d'un allègement de peine maximale. En effet, les deux témoignages se compensent et ne permettent pas d'accuser un prisonnier. Par conséquent, chacun va écoper d'un allègement d'uniquement 1 an.

Nous pouvons également remarquer que cette stratégie est un équilibre de Nash. C'est-à-dire, qu'aucun des deux joueurs n'a intérêt à changer de stratégie. Leurs gains ne seraient que détérioré.

#### 2.3.3 Notion de dilemme

Pour comprendre la notion de dilemme, il nous suffit d'imaginer la réflexion qu'aurait un joueur avant de choisir sa stratégie. En effet, s'il considère que son adversaire décide de se taire alors il a tout intérêt à le trahir en le dénonçant (gain maximal de 5 au lieu de 3 s'il se taisait lui aussi). Dans le cas inverse où il considérerait que son adversaire décide de le trahir, il aurait également tout intérêt à le trahir également afin d'obtenir encore le gain le plus intéressant pour lui, c'est-à-dire un gain de 1 (au lieu de 0 s'il se taisait). Ainsi, il nous semblerait que la stratégie de la trahison soit celle que nous devrions choisir. Cependant, nous oublions un détail. Le prisonnier peut également réfléchir de la manière que nous l'avons fait précédemment. Dans ce cas là, ils obtiendraient tout deux un gain de 1 au lieu d'un gain de 3 s'ils s'étaient tus. De fait, il réside bien dans ce jeu une notion

de dilemme qui réside dans l'absence de communication entre les deux prisonniers et plus précisément dans l'altercation entre l'intérêt individuel et collectif.

### 2.3.4 Déroulement du jeu quantique

Nous allons maintenant voir le dilemme du prisonnier sous sa forme quantique. Pour ce faire, le circuit représentant les différentes étapes à effectuer peut être représenté de la manière suivante :

Prisoner Dilema Circuit.png

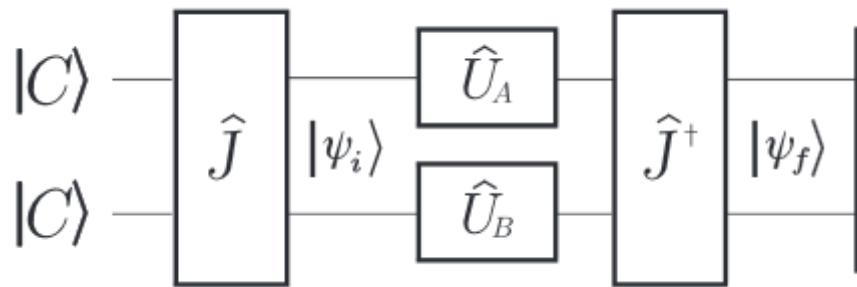


FIGURE 2.1 – Circuit : Dilemme du prisonnier quantique

Dans cette nouvelle configuration, les deux prisonniers détiennent chacun un qubit. Ces derniers forment un système dont l'état est intriqué (ou non séparable). En d'autres termes, les modifications appliquées à un qubit vont nécessairement provoquer des répercussions sur l'état du second qubit, ils sont donc ainsi indirectement liés. C'est cette particularité qui va être exploitée lors du choix des stratégies. Chacun des deux prisonniers va pouvoir effectuer des manipulations sur son qubit.

Tout d'abord, nous allons considérer que chaque stratégie, se taire ou dénoncer, sera notée, respectivement, sous la forme de deux états de base  $|C\rangle$  et  $|D\rangle$ , qui peuvent être écrit sous la forme de deux vecteurs :  $|C\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$  et  $|D\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ .

#### 1. Initialisation

Cette étape correspond à l'intrication des deux qubits par l'intermédiaire d'un opérateur  $\hat{J}$ . Cet opérateur est connu par les deux prisonniers. Ainsi, nous obtenons l'état initial du système intriqué sous la forme :

$$|\psi_i\rangle = \hat{J}|CC\rangle = \cos(\frac{\gamma}{2})|CC\rangle + i\sin(\frac{\gamma}{2})|DD\rangle$$

$\gamma$  représente le taux d'intrication entre les deux qubits. Sa valeur est comprise entre 0 (cas où le système à 2 qubits est séparable) et  $\frac{\pi}{2}$  (cas où le système à 2 qubits est maximalement intriqué).

## 2. Opérateurs locaux et mesure

Chaque prisonnier détient un opérateur qu'il peut appliquer à son propre qubit. On notera  $\hat{U}_1$  et  $\hat{U}_2$ , respectivement, l'opérateur du prisonnier 1 et du prisonnier 2. L'opérateur  $\hat{U}$ , défini comme ci-dessous, représente l'ensemble des stratégies possibles, avec  $0 \leq \theta \leq \pi$  et  $0 \leq \phi \leq \pi/2$  :

$$\hat{U}(\theta, \phi) = \begin{pmatrix} e^{i\phi} \cos(\theta/2) & \sin(\theta/2) \\ -\sin(\theta/2) & e^{-i\phi} \cos(\theta/2) \end{pmatrix}$$

*Remarque :* Nous pouvons constater que les stratégies classiques C et D sont incluses. En effet, chacune d'elle est caractérisée par un opérateur particulier. Soient :

$$\hat{U}(0, 0) = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \leftrightarrow \text{C : "Se taire"}$$

$$\hat{U}(\pi, 0) = X = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \leftrightarrow \text{D : "Dénoncer"}$$

Nous obtenons ainsi l'état du système :

$$|\psi_{ii}\rangle = (\hat{U}_1 \otimes \hat{U}_2) \hat{J} |CC\rangle.$$

Ensuite, il nous suffit d'appliquer la transformation inverse de  $\hat{J}$  nommée  $\hat{J}^\dagger$  afin d'obtenir l'état final du système :

$$|\psi_f\rangle = \hat{J}^\dagger (\hat{U}_1 \otimes \hat{U}_2) \hat{J} |CC\rangle$$

Finalement, nous effectuons la mesure de l'état final  $|\psi_f\rangle$  afin d'obtenir l'un des états de base  $|CC\rangle$ ,  $|CD\rangle$ ,  $|DC\rangle$  et  $|DD\rangle$ .

## 3. Gain

L'état final du système peut être écrit sous la forme suivante :

$$|\psi_f\rangle = \psi_1 |CC\rangle + \psi_2 |CD\rangle + \psi_3 |DC\rangle + \psi_4 |DD\rangle$$

La matrice des gains peut être défini comme suit :

$$\Pi = \begin{pmatrix} |\psi_1|^2 & |\psi_2|^2 \\ |\psi_3|^2 & |\psi_4|^2 \end{pmatrix} = \begin{pmatrix} P_{CC} & P_{CD} \\ P_{DC} & P_{DD} \end{pmatrix}$$

Nous pouvons maintenant exprimer le gain de chaque prisonnier, à l'aide des gains classique fixés précédemment, de la manière suivante :

$$\begin{aligned}\$1 &= 3P_{CC} + 1P_{DD} + 5P_{DC} + 0P_{CD} \\ \$2 &= 3P_{CC} + 1P_{DD} + 0P_{DC} + 5P_{CD}\end{aligned}$$

$\$1$  et  $\$2$  représentent les gains respectifs du prisonnier 1 et 2.  $P_{xy}$  représente la probabilité pour que l'état final soit dans l'état  $|xy\rangle$ . Elle est définie telle que  $P_{xy} = |xy||\psi_f\rangle|^2$ .

Nous pouvons également constater que l'état final  $|\psi_f\rangle$  dépend du choix de stratégie des deux joueurs et ainsi les gains respectifs  $\$1$  et  $\$2$  dépendent également de la stratégie des deux joueurs.

#### 4. Table de gains : Opérateur Z

En utilisant l'opérateur Z,

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

nous pouvons obtenir la table des gains suivante :

| Prisonnier 2 |         | Porte I | Porte X | Porte Z |
|--------------|---------|---------|---------|---------|
| Prisonnier 1 | Porte I | (3 ; 3) | (0 ; 5) | (1 ; 1) |
|              | Porte X | (5 ; 0) | (1 ; 1) | (0 ; 5) |
|              | Porte Z | (1 ; 1) | (5 ; 0) | (3 ; 3) |

Nous pouvons constater que l'application de cette porte Z permet d'obtenir une stratégie quantique qui est à la fois un équilibre de Nash et un Pareto Optimal. En effet, si les deux joueurs choisissent la stratégie quantique, ils n'ont aucun intérêt à changer de position car leurs gains individuels sont au maximum. Dans la configuration classique, on pouvait obtenir un équilibre de Nash ou un Pareto Optimal mais on ne pouvait pas obtenir ces deux caractéristiques en même temps.

– Démonstration des résultats obtenus :

Nous allons expliquer les étapes de calculs afin d'obtenir les gains obtenus pour la stratégie  $(Z, Z)$ .

Soit :

$$\hat{J} = \frac{1}{\sqrt{2}}(I \otimes I + iX \otimes X)$$

Alors :

$$|\psi_i\rangle = \hat{J}|CC\rangle = \frac{1}{\sqrt{2}}(|CC\rangle + i|DD\rangle)$$

Or :

$$Z \otimes Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$$

D'où :

$$|\psi_{ii}\rangle = (Z \otimes Z) \hat{J} |CC\rangle = \frac{1}{\sqrt{2}} (|CC\rangle + i|DD\rangle).$$

Ensuite :

$$\hat{J}^\dagger = \frac{1}{\sqrt{2}} (I \otimes I - iX \otimes X)$$

Ainsi :

$$|\psi_f\rangle = \hat{J}^\dagger (Z \otimes Z) \hat{J} |CC\rangle = \frac{1}{\sqrt{2}} * \frac{1}{\sqrt{2}} (|CC\rangle - i|DD\rangle + i|DD\rangle - i*i|CC\rangle) = |CC\rangle$$

Finalement :

$$\$1 = 3P_{CC} + 1P_{DD} + 5P_{DC} + 0P_{CD} = 3$$

$$\$2 = 3P_{CC} + 1P_{DD} + 0P_{DC} + 5P_{CD} = 3$$

Les autres couples d'opérateurs amènent à des calculs similaires. Par conséquent, nous ne détaillerons pas les calculs des autres stratégies.

## Choix de la porte quantique

Comme nous l'avons vu précédemment, il est possible de définir la matrice, qui représente l'ensemble des stratégies possibles pour les deux prisonniers, de la manière suivante, avec  $0 \leq \theta \leq \pi$  et  $0 \leq \phi \leq \pi/2$  :

$$\hat{U}(\theta, \phi) = \begin{pmatrix} e^{i\phi} \cos(\theta/2) & \sin(\theta/2) \\ -\sin(\theta/2) & e^{-i\phi} \cos(\theta/2) \end{pmatrix}$$

Nous pouvons obtenir l'évolution du comportement du jeu quantique en faisant varier le paramètre  $\gamma$  correspondant au niveau d'intrication du système composé par la paire de qubits détenue par les deux prisonniers [49]. Nous pouvons distinguer 3 types de comportements :

1.  $0 \leq \gamma \leq \arcsin(\frac{1}{\sqrt{5}})$  → Comportement classique
2.  $\arcsin(\frac{1}{\sqrt{5}}) \leq \gamma \leq \arcsin(\frac{2}{\sqrt{5}})$  → Comportement intermédiaire
3.  $\arcsin(\frac{2}{\sqrt{5}}) \leq \gamma \leq \frac{\pi}{2}$  → Comportement quantique

## 2.4 Binary Constraint System Game

Le principe du Binary Constraint System est un moyen de modéliser de nombreux problèmes informatique et logiques, dans la mesure où il est défini par un nombre finit de variables et contraintes formelles, pouvant ensuite être appliquées dans divers domaines. C'est un sujet qui a participé pour donner de l'importance à la théorie de la complexité informatique et l'information quantique. C'est un jeu que l'on peut retrouver implicitement dans les travaux de Mermin concernant le théorème de Bell. Afin d'expliquer ce jeu, nous nous baserons sur le travail présenté dans le célèbre article [8].

### 2.4.1 Principe du jeu

Soient  $v_1, v_2, \dots, v_n$ ,  $n$  variables binaires telles que  $\forall i \in \llbracket 1, n \rrbracket$ ,  $v_i \in \{0, 1\} = \mathbb{Z}_2$ . Soient  $c_1, c_2, \dots, c_m$ ,  $m$  contraintes. Chaque contrainte est une fonction à plusieurs variables binaires et à valeur dans  $\mathbb{Z}_2$  :

$$\forall j \in \llbracket 1, m \rrbracket, \quad c_j : \left\{ \begin{array}{ccc} \mathbb{Z}_2^k & \rightarrow & \mathbb{Z}_2 \\ (v_{i_1}, v_{i_2}, \dots, v_{i_k}) & \mapsto & v_{i_1} \oplus v_{i_2} \oplus \dots \oplus v_{i_k} = z \in \mathbb{Z}_2 \end{array} \right.$$

Un Binary Constraint System se composera alors d'un ensemble de variables et de contraintes. On dit qu'un BCS Game est satisfiable si on peut trouver un  $n$ -uplet  $(v_1, v_2, \dots, v_n)$  qui satisfont chacune des  $m$  contraintes.

Un exemple classique de BCS est celui énoncé dans la version du théorème de Bell introduite par Mermin [6]. Dans cet exemple, on a  $n = 9$  variables et  $m = 6$  contraintes :

$$\begin{array}{ll} v_1 \oplus v_2 \oplus v_3 = 0 & v_1 \oplus v_4 \oplus v_7 = 0 \\ v_4 \oplus v_5 \oplus v_6 = 0 & v_2 \oplus v_5 \oplus v_8 = 0 \\ v_7 \oplus v_8 \oplus v_9 = 0 & v_3 \oplus v_6 \oplus v_9 = 1 \end{array}$$

Dans notre exemple, on se rend bien compte que le jeu n'est pas satisfiable, dans la mesure où l'on ne peut trouver d'affectation pour les variables qui vérifient les 6 contraintes. Nous pouvons aussi remarquer que la somme des équations nous amène à l'absurdité  $0 = 1$ .

Un élément important concernant les BCS, et que l'on peut associer à chaque Binary Constraint System un jeu "non-local" à deux joueurs, nommé Binary Constraint System Game, selon le principe suivant. Soient  $A$  et  $B$  deux joueurs coopérant, mais qui ne peuvent pas communiquer une fois le protocole du jeu entamé. Soit  $R$  l'arbitre du jeu.

L'arbitre  $R$  choisit de manière aléatoire, mais uniforme, une contrainte du jeu  $c_s$  ainsi qu'une variable  $v_t$  intervenant dans la contrainte  $c_s$ . L'arbitre envoie l'indice  $s$  à  $A$  et l'indice  $t$  à  $B$ . Le joueur  $A$  doit renvoyer une affectation des toutes les variables présentes dans la condition  $c_s$ . Le joueur  $B$  doit renvoyer une affectation de la variable  $v_t$ . L'arbitre  $R$  accepte leur réponse, c.a.d le jeu est gagné, si et seulement si :

- L'affectation des variables choisie par  $A$  satisfait bien la condition  $c_s$
- L'affectation de la variable  $v_t$  choisie par  $B$  correspond à celle choisie par  $A$

Une stratégie de résolution du jeu est dite parfaite si elle permet de gagner le jeu de manière sûre. Ainsi, on en déduit que tout BCS Game qui est satisfiable admet une stratégie parfaite classique. Il serait intéressant, par contre, de se demander s'il existe des stratégies quantiques parfaites pour des BCS Games non-satisfiables.

### 2.4.2 Stratégie quantique parfaite

Le travail de Mermin [6, 7], notamment ses découvertes sur les observables, a des répercussions sur les stratégies quantiques pour le BCS Game en particulier pour les 2 exemples qui suivent.

Le premier exemple est celui présenté précédemment, avec  $n = 9$  et  $m = 6$ . Le second exemple est un BCS Game avec  $n = 10$  variables et  $m = 5$  contraintes. On peut représenter ces jeux sous la forme de figures géométriques : les variables sont disposées en fonction de leur appartenance aux conditions. Une condition correspond à une ligne de variables reliées par un trait simple ou double. Le trait simple indique que la somme modulo 2 des variables doit être égale à 0, tandis que le trait double indique une somme modulo 2 égale à 1. Les figures de ces deux jeux sont appelés "magiques", car une stratégie parfaite quantique existe pour résoudre ces jeux, qui ne sont pas résolvables en classique. On représente alors les 2 jeux sur les figures suivantes.

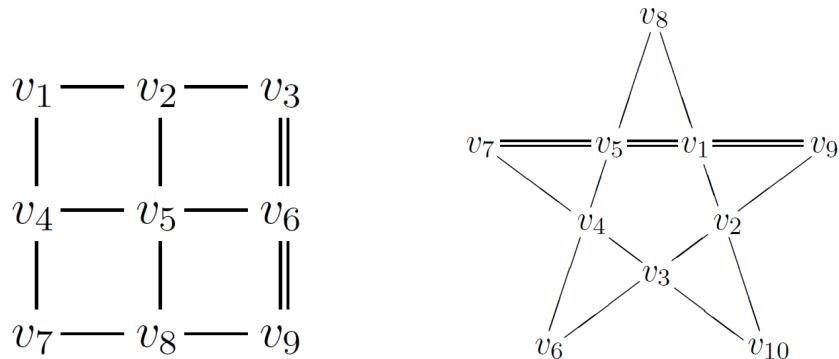


FIGURE 2.2 – Carré magique (à gauche) - Pentagramme magique (à droite)

Afin de comprendre la stratégie quantique proposée par Mermin, on transforme tout d'abord chaque variable  $v_i \in \{0, 1\}$  en variable  $V_i = (-1)^{v_i} \in \{+1, -1\}$ . Chaque contrainte peut alors se redéfinir comme le produit des variables  $V_i$  a valeur dans  $\{+1, -1\}$ . On redéfinit alors la notion de satisfaisabilité pour une

affectation quantique des variables comme une affectation de  $n$  opérateurs Hermitiens  $A_1, A_2, \dots, A_n$  aux variables  $V_1, V_2, \dots, V_n$  telles que ces trois conditions soient remplies :

**Condition 1** : Chaque opérateur  $A_i$  est un observable binaire dont les valeurs propres appartiennent à  $\{+1, -1\}$ , autrement dit,  $A_i^2 = I$ .

**Condition 2** : Chaque couple d'observables  $A_i$  et  $A_j$  appartenant à la même contrainte doivent commuter, autrement dit,  $A_i A_j = A_j A_i$ .

**Condition 3** : Les  $n$  opérateurs  $A_1, A_2, \dots, A_n$  doivent satisfaire chacune des contraintes  $c_s : \{+1, -1\}^k \rightarrow \{+1, -1\}$  agissant sur les variables  $V_{i_1}, V_{i_2}, \dots, V_{i_k}$ , de telle sorte que chaque équation  $c_s(A_{i_1}, A_{i_2}, \dots, A_{i_k}) = I$  ou  $-I$  soit satisfaite.

Une fois ceci défini, le théorème mis en place par Cleve et Mittal [8] nous permet d'avoir une relation entre affectation quantique satisfaisante et stratégie parfaite :

**Théorème 2.4.1.** *Quelque soit le Binary Constraint System considéré, s'il existe une stratégie parfaite pour le BCS Game correspondant, alors il existe une affectation quantique satisfaisante au jeu.*

L'idée derrière cela est que s'il existe une stratégie parfaite au jeu, en utilisant un état maximallement intriqué (de type  $|GHZ_d\rangle$  typiquement), les opérateurs peuvent être créé par projection à partir de la stratégie parfaite, de telle sorte que ces opérateurs satisfont les 3 trois conditions émises précédemment. Par ailleurs, s'il existe une telle affectation quantique, alors toutes les contraintes seront satisfaites et il existera un observable  $A_i$  pour chaque variable  $V_i$ . La preuve complète est détaillé dans l'article [8].

Ainsi, si l'on revient à nos exemples précédents, pour chaque jeu, une affectation quantique satisfaisante faisant office donc de stratégie parfaite est présentée sur les figures ci-contre.

$$\text{avec : } X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\text{et donc : } X^2 = Y^2 = Z^2 = I, \quad XY = iZ, \quad YZ = iX \text{ et } ZX = iY$$

Le lecteur pourra en effet vérifier que le produits des observables sur chaque ligne simple donne bien l'identité, tandis que le produit des observables liées par

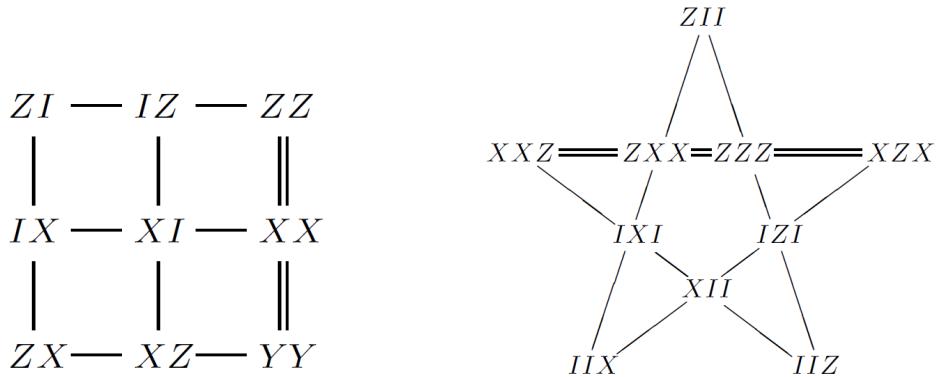


FIGURE 2.3 – Affectations quantiques valides - Carré magique (à gauche) - Pentagramme magique (à droite)

des lignes doubles donne bien l’opposé de l’identité. Pour des simplifications de notation, la juxtaposition d’observables correspond en fait à leur produit tensoriel. On a donc par exemple  $ZX = Z \otimes X$ .

Si l’on se penche par exemple sur la première ligne solution du carré magique, on vérifie bien que le produit donne l’identité :

$$(Z \otimes I)(I \otimes Z)(Z \otimes Z) = (ZIZ) \otimes (IZZ) = (Z^2) \otimes (Z^2) = I \otimes I$$

De même pour la dernière colonne solution du carré magique, on vérifie bien que le produit donne l’opposé de l’identité :

$$(Z \otimes Z)(X \otimes X)(Y \otimes Y) = (ZXY) \otimes (ZXY) = (iYY) \otimes (iYY) = i^2(Y^2) \otimes (Y^2) = -(I \otimes I)$$

### 2.4.3 Condition d’inexistence de stratégie quantique parfaite

Comme discuté dans l’article [10] et proposé par Speelman, il existe pour certains BCS Game un moyen simple de déterminer s’il n’existe pas de stratégie quantique parfaite résolvant le jeu. On étudie pour cela la cohérence des équations obtenues en posant le jeu de manière quantique en tentant de trouver une contradiction.

