Universidad Nacional de Mar del Plata - Facultad de Ingeniería
Departamento de Ingeniería Electrónica

COMPUTACIÓN CUÁNTICA: PROBLEMAS DE CORRESPONDENCIA Y ASIGNACIÓN DE RECURSOS

Por
Omar Gustavo Zabaleta

Tesis Doctoral para optar al grado académico de Doctor en Ingeniería, mención Electrónica

Director de Tesis

Dr. Constancio Miguel Arizmendi

Mar del Plata, Argentina. Agosto de 2013.

a mi familia

Índice General

Abstract

Many important technological problems such as facility assignment, medium access management, dynamic spectrum allocation, can be addressed as decision or matching problems. The usual classic algorithms, heuristics, etc. may become less efficient when the amount of resources or agents involved in the decision matching problem grow beyond a certain amount. Quantum computing takes advantage of quantum mechanical effects such as entanglement and superposition to provide massive performance speedup in certain types of computation problems such as data searching, factorization and encryption. In the course of this thesis quantum decision models are developed and studied as a tool for solving classic decision problems more efficiently. As a generic model of decision problem a quantum dating market model is proposed. The quantum matching model stability is analyzed through Von Neumann entropy calculus and the information about the different possible strategies leading to stable and unstable states is obtained. The performance of quantum and classic strategies is compared showing that the agents capitalizing a Grover quantum search based strategy achieve a much bigger success rate than those playing classics as the number of players grows. Entanglement between player strategies lead to outcomes in the quantum model that are totally unexpected in the decision problem classic formulation. Finally, game theory applied to wireless communications is studied. Interference problems are analysed from the viewpoint of game theory and quantum game solutions allowing fair and efficient resources sharing are proposed. Besides, the medium access problem is treated as a quantum minority game and novel results are presented.

Agradecimientos

Agradezco a Cecilia, la mujer de mi vida, mi compañera incondicional y a nuestro hijo Emiliano que desde que llegó a nuestras vidas solo nos ha aportado felicidad. A mis padres y a mi hermana a quienes les debo ser quien soy. Agradezco a Miguel, mi director, por su enseñanza y sobre todo su compresión en los momentos difíciles. A mis compañeros y amigos con quien comparto todos los días, en especial a Luciana que siempre está dispuesta a convidarme un mate y entablar una charla desestructurada. Agradezco a la educación pública gratuita.

Mar del Plata, Argentina — Omar Gustavo Zabaleta
Agosto de 2013

Introducción

0.1. La computación cuántica

La mecánica cuántica es uno de los pilares de lo que se denomina física moderna. Ésta gobierna el comportamiento y las propiedades de la materia en un modo fundamental, en particular a escala microscópica de átomos y moléculas. A tal escala se producen fenómenos esenciales de mecánica cuántica tales como *Superposición* y *Entanglement*. Los dispositivos que procesan información sacando provecho de estas características de la mecánica cuántica son conocidos como computadoras cuánticas. Dado que el procesamiento de la información cuántica permite llevar a cabo tareas que antes se creían imposibles o inviables, la tecnología de la computación ha traspasado los dominios de la ingeniería electrónica y las ciencias de la computación para introducirse en nuevos mundos tales como los de la física cuántica, la biología y la ingeniería biomédica. Desde el almacenamiento de información usando espines de fotones o electrones hasta la utilización de moléculas orgánicas para sintetizar transistores con el fin de realizar computación a gran escala usando cadenas de ADN, los investigadores avanzan hacia el futuro de la computación por diversos caminos. Por otra parte, la investigación y el desarrollo de estas tecnologías no se limita a entornos académicos, compañías tales como IBM, HP y D-Wave Sys están trabajando en pos de alcanzar la próxima revolución de la computación en un futuro no tan lejano.

La disipación de calor, las pérdidas, y otros fenómenos físicos limitan la capacidad de construir dispositivos de estado sólido. Por otra parte, la computación cuántica sostiene la promesa de resolver de forma eficiente algunos de los difíciles problemas de las ciencias de la computación tales como, la simulación de sistemas cuánticos, la factorización entera, búsqueda en base de datos y el cálculo de logaritmos discretos. Las herramientas de la teoría de la información y de la computación se han extendido para abordar el procesamiento y la transmisión de estados cuánticos. Sin embargo, debe quedar claro que esta teoría de la información basada en los principios cuánticos, de ninguna manera viene a reemplazar la teoría de la información clásica sino que más bien la completa y la extiende.

En esta tesis se analizan las posibilidades de utilizar algoritmos cuánticos, es decir algoritmos que sólo pueden ser implementados en una computadora cuántica, como solución para algunos problemas de las comunicaciones inalámbricas tales como el control de acceso al medio o la distribución óptima de recursos.

0.2. Teoría de Juegos

La teoría de juegos clásica provee de un conjunto de herramientas diseñadas para analizar la toma de decisiones racionales por parte de dos o más agentes que interactúan. Dependiendo de la característica del problema, las acciones de los involucrados podrán ser competitivas (juegos no-cooperativos) ó coalicionales (juegos cooperativos)y el fin será obtener las máximas "ganancias" individuales o globales, respectivamente. Por lo tanto, esta técnica de estudio permite analizar situaciones donde el resultado de las acciones de los individuos (o instituciones) no solo depende de su "jugada" sino también de las acciones del otro o los otros jugadores. Los

modelos de la teoría de juegos son representaciones abstractas de situaciones de la vida real. Esta abstracción abre ampliamente el espectro de aplicación, de manera que permite que los "jugadores" puedan ser seres humanos, instituciones, poblaciones de animales, gobiernos, agentes de mercado, etc., a la vez las estrategias pueden ser de distinta naturaleza.

La teoría de juegos fue inicialmente utilizada en ciencias económicas para modelar problemas de competencia entre compañías, donde un problema típico sería, por ejemplo, ¿debería una empresa incursionar en un nuevo mercado, considerando que sus competidores podrían hacer un movimiento similar (o diferente)? Más tarde surgieron aplicaciones en otras áreas tales como la política y la biología. Hoy en día, la teoría de juegos ha sido ampliamente reconocida como una herramienta importante, para analizar y comprender los conflictos y la cooperación entre individuos en muchos otros campos: tales como la ingeniería, las relaciones internacionales, las ciencias de la computación, etc. son solo algunos ejemplos. En redes de computadoras y telecomunicaciones, un método de acceso o acceso múltiple a un canal permite que varios terminales conectados al mismo medio de transmisión multipunto transmitan y compartan su capacidad. En algunas redes, el ruteo es complicado debido a que no hay una única entidad que se encargue de administrar los caminos: por el contrario, multiples entidades están involucradas en la tarea de seleccionar los caminos. Las complicaciones o la ineficiencia surgen si estas entidades eligen los caminos que optimizan sus propios objetivos, los cuales pueden entrar en conflicto con los otros participantes. Esta situación es analizada en esta tesis mediante técnicas de juegos, donde es posible analizar el desempeño de las entidades que actúan de forma cooperativa frente a las que utilizan estrategias no-cooperativas.

El gran crecimiento que han experimentado las aplicaciones inalámbricas en los últimos años ha generado un crecimiento exponencial en el uso de bandas frecuenciales sin licencia, provocando problemas de escasez en el ancho de banda disponible. Este problema no sólo es debido a la propia limitación del espectro, sino también al deficiente uso que se hace de él, en parte debido a las estrictas políticas de asignación de bandas de frecuencia. En consecuencia, teniendo como objetivo un mejor aprovechamiento de espectro, se analizan aquí soluciones basadas en teoría de juegos cuántica como alternativa a las técnicas existentes de asignación de recursos radioeléctricos.

0.3. Teoría de Juegos Cuántica

La teoría de juegos cuántica es una fusión entre la teoría de juegos clásica y la computación cuántica. En ciertas situaciones es natural pensar que las reglas que deben regir son las reglas de los juegos cuánticos ya que se desarrollan a escalas microscópicas donde rigen las leyes de la mecánica cuántica. Además de su interés intrínseco, los juegos cuánticos brindan una posibilidad para explorar el imponente mundo de la información cuántica. Además, mediante la cuantización de juegos clásicos surgen nuevas técnicas de cooperar, de eliminar dilemas, de alterar equilibrios, etc., lo que ha permitido resolver problemas de decisión en diversas áreas de investigación, tales como sociología, economía y biología, entre otras.

Uno de los objetivos principales de esta tesis es utilizar tales propiedades de la teoría cuántica de juegos para resolver problemas relacionados con las telecomunicaciones.

0.4. Administración de recursos mediante teoría de juegos cuántica

Recientemente, la teoría de juegos ha comenzado a ser aplicada en tanto en redes cableadas como en redes inalámbricas: los jugadores en el juego son usuarios racionales o operadores de redes que controlan sus dispositivos de comunicación. Con el constante crecimiento de las redes wireless, dichos dispositivos se deben enfrentar con recursos limitados para la transmisión (por ejemplo espectro de radiofrecuencia) que impone conflicto de intereses. En un intento por resolver este conflicto, ellos deben tomar ciertas decisiones, tales como transmitir ahora o más tarde, cambiar el canal de transmisión, o adaptar su velocidad de transmisión. Más cerca en el tiempo, un nuevo paradigma denominado *Cognitive Radio*, con el mismo fin que es la utilización eficiente de los recursos, define unos dispositivos con el mismo nombre (Radio cognitiva) que son capaces de extraer la información necesaria del entorno de radio y modificar sus parámetros de transmisión. Una etapa muy importante de esta tecnología emergente radica en los algoritmos de decisión utilizados para la gestión de los recursos, un software incluido en cada miembro de la red (un celular, una computadora, etc.) lo convierte en un dispositivo inteligente capaz de elegir los parámetros para la transmisión. En estos casos, la teoría de juegos se adapta aún mejor ya que los jugadores son dispositivos, lo que asegura una racionalidad en las acciones no siempre presente en las decisiones humanas.

En esta tesis se proponen técnicas de reconfiguración y adaptación al entorno en un contexto de redes inalámbricas distribuidas, más precisamente se proponen técnicas distribuidas de reparto de recursos mediante teoría de juegos cuántica. Como se

describió anteriormente, la teoría de juegos es una herramienta matemática que analiza las interacciones estratégicas entre múltiples agentes que toman decisiones. Por esa razón, resulta adecuada para analizar las prestaciones de este tipo de redes, donde cada nodo debe decidir sus parámetros de configuración de manera competitiva. Sin embargo, la complejidad matemática de los problemas a resolver resulta difícil de abordar computacionalmente. Las algoritmos cuánticos, algoritmos que solo pueden ser corridos en una computadora cuántica, han demostrado ser más eficientes que los clásicos para resolver ciertos problemas matemáticos complejos, tales como la factorización de un número entero, búsqueda en un base de datos desordenada, transformada de Fourier, entre los más importantes. Sus éxitos están basados, en la propiedades inherentes de la mecánica cuántica como superposición, entanglement, interferencia, etc. La alternativa propuesta aquí es la cuantización del modelo de reparto de recursos y utilizar el poder de cálculo basado en el paralelismo natural de la computación cuántica para disminuir la complejidad y acelerar los procesos de decisión.

Una emisora de radio transmite en una determinada frecuencia y se sintoniza el receptor para captarla. Si otros transmisores interfieren la recepción, no quedará más remedio que esperar a que desaparezca el problema. En un mundo ideal, sin embargo, el receptor conmutaría de inmediato a una frecuencia de reserva que transportase también la señal deseada. Tal solución sobrepasa la técnica actual. Quizás el ejemplo que se ha puesto dé la impresión de que el asunto no es tan grave. Pero en el caso de que la interferencia interrumpa una llamada urgente hecha desde un teléfono móvil, la rápida transferencia de la llamada a un canal celular libre sería más que conveniente: podría salvar una vida. Actualmente se trabaja para dotar de esta inteligencia

operativa flexible a radios, teléfonos móviles celulares y otros futuros equipos de comunicaciones inalámbricos. De aquí a diez años, la radiocomunicación con capacidad cognitiva debería permitir a casi todos los sistemas inalámbricos localizar cualquier banda libre del espectro radioeléctrico a su alcance y conectarse a ella para atender mejor al usuario. Mediante una programación adaptable, estos dispositivos inteligentes reconfigurarían sus funciones de comunicación para satisfacer las demandas de las redes de transmisión o de los usuarios.

0.5. Organización y contribuciones de la Tesis

La tesis comienza con dos capítulos introductorios, en el capítulo 1 se presentan nociones básicas de física e información cuántica, así también como la notación matemática necesaria para que los lectores no familiarizados con estos temas puedan seguir con relativa facilidad las aplicaciones que se desarrollan en los capítulos posteriores. Por último, en un sección dedicada al hardware para desarrollo en paralelo, se ilustran los conceptos básicos de una FPGA y se describen una serie de trabajos preliminares surgidos en esta tesis relacionados con el procesamiento digital de señales. En el capítulo 2 se introduce la teoría de juegos clásica y cuántica.

En el tercer capítulo se abordan los problemas de decisión, especialmente aquellos que pueden ser resueltos por medio de modelos estadísticos. En el mismo capítulo se incluye también un modelo de cuántico original del mercado de citas surgido de esta tesis. Mediante el cambio de las condiciones, este modelo de decisión es adaptable a varias aplicaciones, algunas de las cuales serán tratadas aquí. Por medio de modelos tales como el “bandido” y el “mercado de citas” en su versiones clásicas y cuánticas se explicarán en una primera instancia, casi de una manera lúdica, el funcionamiento

de los modelos de decisión que luego serán utilizados para resolver problemas de asignación de recursos de manera óptima.

Una vez finalizada la presentación de los modelos se analizan las métricas y herramientas utilizadas en cada caso para evaluar los resultados que arrojan los modelos, algunas relacionadas directamente con la teoría de juegos, tales como el concepto de pago "payoff", otras surgidas de la teoría de la información tales como la Entropía, que permitirán analizar la conveniencia de utilizar una determinada estrategia. Se presentan resultados utilizando un modelo cuántico del mercado de citas y se lo compara con los obtenidos con modelo clásico análogo.

En el capítulo 4 se presenta el mercado de citas desde el punto de vista de la información asociada con el problema. El problema se analiza bajo los conceptos de máxima y mínima entropía tomados de la teoría de la información. Con la intención de identificar las condiciones de estabilidad se supone que los estados de máxima entropía obedecen al principio de bienestar colectivo. Este principio tiene mucha relevancia al tratar problemas de compartimiento de recursos.

En el capítulo 5 se presenta el estudio de las redes inalámbricas de comunicaciones desde el punto de vista de la teoría de juegos. Se comienza con una descripción breve de los sistemas inalámbricos existentes para luego presentar soluciones a algunos de los problemas tales como los de asignación de recursos, control de acceso al medio, problemas de interferencia, entre otros. En el mismo capítulo se propone un protocolo de comunicación, utilizando las propiedades de la mecánica cuántica y para ser utilizado en sistemas de comunicación cuántica.

La tesis finaliza con la descripción de problemas abiertos, y las líneas de trabajo a encarar en una próxima etapa.

0.6. Publicaciones originadas en esta tesis

- Zabaleta, Omar Gustavo; Arizmendi, Constancio Miguel, "Quantum Search for the Dating Market", Special Issue of Advances and Applications in Statistical Sciences (AASS) (ISSN 0974-6811), paper No.4091034-SS59, August 7, 2009.[1]

- Zabaleta, Omar Gustavo; Arizmendi, Constancio Miguel, "Quantum Dating Market", Physica A: Statistical Mechanics and its Applications, Vol 389, 14, pages 2687-2864, July 15, 2010.[2]

- Zabaleta, Omar Gustavo; Arizmendi, Constancio Miguel, "Quantum decision theory on a dating market" Advances and Applications in Statistical Sciences, v. 6, p. 489 (2011).[3]

- Arizmendi, Constancio Miguel; Zabaleta, Omar Gustavo, "Stability of couples in a quantum dating market", International Journal of Applied Mathematics and Statistics v. 26, p. 143, (2012) [4].

- Arizmendi, Constancio Miguel; Barrangú, Juan Pablo, Zabaleta, Omar Gustavo, "A 802.11 MAC protocol adaptation for Quantum communications‘",2012 IEEE/ACM 16th International Symposium on Distributed Simulation and Real Time Applications, pages 147-150.[5]

- Zabaleta, Omar Gustavo; Barrangú, Juan Pablo; Arizmendi, Constancio Miguel, "Game theory techniques applied to a quantum MAC protocol design", XV Reunión de Trabajo en Procesamiento de la Información y Control, 2013. (Enviado)

0.7. Capítulos de libros

C. M. Arizmendi and O. G. Zabaleta, Advances in QUANTUM MECHANICS, Chapter Name: Quantum Dating Market, Edited by Paul Bracken, Intech 2013, ISBN 978-953-51-1089-7, Printed in Croatia, First published April 2013.[6]

0.8. Presentaciones en Conferencias y Workshops

- C. M. Arizmendi and O. G. Zabaleta, "Quantum decision theory on a dating market". V International Meeting on Dynamics of Social and Economic Systems (DYSES 2010),Benevento, Italy, September 20–25, 2010.

- Zabaleta, Omar Gustavo; Arizmendi, Constancio Miguel "Estrategias cuánticas para conseguir pareja? El juego del mercado de citas". V Workshop Mecánica Estadística Y Teoría de la Información, Mar del Plata, Bs.As., Argentina, Abril 27–29, 2009.

- Zabaleta, Omar Gustavo; Arizmendi, Constancio Miguel "Quantum search for the dating Market". IV International Meeting on Dynamics of Social and Economic Systems (DYSES 09), Pinamar, Bs. As., Argentina. Abril 14-18, 2009.

- De Micco, Luciana; Zabaleta O.G; Gonzalez,C.M; Arizmendi, C.M.; Larrondo, H "Ruido 1/fd implementado en FPGA". IBERCHIP XV Workshop,Buenos Aires, Argentina March 25–27, 2009.

- Luciana De Micco, Omar G. Zabaleta, C. M. González, C. M. Arizmendi and H. A. Larrondo"Implementación en FPGA de un generador de ruido coloreado". IBERCHIP XIV Workshop, Puebla, México February 20–22, 2008.

- O. G. Zabaleta, L. De Micco, C. M. González, C. M. Arizmendi and H. A. Larrondo "Generador de ruido estocástico coloreado mediante FPGA", Proceedings of Designer's Forum. IV Southern Programmable Logic Conference(SPL08).2008. Proceedings of Designer's Forum, ISBN 978-84-612-2376-3, p. 69–73.

- Zabaleta, Omar G. "GCA Based Error Correcting Code", Medyfinol 2006 (XV Conference on Nonequilibrium Statistical Mechanics and Nonlinear Physics) Mar del Plata, Bs. As.,Argentina, 2006.

- López Ruiz, Ricardo; Zabaleta Omar G. and Juan R. Sánchez "Sincronización estocástica de autómatas celulares", Cedi2005 (Congreso español de informática).

- Zabaleta, Omar G. "Statistical complexity behavior in stochastically coupled maps", Trefemac05 (Taller regional de física estadística y aplicaciones a la materia condensada). La Plata, Bs. As., Argentina 2005.

Capítulo 1

Conocimientos previos

1.1. Introducción

La computación cuántica conecta múltiples disciplinas, la física teórica, el análisis funcional y la teoría de grupos, la ingeniería electrónica, la ciencia de la computación y la química cuántica, entre otras. El concepto de computadora cuántica consiste en la aplicación de los principios fundamentales de la física cuántica al campo de la computación. La idea de que era necesaria la existencia de tal dispositivo fue planteada a comienzos de la década del 80 por el premio nobel de Física, Richard Feynman, quien concebía, según lo detallaba en su trabajo [7], que ninguna computadora clásica podía simular ciertos fenómenos cuánticos sin caer en una complejidad exponencial. Esto es, que las computadoras cuánticas, de existir, utilizarían exponencialmente menos espacio y tiempo que las computadoras clásicas para simular sistemas cuánticos reales, incluso se han hecho propuestas de simular sistemas de muchos cuerpos con computadoras cuánticas de manera eficiente [8]. David Deutsch [9], propuso la primera aplicación del principio de superposición de la mecánica cuántica, también llamado paralelismo cuántico, por medio del cual una máquina de Turing puede codificar

muchas entradas en una misma cinta y realizar cálculos con todas las entradas simultáneamente. Pero sin duda alguna, en el campo de las ciencias de la computación algorítmica los avances más trascendentes han venido de la mano de Peter Shor [10] que realizó un algoritmo que, aprovechando las bondades de la computación cuántica, puede factorizar primos en tiempo polinomial, mientras que el mejor algoritmo clásico conocido en la actualidad es exponencial. Por su parte, Lov Grover [11] demostró que es posible extraer información de una base desordenada en la raíz cuadrada de las instrucciones que llevaría hacerlo con una computadora clásica. A pesar de no ser tan impresionante en cuanto a la mejora en la velocidad como lo es el algoritmo de Shor, el algoritmo de Grover ha sido objeto de estudio de un gran número de investigadores, debido a la gran utilidad que tienen los algoritmos de búsqueda en los sistemas de computación.

1.2. Computación Cuántica

Durante los últimos años la teoría cuántica ha encontrado un nuevo campo de aplicación en el ámbito de la información y la computación. La física cuántica permite codificar la información de una manera no-local clásicamente imposible, así como el procesamiento de información con una eficiencia que sobrepasa ampliamente a las computadoras clásicas, las actuales y las previsibles [12]. Algunos de los aspectos notables de la clásica y la teoría cuántica de información son: El teletransporte cuántico, la codificación densa, y la criptografía cuántica. En lo que sigue de esta sección se resumirán los aspectos básicos y necesarios de la mecánica cuántica y luego daremos un recorrido por los algoritmos cuánticos más sobresalientes.

1.2.1. El estado de un sistema cuántico

El estado cuántico es la descripción del estado físico de un sistema cuántico. De acuerdo con el primer postulado de la mecánica cuántica: El estado de cualquier sistema físico cerrado puede ser descrito por medio de un vector de estado v con coeficientes complejos y longitud unitaria en un espacio de Hilbert $\mathcal{H}$, es decir un espacio lineal complejo (espacio de estados) equipado con un producto interno. Para describir modelos realistas de computación cuántica, estaremos interesados en grados de libertad para los cuales el estado es descrito por un vector en un espacio de Hilbert complejo finito. En particular, estamos interesados en sistemas compuestos por sistemas individuales de dos niveles. El estado de cada sistema de dos niveles se describe por medio de un vector en un espacio bidimensional de Hilbert. Para representar un vector de estado utilizaremos, de aquí en adelante, la notación de Dirac $|v\rangle$ donde v indica el autovalor correspondiente a cierto estado cuántico y se pronuncia 'ket v'. De este modo se definen $|0\rangle$ y $|1\rangle$ como los estados base del *qubit*, el equivalente cuántico del bit. Esto es análogo a lo que ocurre en computación tradicional donde un sistema biestable puede estar representado por la tensión en un capacitor de $+5V$ y otro de $0V$. De esta forma podemos codificar un *bit* asignando, por ejemplo, el valor lógico '1' al estado en el cual el voltaje es $+5V$ y '0' al estado en el cual el voltaje en el capacitor es $0V$. Por lo tanto a la base $\{|0\rangle, |1\rangle\}$ para el estado de un qubit se la llama comúnmente *la base computacional*. Como ejemplos de sistemas cuánticos de dos estados podemos pensar en estados spin-up y spin-down de un electrón. Estos bits, tomados a partir del spin de las partículas reciben el nombre de qubits (bits cuánticos).

También, un electrón orbitando un núcleo por ejemplo, puede describirse por un vector en un espacio bidimensional de Hilbert. Según la mecánica cuántica, los valores de energía que puede tomar el electrón están cuantizados, es decir que en lugar de poder tomar cualquier valor de energía, el electrón esta restringido a tomar solo valores de un conjunto discreto. Además, el electrón estará en general en el estado de más baja energía o con menor probabilidad en el primer nivel excitado, pero la cantidad de energía necesaria para excitar el sistema a los próximos niveles es tan alta que es muy poco probable que encontremos niveles de energía mayores al primer excitado. Para un caso como este es posible ignorar, para fines prácticos, el subespacio que comprende los niveles mayores al primer estado excitado de energía, y por lo tanto tenemos un sistema descrito por un vector bidimensional en un espacio comprendido por los dos niveles más bajos de energía.
El estado de una partícula se determina a través de la asignación de una probabilidad, no podemos hablar de un estado 0 ó 1 claramente determinado para partículas cuánticas. Esta es la ventaja que tiene la computación cuántica respecto a la clásica: La lógica de un bit es 0 ó 1, mientras que un qubit contiene el concepto de ambos a la vez.

Para realizar cálculos no triviales son necesarios más de un qubit. Si tomamos por ejemplo dos bits, sus estados posibles son cuatro: 00, 01, 10, 11 y para representar estos estados son necesarios cuatro vectores ortogonales en cuatro dimensiones, formados por el producto tensorial entre $|0\rangle$ y $|1\rangle$.

$$|0\rangle \bigotimes |0\rangle, \quad |0\rangle \bigotimes |1\rangle, \quad |1\rangle \bigotimes |0\rangle, \quad |1\rangle \bigotimes |1\rangle \tag{1.2.1}$$

Clásicamente, son necesarios cuatro pares de bits para representar la misma información que un solo par de qubits. En el texto se utilizará una nomenclatura más compacta para representar los estados de múltiples qubits,

$$|00\rangle, \quad |01\rangle, \quad |10\rangle, \quad |11\rangle.$$

El estado general de un qubit $|\psi\rangle$ es una combinación lineal pesada de los estados de la base, también llamada *superposición* de estados,

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \tag{1.2.2}$$

donde los pesos $\alpha, \beta \in \mathbb{C}$ son denominados *amplitudes de probabilidad*, por lo tanto deben satisfacer $|\alpha|^2 + |\beta|^2 = 1$. Consideremos el ejemplo del electrón orbitando: en general el electrón está en un estado que es combinación lineal entre el estado de menor energía y el primer estado excitado. El tercer postulado especifica que, siendo $|\psi\rangle$ el estado del sistema, la probabilidad de que al medir el qubit el estado sea $|0\rangle$ es $|\alpha|^2$ por lo tanto la probabilidades de que sea $|1\rangle$ es $|\beta|^2$. Cabe aclarar aquí un punto muy importante: Este estado ambiguo del sistema donde, con cierta probabilidad coexisten ambos estados ($|0\rangle$ y $|1\rangle$) tiene como condición que el sistema sea cerrado, es decir que no haya intervención del medio. Dicho de otra manera, si se mide el estado del sistema lo que se obtendrá como resultado es uno de los dos estados $|0\rangle$ ó $|1\rangle$. Se dice que el sistema colapsa hacia uno de los estados de la base. Esta característica difiere claramente de lo que ocurre en la mecánica clásica que establece por ejemplo que una moneda está en uno de los dos estados lógicos (cara ó cruz) antes de la medición y luego la medición lo que hace es revelar este hecho.