Etudions par exemple le BCS-Game, avec  $n = 6$  variables, et  $m = 4$  contraintes, représenté par la figure et les équations suivantes :

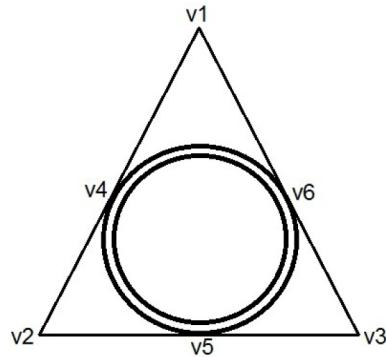


FIGURE 2.4 – Schéma du jeu en exemple

$$\begin{array}{ll} v_1 \oplus v_6 \oplus v_3 = 0 & v_1 \oplus v_4 \oplus v_2 = 0 \\ v_2 \oplus v_5 \oplus v_3 = 0 & v_4 \oplus v_5 \oplus v_6 = 1 \end{array}$$

On suppose alors qu'une affectation quantique satisfaisante existe. On construit alors, à partir des variables  $v_1, v_2, \dots, v_6$ , les variables  $V_1, V_2, \dots, V_6$ , ainsi que les observables  $A_1, A_2, \dots, A_6$  correspondants. On retraduit alors chacune des contraintes avec les observables, ce qui nous donne :

$$\begin{array}{ll} A_1 A_6 A_3 = I & A_1 A_4 A_2 = I \\ A_2 A_5 A_3 = I & A_4 A_5 A_6 = -I \end{array}$$

Partant de la seconde contrainte, qui sera notre équation principale, ce qui nous donne  $A_1 A_4 A_2 = I$ . En multipliant par  $A_2$  à gauche dans la troisième contrainte, on obtient  $A_2 = A_5 A_3$ . En réinjectant dans notre équation principale on a  $A_1 A_4 A_5 A_3 = I$ . En multipliant à droite par  $A_3$  dans la première contrainte, on en déduit que  $A_3 = A_1 A_6$ . D'où la nouvelle expression de l'équation principale  $A_1 A_4 A_5 A_1 A_6 = I$ . En multipliant par  $-A_4$  à gauche dans la quatrième contrainte, on obtient  $A_4 = -A_5 A_6$ . On en déduit alors que  $A_1 A_5 A_6 A_5 A_1 A_6 = -I$ . En utilisant la propriété de commutativité pour les observables  $A_1$  et  $A_6$ , et pour les variables  $A_5$  et  $A_6$  on réarrange les termes de l'équation principale ce qui nous donne  $A_1 A_6 A_5 A_5 A_6 A_1 = -I$ . Or on a bien  $A_1^2 = A_5^2 = A_6^2 = I$  d'après la première condition. Ce qui nous donne finalement l'absurdité  $I = -I$ . Ainsi par ce raisonnement par l'absurde, on en déduit qu'il n'existe pas d'affectation quantique satisfaisante, et donc par contraposée du théorème, qu'il n'existe pas de stratégie quantique parfaite pour ce jeu.

A partir du moment où il n'existe pas de stratégie quantique parfaite pour ce jeu, d'aucuns pourront s'intéresser à trouver une stratégie quantique surpassant les performances des stratégies classiques, pour ce jeu non résolvable parfaitement de manière classique ni quantique.

## 2.5 Minority game

Dans cette section, nous vous présenterons le jeu de la minorité, appelé Minority Game en anglais. Nous tenterons d'expliquer l'origine et le principe général du jeu. Nous introduirons ensuite, comme cela est fait pour le dilemme du prisonnier, le formalisme mathématique qui nous permettra de mieux comprendre l'introduction de stratégies quantiques. Nous étudierons enfin les résultats de l'introduction de telles stratégies, pour 3 et 4 joueurs, puis nous terminerons sur les recherches qui peuvent être menées par rapport à ce jeu.

### 2.5.1 Origine et énoncé du jeu

Le jeu du *Minority Game* est en fait issu à la base du problème du bar d'El Farol. Ce problème est un problème connu de la théorie des jeux, créé en 1994 par W. Brian Arthur, et inspiré d'un bar à San Fe au Nouveau Mexique. Le même problème a été aussi formulé et résolu dynamiquement six ans auparavant [12].

Le problème peut être formulé comme suit : Soit un ensemble fini de personnes, appelé population. Tous les jeudis soir, toutes ces personnes désirent aller au bar d'El Farol. Cependant, ce bar est assez petit, et il n'est alors plus intéressant de se rendre au bar si celui-ci est déjà assez rempli. On définit alors les préférences des personnes selon les conditions suivantes :

- Si moins de 60% de la population se rend au bar, ils passeront tous un meilleur moment que s'ils étaient restés à la maison.
- Si plus de 60% de la population se rend au bar, ils passeront tous un pire moment que s'ils étaient restés à la maison.

De plus, et c'est ce qui rend la situation problématique, il est nécessaire pour chacune des personnes de décider en même temps si elle va ou non au bar. Elles ne peuvent pas attendre la réponse des autres, pour un jeudi particulier, et prendre leur décisions en fonction de cela.

Un aspect dans la résolution du problème est que, si tout le monde utilise la même stratégie pure (totalement déterminée), cea est voué à l'échec. En effet, si la

stratégie déterministe suggère que le bar ne sera pas rempli, alors tout le monde ira au bar, et il sera alors rempli, et inversement.

En théorie des jeux, une des solutions envisageable pour ce genre de problème est d'utiliser ce que l'on appelle en anglais "a mixed strategy", c'est à dire affecter à chaque stratégie pure une probabilité d'être choisie. Dans le cas où l'on ne considère le problème que pour un seul jeudi, on montre qu'il existe un unique Equilibre de Nash symétrique pouvant être atteint à l'aide d'une "mixed strategy" où toutes les personnes choisissent d'aller au bar avec une certaine probabilité. Cette dernière dépend du nombre de personnes dans la population, du seuil à partir duquel on considère que le bar est rempli, et des préférences relatives d'aller au bar rempli ou vide, ou de rester chez soi. D'autres équilibres de Nash peuvent émerger si une ou plusieurs personnes choisissent d'utiliser une stratégie pure, mais ces équilibres ne sont alors plus symétriques.

En outre, Herbert Gintis propose un certain nombre de variantes du problème dans son ouvrage. Dans certains variantes, les personnes peuvent communiquer entre elles avant d'aller au bar. La subtilité de ces variantes est que les personnes ne sont pas obligées de dire la vérité et peuvent donc utiliser le bluff pour maximiser leurs chances d'être satisfaites.

Le Minority Game peut alors être vu comme une variante du problème ci-dessus, ou sa formulation mathématique. Soit  $N$  le nombre de joueurs, correspondant à la taille de la population. Chaque joueur choisit de manière privée une des deux réponses : 0 ou 1. Les choix sont alors comparés, et les joueurs dont le choix est minoritaire gagnent. Si tous les joueurs font le même choix, ou s'il y a le même nombre de joueurs pour chaque choix, alors il n'y a pas de gagnants.

La configuration de jeu la plus répandue est lorsque le jeu est répété sur plusieurs tours. Chaque joueur n'a qu'un choix limité de stratégies, et chaque joueur ne sait rien sur les autres joueurs. Leurs décisions se basent alors sur les précédents cas de gain et sur la performance de leurs stratégies dans le passé. Dans notre cas, on s'intéresse uniquement au cas où les joueurs ne jouent qu'une seule fois.

### 2.5.2 Mise en place du jeu quantique

Dans cette sous-section, on posera toute la théorie permettant de définir la version quantique du MinorityGame. Tout ce formalisme est commun à la théorie des jeux quantiques (comme le Dilemme du Prisonnier quantique par exemple) et dans ce cas est issue du travail de Benjamin & Hayden [13].

On pose alors  $N$  le nombre de joueurs au Minority Game. On définit un profil de stratégie, une affectation du vecteur  $s = (s_1, s_2, \dots, s_N)$ , avec  $s_i$  la stratégie du joueur  $i$ . On parlera d'équilibre complet ou "pur" pour désigner de manière théorie un profil de stratégie avec un certain degré de stabilité, comme par exemple l'équilibre de Nash. La version du jeu, comme précisé ci-dessus, est considérée comme statique : le jeu n'est joué qu'une seule, et on ne prend donc pas en compte l'historique des autres parties. De plus, chaque joueur a une connaissance complète de la structure du jeu.

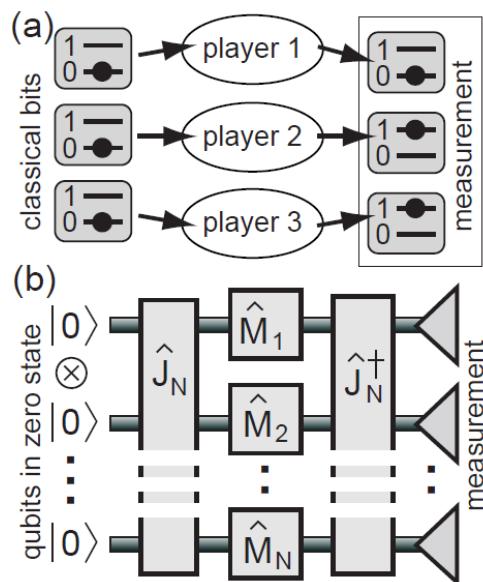


FIGURE 2.5 – Modèles de jeux classiques et quantiques

Sur la figure (a), un modèle de jeu classique général est présenté. Chaque joueur reçoit un bit initialisé à 0, et n'a que deux possibilités d'action par manipulation locale : inverser le bit (ce qui donne 1) ou le laisse tel quel (ce qui donne 0). Ensuite chaque joueur renvoie son bit pour l'état de mesure final où les gains seront alors calculés. Sur la figure (b), est représenté la définition générale d'un jeu quantique à  $N$  joueurs.

Ainsi, pour passer du jeu classique au jeu quantique, le support de l'information classique (le bit) doit être remplacé par le qubit, tout d'abord. Ensuite, ces qubits doivent être mutuellement intriqués. S'ils ne le sont pas, on peut alors bien retrouver une modélisation quantique du jeu classique, mais où aucune stratégie quantique plus performante ne pourra être mise en place, car on n'agirait que sur chaque qubit séparément pour chaque joueur. Cependant, le jeu quantique que l'on

veut mettre en place doit tout de même être une généralisation du jeu classique : on dira que le jeu quantique doit contenir le jeu classique. L'opérateur qui correspond donc à ne pas altérer le bit 0 classique sera l'opérateur unitaire identité en quantique. De même, l'opérateur  $X = \sigma_X$ , opérateur NOT ou opérateur  $X$  de Pauli, doit correspondre à inverser le bit 0 en classique et donc avoir le bit 1. De ce fait, si on restreint les stratégies possibles pour les joueurs aux portes  $\{I, X\}$ , on retrouve les gains du jeu classique.

D'autre part, et afin d'établir une corrélation entre les qubits en entrée, on utilise la paire de portes quantiques présentées précédemment. En effet, comme présenté sur la figure (b), c'est la porte  $J_N N$  qui se chargera d'intriquer les qubits initialisés à  $|0\rangle$ . Si on se restreint aux portes unitaires introduisant une intrication maximale, agissant symétriquement sur  $|1\rangle$  et  $|0\rangle$ , on peut alors l'écrire de manière générale :

$$J_N = \frac{1}{\sqrt{2}}(I^{\otimes N} + iX^{\otimes N})$$

Les  $N$  joueurs partageront donc en réalité un état  $|\psi\rangle$  maximalement intriqué équivalent à  $|GHZ_N\rangle$  exprimé par :

$$|\psi\rangle = J_N|0\rangle^{\otimes N} = \frac{1}{\sqrt{2}}(I^{\otimes N}|0\rangle^{\otimes N} + iX^{\otimes N}|0\rangle^{\otimes N}) = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + i|1\rangle^{\otimes N})$$

A partir de là, on préfèrera utiliser des stratégies déterministes modélisées par des matrices unitaires à appliquer sur son qubit pour chaque joueur. L'utilisation de ce type de stratégie permet de ne pas détruire l'intrication introduite par la porte  $J_N$ . De plus, des équilibres "purs" ne peuvent être atteints qu'uniquement à partir de portes unitaires.

### 2.5.3 Cas où $N = 3$

Dans le cas où  $N = 3$  personnes jouent au Minority Game, on montre que l'introduction d'une stratégie quantique n'apporte pas de nouvel équilibre "pur".

Effectivement, on peut tout d'abord définir la stratégie pure la plus générale pour le joueur  $i$  par

$$s_i = \alpha_i(\beta_i iX + \gamma_i iY) + \zeta_i(\varphi_i I + \theta_i iZ)$$

où tous les  $\alpha_i, \beta_i, \gamma_i, \zeta_i, \varphi_i$  et  $\theta_i$  des coefficients réels tels que :

$$\alpha_i^2 + \zeta_i^2 = \beta_i^2 + \gamma_i^2 = \varphi_i^2 + \theta_i^2 = 1$$

En appliquant la porte  $J_3$  à l'état  $|\psi\rangle$  partagé par les 3 joueurs et après simplification des termes, on remarque alors que les coefficients  $\beta, \gamma, \varphi, \theta$  se simplifient et disparaissent. Ceci nous amène à avoir une probabilité  $p_1$  que le joueur 1 soit minoritaire de :

$$p_1 = \left( \zeta_1 \alpha_2 \alpha_3 \right)^2 + \left( \alpha_1 \zeta_2 \zeta_3 \right)^2$$

Les résultats pour les joueurs 2 et 3 se calculent de manière analogue. On remarque alors que ce sont les mêmes probabilités que celles attendues dans le jeu classique, si on pose  $\alpha^2$  comme la probabilité d'inverser le bit 0 en classique (donc la probabilité d'obtenir 1).

Finalement, les paramètres supplémentaires introduits par les stratégies quantiques n'apportent aucun avantage, et le jeu quantique se résume alors simplement à la version classique, dans le cas où  $N = 3$ .

#### 2.5.4 Cas où $N = 4$

La situation où 4 personnes sont invitées à jouer au jeu de la minorité est différente du cas précédent dans la mesure où l'introduction de stratégies quantique aura une importance sur l'issue du jeu pour les joueurs.

Si l'on s'intéresse dans un premier temps aux stratégies classiques possibles, les joueurs n'ont en fait de meilleur choix que de choisir aléatoirement et uniformément entre répondre  $\{0\}$  (ne pas aller au bar) ou  $\{1\}$  (y aller). Si on liste alors toutes les possibilités de réponses pour les 4 joueurs ( $2^4 = 16$  au total), et que l'on compte le nombre de cas où un joueur  $i$  est gagnant, on remarque que cela n'intervient que dans  $\frac{2}{16} = \frac{1}{8}$  des cas. De plus, dans la moitié des cas, personne ne peut gagner car soit tous les joueurs envoient la même réponse, soit 2 répondent  $\{0\}$  et 2 répondent  $\{1\}$ .

Cependant, lorsque l'on passe à la version quantique du jeu, on découvre alors un équilibre totalement "pur". Par exemple, si le profil de stratégie est  $s=(a,a,a,a)$  avec :

$$a = \frac{1}{\sqrt{2}} \cos\left(\frac{\pi}{16}\right)(I + iX) + \frac{1}{\sqrt{2}} \sin\left(\frac{\pi}{16}\right)(iY - iZ)$$

alors l'état final partagé obtenu est :

$$|\psi\rangle = \frac{1}{\sqrt{8}} \left( |1000\rangle + |0100\rangle + |0010\rangle + |0001\rangle - |1110\rangle - |1101\rangle - |1011\rangle - |0111\rangle \right)$$

Parmi ces 8 états, 2 sont optimaux pour chaque joueur, ce qui nous amène à une probabilité de gain pour chaque joueur de  $\frac{2}{8} = \frac{1}{4}$ , c'est à dire le double de la performance maximale en stratégie classique. Par ailleurs, on a supprimé tous les états qui n'aminaient aucun gain pour aucun des joueurs grâce à cette stratégie (c'est pourquoi la probabilité de gagner double).

Par ailleurs, lorsque les joueurs jouent tous la stratégie  $a$ , on obtient un réel équilibre de Nash. En effet, si un joueur décide de changer unilatéralement de stratégie, il ne peut alors pas améliorer ses résultats, quelque soit la stratégie choisie, unitaire ou non-unitaire (préservant la trace et complètement positive).

Ainsi, en passant de  $N = 3$  à  $N = 4$ , un équilibre de Nash, non atteignable avec des stratégies classiques, émerge. Cet équilibre est aussi un équilibre optimal et équitable, dans la mesure où le gain est le même pour les 4 joueurs. Une fois encore, on constate que le partage d'un état intriqué et l'introduction de stratégies quantiques permettent de surpasser les stratégies classiques.

### 2.5.5 Ouvertures

Une généralisation du Minority Game dans sa version quantique pour  $N$  serait intéressante à mettre place. Comme présenté pour  $N = 3$ , si le nombre de joueurs est impair, la version quantique n'est pas avantagée par rapport au jeu classique. Un nouvel équilibre de Nash apparaît en revanche pour un nombre pair de joueurs, et l'on peut étudier de plus près la stabilité de cet équilibre en fonction du nombre de joueurs  $N$ , en introduisant différentes formes de décohérence, comme cela est traité dans [15].

On pourrait également s'intéresser aux performances obtenues lorsque les joueurs ne partagent pas un état maximalement intriqué. Chen *et al.* montrent que l'on n'obtient pas d'avantage par rapport au cas classique lorsque  $N$  est impair, mais que l'on peut avoir de meilleurs résultats que dans le cas classique lorsque  $N$  est pair, même si l'on n'atteint pas d'équilibre [14].

Par ailleurs, ce jeu peut avoir des applications dans divers domaines. Une des applications assez connue et dans le domaine de l'économie et les marchés financiers, où l'on modélise le marché avec un Minority Game et on utilise alors ce modèle pour gérer le transfert de bien et l'allocation des ressources [18].

On peut aussi étudier le jeu du point de vue de la position des joueurs entre eux. Selon si l'on suppose que les joueurs sont en compétition ou en coopération, les stratégies proposées peuvent évoluer. C'est ce que tente d'investiguer Linde *et al.* dans [19], et d'étudier des stratégies sur la version du jeu à plusieurs tours. Flitney & Greentree étudient quant à eux l'influence des coalitions sur les résultats du jeu, notamment en comparant les résultats quantiques et classiques [16].

Enfin, on peut étudier l'influence de l'environnement d'un joueur et de la corrélation du système quantique partagé par les joueurs et voir les répercussions sur les performances du jeu [17].

## 2.6 Autres jeux quantiques

### 2.6.1 Paradoxe de Parrondo - Parrondo's game

Nous allons, dans cette partie, présenter l'un des paradoxes les plus connus pour son originalité et son "étrangeté" extrême : Paradoxe de Parrondo<sup>1</sup>. Ce dernier met en avant l'idée que deux jeux, considérés comme perdants (i.e., le joueur a une probabilité de perdre supérieure à celle de gagner) séparément, deviennent gagnant lorsque l'ont les associent, certes d'une manière très particulière.

#### Déroulement du jeu classique

Tout d'abord, nous devons exposer et présenter les deux jeux pris séparément afin de pouvoir expliquer le jeu de Parrondo convenablement.

- Jeu A

Ce premier jeu, l'un des plus simples, consiste au lancer d'une pièce. La probabilité afin d'obtenir "pile" (i.e., gagner) est considérée égale à  $p_A$ . A l'inverse, la probabilité d'obtenir "face" (i.e., perdre) est considérée égale à  $(1 - p_A)$ . Afin que le jeu soit perdant, nous allons imposer la condition suivante (cela revient à utiliser des pièces truquées) :  $p_A < \frac{1}{2}$ .

- Jeu B dépendant du capital

Ce jeu va, quant à lui, utiliser deux pièces B et C. Ces dernières se diffèrent par leurs probabilités de gagner ( $p_B \neq p_C$ ). Afin de savoir quelle pièce

---

1. Juan Manuel Rodriguez Parrondo (né le 09 Janvier 1964) est un physicien espagnol de l'Université de Complutense de Madrid

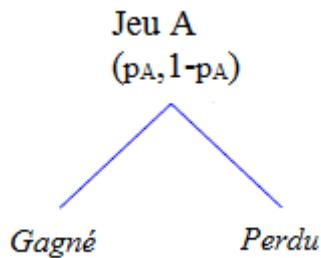


FIGURE 2.6 – Jeu A

nous allons utiliser, il suffit de se référer au capital de gain (qui correspond au nombre de fois gagnée moins celles perdues). En effet, si le capital est divisible par 3, nous choisirons de lancer la pièce B. Par contre, s'il ne l'est pas, alors nous lancerons la pièce C.

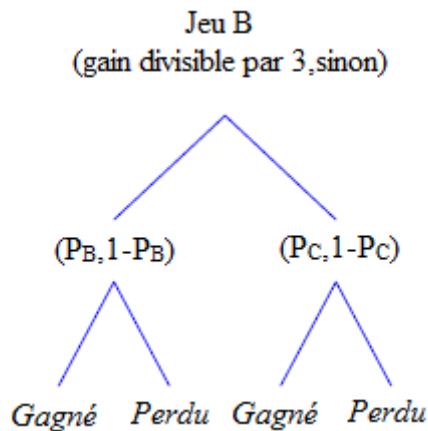


FIGURE 2.7 – Jeu B

On pourrait croire que le jeu B est gagnant. Mais il ne l'est pas. En effet, ceci peut être prouvé de différentes manières, dont celle qui utilise la notion de chaîne de Markov.

#### – Association des jeux A et B

Comme nous l'avons cité précédemment, l'association des deux jeux perdants peut amener à un jeu gagnant. Ceci peut être constaté par de simples simulations numériques.

Nous constatons que le gain tend à être négatif lorsque l'on joue les jeux A et

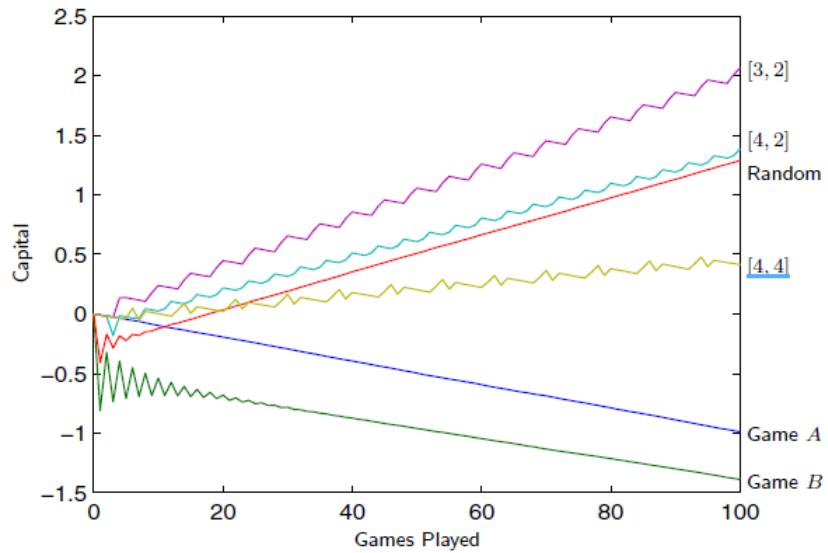


FIGURE 2.8 – Simulations de l’associations des jeux A et B. Le couple  $[a,b]$  indique que nous jouons  $a$  fois le jeu A et ensuite  $b$  fois le jeu B et ainsi de suite jusqu’à qu’on ait fait 100 jeux

B séparemment. Cependant, lorsque l’on joue le couple  $[3,2]$  ou  $[4,2]$ , le gain tend à être positif et fait ainsi de lui un jeu gagnant.

- Jeu B’ (dépendant de l’historique de jeu)

Une autre configuration est également possible. Elle consiste à utiliser un nouveau jeu B, nommée jeu B’. Il se différencie par la condition qui implique l’utilisation de la pièce B ou C. En effet, nous allons, maintenant, nous référer par rapport aux résultats des deux parties précédentes (gagné ou perdu) afin de choisir la pièce B, C, D ou E. Le jeu A est identique à celui vu précédemment. Le principe des jeux peut être représenté de la manière suivante :

- Association des jeux A et B’

Encore une fois, lorsque l’association des jeux est accomplie, nous obtenons un jeu gagnant. En effet, nous pouvons constater ces résultats à l’aide des simulations suivantes :

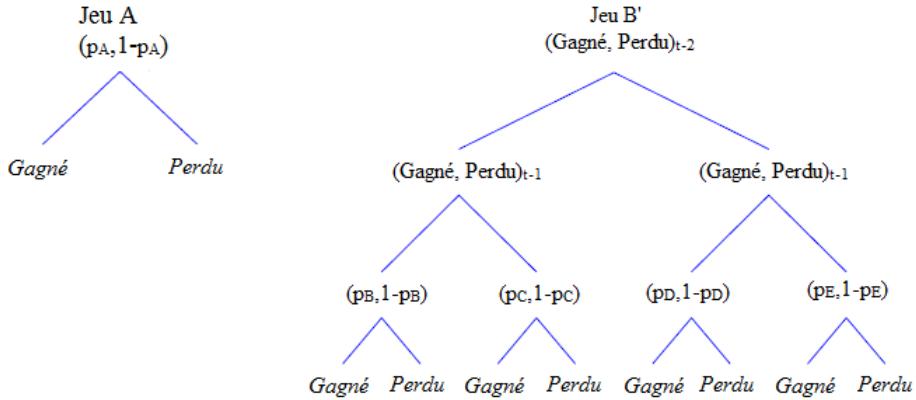


FIGURE 2.9 – Jeu A et B'

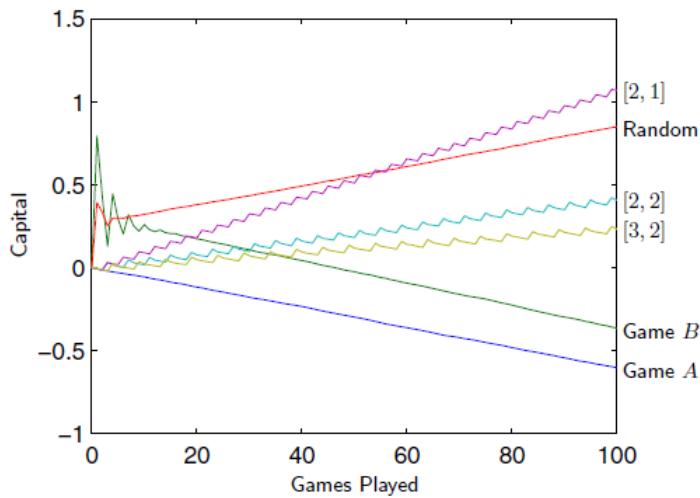


FIGURE 2.10 – Simulations de l'associations des jeux A et B'. Le couple  $[a,b]$  indique que nous jouons  $a$  fois le jeu A et ensuite  $b$  fois le jeu B et ainsi de suite jusqu'à qu'on ai fait 100 jeux

### Déroulement du jeu quantique

- Jeu quantique dépendant du capital

Il est envisageable de transcrire ce jeu de manière quantique. En effet, nous pouvons représenter le jeu A et B sous la forme des circuits quantiques suivants [50] :

Avec les différents paramètres définis de la manière suivante :

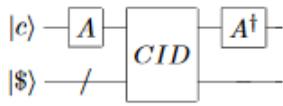


FIGURE 2.11 – Jeu quantique A

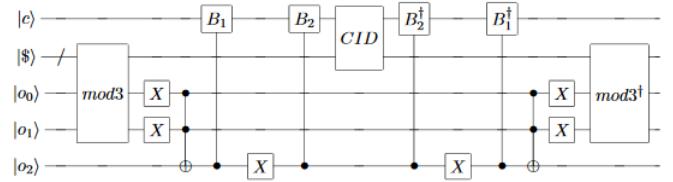


FIGURE 2.12 – Jeu quantique B

- $|c\rangle$  : qubit de registre qui représente l'état d'une pièce quantique
- $|$\rangle$  : n-qubits de registre qui représentent le gain pour chaque joueur n
- $|o\rangle$  : qutrit de registre auxiliaire qui permet de savoir si le gain est un multiple de 3
- $mod3$  : Opérateur qui permet de modifier  $|o\rangle$  si le gain est un multiple de 3
- $X, A, B_1$  et  $B_2$  : Portes quantiques ou opérateurs
- CID : Opérateur qui permet d'incrémenter, si  $|c\rangle$  est dans l'état  $|1\rangle$ , ou décrémenter, si  $|c\rangle$  est dans l'état  $|0\rangle$ , le capital de gain  $|$\rangle$

## 2.6.2 Guerre des sexes

### Déroulement du jeu classique

Ce jeu aborde un problème que rencontre deux conjoints : un homme et une femme. Ces derniers voudraient partager une soirée ensemble. Cependant, l'endroit de rencontre n'est pas commun. L'homme veut aller voir un match de foot tandis que la femme souhaiterait aller à l'opéra. Ils veulent cependant vivre ce moment à deux plutôt que seul, peu importe la destination. Les deux ne peuvent communiquer durant leurs choix.

|  |  | Homme | Opéra              | Foot               |
|--|--|-------|--------------------|--------------------|
|  |  | Femme | $(\alpha; \beta)$  | $(\sigma; \sigma)$ |
|  |  | Opéra | $(\sigma; \sigma)$ | $(\beta; \alpha)$  |
|  |  |       |                    |                    |

Nous considérons que  $\alpha, \beta$  et  $\sigma$  sont les gains respectifs vis à vis de la stratégie choisie. Pour répondre aux conditions imposées par le jeu, nous devons respecter  $\alpha > \beta > \sigma$ . Il faut également noter que dans la notation choisie pour le tableau (à savoir (Gain 1 ; Gain 2)), le gain 1 et le gain 2 correspondent respectivement au gain de la femme et de l'homme. L'objectif de chaque joueur est de maximiser son gain individuel.

Nous pouvons constater que ce jeu détient deux équilibres de Nash : (Opéra,Opéra) et (Foot, Foot). De plus, il ne faut surtout pas que (O, P) ou (F, O) arrive. En effet, le gain est minimal pour cette situation et cela pour les deux joueurs.

### Déroulement du jeu quantique

Voici le circuit quantique qui représente les différentes étapes quantiques qui correspondent au jeu [51].

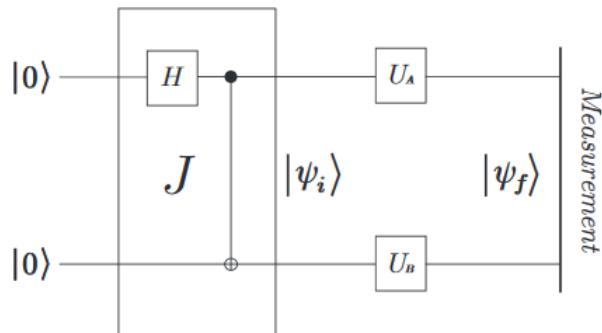


FIGURE 2.13 – Circuit quantique : La guerre des sexes

Chaque joueur dispose d'un qubit. La stratégie "aller à l'opéra" correspond à l'état du qubit  $|O\rangle$  et "aller au foot" correspond à l'état du qubit  $|F\rangle$ . Chaque joueur détient une porte quantique qu'il peut appliquer à son qubit. Ces dernières sont notées  $U_A$  et  $U_B$ .

Cette formalisation quantique est très similaire à celle vue précédemment pour le dilemme du prisonnier. Par conséquent, nous n'énoncerons que les formules de gain :

$$\begin{aligned} \$_A &= \alpha P_{OO} + \beta P_{FF} + \sigma(P_{FO} + 0P_{OF}) \\ \$_A &= \alpha P_{OO} + \beta P_{FF} + \sigma(P_{FO} + 0P_{OF}) \end{aligned}$$

Ainsi, de même que le dilemme de prisonnier, les deux joueurs, homme et femme, sont assurés d'avoir un gain maximal en appliquant une stratégie quantique.

### 2.6.3 Spin flip game

Le Spin Flip Game (SFG), souvent reconnu comme étant le premier jeu quantique, est un jeu faisant intervenir 2 joueurs  $A$  et  $B$ , et un électron. C'est un jeu

non coopératif où chaque joueur va chercher à gagner. Le résultat du jeu n'annonce qu'un seul vainqueur, et donc qu'un seul perdant. Le jeu se présente comme une sorte de pile ou face, où les joueurs vont manipuler à 1 ou 2 reprises l'orientation du spin de l'électron.

### Principe du jeu et stratégie "classique"

Le joueur  $A$  commence par orienter le spin de l'électron vers le haut, c.a.d. vers l'état  $|up\rangle = |u\rangle$ . Le joueur  $B$  a ensuite deux possibilités : soit appliquer la porte  $I$  (identité) ou  $X$  (not) au spin de l'électron dans l'état  $|u\rangle$ . On note  $|down\rangle = |d\rangle = X|u\rangle$ . Ceci est pour le premier tour du jeu.

Pour le second tour du jeu, le joueur  $A$ , tout d'abord, a la possibilité à son tour d'appliquer la porte  $I$  ou  $X$ . Ensuite seulement, le joueur  $B$  peut appliquer la porte  $I$  ou  $X$ .

L'état de l'électron est ensuite mesuré. Comme nous le verrons plus tard, il y a autant de chance d'obtenir le spin orienté vers le haut, qu'un spin orienté vers le bas (similairement au pile ou face). On suppose donc que si son spin est orienté vers le haut, c'est à dire que l'on obtient  $|u\rangle$ , c'est le joueur  $A$  qui gagne. Inversement, si le spin est orienté vers le bas, c'est à dire que l'on obtient  $|d\rangle$ , c'est le joueur  $B$  qui gagne. L'inverse donne le même résultat en terme de gain.

| $A / B$ | $II$  | $IX$  | $XI$  | $XX$  |
|---------|-------|-------|-------|-------|
| $I$     | $III$ | $IIX$ | $XII$ | $XIX$ |
| $X$     | $IXI$ | $IXX$ | $XXI$ | $XXX$ |

FIGURE 2.14 – Portes quantiques finales à appliquer à l'état initial  $|u\rangle$  en fonction des stratégies des deux joueurs

En appliquant chacune des portes correspondant à chacune des possibilités de stratégies choisies par les joueurs, on obtient les états finaux suivants :

| $A / B$ | $II$        | $IX$        | $XI$        | $XX$        |
|---------|-------------|-------------|-------------|-------------|
| $I$     | $ u\rangle$ | $ d\rangle$ | $ d\rangle$ | $ u\rangle$ |
| $X$     | $ d\rangle$ | $ u\rangle$ | $ u\rangle$ | $ d\rangle$ |

FIGURE 2.15 – Etat final du spin de l'électron mesuré en fonction des stratégies des deux joueurs

En supposant que si  $A$  gagne il remporte un gain de  $+1$ , et un gain de  $-1$  si il perd, on obtient le tableau de gain suivant pour le joueur  $A$  :

| $A / B$ | $II$ | $IX$ | $XI$ | $XX$ |
|---------|------|------|------|------|
| $I$     | +1   | -1   | -1   | +1   |
| $X$     | -1   | +1   | +1   | -1   |

FIGURE 2.16 – Tableau de gain pour le joueur  $A$

On remarque que le joueur  $A$  a une chance sur deux de gagner quelque soit sa stratégie adoptée, et il en est de même pour le joueur  $B$ . On retrouve donc le jeu du pile ou face que l'on connaît usuellement ;

### Utilisation d'une stratégie quantique

L'introduction d'une stratégie quantique, comme on peut s'y attendre, va amener une amélioration de la performance du joueur l'utilisant. Suppose que c'est le joueur  $B$  qui décide de passer à une stratégie quantique. Contrairement à précédemment, le joueur  $B$  misera toujours sur un spin de l'électron orienté vers le haut. Le joueur  $A$  gagne donc si le spin est orienté vers le bas.

Ainsi, durant le premier tour, le joueur  $A$  place toujours le spin en position haut  $|u\rangle$ . À présent, le joueur  $B$  choisit d'appliquer la porte  $H$  d'Hadamard au lieu de  $I$  ou  $X$ . Il en résulte donc l'état suivant :  $H|u\rangle = \frac{1}{\sqrt{2}}(|u\rangle + |d\rangle)$ .

Pour le second tour,  $A$  a le choix d'appliquer la porte  $I$  ou  $X$ . Dans les deux cas, l'état résultant reste inchangé par rapport au précédent dans la mesure où :  $I(H|u\rangle) = X(H|u\rangle) = H|u\rangle$ . Le joueur  $B$  rejoue à son tour avec la stratégie précédente, dans le sens où il ré-applique la porte  $H$  à l'état précédent, ce qui nous donne l'état suivant :  $H(H|u\rangle) = H^2|u\rangle = |u\rangle$ .

Ainsi avec cette stratégie, le joueur  $B$  est assuré de gagner au jeu du pile ou face, ou plutôt au jeu d'orientation du spin, ce qui n'est pas possible avec des stratégies classiques. Une fois encore, l'utilisation de stratégies quantiques prouve la puissance et l'efficacité de travailler dans un monde quantique.

## 2.6.4 Jeux quantiques restants

| Nom du jeu              | Résumé, nombre de joueurs   | Références               |
|-------------------------|---|--------------------------|
| Wise Alice game         | Jeu à 2 joueurs, Bob place une balle dans 1 sur 4 emplacements. Alice pose une question fermée à Bob. S'il répond oui, Alice est satisfaite, sinon elle peut demander un dédommagement. Bob peut bouger la balle à une place adjacente après la question d'Alice. | [24, 25, 26, 27, 28, 29] |
| Quantum Bargaining game | Jeu à 2 joueurs, un vendeur et un acheteur. Le vendeur négocie avec l'acheteur pour le prix : faire des affaires pour plus tard et/ou user de chantage.   | [30, 31, 32]             |
| Quantum Ultimatum game  | Jeu à 2 joueurs, un proposeur et un répondeur. Le proposeur doit répartir 100 unités entre lui et l'autre joueur, et fait une proposition au répondeur. S'il accepte, alors les unités sont distribuées. S'il n'accepte pas, personne ne gagne rien.              | [20, 21, 22, 23, 69]     |

FIGURE 2.17 – Tableau regroupant les derniers jeux quantiques présentés dans ce chapitre

## Deuxième partie

# Applications au domaine de l'énergie

# Chapitre 3

## Sécurité et Smart Grid

Le réseau électrique (de l'énergie primaire jusqu'au consommateur final) actuel n'est pas durable dans le temps, tant au niveau environnemental, économique ou encore social. Par conséquent, le développement d'un nouveau type de réseau, réseau nommé intelligent (plus connu sous le nom de "Smart grid"), est primordial. Celui-ci devra faire face aux différents challenges énergétiques. C'est ce que nous proposons d'étudier dans ce chapitre.

### 3.1 Présentation du réseau intelligent ou Smart Grid

Dans cette partie, nous allons présenter un type de réseau électrique en actuel développement : "Smart Grid" ou réseau intelligent. Ce dernier peut être présenté comme un réseau électrique qui utilise différentes technologies afin de rendre les opérations optimales (ou plus efficace), que ce soit au niveau de la production, distribution ou encore au niveau de la consommation. Ces différents processus sont coordonnés de manière autonome. La promesse européenne pour 2020, afin de réduire de 20% des gaz à émissions de serres ; augmenter la production totale en énergies renouvelables à hauteur de 20 % également et une réduction de 20% de la consommation totale énergétique, pourrait être tenue et même améliorée dans le futur avec l'implémentation d'un tel réseau.

#### 3.1.1 Intérêts principaux d'un nouveau type de réseau

##### Intégration de centres de production décentralisés

La production électrique fournie par le réseau actuel dépend fortement et malheureusement des ressources fossiles, qui ne cessent de diminuer. En effet, le sys-

tème électrique français repose sur une production électrique assez centralisée autour de centrales très puissantes. Par conséquent, au vu de son incapacité à accueillir un grand nombre de source d'énergie renouvelable intermittente, il est plus que nécessaire de réfléchir à un nouveau type de réseau qui saurait répondre à ce type de besoin. Le réseau intelligent permet d'intégrer, non seulement, des moyens de production de grande ampleur et centralisé (par exemple des centrales nucléaires) mais également des plus petites installations telles que les systèmes d'énergie renouvelable où les productions venant des consommateurs eux-mêmes (ainsi rendre possible la création de millions de micro sources d'énergie). Il faut également noté que le réseau actuel ne permettra pas de subvenir aux besoins électriques futurs qui vont augmenter de manière assez conséquente.

### **Gestion de la demande et utilisation de technologies d'informations et de communications**

Les types de réseau actuels permettent la navigation d'énergie uniquement dans un seul sens (du producteur vers le consommateur). Tandis que le réseau intelligent permettrait de favoriser le développement de producteurs d'énergie à petite échelle en ayant la capacité de faire circuler l'énergie dans les deux sens.

Les consommateurs vont jouer un rôle important au sein du réseau intelligent. Ils vont permettre d'avoir plus d'informations sur le profil de consommation et ainsi ajuster la production. Ceci afin d'atteindre une production qui s'approche le plus de la consommation, c'est-à-dire un équilibre entre l'offre et la demande, et éviter les pics de demande. Dans cette nouvelle configuration, nous pourrions envisager une tarification variable de l'électricité en fonction de l'heure d'utilisation. Afin de pouvoir rendre cela possible, différentes technologies devront intégrer les installations des consommateurs dont notamment les "Smartmeters". Ces derniers permettront de mesurer la quantité d'énergie consommée par les utilisateurs et également avoir une fonction de régulateur sur la consommation. En effet, le consommateur pourra également modifier sa demande d'électricité à l'aide des données récoltées en temps réel.

### **Intégration des bornes de recharges pour les véhicules électriques**

L'introduction des véhicules électriques est aussi favorisée par les réseaux intelligents. La communication entre le réseau et les véhicules est primordiale pour pouvoir agir correctement. On pourrait imaginer que l'énergie stockée (mais non utilisée par les véhicules) pourrait être utilisée en cas de besoin par le réseau électrique (ce principe est nommé le V2G : "Vehicle to Grid"). Il faut noter également que l'introduction des véhicules électriques permettrait la réduction des gaz à effet

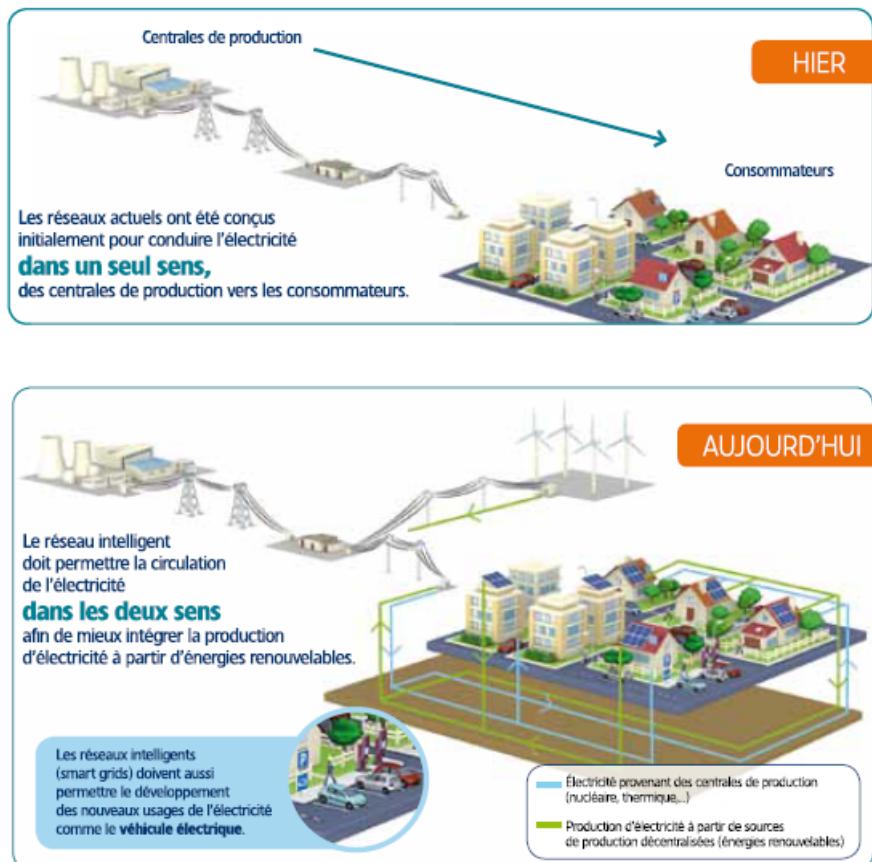


FIGURE 3.1 – Flux d'énergie et d'information (Source ERDF)

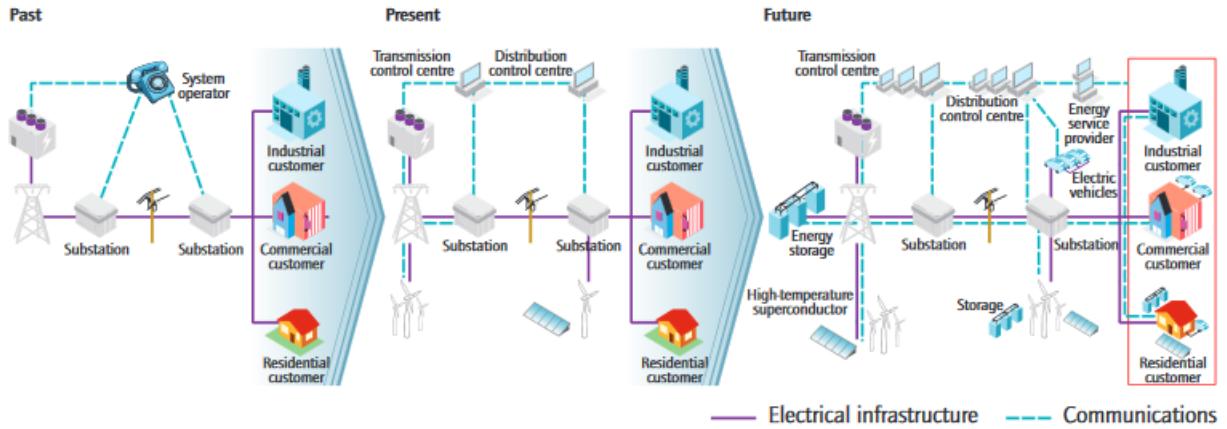
de serre.

### Efficacité et incidents sur le réseau

Par ailleurs, ce réseau permettrait également de réduire les pertes d'énergie et de détecter plus rapidement les problèmes grâce à une prise d'information sur le réseau complet.

#### 3.1.2 Description du système

Nous pouvons représenter l'évolution du réseau électrique comme suit [58] :



Source: Unless otherwise indicated, all material derives from IEA data and analysis.

FIGURE 3.2 – Evolution du réseau électrique

La différence principale repose sur les flux d'action. En effet, le réseau intelligent possède un flux de transmission d'électricité mais également d'un flux d'informations. Ce dernier va permettre de coordonner la production d'électricité et la consommation réelle.

### 3.1.3 Différents secteurs affectés

Nous pouvons distinguer les différents axes, sur lesquels ce type de réseau influerait grandement, et ceci est représenté dans la figure suivante [58] :

### 3.1.4 Smartgrid en France

La France se place parmi l'un des pays les plus avancés dans la recherche et le développement des applications du réseau intelligent. Cette partie visera à présenter brièvement quelques projets déjà en cours.

#### Programme Linky

L'installation de plus de 35 millions de compteurs intelligent (ou communicant) d'ici 2021 est une initiative développée par ENEDIS (anciennement ERDF). Ce projet a été lancé en 2007 et a été déployé depuis le 1er Janvier 2015. L'utilisation d'un tel outil permettrait une gestion plus optimisée de la consommation électrique.

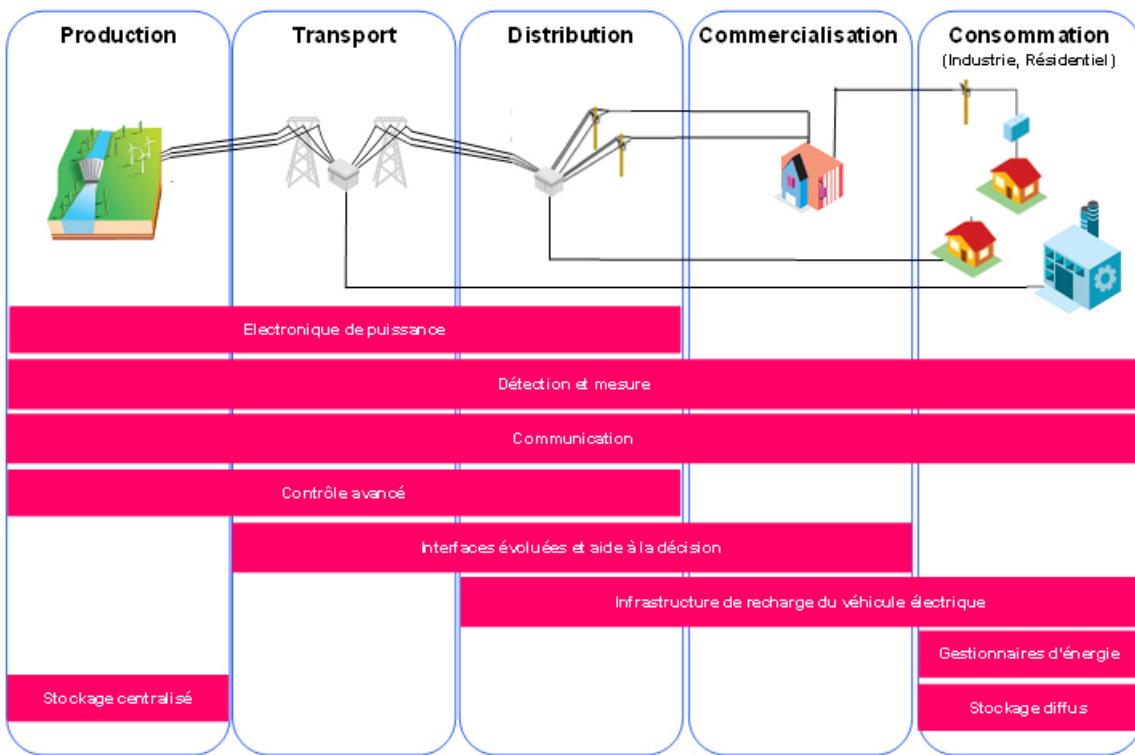


FIGURE 3.3 – Domaines d'applications des technologies des Smartgrids

Ce dernier peut également jouer un rôle d'actionneur en décalant certains usages des consommateurs afin de répondre au mieux à un pic de consommation.