Por último, de acuerdo con el cuarto postulado de la mecánica cuántica, el espacio

de estados de un sistema compuesto es el producto tensorial de los sistemas físicos que lo componen. Como ocurre en la ciencia de la computación clásica, un conjunto de n qubits forman un registro. Desde el punto de vista físico, si consideramos qubits numerados del 1 al n, y que el qubit i está en el estado $|\psi_i\rangle$, entonces el estado del registro cuántico esta dado por $|\psi_1\rangle \bigotimes |\psi_2\rangle \bigotimes \ldots \bigotimes |\psi_n\rangle$, aunque usualmente se escribe de manera abreviada $|\psi_1\rangle|\psi_2\rangle \ldots |\psi_n\rangle$.

1.2.2. Evolución del sistema

La dinámica de un sistema de partículas está determinada por la ecuación de Schrödinger 1.2.3

$$H\psi = i\hbar\frac{\partial}{\partial t}\psi \tag{1.2.3}$$

El *Operador de Hamilton* describe la energía total del sistema en todo tiempo y en general suele tener una forma bastante complicada. Si se analiza el caso simple de una partícula en un campo de potencial estático $V(r)$, la ecuación 1.2.3 se puede escribir de la forma

$$(\frac{-\hbar^2}{2m}\nabla^2 + V(\overrightarrow{r}))\psi(\overrightarrow{r},t) = i\hbar\frac{\partial}{\partial t}\psi(\overrightarrow{r},t) \tag{1.2.4}$$

Si se utiliza $\psi(\overrightarrow{r},t) = \psi(\overrightarrow{r})\cdot\phi(t)$, válido para potenciales de este tipo, el sistema se puede resolver utilizando variables separables,

$$E\phi(t) = i\hbar\frac{\partial}{\partial t}\phi(t) \qquad y \qquad H\psi(\overrightarrow{r}) = E\psi(\overrightarrow{r}) \tag{1.2.5}$$

por lo tanto la solución del sistema dependiente del tiempo $\phi(t) = e^{-i\frac{E}{\hbar}t}$, donde E es la energía del estado ya que cumple

$$\langle H\rangle = \int \psi^*(\overrightarrow{r})(H\psi(\overrightarrow{r}))d^3(\overrightarrow{r}) = E\int \psi^*(\overrightarrow{r})\psi(\overrightarrow{r}) = E \tag{1.2.6}$$

Al problema de autovalores restante $H\psi = E\psi$ se lo denomina *ecuación de Schrödinger independiente del tiempo.*

Si tenemos un problema de valor inicial $\psi(t=0) = \psi_0$ podemos definir un operador $U(t)$ que cumpla

$$HU(t)|\psi_0\rangle = i\hbar\frac{\partial}{\partial t}U(t)|\psi_0\rangle \qquad y \qquad U(0)\psi = \psi \tag{1.2.7}$$

De esta forma se obtiene una ecuación de operadores $HU = i\hbar\frac{\partial}{\partial t}U$, cuya solución es $e^{-i\frac{H}{\hbar}t}$. Por lo tanto U es el *Operador de la evolución temporal* y satisface el criterio

$$|\psi(t+t_0)\rangle = U(t)|\psi(t_0)\rangle \tag{1.2.8}$$

1.2.3. Mediciones

En la física clásica, a los observables de un sistema tales como la posición de la partícula, el momento, la Energía, etc. se caracterizan por ser entidades bien definidas cuyos valores cambian en el tiempo de acuerdo a ciertas leyes dinámicas y que (salvo alguna dificultad técnica) podrían en principio ser observadas sin perturbar el sistema. Una característica importante de los sistemas cuánticos es que esto no lo cumplen.
En física cuántica el concepto clásico de la "localización" de una partícula ha sido reemplazado por el concepto estadístico de "valor esperado" de la posición de una partícula. Esta correspondencia no se restringe solo a la posición de la partícula. De hecho todas las cantidades físicas clásicas de un sistema se pueden describir por medio del valor esperado de un operador apropiado [13]. El valor esperado de cierto operador O para un observable $\mathcal{O}$ se define

$$\langle O\rangle = \int \psi^*(\overrightarrow{r},t)O\psi(\overrightarrow{r},t)d\overrightarrow{r}^3 \tag{1.2.9}$$

y la incerteza

$$\triangle O = \sqrt{\langle O^2 \rangle - \langle O \rangle^2}. \tag{1.2.10}$$

Las mediciones cuánticas se describen por medio de una colección $\{M_o\}$ de operadores de medición actuando sobre el espacio de estados del sistema que está siendo medido. El índice o refiere al resultado de la medición que se espera que arroje el experimento. Los valores medidos o_i son siempre autovalores del operador O. Dicho de otra forma, es imposible observar un estado cuántico ψ sin, al mismo tiempo, forzar al sistema a un estado ψ' que es un autoestado del operador hermítco correspondiente a la cantidad observada .

Para ilustrar el concepto de medición veamos el siguiente ejemplo: Consideremos que el estado $|\psi\rangle$ está compuesto por dos autoestados $|\psi_1\rangle$ y $|\psi_2\rangle$ de la ecuación de Schrödinger independiente del tiempo con los autovalores de energía E_1 y E_2

$$|\psi\rangle = \alpha_1|\psi_1\rangle + \alpha_2|\psi_2\rangle \quad con \quad |\alpha_1|^2 + |\alpha_2|^2 = 1 \tag{1.2.11}$$

El valor esperado de la energía es $\langle H \rangle = |\alpha_1|^2 E_1 + |\alpha_2|^2 E_2$, pero si se realiza la medición, mediremos E_1 ó E_2 con probabilidades $|\alpha_1|^2$ y $|\alpha_2|^2$. Sin embargo, si medimos nuevamente el estado resultante, obtendremos siempre la misma energía que en la primera medición, ya que la función de onda habrá colapsado ya sea a ψ_1 ó ψ_2.

1.2.4. Estados mixtos

En general, cualquier sistema contiene mayor o menor grado de aleatoriedad y desorden, por lo tanto el formalismo de la mecánica cuántica se debe adaptar para tener en cuenta estos efectos. Ésto se hace representando los estados como operadores o matrices densidad (1.2.12) y promediando las fluctuaciones. La barra superior

representa el promedio estadístico sobre las fluctuaciones. Todas las propiedades mensurables del estado están representadas por ρ.

$$\rho = \overline{|\psi\rangle\langle\psi|} \tag{1.2.12}$$

La matriz densidad resulta de utilidad para representar estados mixtos, los cuales se pueden pensar como combinaciones probabilísticas de los estados puros. Matemáticamente, la matriz densidad se puede descomponer siempre como la suma incoherente de estados puros,

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|, \tag{1.2.13}$$

donde $|\psi_i\rangle$ es un estado puro y p_i son probabilidades que están acotadas entre 0 y 1 y cuya suma es 1. En general, esta descomposición no es única.

Como ejemplo, supongamos una fuente S_1 emisora de fotones en dos direcciones, y que emite un estado parcialmente mezclado, esto es, 50 % de los fotones son emitidos en ambas direcciones con polarización horizontal $|HH\rangle$ y el restante 50 % es emitido con polarización vertical $|VV\rangle$, por lo tanto,

$$\rho_{mix} = \frac{1}{2}|HH\rangle\langle HH| + \frac{1}{2}|VV\rangle\langle VV| \tag{1.2.14}$$

ó en forma de matriz

$$\rho_{mix} = \begin{bmatrix} \frac{1}{2} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{2} \end{bmatrix} \tag{1.2.15}$$

Por último, cabe hacer la aclaración que éste no es ni un estado puro ni tampoco un estado completamente aleatorio, sino un estado parcialmente mixto.

1.2.5. Superposición Cuántica

Si bien se ha mencionado esta propiedad de manera superficial, la superposición cuántica es un fenómeno que merece ser presentado con más detalle. En las computadoras clásicas, las señales eléctricas tales como voltajes representan los estados de 0 y 1 de un bit de información. En cambio, en computadoras cuánticas los estados de un electrón se pueden usar como un qubit. La orientación del spin hacia arriba o hacia abajo representa los dos estados 0 y 1 respectivamente. Usando qubits, las computadoras cuánticas pueden realizar operaciones lógicas y aritméticas como lo hacen las computadoras clásicas. Sin embargo, la diferencia importante es que un qubit puede representar la superposición de los estados 0 y 1 [14]. Esta característica de las computadoras cuánticas hace posible la computación paralela de manera "natural". Como cada qubit representa dos estados al mismo tiempo, dos qubits pueden representar cuatro estados simultáneamente, de forma general, n qubits pueden representar 2^n estados. Por ejemplo, cuando usamos dos qubits que son la superposición de los estados 0 y 1 como entrada para una operación, podemos obtener el resultado de cuatro operaciones para cuatro entradas con solo un paso de cálculo, comparado con las cuatro operaciones necesarias en una computadora clásica.

1.2.6. Entanglement

La capacidad computacional de procesamiento paralelo de la computación cuántica, es enormemente incrementada por el procesamiento masivamente en paralelo, debido a una interacción puramente cuántica. Mientras el estado de un sistema clásico se puede especificar por medio de los estados de todos los sistemas que lo constituyen, en la teoría cuántica un sistema combinado puede tener propiedades adicionales, en

cuyo caso los sistemas que lo componen se dice que están entangled o "enredados" unos con otros.

El entanglement cuántico ocurre cuando partículas tales como fotones, electrones e incluso pequeños diamantes [15] interactúan físicamente y luego son separados; el tipo de interacción es tal que cada miembro resultante de un par es descrito de manera apropiada por el mismo estado, que es indefinido en términos de factores importantes tales como posición, momento, spin, polarización, etc. Los estados entangled fueron discutidos por primera vez en el famoso trabajo de Einstein, Podolsky and Rosen (EPR), en el cual ellos intentaban demostrar la incompletitud de la mecánica cuántica [16].

Veamos el ejemplo de dos qubits, que se preparan independientemente y se mantienen aislados, entonces cada qubit forma un sistema cerrado y el estado puede ser escrito en forma de producto. Entonces, si el estado es separable y puro es posible escribirlo como $|\psi\rangle = |\psi_A\rangle \bigotimes |\psi_B\rangle$. El estado $|\psi_1\rangle = |HH\rangle$ es un producto de estados puros y se puede escribir como

$$|\psi_1\rangle = |H\rangle_A \bigotimes |H\rangle_B. \tag{1.2.16}$$

Otro ejemplo muy común es el estado

$$|\psi\rangle = (|HH\rangle + |HV\rangle + |VH\rangle + |VV\rangle)/2, \tag{1.2.17}$$

que se puede escribir como el producto

$$|\psi\rangle = 1/\sqrt{2}(|H\rangle + |V\rangle)_A \bigotimes 1/\sqrt{2}(|H\rangle + |V\rangle)_B, \tag{1.2.18}$$

Otro ejemplo es la matriz 1.2.15 definida más arriba, que representa un estado mixto.

Sin embargo, si se les permite a los qubits interactuar, entonces el sistema cerrado incluye a ambos qubits y no es posible escribir el estado en forma de producto. Cuando este el caso se dice que los qubits están *entangled*, [13]. Debido al *Entanglement* dos partículas subatómicas, permanecen indefectiblemente relacionadas entre sí. Estas partículas forman subsistemas que no pueden describirse separadamente, cuando una de las dos partículas sufre un cambio de estado, la otra lo sufre automáticamente. Y eso ocurre de forma instantánea y con independencia de la distancia que las separe en ese momento. Esta propiedad se manifiesta cuando se realiza una medición sobre una de las partículas.

Una buena medida para medir cuán entangled está un sistema de dos qubits es una magnitud llamada *Concurrencia* [17]. Partiendo del estado más general de dos qubits,

$$|\psi\rangle = \alpha|HH\rangle + \beta|HV\rangle + \gamma|VH\rangle + \delta|VV\rangle \tag{1.2.19}$$

se define $C = 2(|\alpha\delta - \beta\gamma|)$.

De acuerdo a este cálculo, solamente si $C = 0$ el estado es separable. Si $C = 1$ (su máximo valor), el estado está completamente entangled.

Supongamos un experimento en el cual se pretende medir el spin de dos electrones emitidos en direcciones opuestas decayendo a un único estado (single state) cuyo spin total es cero. Esto es, los electrones que conforman el estado tienen diferentes números cuánticos $s = +1/2$ y $s = -1/2$ y de esta manera el spin total del estado singlet es nulo. Para un estado como este la conservación del momento angular requiere que los vectores spin estén orientados en direcciones opuestas. El estado que describe esta situación es (1.2.20), que si se compara con el estado general (1.2.19) se tiene que $\alpha = \delta = 0$ mientras $\beta \neq 0$ y $\gamma \neq 0$. Si se decide por ejemplo medir el primer qubit se

obtendrá aleatoriamente $|0\rangle$ ó $|1\rangle$ con probabilidad $|\beta|^2$ y $|\gamma|^2$ respectivamente. Pero lo interesante del asunto es que si el resultado de la medición resultó ser 0 sabemos con seguridad que una medición del otro qubit resultará 1 y de forma similar, si la medición en primer qubit resulta ser 1, la observación del segundo qubit, con seguridad, arrojará 0 como resultado. Pareciera ser que existe una "misteriosa conexión" entre las dos partículas, pero lo que es más impresionante aún es que experimentos específicos han probado que el fenómeno se mantiene incluso cuando los qubits de $|\phi\rangle$ son trasladados a dos sitios distintos muy alejados. Recientemente investigadores de la ciudad de Viena han establecido el récord en teletransportación cuántica, logrando transmitir datos a través de una distancia aproximada de 144 km [18]. Como se verá más adelante, este peculiar fenómeno de la mecánica cuántica es muy útil en lo que respecta a la computación cuántica y a la teoría de la información cuántica.

$$|\psi\rangle = \beta|\uparrow\downarrow\rangle + \gamma|\downarrow\uparrow\rangle = \beta|01\rangle + \gamma|10\rangle \tag{1.2.20}$$

1.2.7. Compuertas Cuánticas

El operador evolución temporal satisface la condición

$$U^\dagger(t)U(t) = e^{i\frac{H}{\hbar}t} \cdot e^{-i\frac{H}{\hbar}t} = 1 \tag{1.2.21}$$

Los operadores U que cumplen con $U^\dagger = U^{(-1)}$ son denominados *unitarios*. Debido a que la evolución temporal de un sistema cuántico está gobernada por un operador unitario y $U^\dagger = U(-t)$ se deduce que el comportamiento temporal de un sistema cuántico es *reversible*, siempre y cuando no se realice una medición, es decir que el sistema colapse.

Por lo expresado, la evolución temporal de los sistemas cuánticos está matemáticamente descrita por operadores unitarios. Las compuertas de los circuitos cuánticos asociados a los algoritmos cuánticos son operadores unitarios. Un circuito cuántico tiene la misma función que su contraparte clásico, es decir consta de una entrada, una salida y en medio de estas un canal por donde se transmite la información. En el camino, la información ingresada podrá ser modificada por medio de compuertas cuya tarea es transformar el estado de los qubits a su entrada, el estado del sistema a la salida de la compuerta podrá ser parte de la entrada a otra compuerta, tal como ocurre en los circuitos clásicos. De hecho la señal siempre es modificada debido a que el canal de comunicaciones no es ideal. Por tal razón es común asociar las compuertas con operadores unitarios.

Los operadores en el espacio bidimensional de Hilbert se pueden representar con matrices 2×2. Un operador lineal queda completamente determinado por su acción sobre una base, veamos por ejemplo el caso de una del operador NOT que mapea el estado $|0\rangle$ a $|1\rangle$ y $|1\rangle$ a $|0\rangle$. Es más, por ser un operador lineal, mapea la combinación lineal de entradas a una combinación lineal de las salidas, o bien expresado de otra forma, la compuerta NOT mapea el estado general

$$\alpha|0\rangle + \beta|1\rangle \tag{1.2.22}$$

al estado

$$\alpha|1\rangle + \beta|0\rangle \tag{1.2.23}$$

En notación matricial:

$$NOT = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{1.2.24}$$

Recordando que los estados de la base tienen su representación como vectores columna, veamos como actúa la compuerta sobre uno de estos estados:

$$NOT|0\rangle \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \equiv |1\rangle \tag{1.2.25}$$

La compuerta NOT también es conocida por su nombre en inglés "*flip-gate*" ó como *compuerta X*, una de las cuatro compuertas de *Pauli*. En computación clásica la compuerta equivalente es la compuerta *inversora*. La segunda compuerta que correspondería al *buffer* en computación clásica, ya que mantiene en la salida el valor de la entrada, es la compuerta I cuya representación matricial es la matriz identidad. Las otras dos compuertas que aquí presentamos, no tienen sus predecesores en la computación clásica, estas son Y y Z. En lo que sigue presentamos como actúan estas sobre una entrada arbitraria $|\psi\rangle$.

$$Y|\psi\rangle \equiv \begin{bmatrix} 0 & -j \\ j & 0 \end{bmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} -jb \\ ja \end{pmatrix} \equiv -jb|0\rangle + ja|1\rangle \tag{1.2.26}$$

Como se puede observar el efecto que causa Y sobre el estado de entrada es multiplicar por j e intercambiar las amplitudes de probabilidad, donde $j = \sqrt{-1}$ es la unidad imaginaria. Por su parte Z genera sobre la entrada un cambio de fase. Es común recordar a esta compuerta como la que realiza un cambio de signo en el estado $|1\rangle$ de la base computacional.

$$Z|\psi\rangle \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a \\ -b \end{pmatrix} \equiv a|0\rangle - b|1\rangle \tag{1.2.27}$$

La compuerta *Hadamard* H es una de las más utilizadas ya que aplicada sobre alguno de los estados puros de la base crea un estado en superposición uniforme,

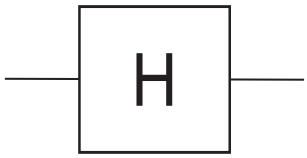

Figura 1.1: Compuerta de Hadamard

$$\begin{aligned} H|1\rangle &\mapsto \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \\ H|0\rangle &\mapsto \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle). \end{aligned} \tag{1.2.28}$$

Si se se observan estas dos últimas expresiones se puede deducir que la transformación de una entrada $|x\rangle$, con $x = 0$ ó $x = 1$, al atravesar la compuerta H, se puede expresar como

$$|x\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle). \tag{1.2.29}$$

La compuerta cuántica $P(\alpha)$ cuyo nombre en inglés es *Phase Gate*, es la última que presentaremos aquí, más información se puede adquirir en libros tales como [13]. Como su nombre hace intuir, esta realiza un cambio de fase, o dicho de otra forma, una rotación de fase y su aplicación sobre un estado arbitrario es la siguiente,

$$P(\alpha)|\psi\rangle = \begin{bmatrix} 1 & 0 \\ 0 & e^{j\alpha} \end{bmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a \\ e^{j\alpha}b \end{pmatrix} = a|0\rangle + e^{j\alpha}b|1\rangle. \tag{1.2.30}$$

Por último se presentan dos compuertas que son de mucha utilidad en los algoritmos cuánticos, la compuerta $CNOT$ y la compuerta C-$\widehat{U}_f$.

La compuerta Control NOT es una compuerta de dos qubits cuya representación matricial y su diagrama circuital son los siguientes.

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{1.2.31}$$

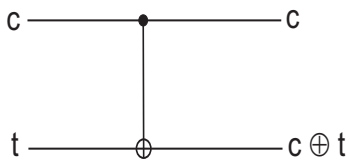

Figura 1.2: La compuerta NOT controlada cambia el estado de $|t\rangle$ solamente si la entrada de control $|c\rangle$ es $|1\rangle$

Esta compuerta actúa sobre dos qubits, el qubit de control y el qubit denominado target. La acción de $CNOT$ está dada por $|c\rangle|t\rangle \rightarrow |c\rangle|c \bigoplus t\rangle$ esto es, la compuerta realiza la operación NOT sobre el qubit target $|t\rangle$ si el qubit de control está en estado $|1\rangle$, en otro caso el estado de t no cambia.

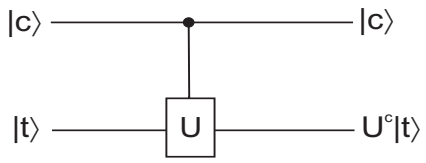

Figura 1.3: La compuerta U controlada cambia el valor de $|t\rangle$ a $U|t\rangle$ solamente si la entrada de control c se activa

Siendo U una compuerta que actúa sobre un solo qubit, la compuerta $U controlada$ es nuevamente una compuerta de dos qubits con un qubit de control y un qubit target. Si se acciona el bit de control entonces U se aplica al qubit de target, en otro caso éste mantiene su estado, esto es $|c\rangle|t\rangle \rightarrow |c\rangle U^c|t\rangle$. En la figura 1.3 se muestra el diagrama circuital para la U controlada.

1.2.8. Circuitos Cuánticos

Un diagrama circuital que describa las secuencias de operaciones cuánticas y mediciones que intervienen en la descripción de algoritmos cuánticos complejos puede resultar muy eficiente. Las compuertas simples presentadas previamente pueden ser ensambladas de forma que formen un arreglo tipo red que nos permita realizar operaciones cuánticas más complicadas que las que pueden realizar cada una de ellas por separado [19]. Un modelo de circuito cuántico es el que muestra en la figura 1.4. Como en el caso clásico, el circuito cuántico consiste en compuertas conectadas por "cables". Los qubits que ingresan desde la izquierda son transportados en el tiempo a través de estos cables y las compuertas, representadas por bloques rectangulares, van actuando sobre ellos.

En este ejemplo el estado de 4 qubits $|\psi_i\rangle = |0000\rangle$ entra en el circuito para ser procesado por las compuertas U_1, U_2, U_3, U_4. Como salida del circuito tenemos el estado de 4 qubits (posiblemente entangled) $|\psi_f\rangle$. Se realiza una medición qubit por qubit en la base computacional $\{|0000\rangle, |0001\rangle, ..., |1110\rangle, |1111\rangle\}$, aunque en algunos casos puede que sea necesario hacer una medición conjunta.

En muchos casos, en lo que se está realmente interesado no es el estado cuántico de salida, sino en la información clásica que indica qué resultado se produjo.

Veremos algunos ejemplos de circuitos en secciones posteriores cuando analicemos algunos de los algoritmos cuánticos más importantes.

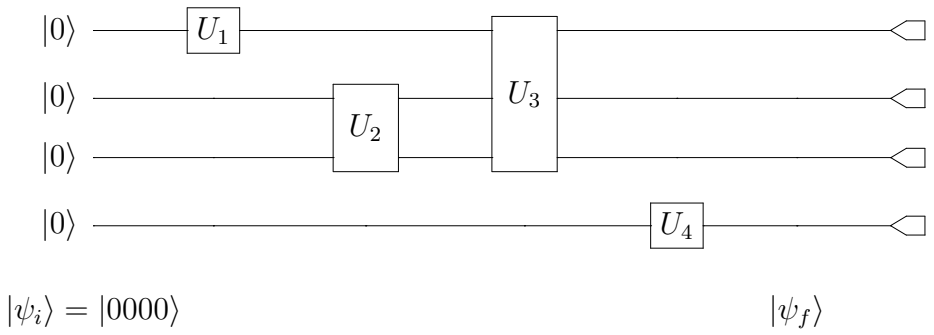

Figura 1.4: *Modelo de circuito Cuántico.*

1.3. Sistemas de Comunicaciones: Entropía e Información Cuántica

La información es física y cualquier procesamiento de la información se desarrolla siempre con medios físicos, esto parece algo obvio pero sus consecuencias no son triviales. En los últimos tiempos han existido avances tanto teóricos como experimentales que han llevado a la composición de una nueva disciplina: una teoría cuántica de la información.

1.3.1. Teoría de la Información Cuántica

En el modelo presentado por Shannon a fines de la década del cuarenta, una fuente de información, un canal de comunicación y un receptor interactúan entre sí. La fuente y el receptor comparten un alfabeto común, $\mathcal{A}$, es decir, un conjunto finito de símbolos que se pueden transmitir a través del canal. Los símbolos del alfabeto $\mathcal{A} = \{\alpha_1, \alpha_2, ..., \alpha_n\}$ se seleccionan de acuerdo a una distribución de probabilidades $p_1, p_2, ..., p_n$.

Si consideramos mensajes o cadena de caracteres $x_1, x_2, ..., x_n \in A^n$ originados por una

fuente sin memoria, un símbolo α aparece con probabilidad $p(\alpha)$ independientemente de los otros símbolos que entren en los lugares restantes de la cadena. El primer teorema de Shannon dice que si $n \gg 1$, la información suministrada por un mensaje genérico de n caracteres ($n \log_2(|A|)$ bits de largo) coincide con la trasmitida por otro mensaje más corto, de longitud $nH(A)$, donde H es la entropía de Shannon

$$H(A) = -\sum_{1 \leq i \leq |A|} p(\alpha_i) \log_2 p(\alpha_i) \tag{1.3.1}$$

En otras palabras, en promedio, cada caracter es compresible hasta un mínimo de $H(A)$ bits.

El equivalente cuántico de la entropía de Shannon es la entropía de Von Neumann,

$$S(\rho) = -Tr(\rho \log_2 \rho), \tag{1.3.2}$$

donde ρ es el operador densidad que describe al sistema cuántico. Dada una descomposición convexa en estados puras $\rho = \sum_{i \in I} p_i |\psi_i\rangle\langle\psi_i|$, se puede demostrar que $S(\rho) \leq H(I)$, valiendo la igualdad si y solo si los vectores ψ son pares ortogonales. Información más detallada sobre entropía y sus propiedades se puede hallar en [12], sin embargo no podemos dejar de mencionar aquí una particularidad: La Entropía $S(\rho_{A,B})$ de un sistema cuántico compuesto por los subsistemas A y B puede ser menor que la entropía de cualquiera de ellos, $S(\rho_A)$ ó $S(\rho_A)$. Esta propiedad no se cumple para la entropía de Shannon. Un claro ejemplo son los estados Einstein-Podolsky-Rosen (EPR) de la forma $2^{-1/2}(|aa'\rangle + |bb'\rangle)$, donde a, b y a', b' son pares ortogonales. La diferencia básica entre la información clásica y la cuántica es que mientras la información clásica se puede copiar perfectamente, la cuántica no. Esto es relevante a los protocolos cuánticos de comunicación debido a que si existiera una forma de copiar de

forma cuántica, entonces sería posible el espionaje en canales cuánticos. Lo que ocurre es que no podemos duplicar un bit cuántico en un estado desconocido sin perturbar el original. Más sobre el teorema de la no-clonación cuántica se puede hallar en [20].