Sur la figure suivante, nous pouvons voir le rôle joué par le compteur intelligent :

Ce compteur utilise le moyen de communication que l'on appelle CPL (Courant Porteur en Ligne). Ce type d'usage permet de transmettre et recevoir des informations via les câbles électriques. Nous ajoutons simplement un signal électrique (qui transporte l'information) au flux électrique. L'Union Internationale des Communications a opté pour le protocole de communication G3, qui plus est le seul supportant le protocole IPv6 qui permet d'assurer via internet la gestion des compteurs.

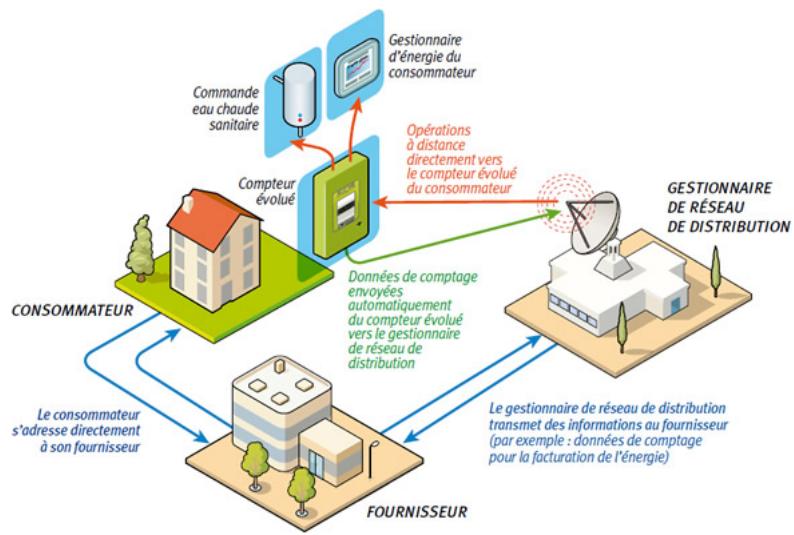


FIGURE 3.4 – Place du compteur intelligent (Source CRE)

### Projet Nice Grid : Quartier solaire intelligent

Nice GRid est un projet développé à Carros depuis 2011. Celui-ci implique 1500 consommateurs résidentiels, tertiaires et industriels dont 300 foyers et 11 clients industriels. Celui-ci est piloté par Enedis et fait partie du projet européen Grid4EU. L'investissement total correspond à environ 30 millions d'euros.

Ce projet a pour but d'optimiser l'exploitation d'un réseau de distribution électrique en incluant des sources d'énergies renouvelables (dont tout particulièrement celle produite par les panneaux photovoltaïques). La gestion de la demande, en faisant contribuer les consommateurs dans la boucle d'action, est également développée afin de réduire les pics de consommations au niveau local. Ce projet vise aussi à tester les possibilités d'ilotage de ce type de réseau et d'observer son comportement dans une telle situation.

Le système global du système est représenté ci-dessous [72] :

Le déploiement des différentes technologies et les différents tests effectués sont présentés sur la figure suivante [72] :

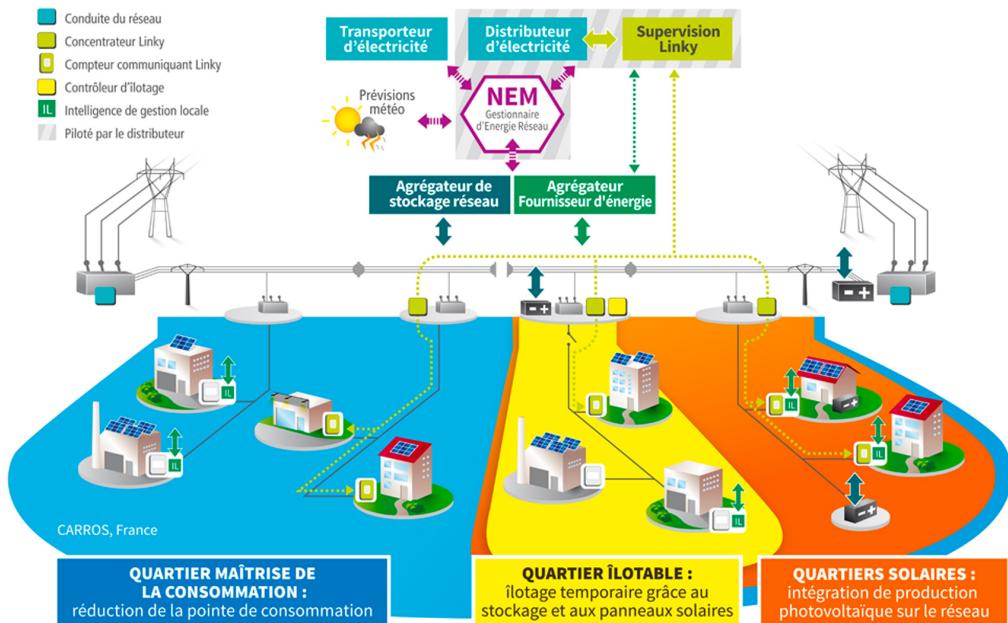


FIGURE 3.5 – Système global

### Projet GreenLys

Ce projet, dont l'investissement correspond à 43 millions d'euros, a été lancé en 2012 par ENEDIS (et d'autres participants tels que ENGIE, Schneider, GEG, ...etc) sur les villes de Lyon et Grenoble afin d'étudier le comportement des technologies des Smart grids en zone urbaine et conditions réelles. Parmi celles-ci, nous pouvons retrouver le système Linky, les outils de gestion en temps réel du réseau, les moyens mis en place afin d'accueillir sur le réseau les sources de productions d'énergies renouvelables ainsi que les bornes de charges de véhicules, et enfin les outils qui permettent les "effacements" de consommation afin d'équilibrer l'offre et la demande.

Les étapes clés du projet sont résumées ci-dessous :

### Projet IssyGrid : Quartier intelligent

IssyGrid est un projet lancé en 2012 au sein de la ville de Issy-Les-Moulineaux. ce dernier vise à tester le fonctionnement du Smart grid à l'échelle de quartier, plus

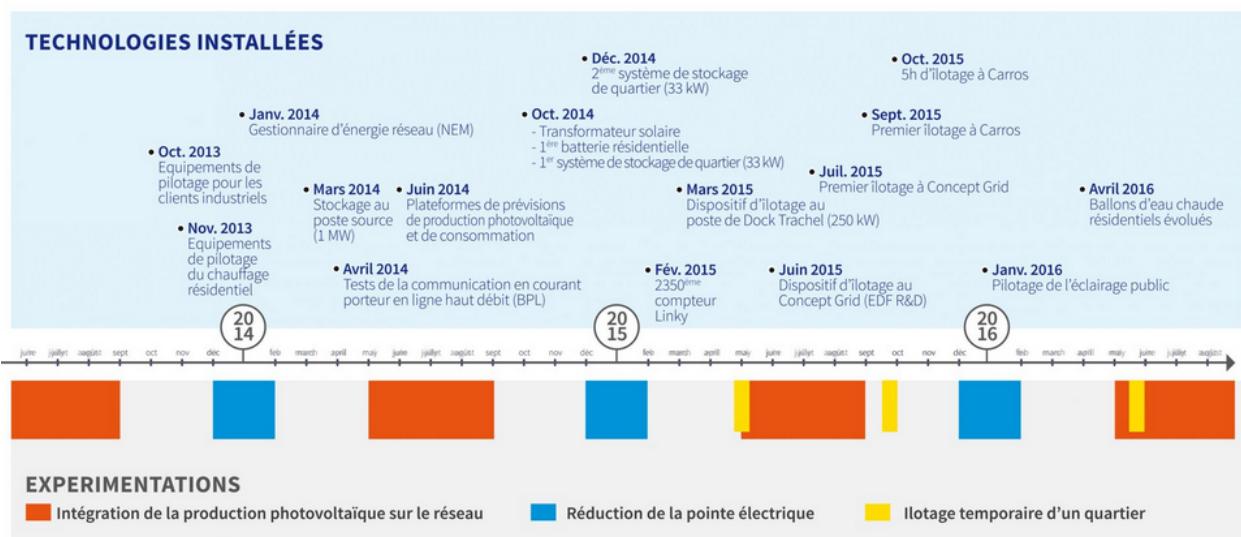


FIGURE 3.6 – Déploiement des technologies

### LES ÉTAPES CLÉS DU PROJET



FIGURE 3.7 – Déroulement du projet (Source ENEDIS)

précisément ceux de Seine Ouest et Fort d'Issy. Ce système gère la consommation et production d'énergie d'environ 2 000 habitants et 5 000 employés sur une surface 100 00 m<sup>2</sup>.

Le système global peut être représenté de la manière suivante :

Celui-ci vise à gérer au mieux la consommation en incluant les nouveaux types



FIGURE 3.8 – Système global (Source ISSY)

d'usage (par exemple les véhicules électriques), intégrer les sources de production d'énergie renouvelables et optimiser la gestion de l'énergie au sein des quartiers.

Les étapes clés du projet sont résumées ci-dessous :

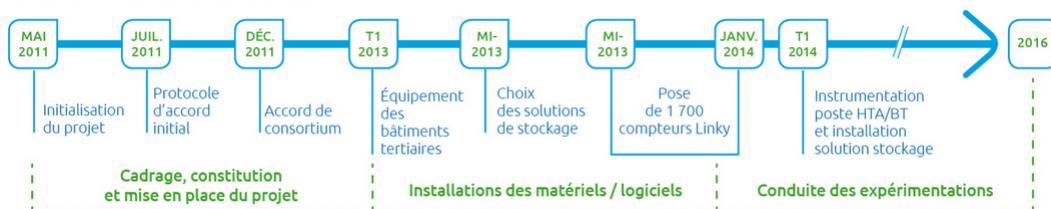


FIGURE 3.9 – Etapes clés du projet (Source ENEDIS)

### 3.1.5 Prédictions pour le futur

Voici un tableau qui résume l'évolution des "Smart Grids" qui devrait avoir lieu [54] :

| 2015-2020   | 2020-2025  | 2025-2030   |
|---|--|---|
| <ul style="list-style-type: none"> <li>Smart meters, demand response, models for demand forecasting</li> <li>Communications through public communication networks, sporadic dedicated fiber channels laid down by utility, and wireless routers</li> <li>Deployment of sensors using fiber and wireless communication for data collection</li> <li>Wireless embraced actively due to low cost of installation with fiber penetrating slowly</li> <li>New appliances with communication devices allow controls through smart meters</li> <li>Existing appliances retrofitted with communication that allow to be turned on and off at a minimum</li> <li>Household communications will be wireless and/or power line communication (PLC).</li> <li>Data will be encrypted from the smart meter throughout the entire grid</li> <li>Integrity of the will be managed through data checksums and comparison</li> <li>Availability of data will be ensured through backup communication channels</li> </ul> | <ul style="list-style-type: none"> <li>Smart meters using dedicated communication channels</li> <li>Demand response across various grids, data analysis and aggregation for demand forecasting</li> <li>Need higher bandwidth need to support demand forecasting and market pricing</li> <li>Metropolitan areas continue to see proliferation of wireless communication</li> <li>Fiber either embedded in electric cables or strung along power lines to carry data from sensors and supporting renewable integration</li> <li>PLC may emerge as the backup communication channel</li> <li>Bandwidth increased to process data for real-time supply forecasting</li> <li>Communication enabled intelligence appliances will dominate the market</li> <li>PLC and wireless will lead communication channels in the household.</li> <li>Data security a key concern with new threats to the integrity of data</li> <li>Data integrity checks based on past patterns and redundant readings</li> <li>Vulnerabilities in wireless will lead to a gradual shift towards fiber.</li> </ul> | <ul style="list-style-type: none"> <li>Smart meters pervasive across households</li> <li>Applications for sophisticated demand-response and demand/supply forecasting.</li> <li>Real-time electricity market will add additional burden to communication</li> <li>Grid communication network will be controlled by the utilities,</li> <li>Sensors for monitoring and diagnostics with self-healing and self-recovery</li> <li>Intelligent computation pervasive in the network</li> <li>Communication will primarily be fiber through the grid with wireless communication in pockets.</li> <li>Substations will use wireless and wired communication for data collection</li> <li>Aggregated data sent via fiber to processing centers</li> <li>PLC will be used for backup communication</li> <li>The transmission and distribution communications networks will start coalescing into a single network.</li> <li>Household appliances will use either wireless or PLC communication.</li> <li>Wireless actively replaced by fiber in most areas for increased security</li> </ul> |

FIGURE 3.10 – Evolution des Smart Grids

## 3.2 Sécurisation des Smart Grid

L'introduction des technologies de communication au sein des réseaux intelligents permet d'améliorer le fonctionnement du système global tout en le rendant plus vulnérable au cyber attaques. Par conséquent, il est plus que nécessaire d'étudier et de rendre plus fiable le niveau de sécurité au sein du réseau [54]. Les performances des Smart Grids dépendent fortement de l'information transmise. Si celle-ci est corrompue, les performances du réseau en sont fortement perturbées.

La sécurité n'est pas un sujet nouveau au niveau technologique. Par conséquent, on pourrait tout simplement envisager de protéger le réseau électrique intelligent en utilisant les mêmes moyens employés que pour Internet. Cependant cela n'est pas la meilleure et la plus adéquate des solutions au vu des caractéristiques, complètement différentes d'Internet, que présente les Smart grids. Par conséquent, il faut opter pour de nouveaux types de cryptages d'informations.

Nous pouvons distinguer deux types de cryptage qui se différencie par la manière dont l'on distribue les clés de codage : clé privée et clé publique. La première, nommée clé privée, consiste à utiliser la même clé afin de coder et décoder le message (l'information). Alors que la clé publique utilise différentes clés pour coder et décoder le message. A partir de là, nous pouvons constater qu'en utilisant la clé privée, nous devons impérativement se partager la clé de cryptage avant que le message soit crypté (à l'aide d'une rencontre physique ou d'un canal sécurisé par exemple). A l'inverse, la clé publique permet d'éviter ce partage en rendant "publique" la clé de codage alors que celle de décodage est privée (les deux clés sont reliées de manière mathématique). Il est cependant possible de "hacker" ce genre de clé en utilisant des moyens sophistiqués, qui prennent, par ailleurs, un certain de temps dépendant de la complexité numérique. Ce type de cryptage n'est donc pas totalement fiable.

Néanmoins, la théorie de l'information quantique apporte des solutions majeurs vis-à-vis de la cryptographie. En effet, la distribution de clés quantique semble être un moyen adapté afin de sécuriser au mieux les transferts d'informations, tel que dans un Smart grid.

Dans l'article [55], il a été démontré expérimentalement que ce type de moyen peut être envisagé afin de répondre convenablement à la demande en terme de sécurité, en utilisant notamment le protocole de communication sécurisé quantique BB84 [1.4](#)

### 3.3 Communiquer plus d'informations avec le Superdense Coding

Une des problématiques, et un des enjeux de la recherche dans ce domaine, est l'amélioration et l'optimisation de la qualité, de la quantité et de l'architecture des communications mises en place pour permettre le fonctionnement efficace et sûr d'un système déployé sur un réseau, comme celui des Smart Grids.

Une des propositions que la théorie de l'information quantique peut formuler, est la transmission d'information contenant elle même de l'information : c'est le principe du Superdense Coding (voir section 1.3 pour la procédure détaillée pour les 2 qubits). En transmettant des qubits ou des qudits (généralisation du qubit à  $d$  états de bases) d'information issus d'un état intriqué partagé avec le destinataire, on peut à l'aide du protocole de Superdense Coding faire émerger un surplus d'information par rapport à la quantité de qubits ou qudits envoyés initialement.

Pour l'étude des différents cas d'application proposés, nous nous placerons alors dans un cas de communication où un certain nombre d'entités doivent communiquer des informations à un contrôleur, ou à une autre entité de même niveau. Afin de simplifier la présentation, nous supposerons que deux entités  $A$  et  $B$  doivent communiquer des informations sur leur fonctionnement à une unité  $S$ . Ce schéma peut être adapté en ajoutant une communication bi-latérale et en ajoutant des entités communiquantes supplémentaires, le principe restera alors le même.

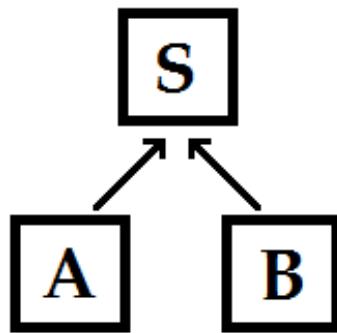


FIGURE 3.11 – Schéma du système simplifié de communication

### 3.3.1 Communication avec 4 choix de messages

Supposons que les deux entités  $A$  et  $B$  veulent communiquer avec  $S$ , mais n'ont besoin que de 4 messages au total. Dans ce cas, ils peuvent choisir de mettre en place un Superdense coding à 2-qubits classique, afin de gagner en quantité et donc en rapidité de transfert d'information avec un rapport de 2.

Pour ce faire, il faut que  $A$  et  $S$  partagent un état de Bell  $|\psi_1\rangle$ , c'est à dire :

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0_A 0_{S_1}\rangle + |1_A 1_{S_1}\rangle)$$

De la même manière,  $B$  et  $S$  doivent également partager un état de Bell  $|\psi_2\rangle$  tel que :

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}(|0_B 0_{S_2}\rangle + |1_B 1_{S_2}\rangle)$$

Les 4 messages possibles que  $A$  et  $B$  peuvent communiquer sont :  $|00\rangle$ ,  $|01\rangle$ ,  $|10\rangle$  et  $|11\rangle$ . Chaque 2-qubit sera interprété comme un message lié à la production, à un besoin d'énergie, ou à tout autre type de message pouvant être communiqué dans un Smart Grid. Une fois le message choisi, chaque entité applique le protocole de Superdense coding avec  $S$  :

- $A$  manipule et envoie son qubit à  $S$
- $B$  manipule et envoie son qubit à  $S$
- $S$  reçoit le qubit de  $A$  et manipule l'état intriqué  $|\psi_1\rangle$  puis mesure
- $S$  reçoit le qubit de  $B$  et manipule l'état intriqué  $|\psi_2\rangle$  puis mesure

Ainsi, au total,  $A$  envoie 1 qubit d'information,  $B$  envoie 1 qubit d'information,  $S$  décode le tout et reçoit donc au total  $2 \times 2$  qubits d'information. Nous avons donc bien un gain de 2, dans la mesure où l'on envoie 2 "unités" d'information pour en recevoir 4 au final.

Cela peut donc permettre de doubler l'efficacité des communications en terme de quantité d'information envoyée, et peut éventuellement permettre d'optimiser les systèmes de type Grid en terme de réponse à une demande, ou d'organisation interne des unités de production, du contrôle de la consommation, et de manière générale, tous les aspects utilisant une quelconque communication.

### 3.3.2 Communication générale dans un système

Dans cette sous-section, nous tenterons de présenter une manière théorique d'utiliser le Superdense coding à 2-qubits (classique) et à  $n$ -qudits afin de pouvoir transmettre le message voulu avec gain d'information, tout en bénéficiant du nombre de messages non limité pour une communication complète.

Si la variété du nombre de message voulant être transmis est  $M = 4$ , on utilisera alors le Superdense coding classique à 2-qubits. Si le nombre  $M$  est inférieur ou égal à 2, on ne peut réduire la quantité de qubit à envoyer, et il suffira alors d'envoyer le qubit correspondant au message. Si le nombre  $M$  est égal à 3, on utilisera alors toujours le même protocole de Superdense coding avec 2-qubits, sauf que les unités  $A$  et  $B$  ne manipuleront leur qubit que de 3 manières différentes pour les 3 messages possibles.

Supposons maintenant que l'unité  $A$  ou  $B$  communiquent de manière classique avec  $S$ , comme le feraient les composants électroniques d'un système d'information industriel, ou comme cela s'opère entre un microcontrôleur et des capteurs ou tout composant électronique. Ils communiquent le plus souvent à l'aide de protocoles de communication très précis, utilisant des registres de données, et des registres d'adresses par exemple, le tout en binaire. Un message sera alors envoyé sous la forme d'une séquence de bits, et on pourra découper le message global pour en déduire l'identifiant de l'expéditeur, le message en lui-même, la partie de contrôle de la séquence, etc.

Si l'on suppose que la taille  $T$  de la séquence de bits à envoyer est paire, et  $T = 2k$  avec  $k \in \mathbb{N}$ , et si l'on veut substituer cette communication classique par une communication utilisant le Superdense-coding, il suffira alors de découper cette séquence en  $k$  parties de 2-bits. Ensuite, pour chaque paire de bits, on applique le Superdense coding classique à 2 qubits. Ainsi, au lieu d'envoyer  $2k$  bits d'information, on envoie à la place  $k$  qubits d'information, ce qui réduit la quantité d'information transmise. Les deux communiquant  $A/B$  et  $S$  devront en outre partager autant de systèmes intriqués pour mettre en place le Superdense coding.

Si la taille de bits à transmettre s'avère impaire, donc  $T = 2k+1$ , avec  $k \in \mathbb{N}$ , il suffira donc de transmettre classiquement le premier bit d'information, et ensuite d'appliquer le même processus que ci-dessus aux  $2k$  bits restants. Cette fois-ci, on devra transmettre au final  $k+1$  unités d'informations (1 bit ou qubit, et  $k$  qubits).

On peut imaginer aussi, à la place d'un découpage de la séquence de bits à

envoyer, de mettre un place un protocole de Superdense coding à  $n$ -qudits en fonction de la taille de la séquence, pour n'envoyer de l'information qu'une seule fois, et que l'unité  $S$  ne décode l'information totale qu'une seule. Ceci nécessite cependant de disposer d'une connaissance théorique du protocole de Superdense coding dans le cas général d'un système à  $n$ -qudits et de pouvoir le réaliser expérimentalement lorsque la taille des données à transmettre s'agrandit. On pourrait cependant imaginer le même type de découpage que pour les 2-qubits, mais avec  $n$ -qubits par exemple. On gagnerait alors en temps d'encodage/décodage en appliquant les portes et les mesures pour plusieurs qubits à la fois.

Les idées présentées de manière générales ci-dessus pourraient donc servir à optimiser de manière quantitative les communications présentes dans les systèmes de types Smart Grid. On pourrait se poser la question de la qualité et de la sécurité des ressources partagées. Pour ce qui est de la sécurité, nous abordons le sujet dans la sectio 3.2. En terme de qualité des données transmises, une idée possible serait d'utiliser le domaine de la correction de code aussi appelé codes correcteurs, notamment les codes quantiques, et tentant de retrouver le code initial à partir de d'un code bruité, ou déterioré, par décohérence par exemple [68].

# Chapitre 4

## Allocation des ressources

### 4.1 Problématique de l'allocation des ressources et théorie des jeux

"L'allocation des ressources est un concept économique qui concerne l'utilisation des ressources rares et notamment les facteurs de production (travail, capital, matières premières) pour satisfaire à court et long terme les besoins de consommation de la population [70]." Ce concept peut être associé à l'énergie, en parlant d'allocation des ressources énergétiques.

"Cette allocation demande, dès que l'activité économique atteint une certaine taille et complexité, de définir un mode d'arbitrage autre que la guerre ou la rapine, et donc des institutions sociales adaptées. Cet arbitrage se fait de façon plus ou moins libre, par le biais des prix de marché, le fonctionnement de ces marchés étant eux-mêmes formalisés par des règles de droit ; ou par les administrations d'État, à l'aide de règles ou de lois.