1.4. Corrección de errores

Un modelo matemático de computación es una abstracción idealizada. Diseñamos algoritmos y realizamos análisis suponiendo que las operaciones matemáticas que realizamos se llevaran a cabo de manera exacta, y sin error. Los dispositivos físicos que implementan un modelo abstracto de computación son imperfectos y de precisión limitada.

Por ejemplo, cuando un circuito digital se implementa en una placa, ruido eléctrico indeseado en el ambiente puede causar que los componentes se comporten de manera distinta a la esperada, y puede causar que los niveles de voltaje (valores del bit) cambien. Estas fuentes de error deben ser controladas o compensadas, de otra forma le pérdida de eficiencia resultante puede reducir la potencia de procesamiento del dispositivo.

Las computadoras cuánticas son más susceptibles a errores que las computadoras digitales clásicas, debido a que los sistemas cuánticos son más delicados y más difíciles de controlar. De ser posible una computadora cuántica a gran escala, será necesaria una teoría cuántica de corrección de errores.

1.4.1. Corrección de errores cuántica

Cuando se discute modelos de error para computadoras clásicas, en general, los errores pueden no afectar bits independientemente, y entonces los modelos de error tienen que tener en cuenta cualquier correlación entre errores en diferentes bits. Esto mismo es cierto para errores en bits cuánticos. Resulta que es más simple describir códigos que afectan qubits independientemente, y por fortuna los conceptos importantes de corrección de errores se pueden entender por medio de estos modelos de error restringidos, por este motivo la mayoría de la literatura trata con estos modelos en los cuales los errores ocurren en qubits únicos independientemente.

Los errores ocurren sobre un qubit cuando su evolución difiere de la deseada. Esta diferencia puede ocurrir debido a un control impreciso sobre los qubits o por la interacción de los qubits con el ambiente. Por ambiente, se entiende todo lo que sea externo al qubit bajo consideración. Un canal cuántico es una descripción formal de como qubits en un determinado entorno son afectados por su medio.

El primero que presentó un sistema de codificación ($9:1$ bits) capaz de detectar y corregir un qubit fue Shor en 1995 [21]. Poco tiempo después, se descubrieron codigos nuevos y más económicos tales como el código de Steane $7:1$ [22] y Caldenbank-Shor [23], y el código 5:1 de Bennett-Brassard, et al. (1996). La idea de la corrección de error cuántica subyace en esconder la información en subespacios de $\mathbb{C}^{2^n}$ para protegerla de la decoherencia y los errores que afectan solamente a unos pocos qubits. Con este fin, si nuestro sistema tiene k qubits (llamados "qubits lógicos"), un código corrector de error codifica sus estados por medio de una incorporación lineal isométrica $\pi : \mathbb{C}^{2^k} \hookrightarrow \mathbb{C}^{2^n}$ con $n > k$. Para una interesante discusión sobre los conceptos generales que involucran a los modelos de corrección de error es recomendable leer [24].

1.5. Hardware para procesamiento paralelo

1.5.1. Introducción

La implementación de circuitos cuánticos es todavía un tema de investigación, y todavía hay un largo camino que recorrer antes de que la primera computadora cuántica aparezca en el mercado. Mientras esto ocurre la investigación se orienta hacia el desarrollo de software y aplicaciones teóricas cuánticas para resolver problemas de forma mas eficiente de lo que lo haría una computadora clásica. Una alternativa para probar la eficiencia de los algoritmos desarrollados para las computadoras cuánticas del futuro es la implementación de éstos en un emulador implementado en hardware. Las placas FPGA (Field Programmable Gate Arrays) son las candidatas naturales para realizar esta tarea, ya que proveen una capacidad de procesamiento en paralelo que permite implementar las compuertas reversibles (condición necesaria para poder emular los algoritmos cuánticos) e interconectarlas con el fin de implementar algoritmos por ejemplo, de forma más eficiente que por software.

1.5.2. Field programmable gate arrays (FPGAs)

Las FPGAs se pueden usar para implementar cualquier diseño de Hardware. Uno de los usos más comunes de estas es el prototipado de una pieza de Hardware que eventualmente será implementado más tarde en una ASIC (Application Specific Integrated Circuit). Sin embargo, las FPGAs están siendo usadas cada vez más como plataformas de producto final. Su uso depende, para un dado proyecto, de los pesos relativos de los rendimientos deseados, el desarrollo, los costos de producción.

Conceptos básicos

La estructura básica de una FPGA consiste de un arreglo bi-dimensional de bloques lógicos y flip-flops con medios para que el usuario configure (a) la función de cada bloque lógico, (b) las entradas y salidas, y (c) la interconexión entre bloques. Las familias de FPGAs difieren unas de otras en la manera física de implementar los programas del usuario, arreglos de los alambres de que se interconectan, y la funcionalidad básica de los bloques lógicos.

Durante el transcurso de esta tesis se desarrollaron trabajos en FPGA relacionados con procesamiento digital de señales. Si bien para procesamiento digital de señales es natural utilizar dispositivos DSP (Digital Signal Processors), las FPGAs cuentan con funciones DSP, sumadas a un mar de otras compuertas y la posibilidad de realizar muchas tareas DSP en paralelo. Los trabajos que brevemente se describen abajo permitieron adquirir experiencia en el manejo de las herramientas y los lenguajes de programación necesarios en cada etapa de diseño con placas de desarrollo ALTERA©.

1.5.3. Implementación en FPGA de un generador de ruido estocástico coloreado

Los ruidos caóticos y estocásticos comparten muchas propiedades estadísticas y dinámicas. Recientemente se ha encontrado la forma de distinguirlos mediante medidas de complejidad. Por lo tanto es esperable que el comportamiento de muchos sistemas físicos sea diferente frente a estos dos tipos de ruido y para poder evaluar esta conjetura en forma experimental se require contar con generadores de ruido en

hardware con características controlables (espectro, densidad de probabilidad, autocorrelación, etc.).

Ha habido gran desarrollo de generadores de ruido en software mientras que su contraparte en hardware está mucho menos desarrollada. En [25] se presenta el diseño e implementación en FPGA de un generador de ruido estocástico coloreado, con espectro de tipo f^{-k} que permite la selección de $k = 1, 2, 3, 4$. Este trabajo es parte de un proyecto de contar con generadores de ruido caóticos y estocásticos diseñados como IP cores e implementados en FPGA para su uso en experiencias con distintos sistemas físicos. El generador incluye básicamente un generador de ruido blanco basado en un mapa caótico, y cuatro bloques que realizan la transformación de ruido blanco a ruido coloreado, dos de los cuales implementan la transformada rápida de Fourier (FFT)y la Transformada Inversa (IFFT). En este trabajo solo se realizaron simulaciones con Simulink de *Matlab*® y software específicos de la placa FPGA utilizada. En trabajos posteriores [26, 27] se realizaron mejoras en el diseño y se lo implementó en placas FPGA de desarrollo.

La simulación eficiente por software de los sistemas cuánticos es una tarea difícil, ya que se necesitan tiempos exponenciales y se requiere mucha memoria para almacenar datos. Es más, a la naturaleza secuencial de la computación basada en software le resulta extremadamente difícil simular la naturaleza paralela de la computación cuántica. La emulación de circuitos cuánticos por medio de tecnologías reconfigurables FPGA resulta se más adecuada y algunos trabajos que en esta área se han realizado son [28, 29]. La computación paralela a nivel de hardware permite una considerable mejora en velocidad de cálculo en comparación con los simuladores de

software, proveyendo además una mejora en la percepción de las exigencias de precisión para simular circuitos cuánticos.
Con base en los conocimientos adquiridos en implementación de circuitos en FPGA, se pretende, como trabajo posterior a esta tesis, continuar con los trabajos de simulación de circuitos cuánticos presentados pero en esta ocasión a nivel de hardware.

1.6. Algoritmos cuánticos

Esta sección comienza con una introducción al procesamiento paralelo y luego se describen algunos de los algoritmos cuánticos más importantes. Los dos primeros son los más sencillos y sirven para ilustrar los ingredientes principales de los algoritmos más útiles y poderosos que se describen luego. Si bien ha crecido mucho más rápido el desarrollo de software que de Hardware, no resulta tan sencillo escapar de los algoritmos cuánticos ya conocidos y estudiados como son el algoritmo de Shor y el algoritmo de Grover. Estos algoritmos, sobre todo el de Shor demuestran el poder de cálculo en paralelo que en el futuro podría realizar una computadora cuántica.

1.6.1. Paralelismo Cuántico

Una definición sencilla de procesamiento paralelo es la habilidad de llevar a cabo múltiples tareas u operaciones simultáneamente.
La necesidad de procesamientos en paralelo se debe a que hay ciertas tareas que no se pueden realizar en tiempos prudenciales con las computadoras actuales. El modelado de una gran cadena de ADN, el pronóstico mundial del tiempo, o el modelado del movimiento de los cuerpos astronómicos son algunos ejemplos.

Hoy en día existen computadoras que incluyen más de un procesador, lo que permite, con los compiladores adecuados, poder realizar software que realice tareas complejas mucho más rápido debido a que se puede asignar a cada procesador distintas tareas menores. Un poder de cálculo aún mayor se logra con los "Sistemas Distribuidos", una colección de computadoras independientes; es decir autónomas, que aparecen ante los usuarios del sistema como una única computadora.

Las computadoras clásicas modernas operan a la enorme velocidad capaz de realizar más de 10^{13} (100 billones, o sea 100 millones de millones) instrucciones lógicas u operaciones aritméticas por segundo, pero su paradigma secuencial implica que estas instrucciones son realizadas una después de la otra, rasgo que se ha mantenido desde la década del 1950. A pesar de que aún no se cuenta con una computadora cuántica capaz de procesar más que unos pocos qubits, la capacidad natural de éstas de procesar datos en paralelo, han despertado el interés en una gran cantidad de investigadores en distintas disciplinas, sobre todo luego de la aparición de poderosos algoritmos que solo pueden ser implementados en computadoras cuánticas y capaces de resolver problemas que clásicamente llevaría años hacerlo.

1.6.2. Algoritmo de Deutsch

El algoritmo de Deutsch es un algoritmo basado en la transformada cuántica de Fourier (QFT). La mayoría de los textos comienzan por explicar este algoritmo debido a que ilustra las ideas claves del paralelismo cuántico y la interferencia cuántica que son utilizadas en todos los algoritmos de mayor utilidad. Al igual que los otros dos algoritmos que se explican posteriormente consta de una compuerta U_f reversible

que "evalúa" una función f y la compuerta de Hadamard $H^{\otimes n}$. En algunos textos se suelen referir a U_f como oráculo y en lugar de decir que se evalúa la función suelen decir que se realiza una consulta al oráculo. De esta forma, la complejidad de los algoritmos se mide por la cantidad de consultas que se hacen al oráculo con el fin de resolver el problema.

El problema de Deutsch se basa en determinar todos los valores de una función $f(x)$, con $f : 0, 1 \to 0, 1$, en un mismo paso de cálculo. El algoritmo ilustra cómo podemos utilizar la interferencia cuántica para obtener esa información global de la función f, y cómo se puede hacer esto de manera más eficiente que lo clásicamente posible.

Supongamos, por ejemplo que queremos evaluar si una función binaria desconocida es constante, ya sea 0 ó 1, o no. Clásicamente tendríamos que aplicar la función dos veces, una con 0 y otra con 1 como entrada. Sin embargo, con el algoritmo cuántico adecuado, una única consulta al oráculo es suficiente. La implementación cuántica del algoritmo de Deutsch se muestra en la fig. 1.5. Como se observa, este circuito tiene dos entradas y dos salidas (la entrada superior es el control y la inferior el target). Una de las entradas se inicializa en $|0\rangle$ y la otra en $|1\rangle$. Ambas entradas son afectadas por la compuerta de Hadamard lo que produce el estado $|\psi_0\rangle$ que ingresa a la compuerta U_f controlada (el oráculo) que se encarga de evaluar la función, $U_f : |x\rangle|y\rangle \to |x\rangle|y \bigoplus f(x)\rangle$. Donde x es la entrada de control e y es la entrada target de la compuerta U controlada. Se puede demostrar que cuando, como en este caso, se ingresa a la compuerta U_f con los dos estados de la base al mismo tiempo, la acción de la compuerta se puede expresar $U_f : |x\rangle(\frac{|0\rangle-|1\rangle}{\sqrt{2}}) \mapsto (-1)^{f(x)}|x\rangle(\frac{|0\rangle-|1\rangle}{\sqrt{2}})$. Debido a

que en este caso en la entrada de control también ingresan ambos estados de la base, el estado del sistema a la entrada de el oráculo es:

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}|0\rangle(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) + \frac{1}{\sqrt{2}}|1\rangle(\frac{|0\rangle - |1\rangle}{\sqrt{2}}), \tag{1.6.1}$$

luego de la aplicación del oráculo el estado del sistema es

$$|\psi_2\rangle = \frac{(-1)^{f(0)}}{\sqrt{2}}|0\rangle(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) + \frac{(-1)^{f(1)}}{\sqrt{2}}|1\rangle(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \tag{1.6.2}$$

Y paso algebraico mediante se obtiene,

$$|\psi_2\rangle = (-1)^{f(0)}(\frac{|0\rangle + (-1)^{f(0)\bigoplus f(1)}|1\rangle}{\sqrt{2}})(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \tag{1.6.3}$$

En el caso de que f sea constante resulta $f(0)\bigoplus f(1) = 0$

$$|\psi_2\rangle = (-1)^{f(0)}(\frac{|0\rangle + |1\rangle}{\sqrt{2}})(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \tag{1.6.4}$$

Luego de la compuerta de Hadamard aplicada sobre el qubit de control el estado del sistema es:

$$|\psi_3\rangle = (-1)^{f(0)}|0\rangle(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \tag{1.6.5}$$

Y por lo tanto, una medición sobre el qubit de control arroja como resultado 0 con probabilidad 1. Sin embargo, si la función es balanceada,$f(0)\bigoplus f(1) = 1$ y el estado a la salida del oráculo resulta,

$$|\psi_2\rangle = (-1)^{f(0)}(\frac{|0\rangle - |1\rangle}{\sqrt{2}})(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \tag{1.6.6}$$

Por último, una aplicación de H sobre el qubit de control,

$$|\psi_3\rangle = (-1)^{f(0)}|1\rangle(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \tag{1.6.7}$$

Si en este caso se mide la línea de control el resultado será 1.

En resumen, el paralelismo cuántico permite que mediante una sola consulta a una caja negra denominada oráculo se resuelva el problema de Deutsch. Si la medición del qubit de control arroja como resultado 0 la función es constante y por el contrario, si el resultado es 1 la función es balanceada.

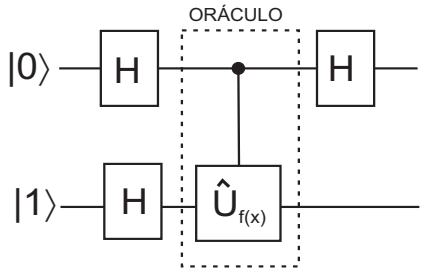

Figura 1.5: Algoritmo de Deutsch. Si la medición del qubit de control arroja como resultado 0 la función es constante y por el contrario, si el resultado es 1 la función es balanceada

1.6.3. Algoritmo de Deutsch-Jozsa

El algoritmo de Deutsch-Jozsa resuelve un problema que es una generalización del problema resuelto por Deutsch. Éste tiene exactamente la misma estructura. Así como en el algoritmo de Deutsch, tiene un circuito reversible (Oráculo) que implementa una función desconocida f, con la salvedad de que este caso f es una función de una cadena de n-bits a un único bit, esto es,$f : \{0,1\}^n \rightarrow \{0,1\}$. El problema aquí es determinar si la función f es constante ($f(x)$ es la misma para todo x) o si está balanceada ($f(x) = 0$ para la mitad de las entradas y $f(x) = 1$ para la otra mitad). La idea no es hacer el análisis detallado de este algoritmo como se hizo con el anterior, sin embargo se hace hincapié en las ventajas de la solución cuántica frente a la clásica. Consideremos inicialmente resolver el problema utilizando un algoritmo clásico. Supongamos que usamos un oráculo para determinar $f(x)$ para exactamente la mitad

de las posibles entradas (hemos hecho 2^{n-1} preguntas a f), y que todas las entradas resultaron ser $f(x) = 0$. A esta altura, podríamos sospechar fuertemente que f es constante. Sin embargo, existe la posibilidad de que si seguimos evaluando f para las restantes 2^{n-1} entradas, esta vez se obtenga $f(x) = 1$, en este caso f estaría balanceada. Por lo tanto,en el peor de los casos, usando un algoritmo clásico no podremos decidir con certeza si f es constante o balanceada evaluando menos de $2^{n-1} + 1$ la función. La propiedad de ser constante o balanceada es una propiedad global de f. Tal como en el problema de Deutsch, un algoritmo cuántico puede tomar ventaja de la superposición y la interferencia cuántica para determinar esta propiedad global de f. El algoritmo de Deutsch-Jozsa determinará si f es constante, o balanceada, haciendo solo una pregunta a la versión cuántica de U_f. Los detalles de funcionamiento se pueden encontrar en [13]. Otros algoritmos tales como el de Simon [30] y de Bernstein-Vazirani [31] sacan provecho del paralelismo cuántico, ambos se basan en el algoritmo de Deutsch-Jozsa.

1.6.4. Algoritmo de Shor

Peter Shor ha demostrado que en un ordenador cuántico se puede implementar un algoritmo de factorización polinómico. Se podría decir que éste marca el final de la seguridad RSA, con la salvedad de que primero se necesita tener a nuestra disposición una computadora cuántica.

En criptografía, RSA (Rivest, Shamir y Adleman) [32] es un sistema criptográfico de clave pública desarrollado en 1977. La seguridad de este sistema reside en la dificultad de encontrar la clave privada a partir de la pública. Descifrar la clave implica factorizar un número n (público) en sus factores primos. Hasta ahora, el método más

eficiente de factorizar grandes números (el algoritmo de Euclides) necesita un tiempo de cómputo que aumenta exponencialmente con el número de dígitos de n, lo que lo convierte en problema NP. Shor, mediante la utilización de la transformada cuántica de Fourier (QFT), resuelve el problema en tiempo polinomial. Dado un número impar n, encontrar un factor propio n se reduce a encontrar el orden de un elemento. Esto es, elegido aleatoriamente un entero positivo m , primo relativo con n , encontrar su orden en Z_n, es decir el menor P tal que $m^P = 1 \mod n$, que a su vez es equivalente a encontrar el período P de la función $f(x) = m^x \mod n$. Es posible encontrar un análisis detallado del algoritmo de Shor en la mayoría de libros relacionados con la computación cuántica e incluso en trabajos específicos tal como el de Eckert-Jozsa [33].

1.6.5. Algoritmo de Grover

El algoritmo cuántico de búsqueda realiza un búsqueda genérica de una solución a un amplio rango de problemas. La idea radica en considerar un problema donde uno puede eficientemente reconocer una buena solución y por lo tanto desea buscar, dentro de una lista de soluciones potenciales con el fin de de encontrar una solución buena. Un ejemplo típico de búsqueda sería reconocer si un entero p es un factor no-trivial de un número N. Un algoritmo sencillo implicaría simplemente buscar dentro de un conjunto $\{2, 3, 4, ..., N\}$ hasta encontrar el factor, pero claro, existe un algoritmo estructurado más eficiente y para nada sencillo que es el mencionado en la sección anterior. Sin embargo, para muchos problemas interesantes no se conocen técnicas que hagan demasiado uso de la estructura del problema y el mejor algoritmo conocido para estos problemas, es el algoritmo de "fuerza bruta" que busca dentro

de un conjunto de soluciones potenciales hasta encontrar una. En general, el número de soluciones potenciales crece exponencialmente con el tamaño del problema, y por esta razón el algoritmo de fuerza bruta no es eficiente. Las mejores búsquedas clásicas conocidas hacen uso, aunque de manera limitada, de la estructura del problema, descartando quizás los candidatos imposibles, o priorizando algunos candidatos más probables, sin embargo la complejidad global de la búsqueda sigue siendo exponencial.

Uno de los mayores sucesos de la computación cuántica resulta ser el algoritmo de búsqueda de Grover. Grover consideró el problema de encontrar un dato "bueno" g, dentro de un conjunto N de soluciones potenciales desordenadas a con $a = \{0, ..., N-1\}$. Utilizando las cualidades inherentes de la computación cuántica, tales como superposición y entanglement, logró desarrollar un algoritmo que disminuye la complejidad de la solución del problema que clásicamente es exponencial a polinomial.

Básicamente, el algoritmo comienza con una superposición uniforme de todos estados $|a\rangle$ que representan a los índices asociados a cada una de las posibles soluciones, considerando, sin riesgo a perder generalidad, que el número de ellas, N, es una potencia de 2. De no cumplirse esta condición se puede extender el espacio de búsqueda al N más próximo que la cumple sin modificar la eficiencia del problema,

$$|\psi_0\rangle \equiv \mathbf{H}|0\rangle \equiv \frac{1}{\sqrt{N}} \sum_{a=0}^{N-1} |a\rangle, \tag{1.6.8}$$

donde $\mathbf{H}$ es la transformación de Walsh-Hadamard. Al igual que en otros de los algoritmos mencionados previamente, se asume que hay un oráculo que evalúa la función $U_f(a)$, siendo $U_f(g) = 1$ para el estado buscado $|g\rangle$, y $U_f(b) = 0$ para cualquiera

de los otros estados $|b\rangle$ (esto es los estados a restantes). La transformación unitaria para encontrar $|g\rangle$ se define generalmente en términos del operador $G_H \equiv -\mathbf{H}S_0\mathbf{H}S_H$, con los operadores inversión $U_R = I - 2|0\rangle\langle 0|$ y $S_H = I - 2\sum_g |g\rangle\langle g|$. Iterando G_H sobre (1.6.8) $\sim O[\sqrt{N}]$ veces se produce un estado cuya amplitud es mayor sobre el ítem buscado $|g\rangle$. Lo que implica que este algoritmo acelera la búsqueda a la raíz cuadrada del tiempo que consume su análogo clásico. Para casos en los que se desean encontrar t items g ó cuando no se conoce la cantidad de items "buenos" de antemano, se puede utilizar un algoritmo de conteo como el propuesto por Shor y luego se aplica este algoritmo de búsqueda que resuelve que este caso resuelve el problema en $O[\sqrt{N/t}]$ pasos [34].

Aunque el algoritmo de Grover fue desarrollado originalmente para que las amplitudes de probabilidad asociadas con el estado inicial tengan una distribución uniforme (1.6.8), trabajos posteriores demostraron que esta condición puede ser relajada de manera que uno pueda trabajar con un estado puro inicial general $|\psi_0\rangle \equiv \mathbf{U}|0\rangle$, lo que implica reemplazar $\mathbf{H}$ por un operador arbitrario $\mathbf{U}$, y luego use el operador $G_H \equiv -\mathbf{U}U_R\mathbf{U}^{-1}U_f$.

Debido a que este algoritmo es una de las herramientas que utilizaremos más adelante, la analizamos de forma más detallada.

El algoritmo se inicializa con n qubits en $|0\rangle$, esto es, $\psi_{ini} = |00.,00\rangle \equiv |0\rangle^{\otimes n}$. El siguiente paso es aplicar una compuerta de Hadamard de $n \times n$ sobre ψ_{ini} para crear un estado $\psi_1 = \frac{1}{\sqrt{N_a}}\sum_{i=0}^{N_a-1}|i\rangle$ superposición de todos los estados de la base. En el mismo paso, se aplica H sobre un qubit auxiliar $|t\rangle$ inicialmente en $|1\rangle$. Los $n+1$ qubits actúan como entradas a una compuerta especial U_f, llamada Oráculo, una caja negra similar a la utilizada por Deutsch y Jozsa, cuyo trabajo es "marcar"

la solución del problema. Los n primeros qubits actúan como líneas de control y el restante es el target.

$$U_f(|a\rangle|q\rangle) = |a\rangle|q \oplus f(a)\rangle \tag{1.6.9}$$

En palabras, como se observa en 1.6.9, la tarea de U_f es evaluar en paralelo todos los ψ_1. Si g es el ítem buscado, entonces $f(g) = 1$, caso contrario $f(a) = 0$. El algoritmo fija el qubit target $|q\rangle$ en $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. El estado del sistema luego de U_f es:

$$|w\rangle(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \longmapsto^{U_f} (-1)^{f(a)}|a\rangle(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \tag{1.6.10}$$

Véase que $|t\rangle$ no sufre modificación ya que es un estado propio.

$$|a\rangle \longmapsto^{U_f} (-1)^{f(a)}|a\rangle \tag{1.6.11}$$

La ecuación 1.6.11 indica que si $f(a) = 1$, esto es cuando $a = g$, se produce un cambio de fase en la amplitud de probabilidad del estado, mientras que si se cumple $a \neq g$ la fase del estado se mantiene. En la figura 1.6.5 se presenta el esquema completo de una iteración de Grover G, que como se puede observar, luego de U_f se aplica $G_R = HU_RH$ que genera una rotación especial alrededor de la media, aumentando la amplitud asociada al dato buscado y disminuyendo las demás. La compuerta G_R consta de dos compuertas Hadamard una a la entrada y otra la salida de una compuerta controlada de rotación de fase U_R.

En la figura 1.6.5 se muestran las distintas modificaciones que sufre el vector de estados inicial, desde la etapa en que existe una distribución uniforme de la amplitud,

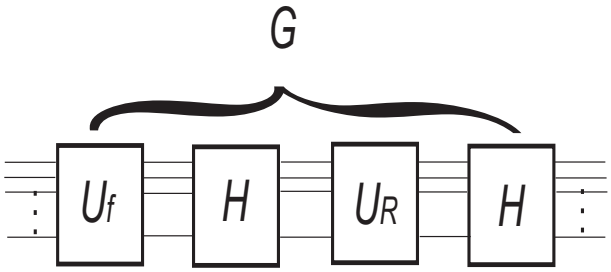

Figura 1.6: Esquema circuital correspondiente a una iteración de Grover

pasando por la inversión de fase del estado correspondiente al índice buscado luego de aplicar U_f en b), la inversión alrededor de la media luego de aplicar G_R en c) y la amplitud resultante luego de una nueva iteración, esto es una nueva aplicación de G, en d), donde se observa que la probabilidad de encontrar el ítem buscado es muy superior a la probabilidad de cualquiera de las otras.

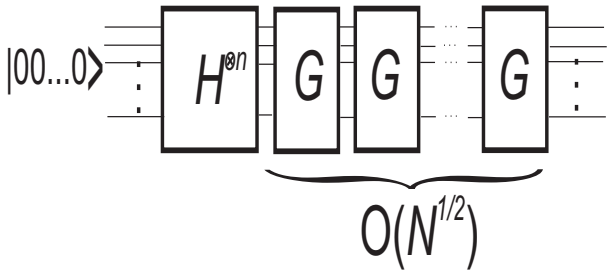

Figura 1.7: Grover Quantum searching algorithm

Se demuestra que luego de aplicar G un número $O(\sqrt{N_w})$ de veces se encuentra el ítem buscado con una probabilidad cercana a 1.

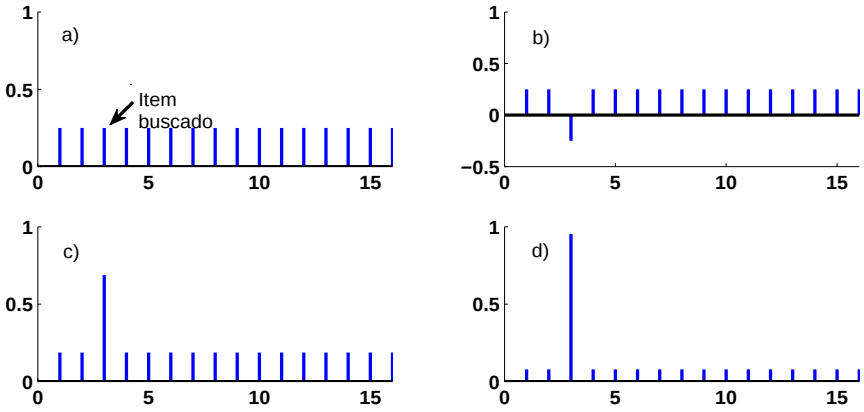

Figura 1.8: Amplitud de probabilidad del estado del sistema en los distintos estadíos del algoritmo de Grover. En a) el estado inicial, en b) luego de U_f, en c) primera inversión alrededor de la media y en d) luego de una nueva aplicación de G

Capítulo 2

Teoría de Juegos

2.1. Introducción

Lo seres humanos no podemos vivir sin interactuar con otros pares, e irónicamente, hemos sobrevivido a pesar de tales interacciones. La producción y el intercambio requieren, en algún nivel, cooperación entre individuos pero es esa misma interacción la que puede llevar, algunas veces, a enfrentamientos desastrosos. Con el afán de predecir el resultado de estos enfrentamientos, tanto en el ámbito social como económico es que surgió una rama de la matemática denominada "teoría de juegos".

Se considera, generalmente, que la teoría de juegos comenzó con la publicación de Von Neumann y Morgenstern "The Theory of Games and Economic Behavior" en 1944. En ese libro se introdujo la idea de que los conflictos se podían analizar mediante modelos matemáticos y proveía la terminología para hacerlo. Sin embargo, años más tarde John Nash, en 1950 con la caracterización del concepto del equilibrio que lleva su nombre, y A. W. Tucker (creador del "Dilema del prisionero"), hicieron grandes contribuciones a la teoría de juegos no-cooperativa.

La teoría de juegos proporciona modelos de situaciones reales, por lo que, frecuentemente, las conclusiones a las que se arriba con dichos modelos, deben considerarse sólo como pautas generales de comportamiento que proporcionarán normas de acción más precisas en tanto que el modelo refleje con más precisión la realidad. Sin embargo, desde la publicación del libro anteriormente citado, la teoría de juegos ha alcanzado un alto grado de sofisticación matemática y ha mostrado una gran versatilidad en la resolución de problemas, de modo que ha demostrado tener el suficiente peso como para ser estudiada como disciplina independiente.

Sus herramientas ayudan a analizar problemas de optimización interactiva. La mayoría de las situaciones estudiadas por la teoría de juegos implican conflictos de intereses, estrategias y trampas. En un juego, varios agentes (o gobiernos, o firmas, etc.) buscan maximizar su utilidad eligiendo determinados cursos de acción. La utilidad final obtenida por cada individuo depende de los cursos de acción escogidos por el resto de los individuos. De particular interés son las situaciones en las que se puede obtener un resultado mejor cuando los agentes cooperan entre sí, que cuando los agentes intentan maximizar sólo su utilidad. Tal el caso de trabajadores y gerentes de una empresa, por ejemplo, quienes tienen intereses opuestos en lo que respecta a los salarios y a las condiciones de trabajo. Es así que existen tanto los sindicatos como las leyes laborales que proveen canales y reglas a través de las cuales se puede abordar cualquier conflicto potencial entre ellos.

Como se mencionó, la teoría de juegos clásica estudia problemas de decisión de

múltiples personas, donde dos o más individuos toman decisiones racionales que influenciarán el bienestar del conjunto. Frecuentemente, la clase de problemas a los que se enfrenta están relacionados con la economía y las ciencias sociales, en temas que van desde problemas de firmas en el mercado a asuntos de política internacional entre naciones. Sin embargo, en los últimos tiempos, sus aplicaciones han alcanzado otras disciplinas en las cuales la toma de decisiones también son de gran importancia. En ciencias de la computación y de las telecomunicaciones, se vienen utilizando las técnicas de la teoría de juegos en diversas áreas, tales como distribución de datos en redes de computadoras o internet [35, 36], competencia en sistemas Cliente-servidor, sistemas peer to peer, [37, 38], seguridad de redes [39], redes de sensores [40], y especialmente la teoría ha sido adoptada en redes inalámbricas para resolver problemas de diseño de protocolos tales como, asignación de recursos, control de potencia, implementación de la cooperación, etc.. La razón para esto radica en la característica desestructurada que estas redes han adquirido, dado que cada nodo toma sus propias decisiones y compite con los otros nodos de forma en pos de obtener la mejor calidad de servicio posible. El principal inconveniente surge debido a que todos los usuarios buscan el mismo fin, lo que obliga a una competencia por los recursos.

Ciertos resultados que se desprenden de la teoría de juegos clásica demuestran que existen ciertos comportamientos de los usuarios racionales que no pueden ser contemplados. Además, cuando la cantidad de jugadores es considerable, la complejidad de los problemas crece exponencialmente. Por estas y otras razones que iremos desarrollando un nuevo marco de análisis donde la base de la teoría de juegos perdure, pero que sume nuevas herramientas resulta adecuado, esto es básicamente el espíritu de la teoría de juegos cuántica.

Los juegos cuánticos son el resultado de relacionar las leyes que rigen la mecánica cuántica con la teoría de juegos clásica. Si bien es una disciplina relativamente joven, el alcance de sus aplicaciones ha crecido rápidamente. La razón principal para este crecimiento es que, a partir del ensayo de David Meyer en 1999 [41], con las contribuciones de Eisert,*et. al* en el mismo año, y otros que los siguieron [42, 43, 44], la teoría de juegos cuántica ha demostrado ser una generalización de la teoría de juegos clásica, donde son posibles nuevos equilibrios y estrategias solamente aplicables bajo leyes cuánticas. Por otra parte, existe una íntima conexión entre la teoría de juegos y la teoría cuántica de las comunicaciones, basta con pensar en que la misión de dos jugadores cualquiera, distantes uno de otro, es principalmente obtener tanta información como les sea posible de una dada situación física con el fin de planear su próxima estrategia. En los juegos de dos o más jugadores donde se introduce información cuántica se abre la posibilidad para un nuevo tipo de estrategia que no se encuentra en los juegos tradicionales. Esto es, las estrategias entangled de los jugadores pueden tener un efecto de "contrato implícito" que previene, ya sea, que los jugadores se beneficien unilateralmente, las traiciones, o bien puede crear una situación cooperativa con el propósito de llegar a un equilibrio global más equitativo.

En lo que sigue de este capítulo, desde el ejemplo, se introducen los principales conceptos de la teoría de juegos, primero desde el punto de vista clásico y luego desde el cuántico.

2.1.1. Juegos

Se denomina juego a la situación interactiva especificada por el conjunto de participantes, los posibles cursos de acción que puede seguir cada participante, y el conjunto de utilidades. Se asume que los participantes poseen cierta racionalidad que los fuerza a elegir con un criterio de maximización de beneficios. Los beneficios no tienen que estar relacionados necesariamente con dinero o fichas, como en el casino por ejemplo. En un ejemplo típico como "La batalla de los sexos", la puja está en que la esposa quiere ir con su esposo al teatro y el esposo quiere ir con su esposa a ver fútbol. En este ejemplo, si ambos se deciden por lo que más les gusta, ambos pierden. No pierden dinero, sino que la recompensa es la satisfacción de estar juntos. Otro ejemplo clásico es el denominado "Gallina" cuyo ejemplo más usado es el que consiste en dos autos enfrentados que se dirigen uno hacia el otro en línea recta y a alta velocidad. Si alguno de los jugadores frena o se desvía pierde, pero si ninguno lo hace ambos pierden, y en tal caso obviamente el dinero es lo de menos. Veamos por ejemplo un posible juego en un problema de telecomunicaciones.

Juego Aloha Ranurado

Se divide el tiempo de transmisión en intervalos. En cada intervalo, un usuario tiene dos posibilidades transmitir (T) o esperar (E). Si solamente un usuario decide transmitir en un determinado intervalo, entonces la transmisión de ese usuario es exitosa. Pero si, por el contrario, múltiples usuarios deciden hacerlo al unísono, entonces todas sus transmisiones son insatisfactorias. Se asume que el pago asociado con una transmisión exitosa es 1, mientras que el costo de transmitir (satisfactorio o no) es c, donde $0 < c < 1$. Un usuario que espera recibe un pago 0; entonces un usuario que

decide transmitir recibe $1 - c$ si la transmisión es exitosa y $-c$ si no logra transmitir. En este juego la meta es el acceso equitativo al medio maximizando la utilidad (en términos de reducción de costos). En redes 802.11, donde la técnica fundamental de acceso al medio es DCF (Función de Coordinación Distribuida), cuando un nodo tiene datos para transmitir, éste decide, de forma autónoma, cuando transmitir, de manera similar a lo que ocurre en el juego Aloha Ranurado. Debido a que el canal inalámbrico es un canal compartido, la transmisión de un nodo usualmente interfiere con la transmisión de otros nodos. De esta manera, si dos nodos vecinos transmiten sus tramas de datos simultáneamente, las transmisiones de ambos fallaran. Por lo tanto, existe una competencia entre los nodos vecinos por transmitir tantos paquetes de datos como les sea posible.

2.1.2. Representación de los juegos

Hay dos formas comunes de representar los juegos, la forma Normal o estratégica y la forma extensiva. En juegos de forma normal, los jugadores mueven simultáneamente. Si el conjunto de estrategias es discreto y finito, el juego puede ser representado por una matriz NxM. En cambio, un juego en forma extensiva especifica el orden completo de movimientos a través de la dirección del juego, generalmente en un árbol de juego. El árbol de juegos es una representación de un juego que describe la estructura temporal. El primer movimiento del juego se identifica con un nodo distintivo que se llama la raíz del juego. Una jugada consiste en una cadena conectada de ramas que comienza en la raíz del árbol y termina, si el juego es finito, en el nodo terminal. Los nodos representan los posibles movimientos en el juego. Las ramas que parten de los

nodos representan las elecciones o acciones disponibles en cada movimiento. A cada nodo distinto del nodo terminal se le asigna el nombre de un jugador de modo que se sabe quién hace la elección en cada movimiento. Cada nodo terminal informa sobre las consecuencias para cada jugador si el juego termina en ese nodo.

2.1.3. Juego estratégico

Un juego estratégico se define como un modelo de toma de decisiones interactivas en el cual los "actores", nombre con que se los conoce usualmente a los jugadores, eligen su plan de acción a la vez, estas elecciones se hacen simultáneamente. El modelo consiste en un conjunto de N jugadores. Para cada jugador existen un conjunto de estrategias o acciones posibles S_i con $i = 1...N$ y una función de pagos $u_i(s_1, s_2, ..., s_N)$ con $i = 1...N$ donde $s_i \in S_i$. La función de pagos mapea el producto cruzado del espacio de estrategias de los jugadores con su conjunto de pagos. Como se puede apreciar, el pago de i a través de u_i no sólo depende de su accionar, sino también del accionar del resto de los jugadores. Esto es lo que diferencia un juego estratégico de un problema de decisión, donde la estrategia depende solo del decisor y el medio que lo rodea. En resumen, un juego se puede denotar por $G(N, S, u)$ donde $S = S_1 \times S_2 \times, ..., S_N$ y $u = u_1 \times u_2 \times, ..., u_N$.

Debido a su alto nivel de abstracción los modelos de juegos se pueden aplicar a una amplia variedad de situaciones. Un jugador puede ser un único ser humano, o cualquier otra entidad que tome decisiones como por ejemplo un gobierno o una mesa de directorio, el líder de un movimiento revolucionario, o bien una flor o un animal, e incluso un nodo en una red de comunicaciones. El modelo no pone restricciones sobre el conjunto de acciones disponibles para los jugadores, por ejemplo, puede contener

desde un conjunto de pocos elementos hasta un enorme conjunto conteniendo planes complicados que cubran una variedad de contingencias. Sin embargo, el rango de aplicaciones del modelo está limitado por el requerimiento de que se debe asociar a cada jugador una relación de preferencias. La relación de preferencia de un jugador puede reflejar simplemente sus sentimientos acerca de los posibles resultados, o en el caso de un organismo que no actúa conscientemente, de las oportunidades de su éxito reproductivo, como puede ocurrir en los sistemas biológicos por ejemplo [45].

2.1.4. Estrategia

Cuando un jugador tiene en cuenta las reacciones de otros jugadores para realizar su elección, se dice que éste tiene una estrategia. Una estrategia es un plan de acciones completo que se lleva a cabo cuando se juega el juego. Se explicita antes de que comience el juego, y prescribe cada decisión que los agentes deben tomar durante el transcurso del juego, dada la información disponible para el agente. La estrategia puede incluir movimientos aleatorios. Para entender de que se tratan las estrategias nada mejor que un ejemplo. Consideremos uno de los juegos más estudiados, el "Dilema del Prisionero": Dos sospechosos de un crimen son puestos en celdas separadas, como no se tiene suficientes pruebas para condenarlos, la policía debe convencerlos de que confiesen. Si ambos confiesan, cada uno será sentenciado a tres años de prisión. Si sólo uno confiesa, el que confiese será liberado y usado como testigo contra el otro, quien recibirá una pena de diez años. Si ninguno confiesa, ambos serán condenados por un cargo menor y tendrán que cumplir una pena de sólo un año de prisión. En resumen, las estrategias posibles que tienen los sospechosos son dos:

- Confesar: El sospechoso opta por traicionar a su compañero. Esta estrategia se

denota aquí con la letra "D".

- Cooperar: El sospechoso decide confiar en su compañero y coopera "C".

Sin embargo, observe que la "suerte" de cada jugador dependerá no solo de su elección sino de la elección del otro competidor. Es muy común representar las posibles estrategias con las respectivas recompensas en una bimatriz. La bimatriz correspondiente a este juego es:

$S_1 \setminus S_2$	D	C
D	3,3	0,10
C	10,0	1,1

Cuadro 2.1: Dilema del Prisionero: D $\equiv$ confesar; C $\equiv$ Cooperar. La cifra de la izquierda de cada celda corresponde a los años de cárcel que debe cumplir el Sospechoso S_1.

2.1.5. Resultado del juego y estabilidad

El resultado de un juego es una cierta asignación de utilidades o pagos (payoff) finales. Se denomina resultado de equilibrio si ningún jugador puede mejorar su utilidad unilateralmente mientras los otros jugadores se mantienen en sus estrategias. Esta situación se conoce como *Equilibrio de Nash* [45] o equilibrio estratégico. Alternativamente, un perfil de estrategias conforma un equilibrio si estas estrategias conforman la mejor respuesta a las otras. Puede suceder que un juego tenga más de un equilibrio de Nash, pero, por otra parte, existen juegos en los que no existe equilibrio estratégico. Un ejemplo interesante para entender la información contenida en el equilibrio de Nash es el juego de ubicación (Location game). Pensemos en n personas que eligen si convertirse o no en un candidato político, y si es así que posición tomar. La distribución de posiciones favoritas está dada por una función densidad f en $[0, 1]$. Un

candidato atrae los votos de un ciudadano cuyas posiciones favoritas están cerca de la suya. Por otra parte, si k candidatos eligen la misma posición, entonces cada uno recibe la fracción $\frac{1}{k}$ de los votos que esa posición atrae. Cada persona prefiere ser el único candidato ganador a un empate por el primer lugar, prefiere empatar en el primer lugar a quedar afuera de la competencia, y prefiere quedar fuera de la competencia que entrar y perder. Cuando $n = 3$ este es un tipo de juego que no tiene equilibrio de Nash. Ningún jugador quiere estar en el medio, ya que los otros jugadores estarán lo más cerca posible del jugador del medio, ya sea desde la izquierda como de la derecha.

Si bien hay muchas maneras diferentes de identificar si una o un conjunto de estrategias son un buen estado de equilibrio, la técnica más común es demostrar que el conjunto de estrategias conforman un Óptimo de Pareto. El equilibrio de Pareto u Óptimo de Pareto es una situación de equilibrio en la cual ningún agente involucrado puede mejorar su situación sin reducir el bienestar de cualquier otro agente. Si bien muchas veces funciona, como se puede apreciar en el siguiente ejemplo del dilema del prisionero, la optimalidad de Pareto suele ser un concepto débil y puede llevar a un analista a resultados erróneos acerca de la conveniencia de elegir determinado estado estable. Este punto se ilustra en un ejemplo sencillo de control de distribución de potencia, pero antes veamos qué sucede en el dilema del prisionero en lo que respecta al equilibrio.

Estabilidad en el juego del Prisionero

Siguiendo con el dilema del prisionero, veamos cuál es la estrategia óptima para cada sospechoso. Si B confiesa, A preferirá confesar, ya que si confiesa obtendrá una pena de 3 años, y si no confiesa obtendrá una pena de 10 años. Si B no confiesa, A preferirá confesar, ya que de este modo será liberado, y si no confesara obtendrá una pena de un año. Entonces, A va a confesar, independientemente de lo que haga B. Análogamente, B también va a confesar independientemente de lo que haga A. Es decir, ambos sospechosos van a confesar y obtener entonces una pena de tres años de prisión cada uno. Éste es el equilibrio estratégico del juego, aunque ineficiente en el sentido de Pareto, ya que se puede reducir la condena de ambos si ninguno confesara.

Un juego sencillo de Distribución de Potencia

Ahora, consideremos un juego de interferencia, por ejemplo el caso de una red inalámbrica de cluster DS-SS que cuenta con un receptor central, y en la cual los nodos restantes ajustan sus niveles de potencia de modo que se maximice su Relación Señal a Ruido mas Interferencia (SNIR) medida en el receptor [46]. Éste es un modelo sencillo pero que resalta las virtudes del modelado del problema en forma de juego. En este caso los jugadores son los nodos de la red (salvando al receptor), el conjunto de acciones son los niveles de potencia disponibles (se supone un número finito de niveles de potencia) y las funciones utilidad de todos los jugadores están dadas por la ecuación 2.1.1, donde p_i es la potencia transmitida por el nodo i, K es una estimación del factor de esparcimiento, h_i es la ganancia (se presume menor que 1) desde el nodo al receptor.

$$u_i(\mathbf{p}) = \frac{h_i p_i}{(1/K)\sum_{k \in N \neq i} h_k p_k} \tag{2.1.1}$$

Dada la característica de los jugadores es de esperar que el único equilibrio de Nash para este juego sea el vector de potencia donde todos los nodos transmiten a su máxima potencia. Sin embargo, este resultado es claramente indeseable debido a tres razones principales (1) la capacidad se ve fuertemente disminuida por el problema cerca-lejos (a menos que los nodos estén todos a la misma distancia del receptor), (2) las SINRs resultantes están distribuidas de forma injusta (el nodo más cercano tendrá una muy superior SINR que el más lejano), y (3) la vida batería se vería considerablemente disminuida. Sin embargo, este resultado es óptimo de Pareto ya que cualquier otra más equitativa distribución de potencia reducirá la utilidad del nodo más cercano, mientras cualquier distribución menos equitativa reducirá la utilidad de los nodos en desventaja. Sobre este escenario la optimalidad de Pareto engaña al analista sobre la conveniencia del resultado. Éste es el ejemplo mas famoso de las situaciones en la que los equilibrios no-cooperativos pueden llevar a resultados ineficientes. La situación que se presenta en los cárteles se puede modelar como un dilema del prisionero. En un cártel, las empresas coalicionan para reducir su producción y así poder aumentar el precio. Sin embargo, cada empresa tiene incentivos para producir mas de lo que fijaba el acuerdo y de este modo obtener mayores beneficios. Por otra parte, si cada una de las firmas hace lo mismo, el precio va a disminuir, lo que resultará en menores beneficios para cada una de las firmas. La misma estructura de interacciones caracteriza el problema de la provisión de bienes públicos (problema del free rider), y del pago voluntario de impuestos. Como se analizará más adelante, también el problema del prisionero surge en redes de telecomunicaciones.

2.1.6. Estrategias puras y mixtas

Un estrategia pura se define como aquella que especifica por adelantado todo lo que el jugador debe hacer. Por otra parte, podemos expandir un juego y permitir que las elecciones de los jugadores sean no-deterministas.

En un juego finito en forma estratégica $G = (N, (S_i)_{i\in N}, (u_i)_{i\in N})$, *una estrategia mixta del jugador* i es una distribución de probabilidad sobre el conjunto de estrategias puras S_i. Al conjunto de todas las estrategias mixtas i del jugador lo denotamos por Δ_i. Para $\sigma_i \in \Delta_i$ y $s_i \in S_i$, $\sigma_i(s_i)$ es la probabilidad que la distribución σ_i le asigna a la estrategia s_i. El *soporte* de una estrategia mixta σ_i es el conjunto de estrategias puras a las cuales σ_i le asigna una probabilidad *estrictamente positiva*.

De acuerdo con la definición anterior, es claro que el conjunto de estrategias mixtas contiene al de las estrategias puras. En este caso, cada σ_i le asigna probabilidad 1 a cierta estrategia pura y probabilidad 0 a las demás estrategias.

Utilidad esperada

Sea $G = (N, (S_i)_{i\in N}, (u_i)_{i\in N})$ un juego finito en forma estratégica. Dado un perfil de distribuciones $\sigma_i = (\sigma_1, ..., \sigma_n) \in \times_{i=1}^{n}$, la *utilidad esperada* del jugador i asociada a este perfil es:

$$u_i(\sigma) = \sum_{s\in S}(\times_{j=1}^{n}\sigma_j(s_j)u_i(s)) \tag{2.1.2}$$

De esta forma, la utilidad esperada de un jugador tiene la misma naturaleza que un valor esperado (matemático); es decir, corresponde a una suma ponderada de todas la utilidades que puede alcanzar el jugador, donde la ponderación de cada una de éstas es la probabilidad de ocurrencia del resultado que genera tales pagos.

En el ejemplo del prisionero, las estrategias D y C son las estrategias puras. Por ejemplo, si el sospechoso S_1 decide si cooperará o no por medio del lanzamiento de una moneda entonces, suponiendo que la moneda no esté cargada, la probabilidad de que coopere es del 50 %. Un equilibrio en el que todos los jugadores usan una estrategia pura es un equilibrio en estrategias puras. En cambio, si al menos uno de ellos utiliza estrategia mixta, el equilibrio es un equilibrio en estrategias mixtas. Veamos un ejemplo más general.

Ejemplo(Un cálculo de Utilidades Esperadas) Analicemos un ejemplo el cuál tiene la distribución de utilidades que se muestra en 2.2. Dado que ningún agente tiene certeza de la elección de su oponente, cada uno de ellos debe asignar probabilidades a las estrategias de acuerdo con sus creencias. Como se observa en la tabla, el jugador 1 puede asignar una probabilidad q a la estrategia x_2 del jugador 2 y por consiguiente, una probabilidad (1-q) a la estrategia y_2. De igual forma, el jugador 2 asigna una probabilidad p a la estrategia x_1 del jugador 1 y una probabilidad $1-p$ a la estrategia y_1.

Esta estrategia mixta del juego es, entonces, $(p[x_1]+(1-p)[y_1], q[x_2]+(1-q)[y_2])$. Por consiguiente, la utilidad esperada del jugador 1 de su estrategia x_1 es $3q+5(1-q)$. De la misma forma, el pago esperado de su estrategia y_1 es $4q + 2(1 - q)$. Similarmente, para el jugador 2, la utilidad esperada de su estrategia x_2 es $2p + 1(1 - p)$ y de su estrategia y_2 es $p + 3(1 - p)$. De manera que los pagos de los jugadores asociados a la estrategia mixta (σ_1, σ_2), donde $\sigma_1 = (p, 1 - p)$, $\sigma_2 = (q, 1 - q)$ son:

Jugador 1:

$$p(3q + 5(1 - q)) + (1 - p)(4q + 2(1 - q)) = 2 - 2pq + 5p - 2q^2$$

Jugador 2:

$$q(2p) + (1-p) + (1-q)(p + 3(1-p)) = 3 + 3pq - 2q - 2p$$

$J_1 \setminus J_2$	(q) x_2	$(1-q)$ y_2
(p) x_1	3,2	5,1
$(1-p)$ x_2	4,1	2,3

Cuadro 2.2: Lanzar la moneda

2.1.7. Juegos NxM

Los juegos denominados $N \times M$ son juegos de dos jugadores, en los cuales un jugador tiene N acciones posibles y el otro tiene M acciones posibles. En un juego así, los pares de utilidades o pagos pueden ser representados también en una matriz y de esta forma ser fácilmente analizable. Es lógico que juegos de este tipo traigan consigo una complejidad inherente que implique en la mayoría de los casos la necesidad de mucho poder de cálculo. El problema del bandido con M armas, que se explicará más adelante, se puede considerar, por ejemplo, como un juego $1 \times M$, una aplicación interesante a las redes inalámbricas se puede encontrar en [47]. Es más, el problema de los matrimonios [48], donde M hombres buscan una mujer de entre un grupo de N candidatas que también tienen acción, puede ser modelado por un problema del bandido bi-direccional $N \times M$ [49, 50].

2.1.8. Estrategia dominante

Una estrategia dominante es la que hace que un jugador esté mejor que si hubiera usado cualquier otra estrategia, sin importar cuál haya sido la estrategia elegida por

el otro jugador. Si cada jugador tiene una estrategia dominante se puede predecir el resultado del juego. Si un jugador no tiene una estrategia dominante pero el oponente sí la tiene, hay que anticipar que el oponente va a usar esa estrategia y elegir la jugada propia de acuerdo a ese supuesto.

2.1.9. Juegos de suma constante

Juegos en los que para cada combinación de estrategias, la suma de los pagos (o utilidades) que recibe cada jugador es la misma. Todas las situaciones de intercambio que no permiten la creación o destrucción de recursos son juegos de suma constante. Los más comunes son los juegos de suma cero, en los cuales los intereses de los jugadores son contrapuestos y por lo tanto la ganancia que reciben unos se equilibra con la pérdida de los otros. El juego del ajedrez es un clásico ejemplo de juego de suma cero.