Dans un sens plus étroit, l'allocation des ressources peut concerter l'arbitrage entre les divers facteurs de production, voire les choix et dosages à faire à l'intérieur d'un type de facteur."

C'est dans ce cadre que l'introduction de la théorie des jeux pour arbitrer la répartition des ressources entre les clients/joueurs prend tout son sens. En effet, les différents demandeurs vont être en concurrence pour obtenir cette ressource rare, ou pour l'obtenir à moindre prix. Utiliser des jeux à plusieurs et surtout non-coopératifs permettrait alors de modéliser cette situation et de pouvoir ensuite proposer des solutions issues directement des outils développés dans la théorie des jeux, à travers la proposition de stratégies optimales ou la recherche d'équilibres

par exemple.

C'est dans cette mesure que nous proposons un certain nombre de cas d'application de jeux non-coopératifs quantiques dans un scénario d'allocation de ressources et de gestion de production mettant en scène plusieurs acteurs en concurrence, modélisés alors comme des joueurs.

## 4.2 Scénario basé sur le Dilemme du Prisonnier

Nous allons voir, dans cette partie, l'intérêt que pourrait avoir l'application du dilemme du prisonnier, sous forme quantique, au sein d'un bâtiment intelligent.

### 4.2.1 Explication du scénario

### 4.2.2 Bâtiment intelligent

Imaginons un bâtiment composé de plusieurs étages (exactement 2 dans notre cas, pour simplifier les calculs). A chaque étage de celui-ci, une consommation propre à l'utilisateur doit être comblée. Afin d'assurer l'alimentation des deux consommateurs, le bâtiment dispose de deux moyens de production d'énergie.

L'un serait un moyen très important tel que le réseau d'électricité considérée comme un réseau disposant d'une puissance pouvant combler aisément les besoins du bâtiment à lui seul. Cependant, ce dernier fournit l'électricité à un prix assez conséquent.

Le second serait le fruit d'un investissement pour l'installation d'un moyen de production d'énergie renouvelable local. Ce dernier proposerait, par conséquent, un coût d'électricité plus intéressant que le réseau d'électricité principal. Cependant, ce dispositif ne permet, pas à lui seul, de combler la consommation des deux consommateurs.

De plus, les deux consommateurs disposent de gestionnaire d'énergie. Ces derniers permettent de basculer entre les différents moyens d'apport en électricité : le réseau principal (EDF) et le système d'énergie renouvelable.

### Choix du système de production d'énergie secondaire

Nous pouvons imaginer d'utiliser des moyens de production d'énergie renouvelable tels que la géothermie, l'énergie solaire ou encore l'énergie du vent.

Cependant, la géothermie semble être un moyen très difficile à exploiter. En effet, ce moyen de production d'énergie dépend fortement de la localisation géographique du site. Ce serait très optimiste de pouvoir penser qu'un tel système pourrait engendrer une production d'électricité à un faible coût (en prenant en compte les frais d'installation).

L'installation d'une éolienne ne serait, elle aussi, pas très simple et bénéfique. Effectivement, les performances d'une éolienne dépendent fortement de la vitesse du vent ( l'énergie est fonction de la vitesse au cube). Cette caractéristique est très fortement détériorée par la présence d'autres bâtiments aux alentours. Ainsi, les éoliennes sont également exclues pour la production d'énergie pour un bâtiment.

Par contre, l'installation de panneaux photovoltaïcs (PV) semble être envisageable. Les contraintes de ce type de production ne sont pas très exigeantes. Nous pouvons imaginer que les PV soient installés sur le toit du bâtiment et ainsi capter l'énergie solaire aisément. Malgré cela, une caractéristique importante des PVs doit être prise en compte, celle de l'efficacité ou rendement de transformation en énergie électrique. Cette dernière est très faible pour des PVs, de l'ordre de 15

Nous opterons donc pour l'installation de PVs.

#### 4.2.3 Stratégies

Supposons que les 2 consommateurs doivent choisir entre l'électricité du réseau principal (Grid) et celle des PVs. Pour correspondre au dilemme du prisonnier, ces derniers ne peuvent communiquer entre eux.

Le tableau des stratégies est présenté ci-dessous :

|               |      | Utilisateur 2 | Grid    | PV |
|---------------|------|---------------|---------|----|
|               |      | Utilisateur 1 |         |    |
| Utilisateur 1 | Grid | (3 ; 3)       | (0 ; 5) |    |
|               | PV   | (5 ; 0)       | (1 ; 1) |    |

L'objectif de chaque joueur est de maximiser son gain individuel. Pour plus de simplicité, nous avons choisi des valeurs arbitraires pour les gains. On pourrait envisager de définir une fonction, qui dépendrait du prix de l'électricité et du choix de l'utilisateur, afin de définir le gain pour chaque joueur.

##### 1. Stratégie (GG)

Dans ce cas, les deux utilisateurs choisissent d'utiliser le réseau principal (EDF). Les deux joueurs ne prennent pas de risques et par conséquent optent

pour le prix le plus élevé. Cette configuration n'est pas celle qui optimise le gain individuel mais elle privilégie le gain mutuel. En effet, plus la consommation est importante, plus le prix de l'électricité proposé par EDF sera faible (ceci n'est applicable que durant les périodes où la demande n'est pas à son maximum).

### 2. Stratégie (GS) ou (SG)

L'un des deux utilisateurs utilise l'énergie solaire (PV) pour satisfaire à ces besoins électriques. Tandis que l'autre opte pour le réseau principal. Par conséquent, la prise de risque est payante dans cette configuration puisque le gain est maximal. Ceci est du au fait que le PV ne peut fournir de l'électricité à bas coût qu'à un seul utilisateur (les moyens d'investissements n'ont pas été suffisant afin de combler la demande de tous les utilisateurs). Par contre, l'autre joueur sera quant à lui dans la moins avantageuse des positions. En effet, vu que la demande d'électricité demandée au "Grid" n'est pas importante (moins importante que celle des deux consommateurs réunis), le prix va devenir très important (plus que dans la situation (G,G)).

### 3. Stratégie (SS)

Cette configuration est la plus dangereuse. Les deux consommateurs décident de consommer l'énergie solaire malgré que la production ne puisse combler aux besoins des deux. Nous pourrions imaginer que, dans ce cas, un autre système de contrôle va combler la différence en faisant appel au réseau (et ceci à un coût non négligeable). Ainsi, les deux consommateurs devront payer le coût de l'électricité venant des PVs mais également une partie supplémentaire due au réseau. Cette configuration met en relief le côté néfaste de l'utilisation commune des PVs par les deux consommateurs.

#### 4.2.4 Réalisation du jeu

Nous allons dans cette partie présenter un système qui permettrait de réaliser les stratégies quantiques [52]. Pour ce faire, les deux éléments principaux qui constituent les outils que disposerait les joueurs (utilisateurs), à savoir la porte  $\hat{J}$  et  $\hat{U}$ , seront étudiés.

##### Porte $\hat{J}$

Chaque joueur détient un qubit en sa possession.  $\psi_1$  correspond au qubit détenu par l'utilisateur 1 et  $\psi_2$  correspond au qubit détenu par l'utilisateur 2. Ces derniers sont dans l'état  $|CC\rangle$  au début du jeu. Nous utilisons l'opérateur  $\hat{J}$  afin d'obtenir un système plus ou moins intriqué (selon la valeur de  $\gamma$ ).

Cet opérateur peut être réalisé de manière concrète et expérimentale à l'aide de l'utilisation de "beam splitters" ( 4 diviseurs de faisceaux, dans le cas qui suit ils réfléchissent 50 % de la lumière) et d'un "cross Kerr medium" (Kerr).

Ce système peut être représenté de la manière suivante :

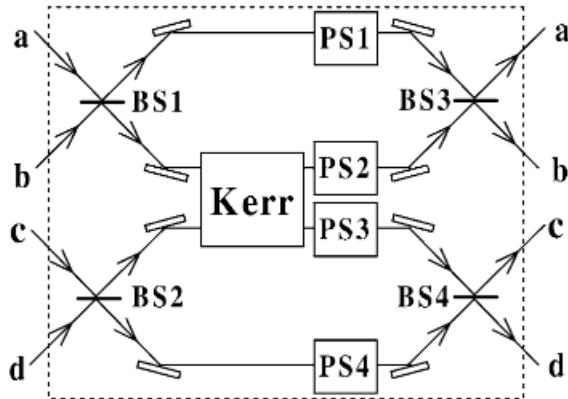


FIGURE 4.1 – Opérateur expérimental J

Sur cette figure, les "beam splitters" sont suivis de la mention BS. Kerr représente le "cross Kerr medium". Et les "phase shifter" sont nommés PS.

Les BS permettent de transformer un couple (a,b) en un couple (a',b') de la manière suivante :

$$\begin{pmatrix} a' \\ b' \end{pmatrix} = \begin{pmatrix} \cos(\frac{\theta}{2}) & -i\sin(\frac{\theta}{2}) \\ -i\sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2}) \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}$$

L'opérateur associé est nommée  $\hat{B}(\theta)$ . Si l'on applique cet opérateur aux couples (a,b) suivants, nous obtenons :

$$\begin{aligned} \hat{B}(\theta)|1\rangle_a|0\rangle_b &= \cos(\frac{\theta}{2})|1\rangle_a|0\rangle_b - i\sin(\frac{\theta}{2})|0\rangle_a|1\rangle_b \\ \hat{B}(\theta)|0\rangle_a|1\rangle_b &= \cos(\frac{\theta}{2})|0\rangle_a|1\rangle_b - i\sin(\frac{\theta}{2})|1\rangle_a|0\rangle_b \end{aligned}$$

Ainsi, si nous considérons  $|C\rangle = |1\rangle|0\rangle$  et  $|D\rangle = |0\rangle|1\rangle$ , nous obtenons :

$$\begin{aligned} \hat{B}(\theta)|C\rangle &= \cos(\frac{\theta}{2})|C\rangle - i\sin(\frac{\theta}{2})|D\rangle \\ \hat{B}(\theta)|D\rangle &= \cos(\frac{\theta}{2})|D\rangle - i\sin(\frac{\theta}{2})|C\rangle \end{aligned}$$

Les "phase shifter", quant à eux, permettent d'assurer les transformations (rotations) suivantes :

$$\begin{aligned}\hat{P}(\phi, -\phi)|C\rangle &= e^{i\phi}|C\rangle \\ \hat{P}(\phi, -\phi)|D\rangle &= e^{i\phi}|D\rangle\end{aligned}$$

Finalement, comme la figure l'indique, le système qui représente  $\hat{J}$  peut être défini comme suit :

$$\hat{J} = \hat{B}_4(-\frac{\pi}{2})\hat{B}_3(-\frac{\pi}{2})\hat{P}(\theta_2, -\theta_2)\hat{P}(\theta_1, -\theta_1)\hat{K}(\gamma)\hat{B}_2(\frac{\pi}{2})\hat{B}_1(\frac{\pi}{2})$$

### Porte $\hat{U}$

Contrairement au dilemme du prisonnier classique où l'on exprime directement sa stratégie (par exemple, à l'aide de la valeur d'un bit : 0 ou 1), la formulation quantique permet de disposer d'un qubit  $\psi$  d'action sur lequel différentes opérations sont possibles pour l'ensemble des joueurs. En effet, l'ensemble de ces opérations est défini par l'opérateur  $\hat{U}$  dont la forme est rappelée ci-dessous :

$$\hat{U}(\theta, \phi) = \begin{pmatrix} e^{i\phi} \cos(\theta/2) & \sin(\theta/2) \\ -\sin(\theta/2) & e^{-i\phi} \cos(\theta/2) \end{pmatrix}$$

avec  $0 \leq \theta \leq \pi$  et  $0 \leq \phi \leq \pi/2$

Ce système peut être représenté de la manière suivante :

Sur celle-ci, nous pouvons remarquer que les types d'éléments utilisés pour la porte  $\hat{J}$  sont également mis en place pour pouvoir assurer la fonction de l'opérateur  $\hat{U}$ , notamment les "beam splitter" (au nombre de 2) ; les miroirs (au nombre de 2) et les "phase shifter" (au nombre de 4). Cette fois-ci, ils sont disposés de manière différente.

De plus, nous pouvons associer les différents éléments afin d'obtenir le résultat souhaité pour  $\hat{U}$  :

$$\hat{U}(\theta, \phi) = \hat{P}(0, -\phi)\hat{U}_y(-\frac{\theta}{2})\hat{P}(\phi, 0)$$

Avec :

$$\hat{U}_y(\frac{\theta}{2}) = \hat{B}(\frac{\pi}{2})\hat{P}(-\frac{\theta}{2}, \frac{\theta}{2})\hat{B}(\frac{\pi}{2})$$

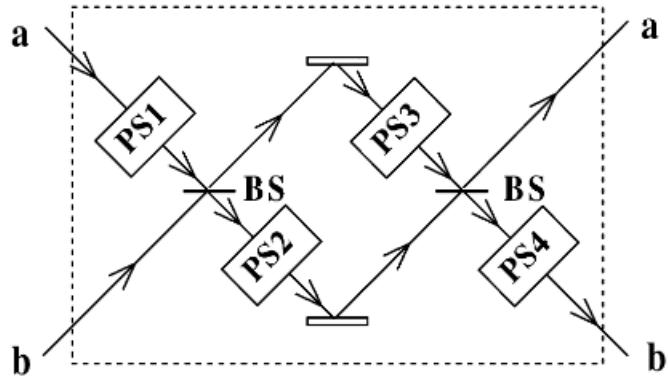


FIGURE 4.2 – Opérateur expérimental U

Ainsi, nous pouvons introduire les notions vues concernant le dilemme du prisonnier pour pouvoir résoudre certains problèmes liés à la gestion d'énergie. En effet, l'utilisation de la théorie de l'information quantique permet de résoudre le problème lié à ce jeu (contrairement à ce qui est fait classiquement) et par conséquent celui rencontré lors du scénario avec la gestion d'énergie au sein d'un bâtiment intelligent.

De plus, nous avons également pu constater que cette application quantique est envisageable au niveau technique. Elle ne requiert pas des outils très évolués mais seulement quelques éléments déjà utilisés dans le monde technologique.

### 4.3 Scénarios basés sur le CHSH et GHZ Game

Dans un environnement de production d'énergie, comme celui d'une centrale ou d'un réseau de production électrique, le problème de réponse à la demande et au besoin d'énergie est un problème récurrent et prépondérant. Diverses solutions sont donc mises en place afin de répondre convenablement à la demande, et afin d'équilibrer l'effort demandé aux diverses unités de production du réseau.

Néanmoins, ces solutions introduisent un besoin de communication important et de qualité pour pouvoir synchroniser les différentes unités de production. Dans le cas où les unités de production ne communiquent pas entre elles directement, elles doivent alors communiquer avec un opérateur central qui va réguler les productions en fonction des demandes. Voulant limiter au maximum la communication avec

cet opérateur central, c'est dans cette configuration que nous proposons quelques scénarios basés sur les jeux quantiques CHSH-Game (2 joueurs) et GHZ/W-Game (3 joueurs) en lien avec cette problématique.

### 4.3.1 Scénario à deux joueurs - CHSH-Game

Notre premier scénario prend place dans un bâtiment industriel quelconque. Ce dernier est équipé d'un système central électrique permettant de distribuer l'énergie aux différentes machines industrielles. Ce système électrique globale reçoit de l'énergie de la part de deux unités de production différentes. Ces deux unités de production fournissent déjà un certain nombre de clients, et aucun d'entre eux ne peut être consacré exclusivement à notre bâtiment. De ce fait, les deux unités de production se relayeront pour répondre aux besoins du bâtiment industriel en question. On suppose que chaque unité de production peut envoyer à chaque itération ou demande 30MW au bâtiment.

Chacune des unités de production ne possède qu'une vision restreinte du système global. En effet, deux capteurs locaux du système renseignent respectivement chaque unité sur le besoin en énergie du système global. Les capteurs associés à chaque unité de production n'observent pas la même partie du système global dans notre cas. De plus, les unités de production ne peuvent en aucun cas communiquer entre elles une fois mises en route. Chaque capteur envoie une information binaire à l'unité de production associée pour lui informer s'il y a un besoin ou non d'énergie. Il peut arriver qu'un seul capteur détecte le besoin en énergie du bâtiment, mais il peut arriver également que les deux capteurs saisissent cette information et vont donc avertir les unités de production de cela. En revanche, si un besoin existe en énergie, on est certain qu'un des 2 capteurs au minimum le détectera.

De son coté, le système global centralise l'énergie reçue de l'exterieur avant de la redistribuer à ses différents sous-systèmes internes. Le système de centralisation ne peut accepter l'énergie que d'une seule unité de production à la fois, de par son dimensionnement. La réception simultanée d'énergie de la part des deux unités entraîne une surcharge au niveau de la centralisation et peut ammener vers une déterioration du matériel. La coordination des unités de production devra donc intégrer cette contrainte pour ne pas endommager et destabiliser le système.

Si, tout de même, il arrive que les deux unités de production fournissent en même temps de l'énergie, un système dit "auxiliaire" s'assurera de protéger le système en absorbant le surplus de charge qui aurait pu causer une déterioration du matériel. Cette unité auxiliaire intervient également en cas de non réponse à la demande du système global. Il s'assurera alors de fournir l'énergie qu'une unité de

production aurait dû fournir en attendant que les unités de production reprennent convenablement leur rôle. Son comportement peut donc s'apparenter à celui d'une batterie, que l'on chargerait ou déchargerait en fonction des réponses des unités de production aux demandes renseignées par les capteurs.

C'est alors dans ce contexte que l'on propose d'introduire le CHSH-Game (voir [2.1](#) pour une définition détaillée) comme jeu quantique afin de permettre la coordination des unités de production pour répondre au mieux aux demandes, en prenant compte les contraintes énoncées ci-dessus.

L'arbitre envoyant les questions sera ici modélisé par les capteurs locaux. Chacun des capteurs enverra donc sa question au joueur auquel il est lié. Les deux joueurs seront effectivement les deux unités de production. Le système global modélisera l'arbitre qui reçoit les réponses de la part des unités de production sous la forme d'information ou d'énergie produite directement. Le système global se charge ensuite de répartir l'énergie reçue, ainsi que d'avertir éventuellement l'unité auxiliaire en cas de réponses non satisfaisantes (surcharge ou non-production). L'unité auxiliaire n'est alors pas considérée comme un joueur à part entière.

Le principal problème sera donc de trouver moyen de coordonner les unités de production pour minimiser la fréquence d'occurrence de cas indésirables (non-production ou surcharge), et ainsi solliciter au minimum l'unité auxiliaire. Une fois la stratégie trouvée, on pourra dimensionner l'unité auxiliaire convenablement. La suite de cette section s'attardera donc sur les résultats qu'offre les stratégies classique et quantiques utilisées pour résoudre le CHSH-Game.

Dans la suite de notre propos, on notera  $P_1$  et  $P_2$  les deux unités de production, on notera  $P_0$  l'unité auxiliaire. La question  $\{1\}$  de la part du capteur indique qu'il y a besoin d'énergie, la question  $\{0\}$  qu'il n'y en a pas besoin. La réponse  $\{0\}$  indique que l'unité ne produit pas, tandis que la réponse  $\{1\}$  indique que l'unité de production va produire de l'énergie.

On définit également un certain nombre de pénalités qui vont correspondre à la fréquence de cas indésirables. On définit alors une pénalité de non-production, qui se produit lorsqu'un capteur au minimum informe d'un besoin et qu'aucune des unités de production ne choisit de produire. On définit ensuite une pénalité de surcharge, lorsque les deux unités de production vont produire simultanément. On définit enfin une pénalité de surproduction lorsque les deux capteurs n'informent d'aucun besoin et que l'une des deux unités de production envoie tout de même de l'énergie. Afin d'évaluer la stratégie de manière globale, on définit une pénalité

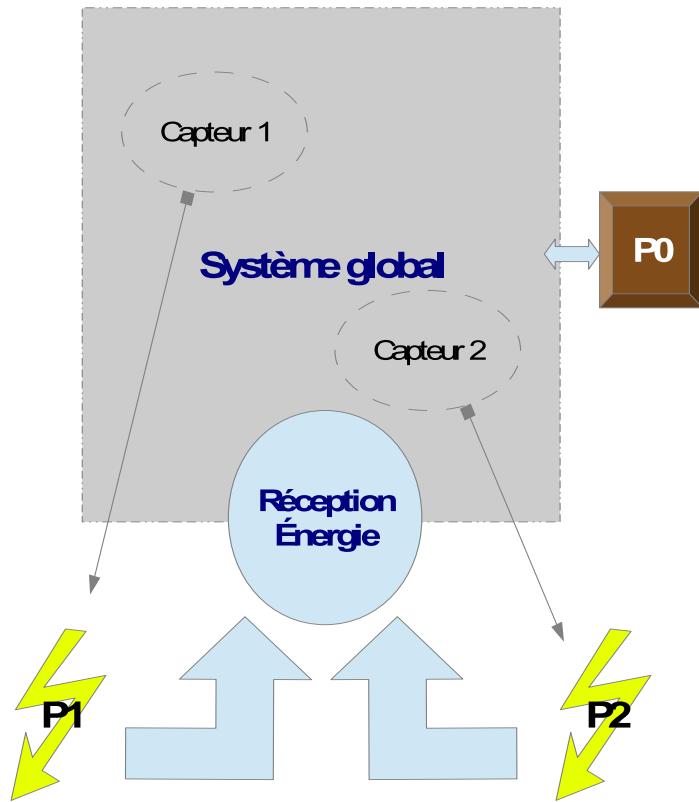


FIGURE 4.3 – Schéma explicatif du système complet

globale comme une moyenne pondérée des trois pénalités ci-dessus. On donne 2 fois plus d'importance et de gravité à la pénalité de surcharge par rapport aux deux restantes, car elle peut engendrer une déterioration du matériel. On aura alors la relation suivante :

$$penalite_{globale} = \frac{1}{2}penalite_{surcharge} + \frac{1}{4}penalite_{non-production} + \frac{1}{4}penalite_{surproduction}$$

### Meilleure stratégie classique

Dans la recherche de la meilleure stratégie permettant de minimiser les cas indésirables, que l'on appellera aussi pénalité, toutes les stratégies classiques ne sont pas acceptables. En effet, les stratégies classiques où un joueur répond la même chose soit la question ne peut être acceptable dans notre cas. En

effet, si une unité de production choisit de ne jamais produire quelque soit le besoin renseigné par son capteur, alors elle devient inutile et l'autre unité de production ne pourra pas assurer le besoin à elle toute seule, comme supposé au départ. Le cas où une unité choisit de toujours produire est également problématique dans la mesure où cela peut multiplier les risques de surcharge, de production lorsqu'il n'y en a pas besoin, et cela n'est pas possible par hypothèse de départ.

Il ne nous reste donc que les stratégies dans laquelle la réponse à une question est le complément de la réponse au complément de la question. Si l'on note  $p_1(x)$  et  $p_2(x)$  la réponse apportée par l'unité de production  $P_1$  et  $P_2$  respectivement, à la question  $x$ , alors on liste les différentes stratégies classiques restantes par ligne :

Stratégie 1 :  $p_1(0) = 0$  ,  $p_1(1) = 1$  ,  $p_2(0) = 0$  ,  $p_2(1) = 1$

Stratégie 2 :  $p_1(0) = 0$  ,  $p_1(1) = 1$  ,  $p_2(0) = 1$  ,  $p_2(1) = 0$

Stratégie 3 :  $p_1(0) = 1$  ,  $p_1(1) = 0$  ,  $p_2(0) = 0$  ,  $p_2(1) = 1$

Stratégie 4 :  $p_1(0) = 1$  ,  $p_1(1) = 0$  ,  $p_2(0) = 1$  ,  $p_2(1) = 0$

On remarque tout d'abord que le cas de surcharge est inévitable quelque soit les stratégies, et qu'il arrive dans  $\frac{1}{4}$  des cas.

On observe ensuite que la stratégie 2 amène à une production de la part de  $P_2$  alors que les deux capteurs envoient l'information  $\{00\}$ . De plus, dans le cas où le second capteur avertit d'un besoin d'énergie, les deux unités de production renverrons  $\{00\}$  ce qui nous amène dans un cas de non-production. On peut établir les mêmes remarques pour la stratégie 3.

Pour ce qui concerne la stratégie 4, elle est plus problématique dans la mesure où lorsque les deux capteurs envoient l'information  $\{00\}$ , les unités de production produisent un cas de surcharge, ce qui va obliger l'auxiliaire  $P_0$  à absorber une quantité double à celle qu'il doit absorber lorsqu'un il y a une surcharge et qu'un capteur au minimum informe d'un besoin en énergie.

On en conclut alors que la meilleure stratégie est la stratégie 1, stratégie consistant à produire lorsqu'on informe d'un besoin, et ne pas produire dans le cas contraire. On évite alors le cas de non-production, car les deux unités de produisent pas uniquement lorsque les deux capteurs leur informent d'un non besoin

d'énergie par la question  $\{00\}$ . On évite également le cas de surproduction de ce fait.

On présente alors ci-dessous, l'évolution des différentes pénalités en fonction du nombre de tours de jeu effectués. On remarque alors que la pénalité de non-production et celle de surproduction est nulle pour cette stratégie. La pénalité de surcharge est bien de 25% comme en théorie, tandis que l'on converge bien vers 12.5% pour la pénalité globale.

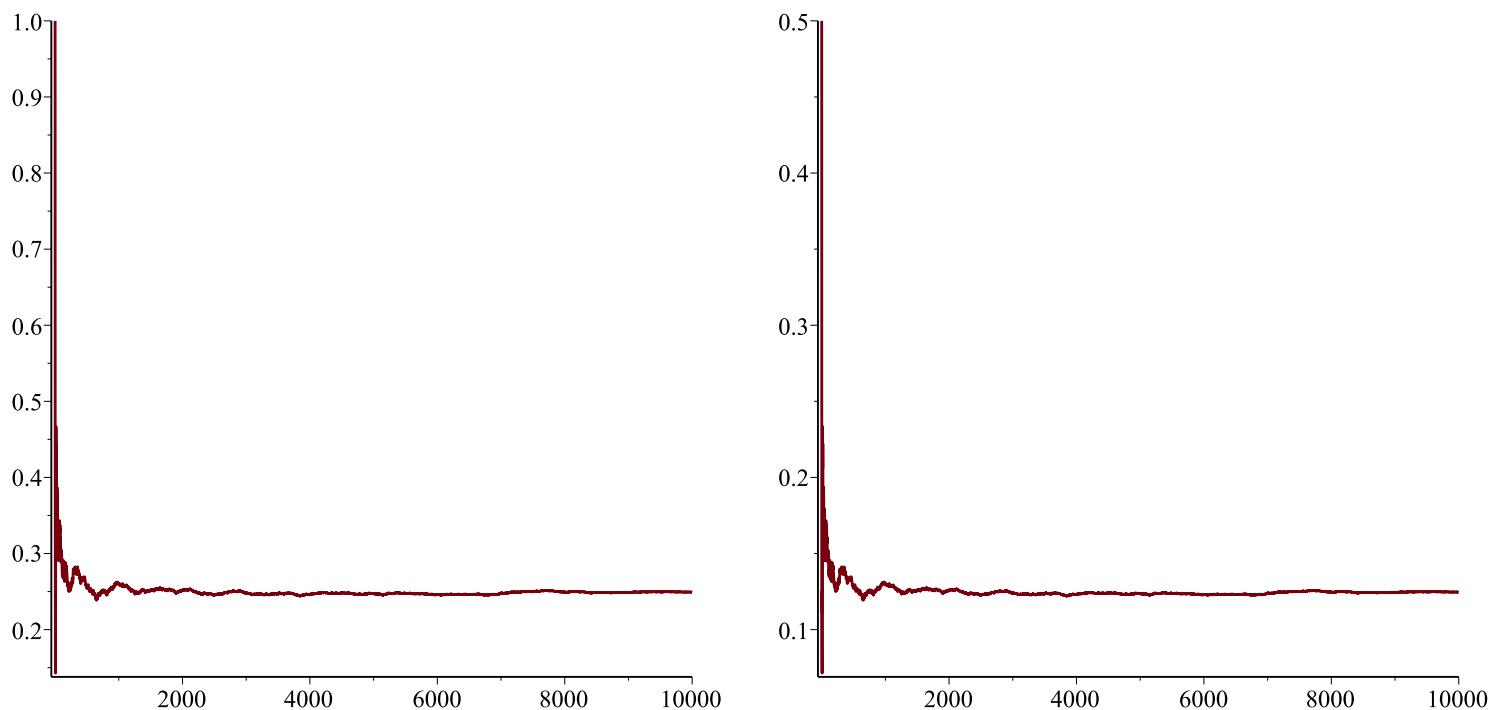


FIGURE 4.4 – Evolution de la pénalité de surcharge (gauche) et globale (droite) au fil des itérations pour la stratégie classique optimale

En ce qui concerne le comportement de l'unité auxiliaire  $P_0$ , il devient avec cette stratégie classique uniquement uni-directionnel, dans la mesure où il ne doit fournir en aucun cas de l'énergie au système, et ne fait qu'absorber l'énergie de surcharge pour préserver le système. Modéliser cette unité  $P_0$  par une batterie ne serait alors pas le meilleur choix. Une des solutions possibles est d'imaginer l'auxiliaire  $P_0$  comme un relais qui couperait le circuit avec une des unités de

production en cas de surcharge, à la place d'absorber cette énergie. Ci-dessous est représenté la sortie de l'auxiliaire  $P_0$ . Une valeur négative implique que l'auxiliaire absorbe le courant de surcharge.

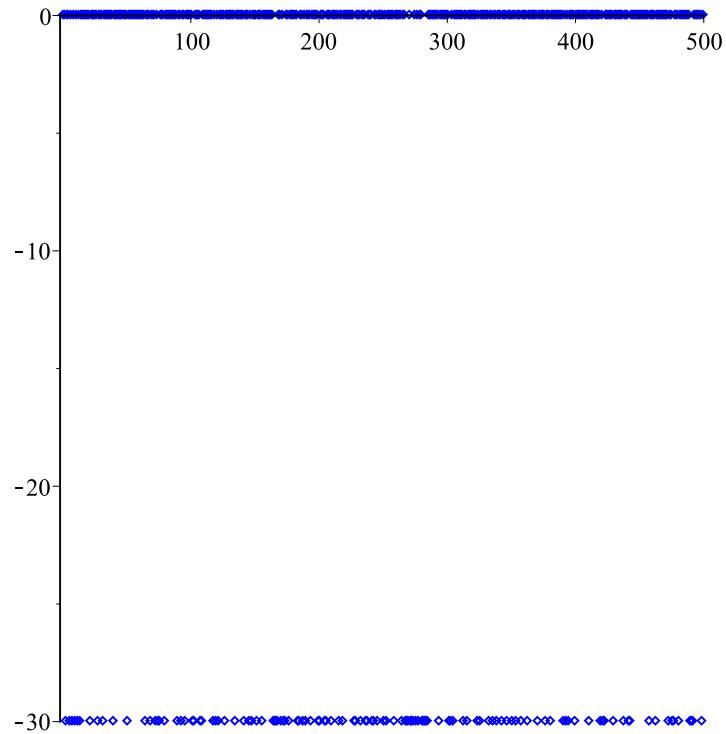


FIGURE 4.5 – Evolution de l'utilisation de l'auxiliaire  $P_0$  au fil des itérations pour la stratégie classique optimale

### Résultats de la stratégie quantique

Dans cette sous-section, on s'intéressera à la performance de la stratégie quantique du CHSH appliquée à notre problème d'allocation de ressources, en étudiant la nature des pénalités atteintes.

Dans cette stratégie, les deux unités de production vont donc partager un état de bell  $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ . L'unité  $P_1$  sera assimilée au joueur  $A$ , et l'unité  $P_2$  sera assimilée au joueur  $B$ , selon les notations posées en section 2.1. Chaque joueur va donc appliquer sa stratégie en fonction de l'information reçue par son capteur, et mesurer son qubit dans la base convenable.

Si l'on cherche à déterminer analytiquement les différentes valeurs de pénalités, il serait plus simple, vu le nombre de cas possibles, de lister les réponses possibles et leur probabilité en fonction des questions, et d'ensuite pouvoir établir de manière simple le calcul.

| Question | Réponse     | Probabilité pour une réponse         | Type de pénalité    |
|----------|-------------|--------------------------------------|---------------------|
| {00}     | {00} / {11} | $\frac{1}{4} * \frac{1}{2} * 0.8536$ | Aucune / Surcharge  |
| {00}     | {01} / {10} | $\frac{1}{4} * \frac{1}{2} * 0.1464$ | Surprod / Surprod   |
| {01}     | {01} / {10} | $\frac{1}{4} * \frac{1}{2} * 0.8536$ | Aucune / Aucune     |
| {01}     | {00} / {11} | $\frac{1}{4} * \frac{1}{2} * 0.1464$ | Nonprod / Surcharge |
| {10}     | {01} / {10} | $\frac{1}{4} * \frac{1}{2} * 0.8536$ | Aucune / Aucune     |
| {10}     | {00} / {11} | $\frac{1}{4} * \frac{1}{2} * 0.1464$ | Nonprod / Surcharge |
| {11}     | {01} / {10} | $\frac{1}{4} * \frac{1}{2} * 0.8536$ | Aucune / Aucune     |
| {11}     | {00} / {11} | $\frac{1}{4} * \frac{1}{2} * 0.1464$ | Nonprod / Surcharge |

FIGURE 4.6 – Probabilités d'occurrence de la réponse en fonction de la question, et pénalité associée

Après calcul à partir du tableau, on se rend en effet compte des différentes valeurs des pénalités théoriques :

$$surcharge = \frac{1}{8} * 0.8536 + \frac{3}{8} * 0.1464 = 0.1616$$

$$nonproduction = \frac{3}{8} * 0.1464 = 0.0549$$

$$surproduction = \frac{2}{8} * 0.1464 = 0.0366$$

$$globale = 0.5 * 0.1616 + 0.25 * 0.0549 + 0.25 * 0.0366 = 0.103675$$

En observant les résultats de la simulation, on voit en effet que les pénalités convergent vers ces valeurs. On en déduit surtout que la pénalité de surcharge est nettement inférieure pour la stratégie quantique par rapport à la stratégie classique. Les pénalités de non-production et de surproduction ne sont pas nulles,

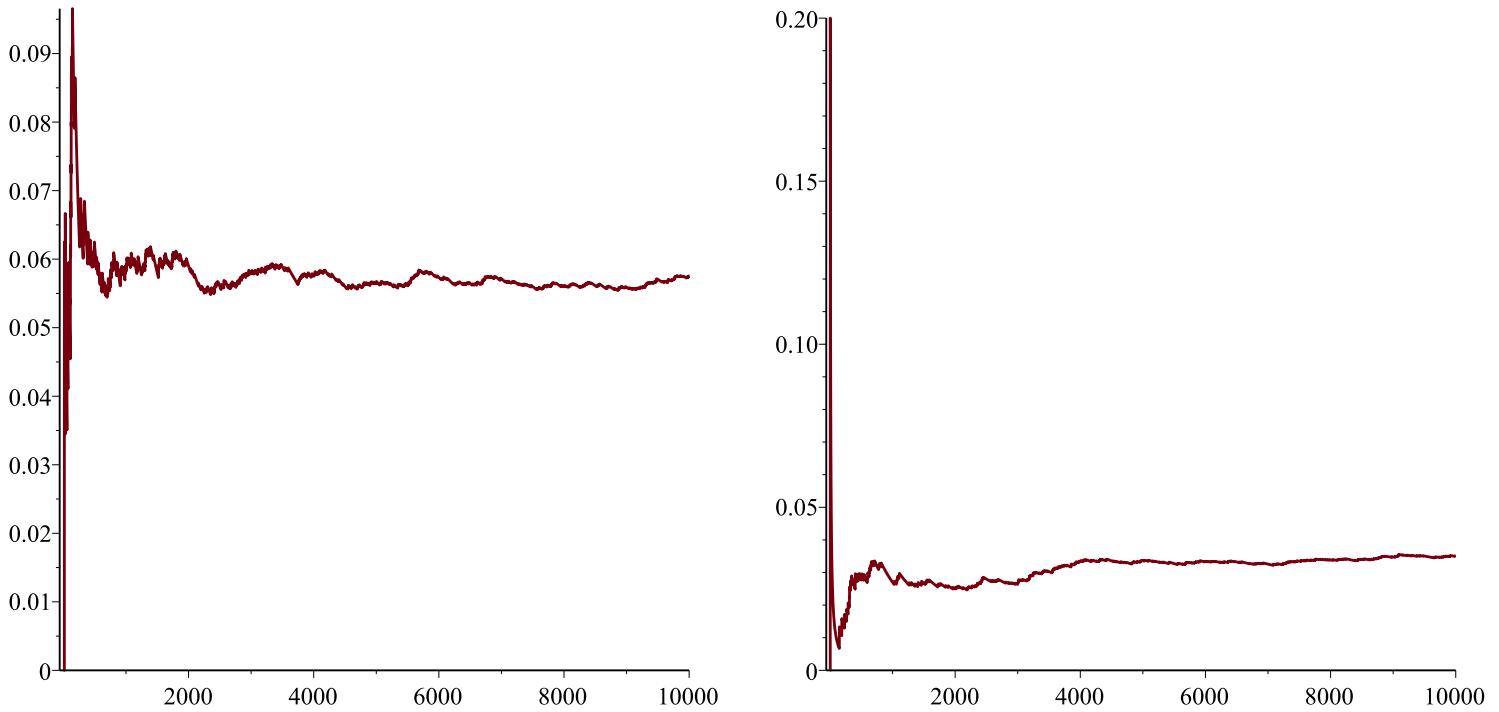


FIGURE 4.7 – Evolution de la pénalité de non-production (gauche) et de surproduction (droite) au fil des itérations pour la stratégie quantique

mais très faibles tout de même. Au final, on obtient une meilleure minimisation de la pénalité globale avec la stratégie quantique.

En ce qui concerne l'unité auxiliaire  $P_0$ , elle n'agit plus maintenant comme unité qui absorbe seulement, mais dans les cas de non-production, l'unité devra produire de l'énergie. On peut alors cette fois-ci la modéliser sous la forme d'une batterie qui se charge et décharge respectivement en cas de surcharge/surproduction et de non-production. Etant donné que les cas de surcharge et surproduction sont plus fréquents que les cas de non-production, la batterie va avoir tendance à plus se charger que de se décharger, ce qui assure bien le fait que la batterie soit chargée et opérationnelle lorsqu'il faudra fournir de l'énergie en cas de non-production des unités  $P_1$  et  $P_2$ .

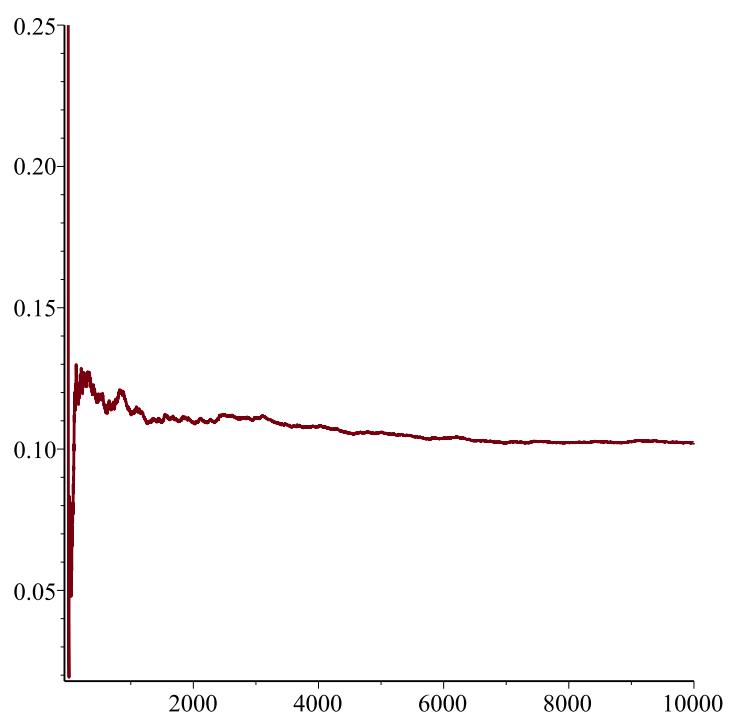
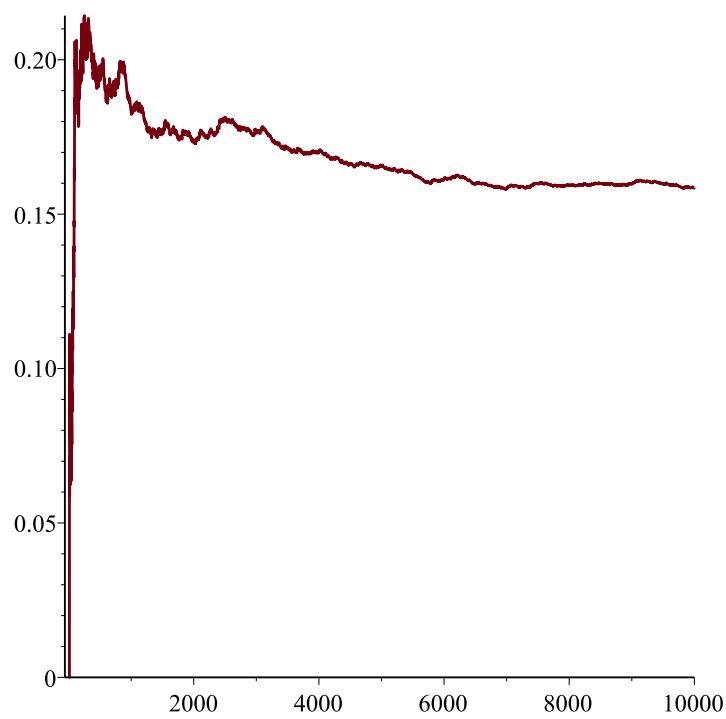


FIGURE 4.8 – Evolution de la pénalité de surcharge (gauche) et globale (droite) au fil des itérations pour la stratégie quantique

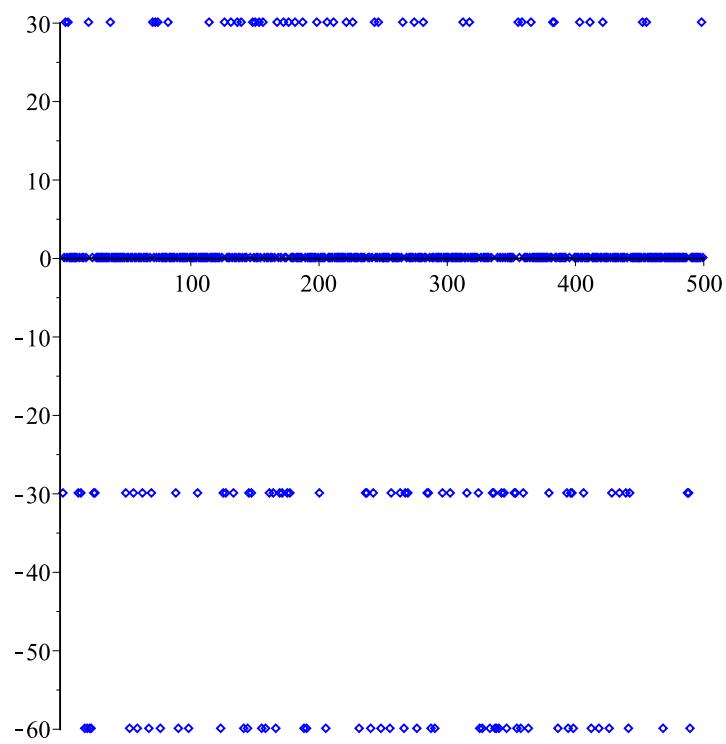


FIGURE 4.9 – Evolution de l'utilisation de l'auxiliaire  $P_0$  au fil des itérations pour la stratégie quantique

### 4.3.2 Premier scénario à 3 joueurs - GHZ-Game

Dans cette partie, nous proposons un scénario analogue à celui présenté pour 2 joueurs (4.3.1), faisant intervenir cette fois ci 3 joueurs et donc modélisé à l'aide du GHZ-Game (voir section 2.2).

Nous nous plaçons toujours dans la cadre d'une structure ou un bâtiment industriel relié à des producteurs extérieurs. Ce bâtiment est relié alors à 3 unités de productions. Les unités peuvent fournir la même puissance à notre bâtiment, mais aucune unité ne peut être consacrée aux besoins de notre bâtiment. Les 3 doivent donc être coordonnées pour répondre au mieux à la demande.

Chaque unité de production dispose toujours d'un capteur local et indépendant aux autres ayant une vision restreinte sur les besoins du bâtiment en énergie. Chaque unité ne peut, en outre, communiquer avec les autres unités de production. Il peut arriver que seul un capteur détecte le besoin en énergie du bâtiment, mais il peut arriver également que plusieurs capteurs saisissent cette information et vont donc avertir les unités de production de cela. En revanche, si un besoin existe en énergie, on est certain qu'un des 3 capteurs au minimum le détectera.

La bâtiment est toujours limité en terme de puissance recevable simultanément. Ce dernier dispose d'une unité centrale d'alimentation qui se charge de répartir l'énergie issue des trois unités aux sous-systèmes ayant un besoin. Si plus d'une, c'est à deux ou trois, unités de production produisent en même temps, l'unité centrale n'est pas dimensionnée pour cette charge, ce qui peut induire une détérioration du matériel. De la même manière que précédemment, une unité auxiliaire sera là pour absorber la puissance supplémentaire d'une ou deux unités selon le cas de figure, pour protéger la structure. Il aura également pour but de fournir de l'énergie lorsqu'aucune unité ne répondra à une demande informée par les capteurs.

On cherchera alors à coordonner les unités de production pour produire lorsque la demande est renseignée par les capteurs, ne pas produire lorsqu'il n'y a pas de besoin, et éviter de produire simultanément, ceci afin de solliciter au minimum l'unité auxiliaire noté  $P_0$ . On dénote aussi les 3 unités de production par  $P_1$ ,  $P_2$  et  $P_3$ .

On définit aussi, comme dans le cas précédents, des pénalités qui nous permettent de connaître la fréquence d'occurrence de cas indésirables (non production, surcharge, ...) et de pouvoir en déduire ensuite les répercussions sur l'auxiliaire  $P_0$ . On définit alors une pénalité de non-production qui se définit par le nombre de fois où les unités de production n'ont pas produit (réponse {000}) alors que les capteurs

ont averti d'un besoin en énergie, sur le nombre total d'itérations du protocole. On définit la pénalité de surproduction, qui intervient lorsque l'on produit alors qu'il n'y a pas de demande. La pénalité de surcharge, sûrement la plus importante, qui donne une indication sur la proportion de cas où deux ou trois unités de production envoient simultanément leur production, ce qui peut entraîner une surcharge du système. Enfin, on définit une pénalité globale, nous permettant d'avoir une appréciation globale du système, telle que :

$$globale = \frac{1}{2}surcharge + \frac{1}{4}nonproduction + \frac{1}{4}surproduction$$

On propose alors, dans ce contexte, d'utiliser le GHZ-Game pour solutionner ce problème d'allocation de ressources. L'arbitre envoyant les question sera modélisé par les 3 capteurs envoyant une information binaire de besoin d'énergie aux unités de production. Par exemple, la question {010} signifie que seulement le second capteur a détecté le besoin en énergie du système. De ce fait, les 3 joueurs, ne pouvant communiquer entre eux, seront les 3 unités de production  $P_1$ ,  $P_2$  et  $P_3$ . Par exemple, la réponse {110} signifie que les deux premières unité vont produire mais pas la troisième (cas de surcharge). Enfin, les 3 joueurs renvoient leur réponse à l'arbitre, qui sera cette fois-ci modélisé par l'unité centrale qui reçoit et redistribue l'énergie dans le système global du bâtiment. C'est l'unité centrale qui se charge en suite de solliciter l'unité auxiliaire convenablement, ce qui place ce dernier en dehors du GHZ-Game, et n'est donc pas considéré comme un joueur à part entière.