2.1.10. Juego repetido

En un juego repetido un grupo fijo de jugadores juega un juego dado repetidamente, observando el resultado de todas las jugadas pasadas antes que comience la siguiente jugada. La posibilidad de observar las acciones y los resultados pasados antes de que comience la siguiente jugada permite que los jugadores padezcan o premien las acciones pasadas, de modo que surgen estrategias que no surgirían en los juegos simples no repetidos. Por ejemplo, repitiendo el juego del dilema del prisionero un número desconocido de veces suficiente grande se puede dar como resultado un equilibrio en el cual ambos prisioneros nunca confiesan.

2.2. Teoría de Juegos Cuántica

Los orígenes de la teoría de juegos cuántica radican en dos disciplinas que en principio parecerían tan disconexas como la teoría de juegos clásica y la mecánica cuántica. Los juegos cuánticos proveen nuevas formas de cooperar, de eliminar dilemas, y de alterar equilibrios. Actualmente hay muchos trabajos sobre modelos de juegos cuánticos y aplicaciones de las más variadas. Sin embargo, los dos trabajos iniciales más importantes son los realizados por Meyer y Eisert *et al*, [41] y [51] respectivamente. El primero mostró que si en el juego clásico de lanzar la moneda, se le permite a un jugador utilizar estrategias cuánticas, y el otro jugador juega clásico, el primero gana siempre. En el segundo trabajo los autores demuestran que mediante la utilización de estrategias cuánticas es posible eliminar el dilema en el "Dilema del prisionero". En esta sección, se describen las principales características de la teoría de juegos cuántica, ver [52].

Dado que los juegos cuánticos son una extensión de los juegos clásicos, siguiendo con la notación utilizada en estos últimos, un juego cuántico está definido por $G\{N, \Theta(\mathbb{H}), \psi_0, S, u\}$, donde N es el número de jugadores, $\Theta(\mathbb{H})$ es el espacio de estados del juego definidos en un espacio bidimensional de Hilbert $\mathbb{H}$. A diferencia de lo que ocurre en los juegos clásicos, en los juegos cuánticos es necesario definir un estado inicial $\psi_0 \in \Theta(\mathbb{H})$, $S = S_1 \bigotimes ... \bigotimes S_N$ es el espacio de estrategias [1], y u es la función de utilidad, donde $u_i : \Theta(\mathbb{H}) \rightarrow \Re$. En los juegos cuánticos, el estado del juego está representado por un qubit o de forma más general, por el producto tensorial de múltiples qubits.

[1] El símbolo $\bigotimes$ denota el producto tensorial de los espacios

2.2.1. Desarrollo de un juego cuántico: Las estrategias de los jugadores

Comencemos aquí a describir de forma general como se desarrolla un juego cuántico. A cada jugador se le asigna uno o más qubits cuyo estado a tiempo cero es el estado inicial. Por medio de una operación local sobre su o sus qubits, el jugador podrá modificar el estado, así obteniendo un vector de estado final. La decisión de cambiar o no su estado depende de la estrategia de cada jugador. Por lo tanto, los operadores que actúan sobre los estados iniciales y que consecuentemente producen las transformaciones, corresponden a las tácticas o estrategias de los jugadores. Por ejemplo, en un juego sencillo de dos jugadores, supongamos que U_1 y U_2 son las transformaciones unitarias que son aplicadas por los jugadores. Estas transformaciones son aplicadas simultáneamente en el caso de un juego estático, ó de forma secuencial en un juego dinámico. En algunas ocasiones puede que exista un referee encargado de preparar el estado inicial del sistema $\psi_0 \in \Theta(\mathbb{H})$ (que generalmente es el estado puro $|00..,0\rangle$) aplicando una operación U_r que transforma a ψ_0 en un nuevo estado, que por ejemplo, podría ser un estado entangled. En tal caso, luego del movimiento de los jugadores el referee debe aplicar $U_r^\dagger$ para deshacer la aplicación inicial de U_r. Por último, se debe hacer la medición para revelar el estado final del juego 2.1. El valor esperado de cada jugador se debe evaluar calculando primero el módulo cuadrado de las proyecciones del estado cuántico final sobre el espacio de vectores base, y luego sumar los números obtenidos pesados por los coeficientes de pago.

Habiendo asignado una estructura de Hilbert al espacio de estrategias de cada

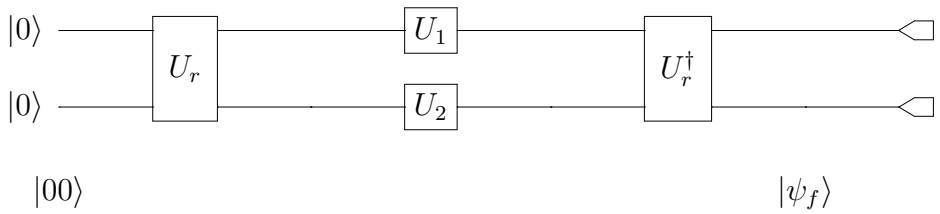

Figura 2.1: Modelo básico de juego cuántico

jugador, es natural describir sus mutuas elecciones como vectores de estado pertenecientes al producto tensorial de sus espacios de Hilbert, este tipo de estrategias se denominan factorizables. Sin embargo, en los juegos cuánticos, se pueden construir estrategias entangled, las cuales no pueden ser descompuestas como productos tensoriales y no se pueden reducir a las anteriores por medio de transformaciones locales solamente. Es a causa de esta estructura más rica, que la Teoría de juegos cuánticos exhibe características más atractivas que la versión clásica.

Con el objeto de ayudar a la comprensión de los componentes principales que conforman un juego cuántico y sus aportes, se presentan aquí dos de los juegos cuánticos más famosos, el primero es el juego de la moneda de Meyer y el segundo es Dilema del prisionero de Eisert *et al.*, que ya fue presentado en secciones anteriores en su versión clásica.

El juego de la moneda clásico consiste en cuatro pasos: En el primer paso el referee coloca la moneda en una caja con la *cara* hacia arriba. En el paso siguiente el señor Q da vuelta la moneda (F) o la deja como está (N). En el paso siguiente el señor P da vuelta la moneda (F) o la deja como está (N). Luego Q realiza el último movimiento, dando vuelta la moneda (F) o dejándola como estaba (N). Cabe aclarar que ninguno conoce el movimiento del otro. Finalmente se abre la caja y si la moneda quedó *cara*

hacia arriba Q gana y recibe un pago $+1$ y P pierde por lo que recibe -1, por el contrario, si la moneda queda *cara* hacia abajo el que gana $+1$ es P y Q pierde y recibe -1.

Veamos ahora una versión cuántica de este mismo juego en el cual se le permite a Q utilizar estrategias cuánticas mientras P solo tiene permitido utilizar estrategias clásicas. En este modelo la cara de la moneda se representa $|0\rangle$ y la cruz esta representada por $|1\rangle$. El estado inicial del sistema es $|0\rangle$. Los movimientos clásicos P se pueden representar por medio del operador identidad I si deja la moneda en la mismo estado ó el operador X que la da vuelta. Por otra parte, como Q tiene permitido jugar cuántico, puede utilizar cualquier operador unitario, en este caso elige utilizar el operador de Hadamard H en las dos oportunidades que le toca jugar. Cuando Q juega H deja el sistema en una superposición, esto es $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, por lo tanto, indistintamente de lo que haga P (X ó I) el estado del sistema no cambia. Luego Q aplica H nuevamente y el estado final es $|0\rangle$. De esta forma, Q siempre gana. En resumen, la utilización de una estrategia cuántica le permite a Q dejar el sistema en un estado que no puede ser alterado por P, lo que le garantiza ganar siempre.

Como se analizó anteriormente, el juego del prisionero clásico tiene un equilibrio de Nash, en el que ambos sospechosos confiesan, pero este no es un equilibrio óptimo, ya que si ambos eligieran no confesar la condición de ambos mejoraría, es decir que tendrían que pasar menos años en la cárcel por falta de pruebas. En la versión cuántica del prisionero de Eisert, el dilema se termina. En notación cuántica, se relacionan las dos posibles soluciones clásicas del problema (confesar) D ó (cooperar) C con dos estados base $|D\rangle$ y $|C\rangle$ de un espacio de Hilbert de dos estados, como por ejemplo un qubit. Por lo tanto el estado completo del juego queda definido por los cuatro

posibles resultados del juego clásico $\{|CC\rangle, |CD\rangle, |DC\rangle, |DD\rangle\}$ donde la primera y la segunda entrada corresponden a la elección del sospechoso S_1 y el sospechoso S_2 respectivamente. El estado inicial del sistema se define $\psi_0 = \widehat{J}|CC\rangle$, donde $\widehat{J}$ es un operador unitario conocido por ambos jugadores

$$J = \begin{pmatrix} \cos(\gamma/2) & 0 & 0 & i\sin(\gamma/2) \\ 0 & \cos(\gamma/2) & -i\sin(\gamma/2) & 0 \\ 0 & -i\sin(\gamma/2) & \cos(\gamma/2) & 0 \\ i\sin(\gamma/2) & 0 & 0 & \cos(\gamma/2) \end{pmatrix} \tag{2.2.1}$$

con $\gamma = [0, \pi/2]$. La compuerta J produce un estado entangled cuando $\gamma = \pi/2$, mientras que para $\gamma = 0$ el entanglement es nulo y se dice que el juego es separable. Las estrategias de los jugadores S_1 y S_2 están representadas por operadores unitarios U_{S_1} y U_{S_2} respectivamente, tomados de un espacio de estrategias S. Dado que los operadores U_{S_1} y U_{S_2} son exclusivos de S_1 y S_2, solo actúan sobre los qubits asociados a ellos, por lo tanto el espacio S se define por un conjunto de operadores unitarios 2×2. El estado del sistema, luego del movimiento de ambos jugadores queda $(U_{S_1} \otimes U_{S_2})|\psi_0\rangle$. Finalmente, se debe aplicar $\widehat{J}^\dagger$ para sacar el juego del estado entangled de modo que se pueda separar los estados de los jugadores y así poder medirlos. Por lo tanto, antes de la detección, el estado del juego es:

$$|\psi_f\rangle = \widehat{J}^\dagger (U_{S_1} \otimes U_{S_2}) \widehat{J}|CC\rangle \tag{2.2.2}$$

y luego de la detección, el sistema colapsa a uno de los cuatro estados de la base. En consecuencia, la recompensa que obtienen es la correspondiente a la matriz de pagos clásica. El pago promedio para S_1 se define como

$$\$_{S_1} = 1P_{CC} + 10P_{CD} + 0P_{DC} + 3P_{DD}, \tag{2.2.3}$$

donde P_{CD}, por ejemplo, es el módulo cuadrado de la proyección del estado $|\psi_f\rangle$ sobre el estado de la base $|CD\rangle$, esto es, $P_{CD} = |\langle CD|\psi_f\rangle|^2$. El pago de S_2 se obtiene cambiando $0 \leftrightarrow 10$ y $10 \leftrightarrow 0$ en 2.2.3. Note, que en este caso, como el pago corresponde a años de cárcel, el objetivo de los sospechosos es minimizar S_i.

Las estrategias de los jugadores quedan determinadas por un conjunto de matrices unitarias que dependen de solo dos parámetros,

$$\widehat{U}(\theta,\phi) = \begin{pmatrix} e^{i\phi}\cos(\theta/2) & \sin(\theta/2) \\ -\sin(\theta/2) & e^{i\phi}\cos(\theta/2) \end{pmatrix} \tag{2.2.4}$$

donde $0 \leq \theta \leq \pi$ y $0 \leq \phi \leq \pi/2$. De esta forma, quedan asociadas las estrategias clásicas "No Confesar" ,y cooperar con su socio, con el operador,

$$\widehat{C} = \widehat{U}(0,0) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{2.2.5}$$

y la estrategia "Confesar" , y entonces traicionar a su compañero, queda determinada por el operador

$$\widehat{D} = \widehat{U}(\pi,0) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \tag{2.2.6}$$

Se demuestra en [51], que si en la conformación del estado inicial $\gamma = 0$, el resultado del juego es el mismo que en la versión clásica, en cambio si $\gamma = \pi/2$ lo que implica un estado inicial completamente entangled, el dilema se termina. Esto quiere decir que el equilibrio del sistema ya no es $\widehat{C} \otimes \widehat{C}$, que como sabemos no es óptimo, sino que existe un equilibrio $\widehat{Q} \otimes \widehat{Q}$ que sí es óptimo ya que no hay estrategia $\widehat{U}(\theta,\phi)$ que mejore la condición de uno de los jugadores sin desmejorar la del otro.

$$\widehat{Q} = \widehat{U}(0,\pi/2) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \tag{2.2.7}$$

La condena que deben cumplir ambos prisioneros en este caso es de 1 año y no 3. Como conclusión se puede observar que nuevamente una propiedad única de los sistemas cuánticos como es el entanglement permite mejorar el resultado de un juego clásico. El resultado es más importante aún si se considera que el modelo del prisionero tiene aplicaciones en areas diversas como la economía, sociología y hasta la ingeniería.

2.3. Bandido de multiple brazos

El problema del bandido con múltiples brazos, originalmente descrito por Robbins [53], es un modelo estadístico de decisión de los más ampliamente usados para el estudio de la adquisición de información y "aprendizaje" por agentes económicos [54]. El factor más importante para que esto ocurra es el grado considerable de maleabilidad que poseen incluso las formulaciones más generales de problemas dentro de este marco. Su nombre procede de pensarlo como un jugador que frente a un grupo de máquinas tragamonedas debe decidir en cual máquina jugar en una secuencia de intentos de modo que se maximice su ganancia. El agente tratará de optimizar su decisiones al tiempo que mejora su información. Existe una importante cantidad de aplicaciones relacionadas con economía y ligadas a ella y se debe a su simplicidad y a que modela de forma concisa la negociación entre "exploración" (probando diferentes brazos en busca del mejor) y la "explotación" (eligiendo el brazo que se cree que da la mejor recompensa).

Ejemplos prácticos del problema del bandido incluyen desde *Ensayos Clínicos* donde se debe experimentar con diferentes tratamientos mientras se minimizan los riesgos para los pacientes, hasta *Ruteo o Encaminamiento Adaptativo* para minimizar los retardos en una red. En el contexto de las telecomunicaciones, más precisamente en

lo que respecta a problemas de acceso dinámico al espectro, el bandido con múltiples brazos resulta adecuado para modelar la toma de decisiones en dispositivos de radio cognitiva [47]. La utilización de reglas de la mecánica cuántica a la gestión de recursos en dispositivos móviles inteligentes podría permitir una mayor eficiencia en la elección de los canales libres y/o la potencia a ser utilizada. En consecuencia, propone aquí un modelo cuántico del problema del bandido como una, y no la única opción para administrar los recursos de los dispositivos que componen una eventual red de comunicaciones inalámbrica. En el capítulo siguiente se analiza en detalle esta aplicación, pero antes, en la sección siguiente se realiza una presentación formal del modelo cuántico del bandido.

2.3.1. Modelo cuántico de bandido con múltiples brazos

El modelo cuántico del bandido utiliza las propiedades de la mecánica cuántica. Esto permite a los jugadores utilizar novedosas estrategias cooperativas y no-cooperativas basadas en el fenómeno de entanglement, o jugar con varias palancas al mismo tiempo amparados por el principio de superposición. Utilizando este modelo, y como parte de esta tesis, se analizó el problema del mercado de citas. En tal caso, el problema del bandido toma carácter bi-direccional ya que existen dos grupos, hombres y mujeres. Los hombres eligen mujeres del grupo que llamamos W, pero a diferencia de lo que ocurre en el bandido convencional, las mujeres eligen si aceptar o no las propuestas de los hombres del grupo M, lo que aumenta la complejidad del problema y el tiempo necesario para arribar al equilibrio. Si solo algunos jugadores utilizan estrategias cuánticas, estos tienen ventajas en juego frente a los que solo juegan clásico [1, 2]. Por otra parte, la cuantización del problema permite acelerar los

tiempos a causa del procesamiento paralelo natural de la computación cuántica.

En otro contexto los jugadores pueden ser productores y consumidores, empleadores y quienes buscan empleo, determinados recursos y los lugares donde ubicarlos, o usuarios secundarios de una red inalámbrica y la banda a la que quieren acceder. El mercado de citas se usa como ejemplo sencillo y fácil de entender, sin embargo, la importancia de estudiar modelos de matching en esta tesis se debe a sus amplias aplicaciones en el contexto de las telecomunicaciones. Por último, la cuantización del problema pretende optimizar los resultados obtenidos a través del modelo clásico. La selección dinámica de canal es un componente importante de los sistemas multi-canal inalámbricos. Esta permite que un transmisor identifique el canal que ofrece las mejores condiciones de radio y que evite la interferencia creada por otros transmisores. En ausencia de interferencia, el problema de selección de canales se puede interpretar como un problema de bandido con múltiples brazos.

Capítulo 3

Teoría de la decisión

3.1. Introducción

La vida cotidiana está colmada de situaciones en las cuales el ser humano toma decisiones, incluso en ocasiones sin darse cuenta, desde que nos levantamos, cuando decidimos como vestirnos por ejemplo hasta el último minuto del día donde debemos decidir el momento en el que nos vamos a ir a dormir. Casi todo lo que un ser humano hace involucra decisiones. Por lo tanto, teorizar acerca de las decisiones es casi como teorizar acerca de las actividades del ser humano.

La Teoría de la Decisión trata del estudio de los procesos de toma de decisiones desde una perspectiva racional. Es el análisis del comportamiento de un individuo frente a una incertidumbre no-estratégica, esto es, la incertidumbre que proviene de lo que llamamos "Naturaleza"(un evento estocástico natural como el lanzamiento de una moneda, la pérdida de cosecha estacional, enfermedad personal, y causas similares),o, en caso de que haya otros individuos involucrados, los comportamientos de estos son tratados como distribuciones estadísticas conocidas por el tomador de decisiones(TD)o

decisor [1]. De acuerdo con esto, el resultado (rendimiento) de una decisión individual depende de la acción de otro agente (naturaleza) sobre el cual no se tiene control. Es importante observar que en este modelo los rendimientos afectan únicamente a quien toma la decisión.

La decisión es un verdadero proceso de reflexión y, como tal, racional y consciente, deliberado y deliberativo. El TD debe identificar cuáles son las decisiones óptimas y como alcanzarlas. Básicamente son problemas con respuestas de "si" o "no". Como tradicionalmente es un área que pertenece a la matemática discreta, las preguntas se responden por medio de una función binaria con valores $\{0, 1\}$.

Desde mediados del siglo XX, la teoría de las decisiones moderna se ha desarrollado producto de la contribución de diversas disciplinas académicas, tales como economía, estadística, psicología, política, sociología y filosofía. Como consecuencia, actualmente, es claramente una asignatura académica con todos sus derechos. A pesar de que el concepto de decisión parece sencillo, no está tan unificado y por lo tanto no existe una única línea de investigación en materia de decisiones,[55].

Si bien la mayoría de los problemas de decisión involucran seres humanos completamente informados y racionales, algunos conceptos teóricos de la teoría de las decisiones se ajustan perfectamente a cualquier clase de tomador de decisiones, esto puede ser una computadora, un celular, o cualquier dispositivo "inteligente" programado para que, basándose en su interacción con el entorno, pueda seleccionar una

[1] El Decisor es el encargado de realizar la selección de alternativas de la mejor manera, en función de sus objetivos

opción de entre un conjunto de posibilidades. Es más, esa suposición de que los hombres son racionales ha sido cuestionada de forma temprana con la evidencia provista por la paradoja de *Allais* [56] y muchas otras paradojas de comportamiento [57], mostrando que los humanos a menudo parecen desviarse de la prescripción de racionalidad de la teoría de las decisiones debido a prejuicios cognitivos y emocionales. Por lo tanto, cuando se lo pone en frente de situaciones que parecen muy similares, sus decisiones pueden ser totalmente diferentes de lo que uno esperaría.

La teoría de juegos y la teoría de la decisión tienen muchos puntos en común, sin embargo la teoría de juegos estudia decisiones en entornos en donde hay interacción. Es decir, que estudia la elección de la estrategia óptima cuando los costos y los beneficios de cada opción no están fijados de antemano, sino que dependen de las elecciones de otros individuos.

3.1.1. Teoría cuántica de la decisión

Fenómenos ampliamente observados de no conmutatividad en patrones de comportamiento exhibidos en experimentos donde seres humanos deben tomar decisiones y realizar elecciones, no se pueden obtener con la teoría de decisión clásica [58] pero pueden ser descritos adecuadamente mediante la unión de la mecánica cuántica y la teoría de decisión. Estas dos teorías han sido combinadas recientemente [58, 59, 60] para tener en cuenta la indeterminación de las preferencias que se determinan solamente cuando la acción tiene lugar. Un agente se describe por medio de un estado que es una superposición de las preferencias potenciales con el propósito de ser proyectado sobre uno de los posibles comportamientos al momento de la interacción. Además del

principal objetivo de modelar la incerteza en las preferencias que no es debida a la falta de información, este formalismo parece ser adecuado para describir fenómenos ampliamente observados de no conmutatividad en patrones de comportamiento.
La inclusión de la cuántica en la toma de decisiones permite el desarrollo de una teoría unificada que puede formalizar el proceso de toma de decisiones no solo por parte de un ser humano en términos de lenguaje cuántico sino también de un sistema cuántico que se pudiera emplear para crear inteligencia artificial [59].

Con el propósito de precisar la matemática del problema es conveniente comenzar con algunas definiciones. Por ejemplo, el ente que toma las decisiones podría ser un ser humano, una sociedad, una computadora, o cualquier tipo de sistema o dispositivo electrónico programado para tomar decisiones.
El proceso de tomar una decisión implica que uno delibere entre varias acciones posibles con diferentes resultados, con el fin de decidir cuál de las acciones elegir. Las acciones posibles se pueden enumerar por un índice $i = 1, 2, ...N$ donde N es el número total de acciones. Sea $\mathcal{A}$ el conjunto de las posibles acciones, donde

$$\mathcal{A} \equiv \{A_i : i = 1, 2, ..., N\} \tag{3.1.1}$$

En el mercado de citas por ejemplo la acción A para un hombre se puede relacionar con la intención "Elegir una mujer", por lo tanto el índice i indica a cuál de las opciones del grupo A elige. A cada acción A_i le corresponde un estado $|A_i\rangle$ en un espacio de Hilbert, que es una función compleja cuyo conjugado hermítico es $\langle A_i|$. Se asume aquí que el producto escalar está definido, tal que los estados de las acciones son ortogonales:

$$\langle A_i|A_j\rangle = \delta_{ij} \tag{3.1.2}$$

El estado de la elección, en general está compuesto por una combinación lineal de las

distintas acciones posibles

$$|\psi\rangle = \sum_i \alpha_i |A_i\rangle \tag{3.1.3}$$

Los coeficientes α_i son definidos por el que toma las decisiones, de manera que $|\alpha_i|^2$ le asigna un peso a la decisión $|A_i\rangle$. La estrategia de cada uno de los "actores" en un problema de decisión estará determinada por los pesos que ellos les asignen a cada una de las estrategias.

3.2. Problemas de Correspondencia: Mercado de citas

Los problemas de correspondencia (matching problems) tienen amplias aplicaciones en contextos sociales y de economía [61, 62]. Como posibles aplicaciones se puede pensar en empleadores-buscadores de empleo, inquilinos-propietarios, hombres y mujeres que buscan una cita [50, 49] o ciliados solitarios y los rituales de cortejo [63]. El futuro no muy lejano de las redes de comunicaciones inalámbricas exige dispositivos celulares capaces de decidir por sí solos la banda del espectro donde transmitir, la potencia de transmisión, e incluso aprender los usos y costumbres de los usuarios. Con ellos llegarán los conflictos de intereses, y las decisiones tomadas por cada uno de ellos estará condicionada por las variables del entorno, donde una de esas variables será la cantidad de usuarios intentando utilizar las mismas bandas. Estos problemas resultan ideales para ser modelados como problemas de decisión, o de forma particular en problemas de matching entre los dispositivos y los posibles recursos a los que aspiran [64, 65].

El problema del matrimonio estable, quizás el primer modelo de matching, fue presentado por Gale and Shapley hace casi cinco décadas [48]. Este asume que cada agente conoce sus preferencias sobre los individuos en el otro extremo del mercado. Si bien, la suposición de información perfecta está lejos de ser una buena aproximación para los mercados, debido a su generalidad, el modelo sigue hoy en día vigente [66]. A pesar de que el modelo metafórico del casamiento entre hombres y mujeres es subjetivo, la importancia de los modelos de matching radica, para nosotros, en sus amplias aplicaciones en contexto de la teoría de las comunicaciones,[67]. Fundamentalmente los problemas de asignación de recursos se caracterizan por un conjunto de recursos y un conjunto de demandas. En ese contexto, cada recurso puede tener una utilidad diferente para cada demanda y el objetivo es típicamente encontrar una asignación entre dos conjuntos de modo que la utilidad se maximice.

El problema del mercado de citas, se enmarca dentro de esta clase de situaciones y se formula de la siguiente manera: Suponga un grupo M de hombres que quieren una cita con alguna mujer de un conjunto S. Cada hombre tiene estrictas preferencias por cada una de las mujeres. De manera similar, cada mujer también tiene una estricta preferencia por cada uno de los hombres. Por otra parte, si un hombre consigue una cita, el recibe una recompensa (afectiva, monetaria, etc.) cuyo "monto" depende de la mujer elegida, y la mujer por su parte también recibe una recompensa acorde con el hombre con el que aceptó salir. La pregunta clave es si existe un conjunto estable de parejas tal que ningún hombre ni mujer tienen un incentivo como para cambiar de compañero la próxima cita. En el contexto de las telecomunicaciones sería, ¿Estarán satisfechos transmisor y receptor de la calidad de comunicación que están teniendo?

o deberán cambiar de banda, transmitir con más potencia, etc.

Motivados por los aportes de la mecánica cuántica a la resolución eficaz de problemas complejos diversos, se realizó un una versión cuántica del mercado de citas, con el propósito de estudiar su desempeño en problemas de matching [2]. A diferencia del juego tradicional, en la versión cuántica los jugadores tienen la posibilidad de utilizar técnicas de la mecánica cuántica, como por ejemplo utilizar un algoritmo de búsqueda cuántico para explorar de manera eficiente sus posibilidades.
Con el objeto de estudiar las propiedades que caracterizan la estabilidad del modelo se estudió el comportamiento estadístico de este modelo cuántico. Las estrategias aplicadas por los agentes causan modificaciones en el estado del sistema completo que se reflejan en la entropía del mismo. Los puntos de máxima y mínima entropía son utilizados como herramientas de caracterización de las estrategias que conducen a los estados estables e inestables del problema [4].

3.3. Mercado de Citas: Modelo cuántico

3.3.1. Introducción

El modelo cuántico del mercado de citas se formuló como un problema del bandido bi-direccional tal como se hizo en otras versiones clásicas del mismo, [50, 49], en donde en un lado del mercado se encuentran los hombres que deben elegir una de las opciones disponibles del otro lado del mercado, cuyas integrantes son mujeres

que también desean una cita. A diferencia de lo que ocurre en el bandido unidireccional, las mujeres también tienen poder de acción, es decir que pueden decidir con qué propuesta quedarse. En el modelo clásico del mercado de citas, los hombres eligen mujeres simultáneamente de un conjunto de N posibilidades basando sus elecciones en experiencias anteriores, valores adquiridos, etc. A diferencia del juego tradicional, en la versión cuántica los jugadores tienen la posibilidad de aprovechar las técnicas de la mecánica cuántica. Propiedades tales como superposición y entanglement, utilizadas de manera inteligente permiten mejorar el rendimiento de los jugadores cuánticos frente a los que juegan con estrategias clásicas.

La toma de decisión de cada hombre implica principalmente el buscar dentro de una gran base de datos la mujer más adecuada de acuerdo con sus gustos o preferencias, en consecuencia es lógico pensar que una estrategia de búsqueda inteligente puede ser de mucha utilidad sobre todo si el espacio de búsqueda es grande. Como no hay una forma de que las mujeres aparezcan ordenadas de acuerdo a las preferencias de cada individuo, la búsqueda es desordenada. El algoritmo de Grover, tal como fue desarrollado en un capítulo anterior, saca ventaja de la superposición de estados cuánticos para encontrar un estado "marcado" de un grupo de posibles estados solución en un tiempo considerablemente menor que cualquier algoritmo clásico conocido [34]. Dicho espacio de estados debe ser trasladable, digamos a un grafo G dentro del cual se pueda encontrar, por medio de la ejecución de un algoritmo, un estado particular que cumpla con las características de búsqueda o bien con una marca distintiva. Cuando nos referimos a "marca distintiva" pensamos en problemas cuya solución algorítmica esta inspirada en procesos físicos, es más, es posible garantizar que el nodo buscado está marcado por un valor mínimo (máximo) de una propiedad física incluida en el

algoritmo.

Si consideramos a la mujer que mejor se ajusta a las preferencias de un cierto hombre como el ítem buscado, la utilización del algoritmo de Grover como herramienta de búsqueda puede ser una muy buena estrategia para cumplir con el objetivo de dicho jugador.

3.3.2. El Modelo

Pensemos en una situación en la cual M hombres y W mujeres participan del juego. Sea un espacio de Hilbert cuyos estados $S_i = \{|0\rangle, |1\rangle, ..., |W-1\rangle\}$ representan los índices correspondientes a las N_w mujeres que participan del juego, y que por lo tanto están disponibles para ser elegidas por el hombre i. Como se puede apreciar, se necesitan $log_2(W)$ qubits para representar el índice de cada mujer. Del mismo modo, se define el espacio $S_j = \{|0\rangle, |1\rangle, ..., |M-1\rangle\}$ de posibles estrategias de una mujer j. El espacio de estados que corresponde a todas las posibles decisiones de los hombres es $S_M = S_0 \bigotimes S_1 \bigotimes ... \bigotimes S_{M-2} \bigotimes S_{M-1}$ donde $\bigotimes$ es el producto de Kronecker. Por último, se define el espacio de estado de parejas posibles, como el espacio que incluye los estados correspondientes a todas la decisiones de los hombres y todas las posibles preferencias de las mujeres $S_C = S_M \bigotimes S_W$.

El vector de estados del hombre i es una superposición cuántica de los estados de la base, esto es $\Psi_i = \sum_{j=0}^{W-1} \alpha_j |j\rangle$, donde $|\alpha_j|^2$ es la probabilidad con que i estaría dispuesto a elegir a la mujer j, y por lo tanto se debe cumplir la condición de normalización $\sum_{j=0}^{W-1} |\alpha_j|^2 = 1$.

3.3.3. Algoritmo de Grover como estrategia

Cualquier algoritmo cuántico se puede pensar como una serie de transformaciones lineales, por lo tanto U puede simbolizar una sola o una cadena de transformaciones sucesivas. Bajo este marco, se propone el uso del algoritmo de Grover como estrategia para acelerar la búsqueda de los hombres en el espacio de posibles parejas.
La tabla 3.1 es un ejemplo que muestra los estados de cuatro mujeres en la primera columna mientras en la segunda columna se alinean características únicas y propias de cada una de ellas, en este caso el color de pelo. Observe que si el jugador esta buscando una mujer con una característica determinada, digamos "castaña", debe ingresar a la tabla por la segunda columna, la de las características, y cuando encuentra lo que busca observa en la primera columna el estado de la mujer elegida, que para el ejemplo es $|3\rangle$. El procedimiento es muy sencillo si tratamos con tablas con pocas filas, pero para grandes bases datos, en el mejor de los casos la tabla debe ser consultada $N_w/2$ veces [68, 69].

woman	feature
$\|0\rangle$	rubia
$\|1\rangle$	morocha
$\|2\rangle$	pelirroja
$\|3\rangle$	castaña

Cuadro 3.1: Ejemplo de una base de datos de mujeres: La columna izquierda contiene los estados de las mujeres y la derecha muestra una letra que representa alguna característica o un conjunto de características de la mujer de la izquierda.

Sea Ψ_0 el estado inicial del sistema que mediante transformaciones unitarias U, estrategias, es transformado a $\Psi_1 = U\Psi_0$. El sistema se encontrará inicialmente en un estado $\psi_{ini} = |00\ldots00\rangle \equiv |0\rangle^{\otimes n}$; como ocurre generalmente en física, en problemas

sin perturbación, el estado cuántico inicial es el de mínima energía. Como se detalló en el capítulo 1, el sistema alcanza un estado con una distribución de amplitudes de probabilidad uniforme luego de que se aplica el operador Hadamard H sobre el estado inicial

$$\psi_1 = H\psi_{ini} = \frac{1}{\sqrt{N_w}} \sum_{i=0}^{N_w-1} |i\rangle. \tag{3.3.1}$$

De esta forma el estado ψ_1 garantiza que existe inicialmente una probabilidad de $1/N_w$ de que un hombre encuentre a la mujer que busca. La estrategia propuesta sería aplicar una serie de transformaciones sobre este estado de modo que se modifiquen las amplitudes haciendo crecer las que corresponden a los índices de las mujeres buscadas y disminuir las otras [2, 70]. Para lograr este objetivo se necesitan básicamente dos compuertas, la primera U_f identifica cuál de todas las posibles soluciones es la correcta

$$|w\rangle(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \longmapsto^{U_f} (-1)^{f(w)}|w\rangle(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \tag{3.3.2}$$

Básicamente realiza una inversión de fase sobre el estado o estados solución del problema. Debido a su propiedad de responder a la pregunta ¿Es w solución del problema? en forma binaria (Si o No), se suele denominar a esta compuerta Oráculo. Consideramos aquí, un caso extremo, donde existe solo una mujer que cubre todas las expectativas del hombre. Luego, una nueva transformación es necesaria y se realiza por medio de una compuerta U_R y dos H cuyo objetivo es realizar una inversión sobre la media de las amplitudes del estado, lo que lleva a amplificar la amplitud del estado buscado. Por lo tanto, el algoritmo garantiza que realizando esta sucesión de transformaciones $G = HU_RHU_f$, una cantidad proporcional a $N^{1/2}$ veces la probabilidad de que el hombre que utiliza esta estrategia cuántica encuentre la mujer que está buscando es cercana a 1. En general, puede ocurrir que sean M las soluciones posibles.

Si se relajan las condiciones de evaluación puede ocurrir que la cantidad de mujeres que encuadren en la categoría de "preferidas" aumente, y por lo tanto el proceso de selección se acelere. Se puede demostrar [71] que en este caso la cantidad necesaria de iteraciones es $\sqrt{\frac{N}{M}}$. Si pensamos en un universo de $N = 1024$ mujeres de entre las cuales un caballero debe elegir, clásicamente debería concertar 512 citas para con un 50 % de exactitud encontrar la que, de acuerdo con sus preferencias es la correcta. En la figura 3.1 se muestra para este ejemplo, en azul, la evolución de la probabilidad de encontrar el estado buscado en cada iteración. En la búsqueda cuántica, como se puede observar, en la iteración 25 la probabilidad de acierto es prácticamente 1. En la misma gráfica se muestra como en cambio las probabilidades de los otros estados decrece (curva roja).

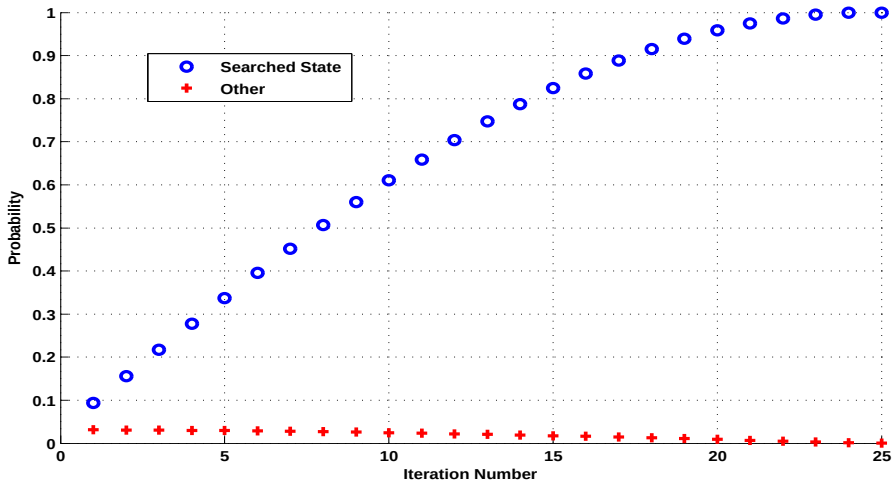

Figura 3.1: La probabilidad de encontrar el item buscado crece en cada iteración (curva azul). En contraste se presenta en la misma gráfica el decrecimiento de la probabilidad correspondiente a un estado cualquiera (curva roja). El ejemplo es para una base de 1024 datos.

En resumen, el juego del mercado de citas al igual que otros problemas enmarcados

en la categoría de problemas de correspondencia, cuenta con dos etapas principales, la primera es la de "Exploración" y la segunda es la etapa de "Explotación", el tiempo que dura cada etapa depende de la estrategia de cada jugador. La utilización del algoritmo de Grover en la etapa de exploración como estrategia para encontrar una pareja que cumpla con las condiciones del interesado permite una ventaja de éste por sobre los jugadores que utilizan estrategias clásicas. Si se supone que ambos jugadores pueden realizar una misma cantidad de intentos, en promedio el jugador cuántico superará al clásico. Si para el caso de $N = 1024$ se permite al jugador clásico más intentos que al cuántico, se puede observar en la gráfica que sus chances se equiparan cuando el jugador clásico realiza 512 intentos y el jugador cuántico 8, en ese instancia ambos tiene las mismas probabilidades y dependerán solo de las decisiones de las mujeres elegidas. Es interesante observar también que si todos los hombres utilizan la estrategia cuántica, ninguno toma ventaja por sobre el otro, y la estabilidad se alcanza rápidamente.

Cuántico vs Clásico

Con la finalidad de comparar la eficiencia del planteo cuántico frente al clásico, consideramos que algunos jugadores juegan cuántico y otros clásico. Para esto sigamos la evolución de agentes representativos de cada grupo, Q y C respectivamente. Q, que juega cuántico puede mantener su estado como una combinación lineal de todos los eventuales resultados cuando se aplican las transformaciones unitarias tales como las descriptas arriba para el algoritmo de Grover, siempre que no se realice ninguna medición que haga que colapse a alguno de ellos. Por otra parte, la única manera que tiene C para buscar en una base de datos de este tipo es consultar secuencialmente los

elementos y probar si cumplen la condición hasta que se alcanza el objetivo. Para una lista de N datos, la búsqueda por fuerza bruta, como se denomina este procedimiento, requiere en promedio $O(N/2)$ comparaciones.

Se presentan dos juegos diferentes donde los hombres quieren salir con la misma mujer: En el primero un jugador Q le da al jugador C la oportunidad de jugar primero y ambos tienen una solo un intento por turno, lo que significa solo una pregunta al oráculo. El segundo juego, con el fin de que Q juegue con desventaja, se establece de forma que C puede jugar $N/2$ veces, mientras que Q sólo una vez, y además el jugador C juega primero nuevamente. Para este último caso, se analizaron dos alternativas para el jugador clásico: en la primera juega sin memoria de su anterior resultado y por lo tanto, en cada intento tiene una probabilidad $1/N$ de encontrar a la mujer elegida para su cita, la otra alternativa le permite al jugador clásico los resultados desfavorables anteriores de modo de evitar elegirlos nuevamente y disminuir el conjunto de selección en cada intento.

Los jugadores que invitan primero a la mujer elegida tienen más chances de tener éxito, así como el que invita a la misma mujer más veces. Sin embargo, la mujer tiene la última palabra, y por lo tanto el éxito de cita para cada jugador depende de las preferencias de la mujer. Entonces, definamos P_c^i como la probabilidad de que la mujer i acepte salir con el jugador clásico y P_q^i a la probabilidad de que acepte la propuesta de Q. Con el objeto de comparar desempeños, consideramos que juegan $T = 1000$ veces por turnos y contamos las veces que tienen éxito, luego calculamos, para cada probabilidad de aceptación de la mujer, el valor medio de la diferencia relativa entre los éxitos de Q y C como $D/T = \frac{Qsuccess - Csuccess}{T}$.

Inicialmente, ambos jugadores comienzan con el sistema en el estado $\psi_1 = \frac{1}{\sqrt{N_w}} \sum_{i=0}^{N_w-1} |i\rangle$, por lo tanto la probabilidad de seleccionar es la misma para ambos, $p(w_i) = 1/N$. En el paso siguiente el Oráculo marca uno de los estados de las probables mujeres de acuerdo con las preferencias de los hombres.

Los resultados son sumamente dependientes del cardinal del conjunto de mujeres, N, debido a que, como ya se mencionó, el algoritmo cuántico necesita $O(\sqrt{}(N))$ pasos para encontrar la pareja elegida por el jugador Q mientras C necesita $O(N)$ pasos para la misma tarea. Para el caso en el que solo existe una mujer y un hombre, por ejemplo, es un caso trivial donde clásico y cuántico no se sacan ventajas de búsqueda y el éxito de ambos dependerá solamente de las preferencias de la mujer, esto es, si $P_c > P_q$ entonces $D/T < 0$ y el jugador cuántico tendrá éxito si $P_q > P_c$. No es usual que ambos jugadores tengan oportunidades similares en los juegos cuánticos, tales como, por ejemplo el juego de la moneda de Meyer [41] donde el jugador cuántico siempre le gana al clásico en un juego *"mano a mano"*. Para un juego en el que existen 2 mujeres Q utiliza solamente un paso, pero C necesita dos para encontrar la pareja correcta. En este caso Q gana si $P_q > P_c/4$. Las condiciones para el éxito de Q se mejoran a medida que crece N, pero no de manera monótona. Para facilitar la comprensión, se presentan a continuación los resultados de simulaciones para un conjunto de tamaño $N = 8$.

Bajo las condiciones del primer juego, ambos jugadores tienen solamente un intento por turno. Debido a que C no puede modificar las amplitudes del estado ψ_1, tiene una probabilidad de 12,5 % de estar estar en lo cierto. Por otra parte, Q con el algoritmo de Grover como su estrategia, puede modificar las amplitudes de los

estados para aumentar sus chances de ganar, alcanzando una probabilidad de 78 % de encontrar a la mujer preferida con solo una iteración. La figura 3.3.3 muestra los resultados de esa situación para diferentes combinaciones de P_c^i y P_q^i. El eje vertical representa los valores D/T como función de P_c^i y P_q^i respectivamente. D/T es positiva para todos los valores de P_c^i y P_q^i values utilizados en la simulación, lo que implica que incluso a los extremos de cumplirse $P_c^i >> P_q^i$, el rendimiento del jugador Q es mejor. Sin embargo, hay una región muy pequeña no mostrada en la figura en la cual $P_c^i \approx 1$ y $P_q^i \approx 0$ que corresponde a un predominante C.

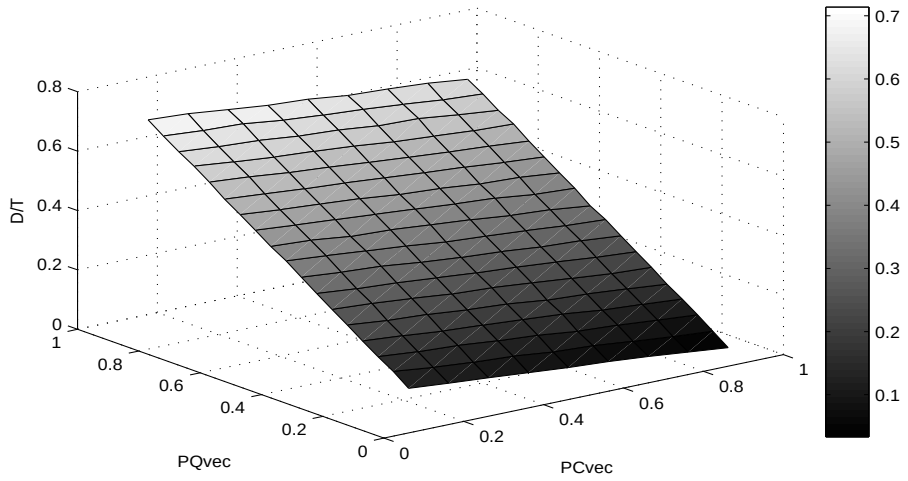

Figura 3.2: Primer juego: Un intento para ambos jugadores. Diferencia media en el número total de éxitos de Q y C, $D/T = \frac{Qsuccess - Csuccess}{T}$, para diferentes probabilidades de aceptación de las mujeres, P_c^i y P_q^i. El jugador Q supera a C en todos los casos mostrados. No se muestra en gráfico la pequeña región donde C prevalece.

Bajo las condiciones del segundo juego, el jugador C tiene permitido hacer $\frac{N}{2} = 4$ intentos antes de que juegue Q. Luego de cada intento de C el sistema es forzado a colapsar hacia un estado base , entonces un tercero, que podría ser el oráculo, prepara los estados nuevamente y marca la solución. Como explicamos anteriormente, el hecho

de marcar el estado tiene incidencia en la fase del estado pero no en su amplitud, en consecuencia, para el jugador C, la probabilidad de que el estado resulte el que el Oráculo señaló es, marcado o no, $1/N = 1/8$ Aunque, gracias a su insistencia, intenta $\frac{N}{2} = 4$ veces, sus posibilidades de cita aumentan considerablemente con respecto al primer caso. La figura 3.3.3 los resultados correspondientes, donde es posible apreciar que el jugador clásico comienza a superar a Q cuando $P_c^i >> P_q^i$, esto es, cuando la mujer tiene una marcada preferencia por el jugador C.

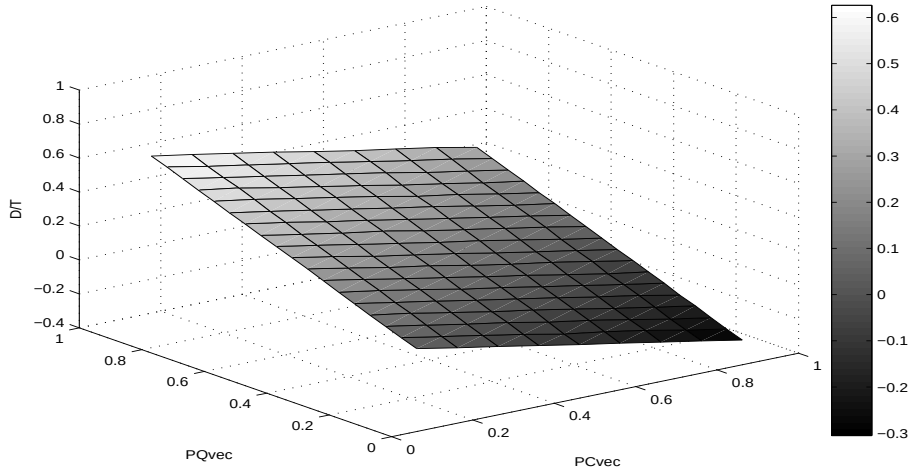

Figura 3.3: Segundo juego: El jugador clásico C tiene cuatro intentos mientras Q tiene solo uno. Diferencia media en el número total de éxitos de Q y C, $D/T = \frac{Qsuccess - Csuccess}{T}$, para diferentes probabilidades de aceptación de las mujeres P_c^i y P_q^i. C supera a Q mientras se cumple $P_c^i >> P_q^i$

La probabilidad de que C encuentre la mujer elegida puede incrementarse a $\frac{1}{2}$ si usa el algoritmo de fuerza bruta, de hecho el único conocido para buscar en una base de datos desordenada. Como se muestra en la figura 3.3.3, cuando C tiene $\frac{N}{2} = 4$ intentos y Q tiene solo uno, las chances de C de tener una cita aumentan, y hay zonas del gráfico donde $D/T < 0$. esto implica que el jugador C supera al

jugador Q. Sin embargo, para que esto ocurra, las preferencias de la mujer deben ser considerablemente mas grandes para el jugador clásico, $P_c^i > 2P_q^i$.

3.4. Conclusión del capítulo

Los dispositivos inalámbricos de transmisión son cada día más inteligentes. Son capaces de decidir por sí solos la banda del espectro en la cual transmitir, la potencia de transmisión, utilizada, e incluso aprender los usos y costumbres de los usuarios. En este contexto, una red de comunicaciones es claramente una red de decisión, donde cada dispositivo realiza la acción que maximiza su medida de rendimiento esperada, basado en la evidencia y su conocimiento. Asimismo, las decisiones de cada agente de la red estará condicionada donde una de esas variables, por ejemplo, es la cantidad de usuarios intentando utilizar las mismos recursos. Resumiendo, estos problemas resultan ideales para ser modelados como problemas de decisión, o de forma particular como problemas de matching entre los dispositivos y los posibles recursos a los que aspiran.

En este capítulo hemos presentado una formulación cuántica para problemas de matching, específicamente para el juego del mercado de citas. En ese marco las mujeres son representadas por estados cuánticos cuyas amplitudes deben ser modificadas por las estrategias de selección de los hombres, de forma que crezca la amplitud de un estado particular y decrezcan las otras, con el objetivo final de alcanzar la mejor elección posible cuando el juego termina. Esta tarea implica un gran consumo de tiempo, un tiempo de ejecución $O(N)$ para un algoritmo probabilístico clásico, siendo N el tamaño de la base de datos de mujeres.

El algoritmo de búsqueda cuántico de Grover es usado como una estrategia de juego

que le permite al hombre encontrar a la pareja elegida en un tiempo $O(\sqrt{N})$. Como consecuencia, si todos los hombres usan estrategias cuánticas, a ninguno le va mejor que los otros, y la estabilidad se obtiene rápidamente.

El desempeño de jugadores cuánticos vs. clásicos depende del número de jugadores N. En el juego "mano a mano" no hay ventaja de ninguno y solo mandan las preferencias de las mujeres. La equidad de posibilidades entre jugadores clásicos y cuánticos no es usual en la mayoría de los juegos cuánticos "mano a mano". Las chances de ganar para el jugador cuántico mejoran cuando aumenta N y se mantiene el número de intentos, pero no de manera monótona. La comparación de los rendimientos entre cuánticos y clásicos muestra que para el mismo número de intentos, el enfoque cuántico es mejor que el clásico. Si el juego se fija de modo que el jugador clásico tenga $\frac{N}{2}$ y cuántico tenga solo una, el primero comienza a tener ventaja sobre el segundo cuando su probabilidad de ser aceptado por la mujer elegida es mucho mayor que la probabilidad que tiene cuántico de ser elegido por ella. Debido a que el entanglement cuántico mejora la "velocidad" con que evolucionan ciertos estados [72], en los análisis siguientes se introducirá entanglement entre jugadores con el propósito de observar si esta condición provee alguna ventaja a los jugadores y cambia las soluciones estables.

Capítulo 4

Parejas estables en el modelo cuántico del mercado de citas

En la capítulo anterior se presentó un modelo cuántico del mercado de citas. Como se pudo apreciar, en la aproximación cuántica las amplitudes de probabilidad asociadas con los estados que representan a las mujeres son modificados por medio de las estrategias de selección que aplican los hombres con el fin de alcanzar la mejor elección cuando el juego concluya. Continuando con el modelo, en este caso nos enfocamos en la información asociada con el problema del mercado de citas. Debido a que se permitirán estrategias mixtas, resulta más adecuado utilizar la matriz de densidad para describir el estado del sistema, en lugar de la función de onda. El problema se analiza bajo los conceptos de máxima y mínima entropía tomados de la teoría de la información. Si bien las acciones de los jugadores se basan en las utilidades que pueden obtener, sus experiencias pasadas, sus creencias, etc., no estamos directamente interesados en esas causas sino más bien en las consecuencias de las decisiones que ellos toman, esto es, la influencia de las estrategias que ellos aplican sobre la estabilidad del sistema. El principio de *Bienestar Colectivo* establece que *un sistema es*

estable solamente si se maximiza el bienestar de todos por sobre el bienestar individual[44]. Con la intención de identificar las condiciones de estabilidad se supone que los estados de máxima entropía obedecen al principio de bienestar colectivo.

4.0.1. Las estrategias

Las estrategias empleadas por los jugadores cambian el estado del sistema, es decir, que el sistema evoluciona hacia un nuevo estado, o eventualmente permanece en el estado actual. Es así que, en lo juegos cuánticos, las estrategias de los jugadores se representan por medio de operadores unitarios, conocidos en la teoría de la mecánica cuántica como operadores evolución relacionados con el Hamiltoniano del sistema.
Si se define U_i como el operador que corresponde a la estrategia del jugador i, el operador estrategia de N-jugadores resulta $U = U_0 \bigotimes U_1 ... U_i \bigotimes ... \bigotimes U_{N-1}$. Inicializado el sistema en un estado puro $|\Psi_0\rangle$, los jugadores aplican sus estrategias U con el objeto de modificarlo en función de sus preferencias, esto es modificando las amplitudes de probabilidad asociadas con con cada estado de la base. Como consecuencia, la evolución del sistema hacia un estado $|\Psi_1\rangle$ esta dada por $|\Psi_1\rangle = U|\Psi_0\rangle$. Para el caso que nos ocupa, si se denotan Ψ_0 como estado inicial y Ψ_1 el final del sistema de parejas, U surge de las estrategias de los hombres U_M mujeres U_W a través de $U = U_M \bigotimes U_W$; donde U_M es aplicada por los hombres sobre los qubits que identifican a las mujeres, mientras la acción de las mujeres sobre los estados que identifican a los hombres esta dada por U_W.