### Meilleure stratégie classique

On s'intéresse alors dans cette sous-section à la meilleure stratégie classique pouvant être mise en place par les 3 joueurs, de telle sorte à minimiser au mieux les pénalités, et principalement la pénalité globale. Toutes les stratégies ne sont pas envisageables pour les 3 joueurs, et cela est dû au contexte d'application du GHZ-Game. En effet, aucune unité de production ne peut être consacrée à notre système, cela implique qu'aucun joueur ne peut adopter la stratégie de toujours répondre {1}. De plus, chaque unité doit produire de l'énergie pour le système, donc la stratégie de toujours répondre {0}. Il ne reste alors que les 8 stratégies possibles suivantes :

Stratégie 1 :  $p_1(0) = 0$ ,  $p_1(1) = 1$ ,  $p_2(0) = 0$ ,  $p_2(1) = 1$ ,  $p_3(0) = 0$ ,  $p_3(1) = 1$

Stratégie 2 :  $p_1(0) = 0$ ,  $p_1(1) = 1$ ,  $p_2(0) = 0$ ,  $p_2(1) = 1$ ,  $p_3(0) = 1$ ,  $p_3(1) = 0$

Stratégie 3 :  $p_1(0) = 0$ ,  $p_1(1) = 1$ ,  $p_2(0) = 1$ ,  $p_2(1) = 0$ ,  $p_3(0) = 0$ ,  $p_3(1) = 1$

Stratégie 4 :  $p_1(0) = 0$ ,  $p_1(1) = 1$ ,  $p_2(0) = 1$ ,  $p_2(1) = 0$ ,  $p_3(0) = 1$ ,  $p_3(1) = 0$

Stratégie 5 :  $p_1(0) = 1$ ,  $p_1(1) = 0$ ,  $p_2(0) = 0$ ,  $p_2(1) = 1$ ,  $p_3(0) = 0$ ,  $p_3(1) = 1$

Stratégie 6 :  $p_1(0) = 1$ ,  $p_1(1) = 0$ ,  $p_2(0) = 0$ ,  $p_2(1) = 1$ ,  $p_3(0) = 1$ ,  $p_3(1) = 0$

Stratégie 7 :  $p_1(0) = 1$ ,  $p_1(1) = 0$ ,  $p_2(0) = 1$ ,  $p_2(1) = 0$ ,  $p_3(0) = 0$ ,  $p_3(1) = 1$

Stratégie 8 :  $p_1(0) = 1$ ,  $p_1(1) = 0$ ,  $p_2(0) = 1$ ,  $p_2(1) = 0$ ,  $p_3(0) = 1$ ,  $p_3(1) = 0$

On remarque tout d'abord quelque soit la stratégie, on ne peut empêcher les cas de surcharge avec cette stratégie. Pour rappel, les cas de surcharge interviennent lorsque les réponses de la part des unités de productions sont : {011}, {101}, {110} ou {111}. On a alors 50% de pénalité de surcharge quelque soit la stratégie.

La meilleure stratégie classique sera donc celle qui minimise les autres pénalités (non-production et surproduction). En effectuant une analyse comme fait dans le scénario à 2 joueurs, on en conclut que c'est la stratégie 1 qui est la meilleure. Cette stratégie consiste en effet à répondre la question envoyée par l'arbitre. Ainsi, si le capteur avertit d'un besoin, l'unité produira à chaque fois, et inversement, s'il n'y a pas de besoin averti par son capteur, alors l'unité ne produira pas. Avec cette stratégie, on annule totalement les pénalités de non-prduction et de surproduction. Ceci nous amène donc à une pénalité globale de 25%.

En ce qui concerne le comportement de l'unité auxiliaire  $P_0$ , il devient avec cette stratégie classique uniquement uni-directionnel, dans la mesure où il ne doit fournir en aucun cas de l'énergie au système, et ne fait qu'absorber l'énergie de surcharge pour préserver le système. On se retrouve alors dans la même configuration que pour 2 joueurs. L'auxiliaire  $P_0$ , étant donné qu'il ne fournit à aucun moment de

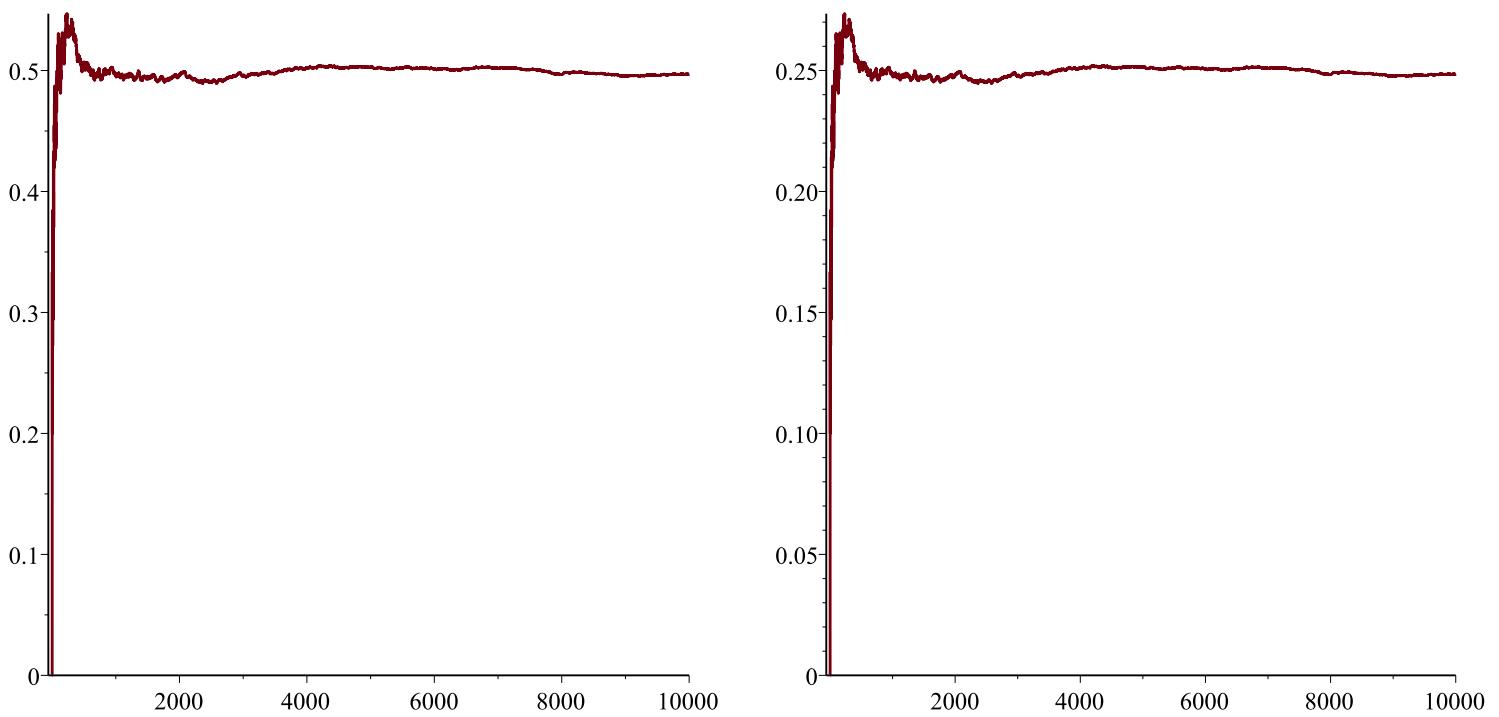


FIGURE 4.10 – Evolution de la pénalité de surcharge (gauche) et globale (droite) au fil des itérations pour la stratégie classique optimale

l'énergie, doit être modélisé par système qui ne se contenterait que d'absorber et d'utiliser autrement cette énergie pour ne pas la perdre. On pourra alors imaginer relier cet auxiliaire vers un autre système demandant de l'énergie, rendant alors  $P_0$  comme un redirigeur de surplus de production.

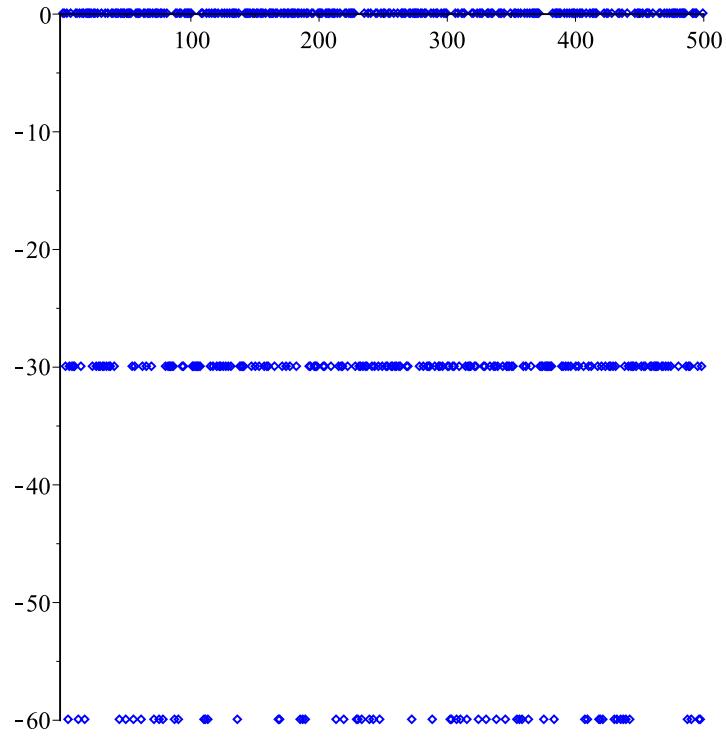


FIGURE 4.11 – Evolution de l'utilisation de l'auxiliaire  $P_0$  au fil des itérations pour la stratégie classique optimale

### Stratégie quantique du GHZ-Game

Dans cette sous-section, on s'intéressera à la performance de la stratégie quantique du GHZ appliquée à notre problème d'allocation de ressources, en étudiant la nature des pénalités atteintes.

Dans cette stratégie, les trois unités de production vont donc partager un état  $|\psi\rangle$  :

$$|\psi\rangle = \frac{1}{2}(|000\rangle - |011\rangle - |101\rangle - |110\rangle)$$

L'unité  $P_1$  sera assimilée au joueur  $A$ , l'unité  $P_2$  sera assimilée au joueur  $B$ , et l'unité  $P_3$  sera assimilée au joueur  $C$  selon les notations posées en section 2.2. Chaque joueur va donc appliquer sa stratégie en fonction de l'information reçue par son capteur, et mesurer son qubit dans la base convenable.

Si l'on cherche à déterminer analytiquement les différentes valeurs de pénalités, on peut utiliser le même raisonnement que celui mené pour le scénario à 2 joueurs. Après études des cas, en fonction de la question et de la réponse, et calcul des probabilités, on obtient alors les valeurs suivantes :

$$\begin{aligned}
 \text{nonproduction} &= 4 * \frac{1}{8} * \frac{1}{8} = \frac{1}{16} = 0.0625 \\
 \text{surcharge} &= 6 * \frac{1}{8} * \frac{1}{4} + 16 * \frac{1}{8} * \frac{1}{8} = \frac{7}{16} = 0.4375 \\
 \text{surproduction} &= 0 \\
 \text{globale} &= \frac{7}{32} + \frac{1}{64} + 0 = \frac{15}{64} = 0.234375
 \end{aligned}$$

On remarque alors que la probabilité de non-production est supérieure à celle que l'on obtient avec une stratégie classique, mais que cela reste assez faible. Pour le cas de suproduction, il n'intervient dans aucun des deux cas. Cependant, nous avons une légère amélioration de la pénalité de surcharge, qui était de 0.5 pour le cas classique. Ceci nous amène alors à une amélioration de la pénalité globale associée à la stratégie quantique.

Enfin, en ce qui concerne l'unité auxiliaire  $P_0$ , elle peut être modélisée sous la forme d'une batterie qui se charge et décharge respectivement en cas de surcharge et de non-production. Etant donné que les cas de surcharge sont plus fréquents que les cas de non-production, la batterie va avoir tendance à plus se charger que se décharger. Ce désavantage assure cependant que la batterie soit chargée et opérationnelle lorsqu'il faudra fournir de l'énergie en cas de non-production des unités  $P_1$ ,  $P_2$  et  $P_3$ .

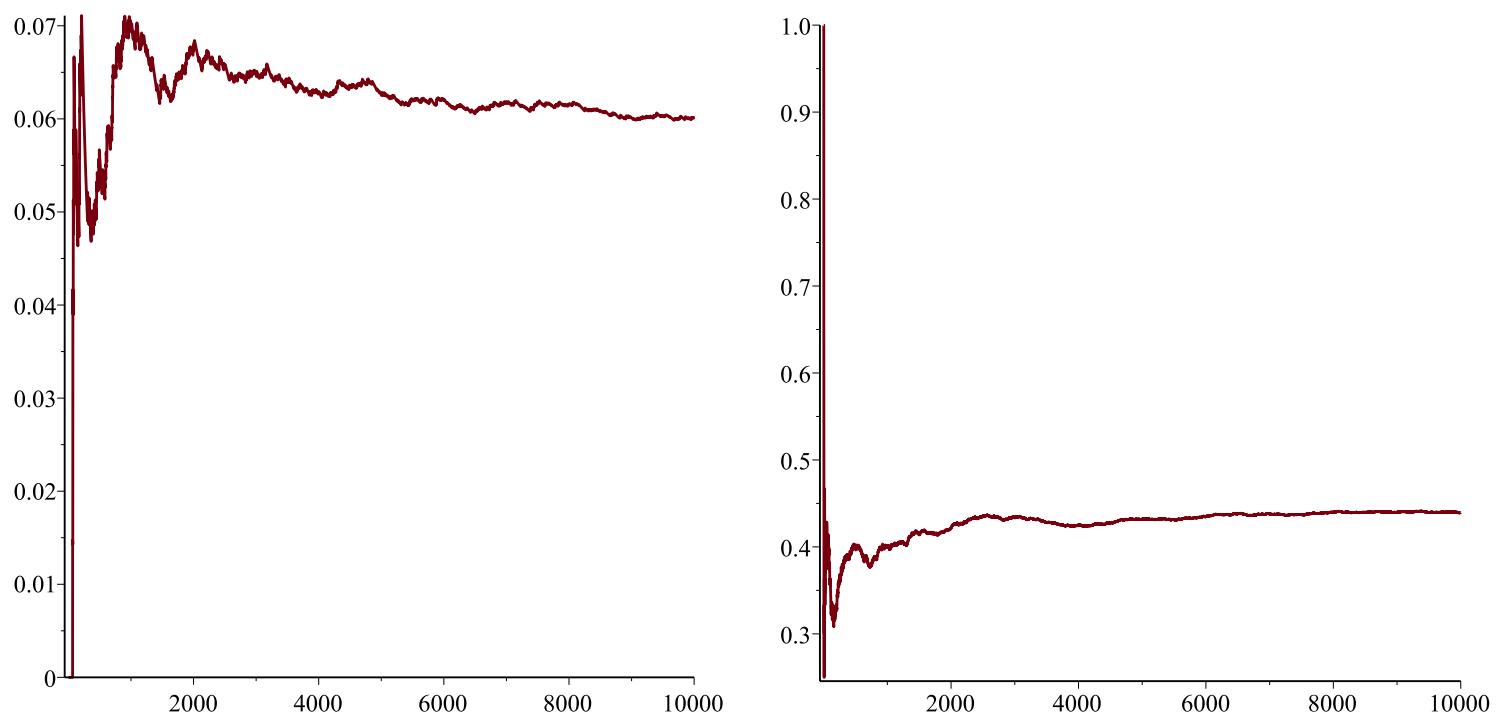


FIGURE 4.12 – Evolution de la pénalité de non-production (gauche) et de surcharge (droite) au fil des itérations pour la stratégie quantique

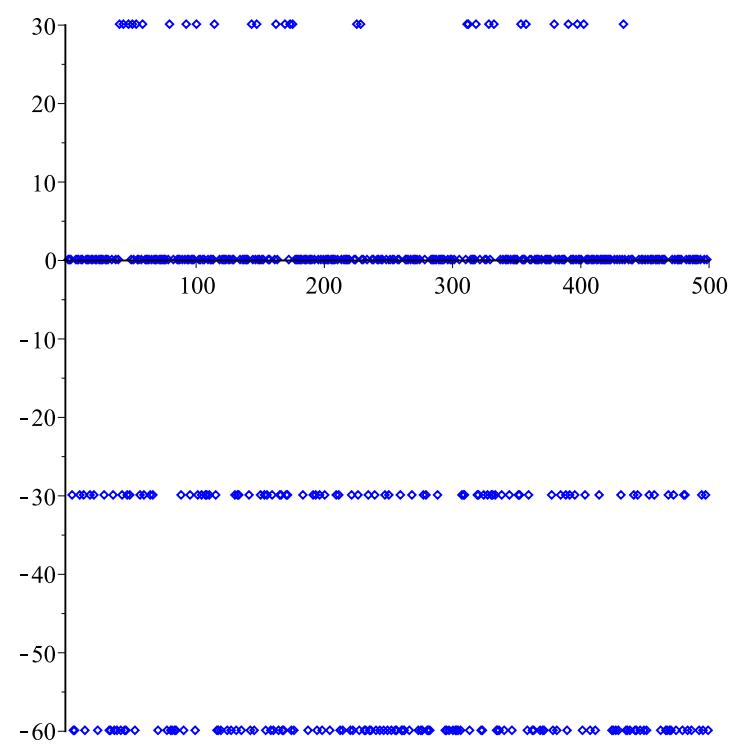
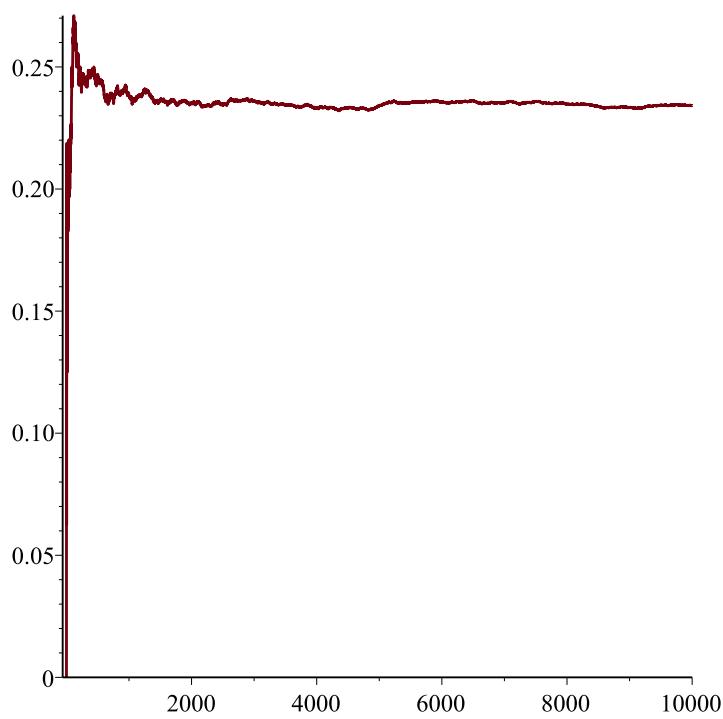


FIGURE 4.13 – Evolution de la pénalité de globale (gauche) et de l'utilisation de l'auxiliaire  $P_0$  au fil des itérations pour la stratégie quantique

### 4.3.3 Second scénario à 3 joueurs - W-Game

Pour ce dernier scénario, nous nous placerons dans l'habitation d'un particulier. Celui-ci a fait le choix d'être un peu plus autonome que les autres consommateurs, et de disposer de sources d'énergie alternatives. Ainsi, il va disposer de trois sources d'énergie au total : le réseau électrique national (Grid), une association de panneaux photovoltaïques (PPV), et une mini-éolienne (EOL).

Le consommateur désire installer un système qui va gérer les trois sources, et les faire participer à tour de rôle pour exploiter l'énergie de chacun, et ne pas user d'une source en particulier. De plus, on doit pouvoir gérer la disponibilité de chaque source, notamment des énergies renouvelables.

Le système que nous proposons réagira comme suit. A chaque tour, au maximum 2 sources seront choisies par le système. En effet, s'il y a du vent et du soleil, on choisira alors les deux sources PPV et EOL, ce qui nous permet de ne pas payer et utiliser le Grid. S'il n'y a pas de vent et du soleil, on utilisera les sources PPV et Grid. S'il n'y a pas de soleil mais du vent, on utilisera les sources EOL et Grid. S'il n'y a ni vent, ni soleil, on n'utilisera que le Grid. Ce dernier cas nous intéressera moins dans la mesure où c'est le cas qui concerne la majorité des consommateurs en France.

Ainsi, si l'on retient les 3 premières possibilités, le système choisira à chaque fois 2 sources parmi 3. C'est dans ce contexte que l'idée d'associer ce système de régulation de production au W-Game prend tout son sens. En effet, dans le W-Game, l'arbitre choisit aléatoirement 2 joueurs parmi 3 pour jouer au CHSH Game en fin de compte. Dans notre cas, c'est le système d'alimentation de l'habitation qui va choisir 2 sources parmi 3. La présence de vent et/ou de soleil peut être vue comme aléatoire dans un sens, ce qui rapproche le fonctionnement du système et du W-Game.

Les 3 sources vont donc partager un état quantique de type  $|W\rangle$ , et l'un des joueurs sera mi de côté en fonction de l'état météorologique. Ensuite, on pourra définir les conditions de gain afin de satisfaire au mieux les besoins en utilisation des batteries associées aux énergies renouvelables, et ceci doit être ensuite traduit par l'utilisation de stratégies quantiques permettant de tendre vers des meilleurs résultats. Ainsi, si l'on change la condition de gain, la stratégie quantique du CHSH-Game ne serait

## 4.4 Scénario basé sur le Minority Game

Un autre scénario que nous présentons dans cette section, permettant de mettre en application les résultats de jeux quantiques, est un scénario basé sur le Minority Game (voir section 2.5). Le problème prend toujours place dans un contexte d'optimisation de l'allocation des ressources en fonction des unités de production et des unités consommatrices.

Prenons place alors dans un bâtiment abritant 4 entreprises. Chaque entreprise possède un étage du bâtiment, et chaque étage est isolé énergétiquement des autres : l'énergie demandée et reçue est donc propre à chaque entreprise. On dénote par  $E_1$ ,  $E_2$ ,  $E_3$  et  $E_4$  les quatres entreprises, qui constituent les consommateurs.

Du côté producteur, on dispose de deux sources : le réseau électrique et une association d'un certain nombre de panneaux photovoltaïques. On notera alors par *Grid* et *PPV*, respectivement, les deux sources citées à l'instant. On considère également que la source *PPV* est plus avantageuse par rapport au *Grid*, de par le prix principalement, et que donc les entreprises vont tenter d'en bénéficier au maximum à la place du *Grid*. Enfin, la source *PPV* n'est dimensionnée que pour répondre aux besoins d'une seule entreprise.

L'utilisation du Minority Game pour cette situation intervient dans la mesure où toutes les entreprises vont vouloir utiliser la source *PPV* en priorité. On propose alors une stratégie quantique basée sur la version quantique du Minority Game à 4 joueurs (voir section 2.5.4) permettant de gérer l'attribution de l'énergie solaire aux différentes entreprises.

Tout d'abord, les 4 entreprises vont partager un état quantique intriqué afin de pouvoir appliquer la stratégie quantique. Chaque entreprise possède donc un qubit de l'état  $|\psi\rangle$  défini par :

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left( |0_{E_1} 0_{E_2} 0_{E_3} 0_{E_4}\rangle + i |1_{E_1} 1_{E_2} 1_{E_3} 1_{E_4}\rangle \right)$$

A chaque tour du jeu, sachant que chaque tour est indépendant des autres, l'entreprise qui désire jouer au jeu, et donc qui veut pouvoir bénéficier de la source *PPV*, va appliquer une stratégie quantique (une opération unitaire) sur son qubit, puis le mesurer et l'envoyer directement au système gérant la source d'énergie solaire. Aussi l'entreprise qui choisit de ne pas "tenter sa chance" avec la source *PPV* et choisit le *Grid* ne va pas agir sur son qubit et ne va pas le mesurer ni l'envoyer au système gérant le *PPV* : son comportement peut s'apparenter à uniquement appliquer l'identité sur son qubit.