4.0.2. Matriz densidad y Entropía del sistema

Puede ocurrir que los jugadores no tengan certeza de qué estrategia aplicar, es decir, por ejemplo, que puede ocurrir y de hecho es lo más común, que algún jugador

se decida por una estrategia U_a con probabilidad p_a y otra U_b con probabilidad $p_b = 1 - p_a$. Esta situación se representa por medio de lo que se conoce como juego con estrategias mixtas. Aunque el sistema completo se puede representar perfectamente a través de su vector de estados, cuando se trata con estados mixtos, el operador densidad resulta más adecuado para esta tarea. El operador densidad fue formulado por von Neumann para describir un ensamble mixto en el cual cada miembro tiene una cierta probabilidad de estar en un determinado estado. Para una base de funciones de onda concreta, se llama matriz densidad a la matriz que representa al operador densidad del sistema. En otras palabras, el operador densidad, representa la mezcla estadística de todos los estados puros y se define mediante la ecuación

$$\rho = \sum_i p_i |\Psi_i\rangle\langle\Psi_i|, \tag{4.0.1}$$

donde los coeficientes son positivos y suman uno. El análogo cuántico de la entropía clásica fue formulada por von Neumann [73] y se define mediante la siguiente expresión

$$S(\rho) = -Tr\{\rho \log_2 \rho\}. \tag{4.0.2}$$

Mediante el uso del operador densidad y un criterio de máxima o mínima entropía, se pueden hallar los estados estables del mercado de citas cuántico.

Sea un sistema que inicialmente se encuentra en el estado puro $\rho_0 = |\Psi_0\rangle\langle\Psi_0|$, el operador densidad que representa la evolución bajo la acción de las estrategias U_a y U_b con probabilidades p_a y p_b es

$$\rho_1 = p_a U_a \rho_0 U_a^\dagger + p_b U_b \rho_0 U_b^\dagger. \tag{4.0.3}$$

4.0.3. Modelo $N = 2$

Con la finalidad de clarificar las particularidades del modelo, se utiliza un ejemplo simple que involucra dos mujeres y dos hombres que interactúan por T períodos de tiempo. $\Psi_0^i = \alpha|0\rangle + \beta|1\rangle$ representa el estado de decisión inicial del hombre i como una superposición lineal de sus dos elecciones posibles que son la mujeres 0 or 1. Sin pérdida de generalidad considere que se cumple $\alpha = 1$ y $\beta = 0$ en el estado inicial de ambos hombres, que es consistente con pensar que ambos comparten la preferencia por una de las dos mujeres. En consecuencia, el vector inicial masculino es $\Psi_0^M = \Psi_0^0 \bigotimes \Psi_0^1 = |00\rangle$, donde el primer qubit representa la elección del hombre 0 y el segundo a la elección del hombre 1.

Debido a que el estado puro inicial no es estable, en el transcurso del juego este cambiará para tomar una forma más general $\Psi_a^M = \sum_{i=0,j=0}^{1} \alpha_{ij}|ij\rangle$ con probabilidad p_a y $\Psi_b^M = \sum_{i=0,j=0}^{1} \beta_{ij}|ij\rangle$ con probabilidad p_b. Como las mujeres tienen la última decisión, ellas deben evaluar las proposiciones de los hombres y decidir cuál aceptar y cuál rechazar. Consideremos a modo de ejemplo que la mujer 0 elige al hombre 0 con probabilidad p_{0m} y al hombre 1 con probabilidad $1 - p_{0m}$, de forma similar asumimos para la mujer 1 pero en este caso p_{1m} es la probabilidad de que esta última elija al hombre 0. Esa condición no afecta la estabilidad del sistema pero dependiendo de las probabilidades sí afecta la máxima o mínima entropía del sistema de parejas. La ecuación 4.0.4 muestra el operador densidad que corresponde a las preferencias de las mujeres, cuya matriz asociada está compuesta por elementos distintos de cero solo en la diagonal.

$$\rho_{w0} = p_{0m}p_{1m}|00\rangle\langle 00| + p_{0m}(1-p_{1m})|01\rangle\langle 01| + (1-p_{0m})p_{1m}|10\rangle\langle 10| + (1-p_{0m})(1-p_{1m})|11\rangle\langle 11|. \tag{4.0.4}$$

El producto directo de todas las proposiciones posibles de los hombres con todas las posibles decisiones de las mujeres genera un posible vector de estado de parejas $\Psi_0^P = \sum_{i=0}^{15} |i\rangle$. El índice i es un número de cuatro qubits, las primeros dos qubits representan las elecciones de los hombres 0 y 1 respectivamente y los otros dos son las posibles elecciones de las mujeres, luego, el número de posibles parejas es 16. Por ejemplo, el estado $|0101\rangle$ corresponde al caso en que eel hombre 0 elige a la mujer 0 y ella lo acepta y lo mismo ocurre con el hombre 1 y la mujer 1. Note que algunos estados corresponden a citas posibles, mientras otros corresponden a casos donde no se concreta ninguna cita, o casos donde solo es posible una cita, el estado $|0001\rangle$ es un ejemplo de esto último donde el hombre 0 elige a la mujer 0 y ella acepta pero por otro lado el hombre 1 también elige a la mujer 0 pero ella lo rechaza y la mujer 1 no recibe ninguna proposición.
Conforme el juego progresa, las probabilidades asociadas con los "desencuentros" deben decrecer, debido a que se asume que la gente prefiere estar en pareja a estar sola.

Los movimientos o estrategias de cada jugador están asociados con operadores rotación $U_i(\theta)$ (4.0.5) aplicados sobre cada uno de sus qubits, donde $0 \leq \theta \leq \pi$. Como se detalla en [74] cualquier operación sobre un qubit se puede descomponer como un producto de rotaciones. Finalmente, en el caso general donde los jugadores tienen 2^n opciones, cada estrategia pura U está compuesta por n $U_i(\theta_k)$ diferentes, siendo k el estado de cada qubit.

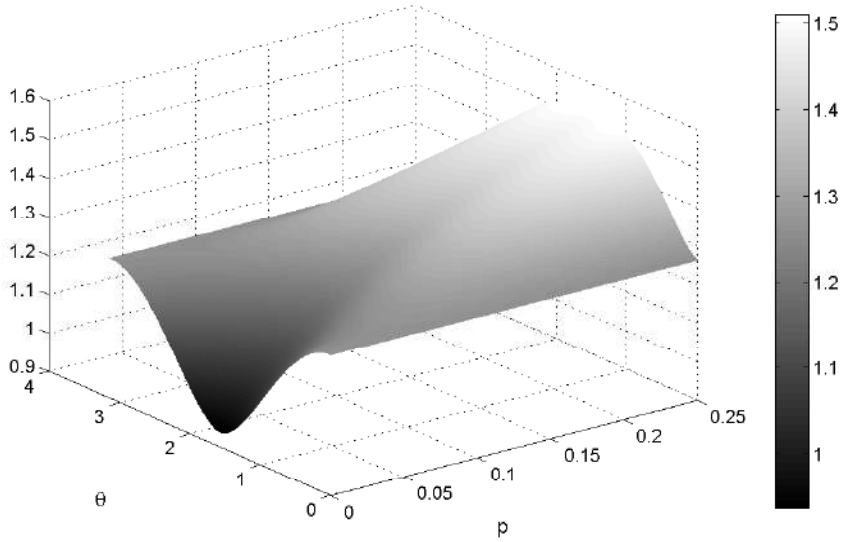

Figura 4.1: Entropía cuántica correspondiente a la situación en la que el jugador 0 varía la probabilidad p de aplicar la estrategia U_0^0

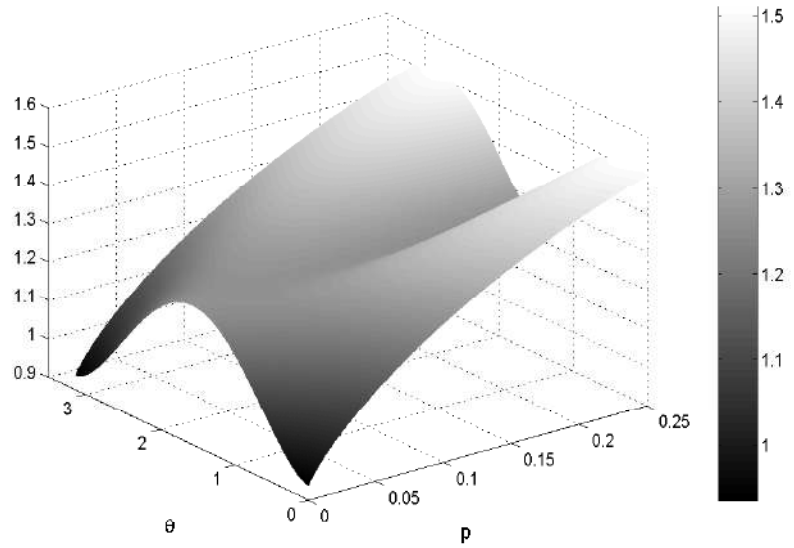

Figura 4.2: Entropía cuántica correspondiente a la situación en la que el jugador 1 varía la probabilidad p de aplicar la estrategia U_0^1

$$U(\theta) = \begin{pmatrix} cos(\theta/2) & sin(\theta/2) \\ -sin(\theta/2) & cos(\theta/2) \end{pmatrix} \tag{4.0.5}$$

Sea p_0 la probabilidad de que el jugador 0 aplique la estrategia U_0^0 y $1 - p_0$ la probabilidad de que opte por aplicar la estrategia U_1^0 al estado inicial Ψ_0^i, mientras U_0^1 y U_1^1 son las estrategias que el hombre 1 aplica con probabilidades p_1 y $1 - p_1$ respectivamente. Los operadores estrategia utilizados en los ejemplos se definen abajo, las ecuaciones 4.0.6 y 4.0.7 son aplicadas por el hombre 0. Ambos transforman el estado inicial $|0\rangle$ en estados que son superposición lineal de $|0\rangle$ and $|1\rangle$, lo que representa estados con probabilidades diferentes de elegir una u otra mujer. Por otra parte, las estrategias aplicadas por el hombre 1 son presentadas en 4.0.8 y 4.0.9.

Las figuras 4.1 y 4.2 muestran dos situaciones en las cuales la entropía del sistema varía considerablemente como función de las entropías aplicadas por los jugadores. La Figura 2, por ejemplo, muestra un caso en el cual el hombre 1 aplica sus estrategias con una probabilidad fija, solo variando el ángulo θ mientras el otro hombre (0) varía tanto el ángulo de rotación del operador estrategia como la probabilidad p. En todos los casos presentados, y con el fin de simplificar la presentación de los resultados, la matriz densidad perteneciente a las mujeres no cambia.

$$U_0^0 = U(\theta) \tag{4.0.6}$$

$$U_1^0 = U(\theta)U(\pi) \tag{4.0.7}$$

$$U_0^1 = U(\theta) \tag{4.0.8}$$

$$U_1^1 = U(-\theta) \tag{4.0.9}$$

Por ejemplo, si ambos hombres eligen la misma mujer con probabilidad uno, ésto está representado en la figura 4.1 con $p = 0$, la situación es completamente inestable ya que es imposible que la mujer elija a los dos hombres al mismo tiempo (asumimos). Esto corresponde a a entropía mínima como se puede observar fácilmente en la figura. Luego, dependiendo de las estrategias, aplicadas por los hombres, la entropía del sistema completo, esto es, la entropía del sistema parejas cambia alcanzando máximos y mínimos de entropía. A medida que p crece, la mezcla de estrategias también crece produciendo un incremento en la entropía que indica una tendencia a la estabilidad. La mezcla de estrategias implica que las proposiciones de los hombres están menos centradas en una única mujer. La figura 4.2 muestra el caso donde el rol de los hombres cambia, es decir que el hombre 0 fija las probabilidades de sus estrategias mientras el 1 varía la suya. Aunque para un ángulo θ fijo, como se espera, los puntos de entropía mínima están localizados donde el jugador aplica una estrategia pura ($p = 0$), para $\theta = \pi/2$ el valor de la entropía no cambia sin importar el valor de p. Ésto es así debido a que U_0^0 y U_1^0 son equivalentes y por lo tanto el jugador 1 está aplicando una estrategia pura. Por último, un resultado que no se muestra en las figuras, pero que resulta intuitivo, es que la entropía máxima crece cuando las preferencias de las mujeres por ambos hombres son los mismas.

De esta manera, los puntos de máxima y mínima entropía se pueden usar para identificar estados estables. Sin embargo, estos estados pueden no coincidir con los estados de equilibrio del juego, debido a que las utilidades de los jugadores no se han tenido en cuenta.

4.1. Conclusión del capítulo

Como una continuación del análisis del modelo cuántico del mercado de citas que tiene en cuenta el aprendizaje progresivo y que representa a las mujeres con estados cuánticos cuyas amplitudes asociadas deben ser modificadas por las estrategias de selección de los hombres, nos concentramos en la información asociada al problema. Debido a que tratamos con estrategias mixtas, se adopta en este caso el formalismo de la matriz densidad para describir el sistema. Aunque ciertamente las decisiones de los jugadores están basadas en los pagos, en la experiencias previas, creencias, etc., nuestro interés no radica en esas causas sino en las consecuencias de las decisiones que ellos toman, esto es, en la influencia que tienen las estrategias que los jugadores adoptan sobre la estabilidad del sistema cuántico por medio de la equivalencia entre estados de entropía máxima y esos estados que obedecen al Principio de Bienestar Colectivo cuya premisa es: un sistema es estable solo is este maximiza el bienestar de lo colectivo por sobre el bienestar del individuo. Esta premisa volverá a resurgir en capítulos posteriores donde se traten redes de comunicaciones. Allí se deberá priorizar la "salud" de la red como un todo por sobre el rendimiento de cada nodo en particular. Los puntos de Máxima y Mínima entropía son usados para encontrar estrategias características que conducen a estados estables o inestables. Sin embargo, con el propósito de encontrar estados de equilibrio de Nash, deben ser consideradas las utilidades de los jugadores.

La entropía máxima o mínima no solo depende de las estrategias de los hombres sino también de las preferencias de las mujeres, alcanzando su valor máximo cuando ellas no tienen preferencias, es decir, cuando la probabilidad de elegir a cualquiera de los hombres es la misma. Por otra parte, la entropía mínima corresponde a una situación

en que los hombres ponen todas sus fichas a una solo mujer, sin dar oportunidad a ninguna otra. Una situación semejante a la que puede ocurrir con un dispositivo que, basándose en su experiencia pasada elige con máxima probabilidad el canal de frecuencia que a priori sería el menos congestionado.

Capítulo 5

Teoría de juegos aplicada a las telecomunicaciones inalámbricas

5.1. Introducción

El objetivo de este capítulo es el estudio de las redes inalámbricas de comunicaciones desde el punto de vista de la teoría de juegos. El tema central es la administración de los recursos de libre acceso, una tarea que es de máxima importancia cuando éstos son limitados [75]. El control de potencia, por ejemplo, es un tema central en el diseño de sistemas de comunicación multiusuario con interferencia limitada, en los cuales el rendimiento de cada usuario depende no solo de su asignación de potencia, sino también de la asignación de potencia del resto de los usuarios. El control de acceso al medio también es otro tema que abordaremos desde el punto de vista de los juegos ya que, al igual que en el caso anterior resulta natural modelar estos problemas como una competencia entre usuarios que buscan cumplir un objetivo, la mayoría de las veces de manera egoísta pero otras con el fin de favorecer el bien común de toda la red. Antes de abordar los problemas específicos que hemos analizado como parte de esta tesis, se introducirán algunos temas relacionados con la teoría de las comunicaciones que luego se mencionarán, tales como radio cognitiva, redes de radio cognitiva

y acceso oportunista al medio. Esto permitirá al lector, no solo seguir los problemas planteados sino pensar en otras aplicaciones no tratadas aquí.

5.2. Sistemas de Comunicaciones inalámbricos

Comenzaremos presentando los sistemas celulares porque son, de alguna forma, la base cualquier otro tipo de sistema inalámbrico. Una red celular consiste en un número de estaciones base (BS) fijas, una por cada célula o celda. El área total de cobertura se divide en celdas y un móvil se comunica con la o las BS más cercanas. Dicho de otra forma, el área cubierta por una estación base, esto es, el área desde la cual llegan llamadas entrantes a la BS, se llama Celda. En general, se grafica como una región exagonal con la estación base en el medio. Debido a que no siempre se cuenta con superficies altas que permitan una buena cobertura, como la terraza de un edificio o el tope de un cerro donde poder ubicar las antenas, las estaciones base no están dispuestas de forma regular en las ciudades. Asimismo, se eligen los usuarios móviles conectados a una estación de base por las buenas vías de comunicación en lugar de la distancia geográfica.

El enlace inalámbrico de una estación base hacia los usuarios móviles se denomina, enlace descendente o simplemente bajada, y el enlace desde los usuarios a una estación base se denomina enlace ascendente o subida. Por lo general hay muchos usuarios conectados a una única estación base. Para el canal de enlace ascendente, cada usuario conectado a una estación base dada transmite su propia forma de onda, y el de estación base recibe la suma de las formas de onda de los distintos usuarios más ruido.

Siguiendo con la descripción, podemos mencionar las LAN inalámbricas (redes de área local). Estas están diseñadas para velocidades de datos más altas que los sistemas celulares, pero por lo demás son similares a una sola célula de un sistema celular. Éstas son usadas para conectar computadoras portátiles y otros dispositivos portátiles en la red de área local dentro de un edificio de oficinas o ambientes similares. En este tipo de sistemas, la movilidad esperada es poca y su principal función es la de permitir la portabilidad. La familia IEEE 802.11 contiene los principales estándares para redes LAN inalámbricas. Existen normas de menor escala, como Bluetooth o una más reciente basada en la comunicación de banda ultra ancha (UWB), cuyo propósito es reducir el cableado en una oficina y simplificar las transferencias entre oficina y los dispositivos de mano. Finalmente, existe otro tipo de LAN llamado red ad hoc. Las redes Ad-Hoc son la última frontera en comunicación inalámbrica. Aquí, en lugar de un nodo central (estación base) a través del cual fluye todo el tráfico, los nodos son todos equivalentes. La red se auto-organiza sobre vínculos entre varios pares de nodos y elabora las tablas de enrutamiento utilizando estos enlaces. Aquí los problemas de enrutamiento, la difusión del control información, etc, son preocupaciones importantes, aunque los problemas de re-instalación y colaboración distribuida entre los nodos son también áreas activas de investigación actual.

Las redes inalámbricas modernas, tales como las redes de sensores, las redes de malla, los sistemas de computación ubicua, comparten unas serie de necesidades básicas, como lo son la auto-configuración, la operación descentralizada y el ahorro de energía. Al mismo tiempo, los dispositivos intervinientes necesariamente están evolucionando hacia modelos tecnológicamente más sofisticados e “inteligentes” con la

capacidad de adaptarse a cualquier cambio que el medio les presente. Cada nodo que ejecuta un protocolo distribuido debe tomar sus propias decisiones, que pueden estar condicionadas por las reglas o algoritmos de un protocolo, pero en última instancia, dicho nodo tendrá cierta libertad de acción en el establecimiento de parámetros o cambiar el modo de operación. Estos nodos son entonces, agentes autónomos, tomando decisiones en lo que respecta a la potencia de transmisión, el reenvío de paquetes, tiempo de espera (backoff), etc. En lo que respecta a la toma de decisiones, es importante pensar en cuál es el objetivo que persiguen los nodos. Es decir, en algunos casos los nodos puede que busquen el bien de la red en su conjunto, mientras que en otros casos actúen de manera egoísta, buscando satisfacer solo sus propios intereses. Por último, pueden existir también nodos cuyo fin sea el de arruinar el buen desempeño de la red para otros usuarios.

Las redes inalámbricas de sensores son un tipo particular de redes Ad-Hoc, en el cual los nodos son sensores inteligentes, dispositivos pequeños (aproximadamente del tamaño de una moneda) equipados con funcionalidades avanzadas de sensado (térmico, presión, acústica y otros, son ejemplos de esas capacidades de sensado), un pequeño procesador y un transmisor inalámbrico de corto rango. En este tipo de redes, los sensores intercambian información con el ambiente de forma ordenada con el fin de construir una vista global de la región monitoreada, la cual es accesible a un usuario externo a través de uno o mas nodos de gateway. Debido a que la posición de estos sensores es generalmente inaccesible (operaciones de socorro en zonas de desastre, terrenos inaccesibles, etc.), los protocolos y los algoritmos deben ser capaces de autoorganizarse ante un eventual cambio en las condiciones del medio, por ejemplo.

El espectro radioeléctrico puede ser considerado, a todos los efectos, como un recurso natural limitado. Es por esto que el uso que de él hacen los diferentes sistemas de comunicaciones se encuentra regulado de manera local en cada país. Si analizásemos actualmente porciones de este espectro nos encontraríamos con que el grado de ocupación de las bandas que lo conforman es muy diferente. Algunas bandas se encuentran desocupadas buena parte del tiempo mientras que en otras el nivel de ocupación es extremadamente elevado. El hecho de que exista un evidente desaprovechamiento del espectro es una de las causas que ha motivado, en los últimos años, el desarrollo del concepto de Radio Cognitiva[76].

Los Sistemas de Radio Cognitiva deben poseer la capacidad de analizar el espectro radioeléctrico sobre un amplio rango de frecuencias con el objetivo de detectar esos canales desocupados, también llamados "claros espectrales". Basándose en la disponibilidad de canales y otra información adicional extraída del medio, ciertos usuarios pueden ocupar un canal que cumpla con los requisitos necesarios para efectuar su comunicación. Un dispositivo de radio cognitiva es un sistema de radiofrecuencia capaz de tomar información de su ambiente para mejorar su rendimiento, y en consecuencia aumentar el rendimiento de toda la red . Por ejemplo, puede monitorear el espectro y elegir las frecuencias que minimicen la interferencia existente en la comunicación activa. De esta manera, una red cognitiva, puede responder a las necesidades de un usuario particular, dentro de las políticas que define el operador, al mismo tiempo que optimiza los recursos generales.

En resumen, en una red inalámbrica multiusuario los servicios son provistos a múltiples usuarios, los cuales se asume que son lo suficientemente racionales como

para poder alcanzar el más alto desempeño. Además, debido a que el acceso al canal de un nodo influye sobre los nodos vecinos, la teoría de juegos, por naturaleza, resulta ser una herramienta útil y poderosa para el desarrollo y la investigación de este tipo de redes. Una de la aplicaciones mas interesantes de los juegos es como herramienta para crear esquemas de cooperación entre entidades tales como nodos, terminales o proveedores de red, donde la estabilidad de las soluciones para los jugadores se obtiene a través del concepto de equilibrio [77]. En la mayoría de los casos, los problemas a resolver están relacionados con el diseño y optimización de protocolos de ruteo y de asignación de recursos. En esta sección vamos a repasar algunos casos típicos donde la teoría de juegos ha sido aplicada y posteriormente analizaremos los casos en los que la teoría de juegos cuántica impone mejoras.

La aplicación de la técnica de juegos en redes se aplica en distintos niveles de los protocolos en el modelo OSI (Open Systems Interconnection). El modelo OSI divide en capas, más precisamente siete, el proceso de transmisión de la información entre equipos informáticos, donde cada capa se encarga de ejecutar una determinada parte del proceso global [78, 79]. Las pilas o capas de protocolos no son más que una serie de pequeños protocolos ordenados de manera jerárquica trabajando juntos para llevar a cabo la transmisión de los datos de un nodo a otro de la red. Algunos juegos tienen lugar a nivel de capa física, tales como Juegos de Control de Potencia o de Adaptación de forma de onda son problemas típicos de mejoramiento del rendimiento a este nivel. En la capa física, el rendimiento es medido generalmente en términos de la relación señal a interferencia más ruido (SINR) en los nodos. Cuando los nodos de la red responden a los cambios percibidos en la (SINR) adaptando su señal, se produce un

proceso de toma de decisiones en la capa física. Un ejemplo es el denominado "Juego de Interferencia" que se desarrolla en la siguiente sección.

Otros juegos se desarrollan a nivel del control de acceso al medio. En esta capa, usuarios egoístas buscan maximizar su utilidad mediante la obtención de una proporción arbitraria del acceso al canal. Esta acción, sin embargo, disminuye la capacidad de otros usuarios de acceder al canal, por ejemplo en el juego Aloha Ranurado, que fue presentado anteriormente en el 2 [1].

Como parte de esta tesis se ha analizado la posibilidad de adaptar el protocolo MAC 802.11 para su uso en comunicaciones cuánticas [5]. Cabe aclarar que las familias IEEE 802.11 son los principales estándares que definen las características una red LAN inalámbrica. En ellos se encuentran las especificaciones tanto físicas como a nivel MAC (Medium Access Control), que hay que tener en cuenta a la hora de implementar una red de área local inalámbrica [81]. En este trabajo, proponemos un nuevo método de control de acceso al medio capaz de ser utilizado tanto en comunicaciones cuánticas como clásicas. Dado que, las comunicaciones cuánticas prometen maneras seguras para enviar información valiosa, serán necesarias redes de dispositivos cuánticos y métodos de control de acceso al medio que eviten la pérdida de información. Por otro lado, como las colisiones excesivas son frecuentes en redes inalámbricas clásicas congestionadas, hemos sacado provecho del paralelismo cuántico y el entanglement cuántico multipartito para diseñar una subcapa MAC que proporciona los dispositivos de un acceso eficiente y equitativo al canal.

[1] ALOHA ranurado es un protocolo alternativo al protocolo Aloha original que consiste en dividir el tiempo en intervalos discretos, llamados ranuras, correspondientes cada uno a la longitud de una trama. Este método mejora en rendimiento al ALOHA puro (ya que algunas colisiones son evitadas) y se utiliza un reloj que marca los comienzos de las ranuras (o intervalos). Solamente se permite transmitir una trama al comienzo de una ranura y, si la estación se encuentra en mitad de ella, deberá esperar hasta el comienzo de la siguiente para enviar datos, ver [80] para mayor información.