La stratégie quantique optimale pour 4 joueurs, comme présenté en section [2.5.4](#), est notée  $a$  et est définie par :

$$a = \frac{1}{\sqrt{2}} \cos\left(\frac{\pi}{16}\right)(I + iX) + \frac{1}{\sqrt{2}} \sin\left(\frac{\pi}{16}\right)(iY - iZ)$$

Le système gérant l'attribution de l'énergie solaire reçoit alors les valeurs mesurées pour chaque joueur et va donc délivrer l'énergie solaire au joueur minoritaire.

Si les 4 entreprises choisissent de participer au jeu, l'énergie sera donc délivrée à la seule entreprise minoritaire. Si toutes les entreprises répondent toutes la même réponse, ou si deux entreprises répondent  $\{0\}$  et deux autres répondent  $\{1\}$ , alors aucune des entreprises ne recevra de l'énergie du PPV.

Si 3 entreprises choisissent de participer au jeu, l'énergie sera donc délivrée à la seule entreprise minoritaire. Si les 3 entreprises répondent toutes la même réponse, alors aucune de ces 3 trois entreprises ne recevra d'énergie solaire.

Si seulement 2 entreprises choisissent de participer au jeu, alors le système solaire délivrera de l'énergie à l'entreprise qui aura envoyé  $\{1\}$  alors que l'autre a envoyé  $\{0\}$ . On peut supposer que les entreprises ne connaissent pas le protocole de décision du système PPV lorsque deux joueurs jouent. De même, si les 2 entreprises répondent la même réponse, alors aucune de ces 2 entreprises ne recevra d'énergie solaire.

Dans le cas où les 4 entreprises jouent, comme détaillé en section [2.5.4](#), si les 4 entreprises jouent la stratégie quantique  $a$ , alors chaque entreprise a 25% de chances d'obtenir de l'énergie de la part des panneaux photovoltaïques. Cette stratégie quantique permet une efficacité et une équité entre les entreprises, et on ne peut faire mieux avec une stratégie classique (12.5% en classique).

Si l'on se place dans le cas où une entreprise choisit dès le départ d'utiliser le Grid, c'est à dire que 3 entreprises vont jouer au Minority Game pour la source PPV, c'est alors un nouveau cas de figure non étudié dans la partie théorique de présentation du jeu. En effet, les 4 joueurs partageront toujours l'état intriqué  $|\psi\rangle$ , même si un des joueurs ne participe pas. Cependant, le qubit du joueur qui ne joue pas ne sera ni modifié, ni mesuré. Les trois autres joueurs vont alors appliquer leur stratégie quantique car ils ont décidé de jouer. Si l'on suppose que c'est la première entreprise qui ne joue pas, alors on obtient alors l'état final  $|\psi_3\rangle$  après application des stratégies, tel que :

$$|\psi_3\rangle = I \otimes a \otimes a \otimes a |\psi\rangle = \frac{1}{\sqrt{2}} \left( |0\rangle (a|0\rangle)(a|0\rangle)(a|0\rangle) + i|1\rangle (a|1\rangle)(a|1\rangle)(a|1\rangle) \right)$$

Or, en utilisant l'expression de  $a$ , on peut établir que :

$$a|0\rangle = \frac{1}{\sqrt{2}} \left[ \left( \cos \left( \frac{\pi}{16} \right) - i \sin \left( \frac{\pi}{16} \right) \right) |0\rangle + \left( \sin \left( \frac{\pi}{16} \right) + i \cos \left( \frac{\pi}{16} \right) \right) |1\rangle \right]$$

$$a|1\rangle = \frac{1}{\sqrt{2}} \left[ \left( \sin \left( \frac{\pi}{16} \right) + i \cos \left( \frac{\pi}{16} \right) \right) |0\rangle + \left( \cos \left( \frac{\pi}{16} \right) + i \sin \left( \frac{\pi}{16} \right) \right) |1\rangle \right]$$

En injectant ces résultats dans l'expression de  $|\psi_3\rangle$ , on obtient alors un état équivalent à :

$$|\psi_3\rangle \sim \frac{1}{4} \left( |0000\rangle + |0001\rangle + |0010\rangle + |0011\rangle + |0100\rangle + |0101\rangle + |0110\rangle + |0111\rangle + |1100\rangle + |1101\rangle + |1110\rangle + |1111\rangle + |1000\rangle + |1001\rangle + |1010\rangle + |1011\rangle \right)$$

Les trois joueurs  $E_2$ ,  $E_3$  et  $E_4$  vont donc mesurer leur qubit et l'envoyer au PPV. Ainsi, le premier qubit n'est pas à considérer dans l'état global partagé par les 4 joueurs lors de la mesure, mais seulement les 3 derniers. Le lecteur pourra alors remarquer que chaque joueur dispose de la même probabilité de gain qui est de  $\frac{4}{16} = \frac{1}{4} = 25\%$ , qui est alors la même que celle obtenue lorsque 4 joueurs choisissent de jouer pour la source PPV.

Si l'on se place maintenant dans le cas où 2 entreprises vont jouer au Minority Game pour la source PPV, c'est aussi un nouveau cas de figure non étudié dans la partie théorique de présentation du jeu. Comme précédemment, les 4 joueurs partageront toujours l'état intriqué  $|\psi\rangle$ . Si l'on suppose que ce sont les deux premières entreprises qui ne jouent pas, alors on obtient alors l'état final  $|\psi_2\rangle$  après application des stratégies, tel que :

$$|\psi_2\rangle = I \otimes I \otimes a \otimes a |\psi\rangle = \frac{1}{\sqrt{2}} \left( |00\rangle (a|0\rangle)(a|0\rangle) + i|11\rangle (a|1\rangle)(a|1\rangle) \right)$$

On remplace alors l'expression de  $a|0\rangle$  et de  $a|1\rangle$  dans l'équation ci-dessus ce qui nous donne un état équivalent à :

$$|\psi_2\rangle \sim \frac{1}{\sqrt{8}} \left( |0000\rangle + |0001\rangle + |0010\rangle + |0011\rangle + |1100\rangle + |1101\rangle + |1110\rangle + |1111\rangle \right)$$

Les trois joueurs  $E_2$ ,  $E_3$  et  $E_4$  vont donc mesurer leur qubit et l'envoyer au PPV. Ainsi, les deux premiers qubits ne sont pas à considérer dans l'état global partagé par les 4 joueurs lors de la mesure, mais seulement les 2 derniers. On rappelle que pour 2 joueurs, c'est le joueur qui envoie 1 alors l'autre a envoyé 0 qui est considéré comme gagnant par le système d'attribution du PPV. On pourra alors vérifier que chaque joueur dispose de la même probabilité de gain qui est de  $\frac{2}{8} = \frac{1}{4} = 25\%$ , qui est alors la même que celle obtenue lorsque 4 ou 3 joueurs choisissent de jouer pour la source PPV.

Ainsi, la source énergétique que constitue cette association de panneaux solaires pourra grâce à ce "protocole" répartir l'énergie équitablement entre les étages demandant de l'énergie. En recevant les mesures de la part des joueurs engagés dans la partie à un tour donné, il saura combien de il y a joueurs, qui ils sont, comment déterminer s'il y a une minorité ou non, et qui est le minotaire. L'avantage d'introduire une stratégie quantique permet aux joueurs d'atteindre des probabilités de gain supérieures à une stratégie classique basique. L'intrication joue encore une fois un rôle prépondérant dans ce processus. On supprime également la nécessité de disposer d'une unité centralisant toutes les demandes des clients, puis communiquant avec la source PPV, puis ensuite seulement attribuant arbitrairement ou aléatoirement (jet de dés par exemple) l'énergie à une entreprise.

# Conclusion

## Synthèse des résultats

A la fin du projet, nous sommes arrivé à un résultat satisfaisant, que l'on peut étudier en deux temps.

Tout d'abord, et c'est ce qui fait l'objet de la première partie du rapport, nous avons pu introduire un certain nombre de protocoles de communication quantique, et établir un état de l'art assez fourni et détaillé des jeux quantiques les plus répandus.

Dans la seconde partie, nous avons pu saisir les enjeux du futur de l'énergie en terme de communication dans les Smart Grid notamment, et concernant le problème d'allocation de ressources et de sécurité. Nous avons pu à ce titre proposer 5 scénarios différents mettant en scène un système énergétique et un jeu quantique permettant de modéliser et de proposer une résolution quantique du problème.

Enfin, certaines pistes proposée au cours du projet n'ont pas pu être développées par manque de temps et de moyens matériels. Nous les présentons alors dans la dernière sous-section 4.4 du rapport, afin de garder une trace écrite de ces idées, et de pouvoir les développer par la suite, par nous même, ou permettre à d'autres scientifiques de s'approprier ces idées.

## Bilans personnels

### Bilan personnel - Hamza

C'est un projet qui fut intéressant pour moi sous divers aspect. Il me permit de découvrir de nouveaux jeux quantiques, et donc d'agrandir notre culture dans ce domaine. Cela pourrait nous donner des idées et des perspectives pour des travaux de recherches futurs, dans ce domaine ou dans un autre. Le projet me permit également de lier cette discipline, qu'est la théorie de l'information quantique, à

une application et un cas concert d'implémentation. J'ai également pu apprendre à travailler des collègues d'autres spécialités, et à m'exprimer de manière claire pour établir une connexion entre les disciplines. Enfin, cela m'a aussi permis de développer mes connaissances dans le domaine de l'énergie et de la physique quantique.

## Bilan personnel - Ismaël

Ce projet s'est révélé très enrichissant dans la mesure où il nous a permis d'avoir une approche concrète de notre futur métier d'ingénieur. En effet, le respect des délais, la prise d'initiative et le travail en équipe seront des aspects essentiels de notre futur métier. Au terme de ce projet, nous avons acquis de nombreuses connaissances ou compétences nouvelles concernant la théorie des jeux ainsi que sur les principes de gestion d'énergie. Nous avons pu enrichir nos connaissances sur le principe des réseaux électriques actuels et futurs. Ce projet, qui allie des compétences informatiques et énergétiques, nous a également permis de faire "réellement" de la recherche pure. En effet, le sujet était, dès le départ, très ambitieux et mais nous avons pu constater par la suite qu'il n'était pas sans utilité. Les recherches scientifiques s'accentuent énormément sur ce nouveau type d'application.

## Poursuite et ouvertures

L'un des sujets le plus intéressants que nous n'avons pas eu le temps de développer, est de trouver une alternative à la communication bas débit implantée présentée dans l'article [53] de Mr. Fei Gao entre autres, qui nous a rencontré pour nous faire part de cette problématique. L'idée était de remplacer cette communication par une communication quantique.

D'autre part, nous aurions aimé pousser plus loin l'étude des multiplexeurs quantiques, et de voir si une application au monde de l'énergie ne serait pas possible, notamment à des fins de communication où d'implémentations dans des systèmes électroniques.

Un sujet moins en rapport avec l'énergie mais qui nous intéresse, et de pouvoir développer un protocole de Superdense Coding pour les qutrits, et d'éventuellement voir l'influence du type d'intrication partagé sur les performances du Superdense coding.

Enfin, on pourrait imaginer une application concrète du protocole quantique de téléportation ou de sécurité (BB84 - B92) à des fins de sécurisation des données

par exemple. Une idée aussi survenue en fin de projet est d'envisager d'utiliser les algorithmes de Grover et de Deutsch-Jozsa pour optimiser les temps de calculs liés au algorithmes gérant le domaine énergétique.

Nous espérons que nos travaux serviront d'inspiration aux chercheurs, ingénieurs et techniciens afin d'implémenter, repenser, améliorer et déduire de nouvelles technologies et systèmes qui faciliteraient la vie de l'être humain sur notre Terre.

# Bibliographie

- [1] Zimmermann, M. (2014). Towards a Covariant Classification of Nilpotent Four-Qubit States. Imperial College London.
- [2] Borsten, L. (2013). Freudenthal ranks : GHZ vs. W. Version 2. Journal of Physics A : Mathematical and Theoretical 46.45 , p. 455303.
- [3] Clauser J.F., Horne M.A., Shimony A., Holt R.A. An Experiment to Test Local Hidden-Variable Theories. Physical Review Letters 23 (15 1969), pp. 880–884.
- [4] Clauser, F. ; Horne, M. A. ; Shimony, A. ; Holt, R. A. Proposed Experiment to Test Local Hidden-Variable Theories, Physical Review Letters, volume 23, pages 880-884, 1969.
- [5] Bojic, A. (2013). A New Quantum Game Based on CHSH Game. JIOS, VOL. 37, NO. 1. UDC 004.832 :519.83.
- [6] Mermin, N. D. (1990). Simple unified form for the major no-hidden-variables theorems. Phys. Rev.Lett., 65(27) :3373–3376.
- [7] Mermin, N. D. (1993). Hidden variables and the two theorems of John Bell. Rev. Mod. Phys., 65(3) :803–815, 1993.
- [8] Cleve R., Mittal R. (2013). Characterization of Binary Constraint System Games. arXiv :1209.2729v3.
- [9] Weber, N. (P2016). Fondements de la mécanique quantique et paradoxes. UTBM, AC20.
- [10] Kumar, N. (Y9378). Quantum Non-Local Games. Indian Institute of Technology, Kanpur.
- [11] Budai Lucas, Jaffali Hamza, Nounouh Ismaël. (P2014) Principes fondamentaux de l'information quantique. UTBM, AC20.
- [12] B. A. Huberman, T. Hogg. (1988). "The Ecology of Computation", Studies in Computer Science and Artificial Intelligence, North Holland publisher, page 99.
- [13] Simon C. Benjamin, Patrick M. Hayden. (2001). Multi-Player Quantum Games. Centre for Quantum Computation, Clarendon Laboratory, University of Oxford, OX1 3PU, UK.

- [14] Qing Chen, Yi Wang, Jin-Tao Liu, Ke-Lin Wang. (2004). N-player quantum minority game. University of Science and Technology of China. Physics Letters A 327 (2004) 98–102. Elsevier.
- [15] Adrian P. Flitney, Lloyd C. L. Hollenberg. Multiplayer Quantum Minority Game With Decoherence. Centre for Quantum Computer Technology, School of Physics, University of Melbourne Parkville, VIC 3010, Australia. Quantum Information and Computation, Vol. 0, No. 0 (2005) 000–000.
- [16] Adrian P. Flitney, Andrew D. Greentree. (2008). Coalitions in the quantum Minority game : classical cheats and quantum bullies. Elsevier Science.
- [17] M. Ramzan, M. K. Khan. (2013). Environment-assisted quantum Minority games. Department of Physics Quaid-i-Azam University Islamabad 45320, Pakistan. arXiv :1102.5056v2
- [18] Janez Lev Kocevar, Rudolf Podgornik, Sašo Polanec. (2010). Seminar Minority Game. University of Ljubljana.
- [19] Jona Linde, Joep Sonnemans, Jan Tuinstra. (2014). Strategies and evolution in the minority game : A multi-round strategy experiment. Games and Economic Behavior, Elsevier.
- [20] R. Vilela Mendes. (2002). Quantum games and social norms : The quantum ultimatum game. arXiv :quant-ph/0208167v1
- [21] Piotr Frackiewicz, Jan Sladkowski. (2013). Quantum Information Approach to the Ultimatum Game. Int J Theor Phys DOI 10.1007/s10773-013-1633-0
- [22] R. Vilela Mendes. (2004). The Quantum Ultimatum Game. Quantum Information Processing, Vol. 4, No. 1, February 2005.
- [23] Ismael Martínez-Martínez. (2014). A connection between quantum decision theory and quantum games : The Hamiltonian of Strategic Interaction. Journal of Mathematical Psychology 58 (2014) 33–44, Elsevier.
- [24] Charles V. Benton. Mathematical Physics Research at the Cutting Edge. p261-262.
- [25] Andrei Y. Khrennikov. Ubiquitous Quantum Structure : From Psychology to Finance. p166-122.
- [26] Andrey Grib, Georges Parfionov. (2002). Can the game be quantum ? Alexandre Friedmann Laboratory of Theoretical Physics, St.Petersburg University of Economics and Finances. arXiv :quant-ph/0206178v1
- [27] Edward W. Piotrowski, Jan Sladkowski. (2002). An invitation to Quantum Game Theory. arXiv :quant-ph/0211191v1
- [28] Andrey Grib, Georges Parfionov. Macroscopic quantum game. quant-ph/0211068.

- [29] A.A.Grib, A.Yu.Khrennikov, K.Starkov. (2003). Probability amplitude in quantum like games. arXiv :quant-ph/0308074v1
- [30] Edward W. Piotrowski, Jan Sladkowski. Quantum Bargaining Games. *Physica A* 308 (2002) 391.
- [31] J. Harsanyi, R. Selten. A generalized Nash solution for two-person bargaining games with incomplete information, *Management Science* 14 (1972) P80–P106.
- [32] Philip Vos Fellman, Jonathan Vos Post. Quantum Nash Equilibria and the Nash Bargaining Problem.
- [33] A.P. Flitney, D. Abbott. (2002). An introduction to quantum game theory. arXiv :quant-ph/0208069v2
- [34] John Watrous. Lecture 20 : Bell inequalities and nonlocality. University of Calgary, CPSC 519/619 : Quantum Computation
- [35] Zhengfeng Ji. (2013). Binary Constraint System Games and Locally Commutative Reductions. arXiv :1310.3794v2
- [36] James M. Chappell, Azhar Iqbal, Derek Abbott. (2012). N-Player Quantum Games in an EPR Setting. *PLoS ONE* 7(5) : e36404. doi :10.1371/journal.pone.0036404.
- [37] Richard Cleve, Peter Hoyer, Ben Toner, John Watrous. (2010). Consequences and Limits of Nonlocal Strategies. arXiv :quant-ph/0404076v2
- [38] Dave Bacon. CSE 599d - Quantum Computing Quantum Entanglement and Bell's Theorem. Department of Computer Science & Engineering, University of Washington.
- [39] Adrian P. Flitney, Maximilian Schlosshauer, Christian Schmid, Wieslaw Laszkowski, Lloyd C. L. Hollenber. (2008). Equivalence between Bell inequalities and quantum Minority game. arXiv :0803.0579v2
- [40] Michel Boyer. (2004). Extended GHZ n-player games with classical probability of winning tending to 0. arXiv :quant-ph/0408090v4
- [41] Joseph Ng, Derek Abbott. (2000). Introduction to Quantum Games and a Quantum Parrondo Game.
- [42] ZHENGFENG JI. (2014). Lecture 1 : Introduction to QuantumGames. QIC 890/891 : SELECTED ADVANCED TOPICS IN QUANTUM INFORMATION.
- [43] A. Iqbal, A.H. Toor. (2008). Quantum Cooperative Games. arXiv :quant-ph/0108091v2
- [44] Ahmad Nawaz, A. H. Toor. (2013). Quantum Games and Quantum Discord. arXiv :1012.1428v1

- [45] FAISAL SHAH KHAN. (2009). QUANTUM MULTIPLEXERS, PAR-RONDO GAMES, AND PROPER QUANTIZATION. arXiv :0906.0645v1
- [46] A.P. Flitney, J. Ng, D. Abbott. (2002). Quantum Parrondo's Games. arXiv :quant-ph/0201037v3
- [47] Andris Ambainis, Arturs Backurs, Kaspars Balodis, Agnis Skuskovniks, Juris Smotrovs, Madars Virza. (2011). Worst case analysis of non-local games. arXiv :1112.2856v1
- [48] Angsheng Li, Xi Yong. (2014). Entanglement Guarantees Emergence of Cooperation in Quantum Prisoner's Dilemma Games on Networks. DOI : 10.1038/srep06286.
- [49] Jiangfeng DU, "PLAYING PRISONER'S DILEMMA WITH QUANTUM RULES", Fluctuation and Noise Letters, Vol. 2, No. 4, 2002
- [50] Piotr Gawron et Jaroslaw A. Miszczak, "Quantum Implementation of Parrondo's Paradox ", <https://arxiv.org/pdf/quant-ph/0502185.pdf>
- [51] Jiangfeng DU and al., "Remark On Quantum Battle of The Sexes Game", 2001.
- [52] Lan Zhou et Le-Man Kuang, "Proposal for optically realizing a quantum game", Elsevier, 2003.
- [53] Nanfang Yang, Damien Paire, Fei Gao, Abdellatif Miraoui, Weiguo Liu. (2015). Compensation of droop control using common load condition in DC microgrids to improve voltage regulation and load sharing. Electrical Power and Energy Systems 64 (2015) 752–760. Elsevier.
- [54] Stephen F. Bush, Sanjay Goel, Georges Simard. (2013). IEEE VISION FOR SMART GRID COMMUNICATIONS : 2030 AND BEYOND ROADMAP. IEEE SMART GRID RESEARCH.
- [55] Richard J. Hughes, Jane E. Nordholt, Kevin P. McCabe, Raymond T. Newell, Charles G. Peterson, Rolando D. Somma. Network-Centric Quantum Communications with Application to Critical Infrastructure Protection. LA-UR-13-22718 (version 2)
- [56] Chun Zhang, Wei Wu, Hantao Huang, Hao Yu. (2012). Fair Energy Resource Allocation by Minority Game Algorithm for Smart Buildings. 978-3-9810801-8-6/DATE12 EDAA.
- [57] Hong Guo et al., Decision Support Systems 46 (2008) 318-332, Elsevier
- [58] "Technologie roadmap", IEA International Energy Agency, 2011.
- [59] Frank Tabakin. (2015). OVERVIEW QDENSITY/QCWAVE : A MATHEMATICA QUANTUM COMPUTER SIMULATION. Preprint submitted to Elsevier.

- [60] Garry Bowe. (2001). Classical information capacity of superdense coding. Department of Physics, Australian National University, Canberra, A.C.T. 0200, Australia.
- [61] Lin Qing. (2008). The generation of Entangled Qudits and their Application in Probabilistic Superdense Coding. CHIN. PHYS. LETT. Vol. 26, No. 4 (2009) 040301.
- [62] Matrin Lukac, Aikaterini Mandilara. (2016). Quantum Algorithmic Complexity of Three-Qubit Pure States. 0195-623X/16 IEEE. DOI 10.1109/ISMVL.2016.37
- [63] Arijit ROy, Dibyendu Chatterjee et Subhasis Pal, "Synthesis of quantum multiplexers circuits", IJCSI, VOL.9, January 2012
- [64] [https://fr.wikipedia.org/wiki/D%C3%A9coh%C3%A9rence\\_quantique#Annexe:\\_Formalisme\\_math%C3%A9matique\\_de\\_la\\_d%C3%A9coh%C3%A9rence](https://fr.wikipedia.org/wiki/D%C3%A9coh%C3%A9rence_quantique#Annexe:_Formalisme_math%C3%A9matique_de_la_d%C3%A9coh%C3%A9rence)
- [65] [https://en.wikipedia.org/wiki/Quantum\\_pseudo-telepathy#The\\_Mermin-Peres\\_magic\\_square\\_game](https://en.wikipedia.org/wiki/Quantum_pseudo-telepathy#The_Mermin-Peres_magic_square_game)
- [66] [https://fr.wikipedia.org/wiki/Probl%C3%A8me\\_du\\_bar\\_d'El\\_Farol](https://fr.wikipedia.org/wiki/Probl%C3%A8me_du_bar_d'El_Farol)
- [67] [https://en.wikipedia.org/wiki/El\\_Farol\\_Bar\\_problem](https://en.wikipedia.org/wiki/El_Farol_Bar_problem)
- [68] [https://fr.wikipedia.org/wiki/Code\\_quantique](https://fr.wikipedia.org/wiki/Code_quantique)
- [69] [http://label2.ist.utl.pt/vilela/Cursos/Gam\\_Neuro.pdf](http://label2.ist.utl.pt/vilela/Cursos/Gam_Neuro.pdf)
- [70] [https://fr.wikipedia.org/wiki/Allocation\\_des\\_ressources](https://fr.wikipedia.org/wiki/Allocation_des_ressources)
- [71] <https://commons.wikimedia.org/wiki/File:4to1mux.png?uselang=fr>
- [72] <http://www.nicegrid.fr/enjeux-du-demonstrateur/>