5.2.1. Juego de Interferencia

Los juegos de interferencia son utilizados para modelar redes inalámbricas debido a que permiten caracterizar muy bien su entorno. En estos sistemas, múltiples transmisores (nodos de una red) con distintos incentivos y con libertad de elegir los parámetros de operación comparten el medio. Como se puede observar en la figura (5.1) que modela de forma genérica el canal, la potencia transmitida por cada transmisor hacia un determinado receptor no solo actúa sobre éste, sino que, también contribuye al nivel de interferencia en los otros receptores [82]. En dicho modelo, la señal se propaga desde cada antena transmisora a cada una de las antenas receptoras, lo que permite representar la transmisión a través de una matriz, a la que llamaremos aquí H, cuyos elementos h_{ij} representan la transferencia entre la antena emisora i y la antena receptora j. En consecuencia, la correcta decodificación de la señal en un enlace dependerá de la relación señal a ruido e interferencia (SINR) recibida. De esta forma, se considera que la transmisión de un nodo es satisfactoria cuando la amplitud de la señal captada por el receptor es mayor que la suma de las señales que recibe de los otros jugadores, más el ruido ambiental. Por último, es importante observar que el rendimiento particular de cada jugador dependerá no solo de sus decisiones sino también de las decisiones tomadas por el resto. Para ilustrar esto, pensemos por ejemplo que una estrategia posible sería transmitir con la mayor potencia posible. Esta estrategia, si bien podría asegurar al jugador una transmisión exitosa, el excesivo consumo de energía acortaría críticamente la duración de la batería, sin considerar el perjuicio de esta decisión sobre los otros usuarios. Por otra parte, si todos los jugadores eligen esta misma estrategia también el éxito de la transmisión estaría comprometido. En

resumen, la interferencia mutua creada se traducirá en un rendimiento global por debajo del óptimo, así también como un consumo innecesario de energía y/o fallas de transmisión. Un juego de este tipo se presentó en el capítulo (2) como ejemplo de la utilidad de la teoría de juegos. En aquella oportunidad, como dato relevante se observó que el nivel óptimo de Pareto no garantiza el menor consumo posible de energía.

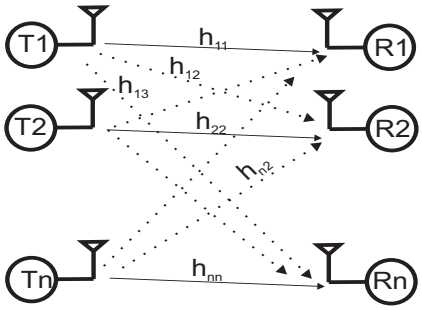

Figura 5.1: Modelo de Interferencia

Suponga un escenario [83] en el cual los usuarios operan sobre un total de K canales de ancho Δf. Se asume aquí que el usuario i tiene permitido transmitir una potencia total P_i la cual distribuirá en los distintos canales. De esta forma, el vector de potencias que puede transmitir cada jugador es $\mathbf{p}_i = (p_i(1), ..., p_i(K)) \in [0, P_i]^K$, donde p_k es la potencia transmitida en el canal k. Dada la característica no cooperativa del juego, se cumple la igualdad $\sum_{k=1}^{K} p_i(k) = P_i$, es decir que todos los usuarios desearán aprovechar al máximo su potencia. Por último, la utilidad de los jugadores se mide por medio de la expresión

$$C^i(\mathbf{p}_1, ..., \mathbf{p}_N) = \sum_{k=1}^{K} log_2 \left(1 + \frac{|h_{ii}|^2 p_i(k)}{\sum_{j \neq i} |h_{ij}|^2 p_j(k) + \mathbf{n}(k)} \right), \tag{5.2.1}$$

donde C^i es la capacidad [84] disponible para el jugador i dada la distribución de

potencias $\mathbf{p}_1, ..., \mathbf{p}_N$. El término $\mathbf{n}(k)$ representa el ruido externo presente en cada receptor. En consecuencia $\mathbf{C} = \{C^1, ..., C^N\}$ es el vector de pagos, mientras que las estrategias de los jugadores están representadas por la manera en que decidan distribuir su potencia en los distintos canales.

El juego de Interferencia Gaussiano es un juego no-cooperativo de N jugadores. Éste modela el proceso de usuarios independientes tratando de optimizar su velocidad de transferencia de datos de manera independiente en condiciones de potencia limitada y de interferencia de los otros usuarios. La técnica de llenado iterativo (Iterative Water Filling (IWF)), es una estrategia muy conocida de distribución subóptima del espectro en la cual cada usuario ajusta sucesivamente su espectro de potencia considerando a la interferencia de los otros usuarios como ruido. Bajo ciertas condiciones, este proceso iterativo converge a un punto fijo que es precisamente el equilibrio de Nash del juego de interferencia, ver [82]. Sin embargo, este método no siempre resulta bien para todos los usuarios, es más, existen casos en los cuales es posible otro esquema de distribución de potencia, donde, aún actuando de manera egoísta, los usuarios obtienen mejores resultados. En [83], se analiza el desempeño de la estrategia IWF para el caso $N = 2$, en cuyo caso se observa que, si bien hay canales en las cuales el IWF es óptimo, en otros se produce la situación conocida como Dilema del Prisionero (DP). Cabe recordar que en el DP, el sistema tiene un equilibrio de Nash que no es óptimo, esto debido a la naturaleza no cooperativa de los usuarios. Sin embargo, un mejor rendimiento es posible si se utilizan herramientas cuánticas, como se presentó en el capítulo (2). En consecuencia, se propone aquí un modelo cuántico de distribución de potencia como solución para eliminar el dilema y alcanzar una repartición de los recursos más eficiente y equitativa para todos los usuarios.

Juego de interferencia Cuántico

Se describe aquí el juego de interferencia cuántico para un caso particular en el que existen $N = 2$ usuarios y $K = 2$ canales. Al igual que en el caso clásico, el canal se caracteriza a través de las matrices de transferencia H, cuyos elementos h_{ij} representan la transferencia entre la antena emisora i y la antena receptora j. En este caso, las matrices que caracterizan el canal para cada frecuencia se definen en (5.2.2)

$$|H(1)|^2 = |H(2)|^2 = \begin{bmatrix} 1 & h \\ h & 1 \end{bmatrix} \tag{5.2.2}$$

donde se ha considerado $|h_{12}(k)|^2 = |h_{21}(k)|^2 = h$, siendo $k = 1, 2$ las dos posibles bandas de frecuencia compartidas por los usuarios. Además, se define $\psi_{AB} = |00\rangle$ como el estado inicial del sistema que corresponde a la "Selección de los usuarios", en el cual el qubit de la izquierda representa la selección del usuario A y el de la derecha la selección del usuario B. Consideramos aquí que 0 equivale a "Cooperar" y 1 equivale a "No Cooperar", de esta forma, $|00\rangle$ es, por ejemplo, el estado del sistema cuando ambos optan por cooperar.

Las utilidades de los jugadores están dadas por (5.2.1), donde se ha establecido que el canal cumple con $|h_{12}(k)|^2 = |h_{21}(k)|^2 = h$ siendo $k = 1, 2$ las dos posibles bandas de frecuencia compartidas por los usuarios. Además, se considera una situación imparcial en la que ambos tienen la misma limitación de potencia P y donde la matriz de distribución de potencia se define de la siguiente manera,

$$P. \begin{bmatrix} 1-\alpha & \alpha \\ \beta & 1-\beta \end{bmatrix} \tag{5.2.3}$$

para $0 \leq \alpha, \beta \leq 1$. De esta manera, las utilidades de los usuarios A y B para este problema resultan:

$$C^A = \frac{1}{2} log_2 \left(1 + \frac{(1-\alpha)}{SNR^{-1} + \beta \cdot h}\right) + \frac{1}{2} log_2 \left(1 + \frac{\alpha}{SNR^{-1} + (1-\beta) \cdot h}\right) \quad (5.2.4)$$

$$C^B = \frac{1}{2} \log_2(1 + \frac{\beta}{SNR^{-1} + (1-\alpha) \cdot h}) + \frac{1}{2} \log_2(1 + \frac{(1-\beta)}{SNR^{-1} + \alpha \cdot h}) \quad (5.2.5)$$

donde $SNR = P/N$.

Recordemos el Dilema del Prisionero definido anteriormente, donde cada jugador tiene dos opciones, cooperar (C) o no cooperar (D). Como se muestra en la tabla (5.1), la suerte de cada jugador, depende de las decisiones que ambos tomen en cada ocasión. Para que exista la situación conocida como dilema del prisionero es requisito que las utilidades percibidas por ellos en cada una de las combinaciones cumplan con $t > r > p > s$ y $2r > t + s$. Otras relaciones entre estas magnitudes conducen a otros tipos de situaciones que no analizaremos aquí.

En este problema, se define cooperar al acto de transmitir en uno de los dos canales por parte de un usuario, proveyendo al otro usuario de un canal libre de interferencia. Por otra parte, cuando el usuario decide competir (no cooperar) distribuye su potencia entre las dos bandas, de esta forma α y β se interpreta como el nivel de competencia de A y B respectivamente. Es decir, por ejemplo, que la completa cooperación entre ambos está dada por $\alpha = \beta = 0$.

Las filas de la tabla corresponden a las decisiones del jugador 1 y las columnas a las decisiones del jugador 2. Las utilidades han sido representadas aquí de forma más general, el primer valor entre paréntesis corresponde a la utilidad percibida por el jugador 1 y el segundo valor corresponde a la utilidad del jugador 2.

	D	C
D	(p, p)	(t, s)
C	(s, t)	(r, r)

Cuadro 5.1: Matriz de pagos. Entre paréntesis, el primer valor corresponde a la utilidad percibida por el jugador 1 y el segundo valor corresponde a la utilidad el jugador 2. Las distintas opciones están representadas por sus denominación original en inglés: r = reward, p = punishment, t = temptation, and s = sucker's payoff.

- t (temptation) es la utilidad de un jugador por desertar mientras el otro coopera.
- r (reward) es la utilidad recibida por cada uno si los dos cooperan.
- p (penalty) es la utilidad recibida por cada uno si los dos desertan.
- s (sucker's payoff) es la utilidad de un jugador por cooperar mientras el otro deserta.

E prisionero clásico tiene una estrategia dominante que es (D, D), cuya recompensa es (p, p), un equilibrio no óptimo ya que si ambos cooperaran (C, C), obtendrían mayores utilidades (r, r). El equilibrio desfavorable se debe a que si solo uno de los jugadores cambia su estrategia a C mientras el otro mantiene la suya en D, el que cambia sufre una disminución en la utilidad percibida, por lo que, en promedio, ambos prefieren no arriesgar y asegurarse una utilidad $p < r$ antes que arriesgarse y recibir $s < p$. Además, la situación (C, C) es muy inestable, ya que si uno de los jugadores confía en que su "compañero" va a cooperar su mejor opción es traicionarlo D y obtener la mejor utilidad posible $t > r$.

Por otra parte, si se realiza un sistema de distribución de potencia que trabaje bajo las reglas de la mecánica cuántica, las condiciones cambian favorablemente para ambos usuarios. El circuito de la figura (5.2) muestra las distintas etapas del sistema de selección.

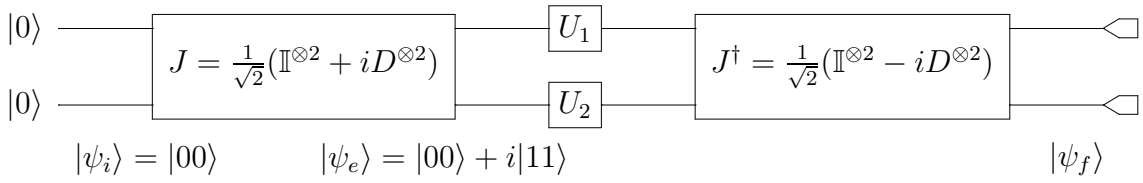

Figura 5.2: Circuito del Juego de Interferencia Cuántico

Como se puede observar, al estado inicial del sistema $|00\rangle$ se le aplica una transformación conocida por ambos jugadores que prepara el estado entangled $|\phi_e\rangle$. Sobre este estado operan los usuarios a través de sus estrategias U_1 y U_2, cuya expresión matricial esta dada por (5.6.3) y por lo tanto dependerán de los parámetros $0 \leq \theta \leq \pi$ y $0 \leq \phi \leq \pi/2$ elegidos. Además en la figura (5.4) presentamos un posible circuito de la compuerta J, que como se observa consta de una compuerta Hadamard y una compuerta c-U (ó U controlada). La compuerta U, en este caso, es (iX) donde X es la compuerta NOT e $i = e^{i\pi/2}$.

Uno de los problemas a los que nos enfrentamos al utilizar una computadora cuántica para resolver un problema clásico, es la carga de los datos del problema. Es sabido que para que las propiedades cuánticas de superposición se mantengan es necesario que el sistema esté aislado, es decir, que no haya interacción con el medio, es por esto que es necesario un procedimiento de carga de datos que no viole dicha condición. Chao-Yang Pang [85] presentó un esquema cuántico de carga de datos para hacer que una computadora cuántica sea compatible una memoria clásica. Dicho esquema, permite cargar gran cantidad de datos en registros cuánticos al mismo tiempo.

$$U_i(\theta, \phi) = \begin{pmatrix} e^{i\phi}\cos(\theta/2) & \sin(\theta/2) \\ -\sin(\theta/2) & e^{i\phi}\cos(\theta/2) \end{pmatrix} \tag{5.2.6}$$

Las posibles combinaciones de $U_i(\theta, \phi)$ son infinitas, sin embargo, el subconjunto

$S_0 = \{U(\theta, 0) | \theta \in [0, \pi]\}$ reúne el conjunto de estrategias cuyos resultados no exceden lo que podría esperarse del modelo clásico. Por ejemplo, las estrategias clásicas puras están relacionadas con los siguientes operadores:

$$C \equiv U(0,0) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad y \quad D \equiv U(\pi, 0) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \tag{5.2.7}$$

En la figura (5.3) se presenta la utilidad del usuario B: Se marcan allí los casos más relevantes, tanto de acciones clásicas de los usuarios, que como es de esperar no exhiben diferencias con respecto al modelo clásico tradicional, como así también los resultados de aplicar estrategias puramente cuánticas.

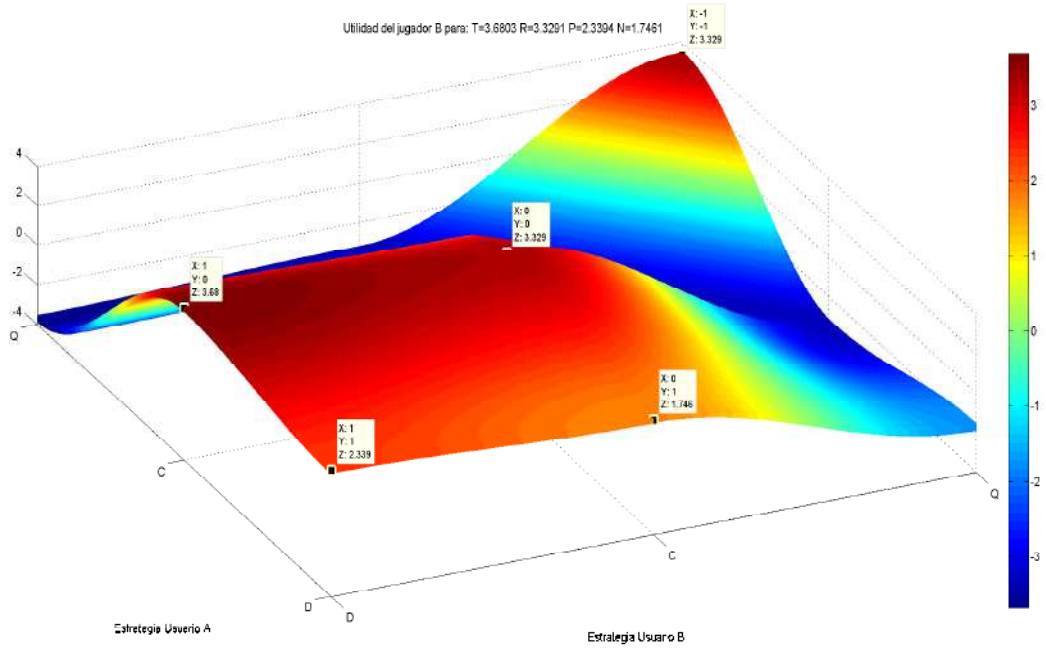

Figura 5.3: Dilema del Prisionero: Para los cálculos se consideró una $SNR = 20db$,$h_1 = h_2 = h = 0{,}225$ y $\alpha = \beta = 0{,}5$. Con estos valores de los parámetros se produce el problema del dilema del prisionero para el cual la mejor solución para los usuarios es (Q, Q).

Claramente se puede apreciar que en este nuevo modelo surge una situación que

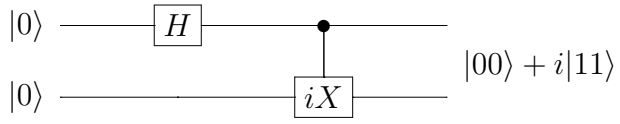

Figura 5.4: Un ejemplo de circuito de J para generar el estado entangled $|00\rangle + i|11\rangle$

favorece a ambos usuarios cuando ambos aplican la estrategia cuántica Q, cuya expresión matricial es (5.2.8). Este es un equilibro en el sentido de Pareto, ya que cualquier intento por mejorar sus recursos por parte de alguno de los usuarios irá en el desmejoramiento del otro y por lo tanto es la situación más favorable para ambos.

$$Q \equiv U(0, \pi/2) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \tag{5.2.8}$$

Si bien, se ha analizado el caso en el que existen dos usuarios, los resultados se pueden extender a casos de $N > 2$. Si bien el análisis que implica encontrar los equilibrios en juegos de muchos jugadores resulta más complejo, también resulta más interesante. En [86], por ejemplo los autores han demostrado que para el dilema del prisionero cuántico de tres jugadores también es posible encontrar un equilibrio de Nash con eficiencia de Pareto si el estado inicial está completamente entangled. Como se puede inferir fácilmente, la existencia de un equilibrio único y óptimo es esencial para la salud de la red en su conjunto.

5.3. Control de Acceso al Medio (MAC)

Un canal con acceso múltiple refiere a muchos transmisores enviando a un único receptor. La potencia de transmisión puede variar con cada transmisor, pero el ancho de banda del receptor se debe dividir entre los diferentes usuarios. Ejemplo de canales

de múltiple acceso incluyen una Eternet conectada a muchas computadoras, líneas de telefonía standard (que son multiplexadas en el tiempo entre muchas señales de voz), y la transmisión entre un móvil y la estación base en sistemas celulares. El objetivo de las comunicaciones multiusuario es el de utilizar los recursos limitados del sistema (potencia y ancho de banda) de manera eficiente creando la menor interferencia posible entre usuarios.

El recurso de sistema más importante a distribuir es el ancho de banda, ya que este es asignado por las comisiones de comunicaciones, y en general es escaso (o caro). El ancho de banda se divide en canales, usando un método de canalización basado en tiempo, frecuencia, o división de código.

5.4. Juego cuántico de las minorías

El juego de las minorías surge como un modelo simple de múltiples agentes para estudiar la toma de decisiones estrategias. En su versión clásica ha sido utilizada, por ejemplo, como un modelo interactivo de vender y comprar en el mercado de valores [87]. En su expresión más simple, en cada paso los agentes deben elegir independientemente entre un par de opciones descritas “0” y “1”. Como resultado, los agentes que hayan elegido la opción menos popular son recompensados con $r = 1$, mientras los integrantes de la mayoría obtienen $r = 0$.

El juego ha ganado mucho interés debido a que se cree que éste captura una característica muy importante de los sistemas en los cuales los agentes compiten por recursos limitados, tales como, operaciones en el mercado financiero ó la elección de la noche correcta para visitar un bar abarrotado de gente, [88], entre otras. Sin embargo, como se presenta en [89], el juego de las minorías puede también ser de mucha

utilidad en otras situaciones, tales como las redes de comunicaciones, y ya no solo como método de análisis, sino que también es potencialmente útil para desarrollar algoritmos para el compartimiento de recursos.

Por otra parte, la teoría de juegos cuántica ha avanzado de manera promisoria en aplicaciones relacionadas con el procesamiento de la información cuántica [90]. Así mismo, existen situaciones que involucran la interacción competitiva de agentes donde el lenguaje más apropiado resulta ser el de la mecánica cuántica [4]. Las principales ventajas surgen al compartir estados entangled que permiten el intercambio de información entre usuarios. Las subastas cuánticas, las votaciones cuánticas, ó las comunicaciones cuánticas [91] son algunos ejemplos de esto.

En esta línea, en [92, 93] se presentan versiones cuánticas del juego de las minorías, donde, bajo ciertas condiciones, ofrecen mejoras respecto a la versión clásica. Con base en estos antecedentes, en esta sección analizamos la aplicación del juego de las minorías a la teoría de las comunicaciones. Si bien, por naturaleza la idea está dirigida a la aplicación en el terreno de las comunicaciones cuánticas, también se puede pensar en un módulo cuántico capaz de controlar la distribución de los recursos en una red de comunicaciones tradicional, en el cual internamente gobiernen las leyes de la física cuántica, pero que las entradas y salidas del mismo sean señales clásicas [5]. A continuación se presenta un ejemplo de aplicación del juego de las minorías como parte del diseño de un sistema de comunicaciones cuánticas, más precisamente el control de acceso al medio.

5.5. Técnicas de la teoría de juegos aplicadas al diseño de protocolos MAC cuánticos

En este trabajo se propuso un protocolo para compartir el acceso a medio cuántico. El diseño utiliza las propiedades de la teoría de juegos para resolver las dificultades que se presentan en las redes inalámbricas, especialmente los problemas de colisión. En la mayoría de las redes inalámbricas los usuarios toman decisiones individuales sin importar las decisiones de los demás, simplemente porque la información intercambiada por ellos es mínima o inexistente, ocasionando una reducción en la capacidad total del sistema. Por otra parte, las propiedades de auto organización del juego de las minorías son adecuadas para modelar y resolver problemas de compartimiento de recursos limitados. Asimismo, el protocolo MAC propuesto mejora al clásico incrementando la probabilidad de evitar colisiones. En resumen, la propuesta contribuye no solo al desarrollo de las redes cuánticas futuras sino también al desarrollo de técnicas modernas de compartimiento de recursos en las redes actuales.

5.6. Descripción de protocolo cuántico

El objetivo principal del protocolo de acceso es evitar, o al menos minimizar la probabilidad de que dos o más dispositivos transmitan simultáneamente y que sus datos resulten dañados (evitar colisiones). Para tratar con las características dinámicas de la topología wireless, el modelo maneja el acceso al canal de dos modos diferentes, dependiendo si la red es centralizada o distribuida. En pos de aprovechar ambas topologías, el sistema se adapta de forma de discriminar si es necesario considerar una red centralizada o descentralizada. En el primer caso, las decisiones son tomadas por el Access Point (AP), mientras que en el segundo caso la coordinación es reglamentada

por un método cuántico de decisión basado en la teoría de juegos. Cuando algunos usuarios están dentro del rango de alcance y otros no, el juego se establece entre los primeros y aquel que fue autorizado por el AP., de esta forma, los usuarios de la red son los jugadores, sus estrategias son transmitir o no transmitir en un intervalo de tiempo particular y su objetivo es realizar una transmisión exitosa.

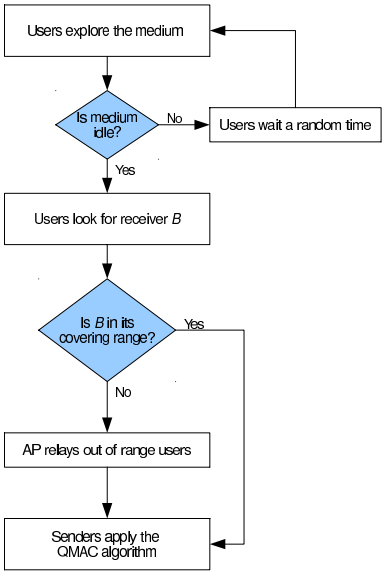

Figura 5.5: Diagrama de flujo del protocolo QMAC

Supongamos que el usuario A desea transmitir datos al usuario B. Entonces el usuario A sensa la disponibilidad del canal, si éste no está disponible, espera un tiempo aleatorio y luego repite esta operación. Si el medio está libre, A busca a B. Si B está disponible, el transmisor crea un par EPR y envía una parte a B a través del canal cuántico. Luego, por medio de un proceso de teleportación la información es compartida. Por otra parte, es posible que más de un usuario necesite transmitir información a A, en este caso se deben establecer reglas de acceso. Esto quedará más claro más adelante cuando se presente el protocolo de acceso al medio.

En otro caso, cuando A no está dentro del rango de alcance de B, comienza un

modo de comunicación orientada, en otras palabras, el AP toma el control. Éste crea un estado entangled W (5.6.1), con amplitudes a, b, c que dependen de la prioridad de cada usuario.

$$|W\rangle = a|001\rangle + b|010\rangle + c|100\rangle, \tag{5.6.1}$$

Por ejemplo, el primer qubit del estado multipartito es del AP mientras que los otros qubits son enviados a los usuarios. El AP mide su qubit, si colapsa a cero, las amplitudes de probabilidad determinan que usuario transmitirá, y será aquel que al medir su qubit obtenga 1 como resultado. De esta manera, se evita en este protocolo evitar las colisiones.

5.6.1. Control cuántico de acceso al medio

Así como jugadores en un juego no-cooperativo, las decisiones y las consecuencias de los nodos en una red ad-hoc tienen influencia en las decisiones y las consecuencias de otros nodos de la red. Una versión cuántica del "juego de las minorías" es propuesto como modelo para describir la situación de un grupo de usuarios tratando de transmitir en una red ad-hoc.

Pensemos en el caso en que existen dos canales de comunicación y dos usuarios, antes de extender el análisis al caso más general en el que existan múltiples usuarios y canales. Supongamos que dos usuarios a los que llamaremos Alice (A) y Bob (B) desean transmitir un mensaje a través de dos canales, digamos 0 y 1, que por simplicidad vamos a considerar que solo pueden transmitir uno a la vez. Lo más conveniente sería que en cada intervalo de tiempo los usuarios elijan transmitir por distintos canales, lo que evitaría colisiones. Sin embargo, debido a que los usuarios no tienen información de las decisiones e los otros, existe una probabilidad de que

ambos elijan el mismo canal y está dada por $p_w = p(A,0) \cdot p(B,0) + p(A,1) \cdot p(B,1)$, donde $p(i,j)$ significa que el jugador i selecciona el canal j. Para el problema clásico, la probabilidad de que A and B elijan el mismo canal alcanza su máximo, $\frac{1}{2}$, cuando $p(i,j) = 0{,}5$.

El circuito de la figura 5.6, muestra el modelo de acceso al medio general para N usuarios. El sistema cuántico se establece en el estado $\psi_i = |00..,0\rangle$. Luego, este estado inicial del sistema es afectado por una transformación J conocida por todos los usuarios, la que prepara el estado entangled. Los usuarios producen la modificación de este estado el sistema realizando operaciones locales sobre los qubits que les fueron asignados. Finalmente, el estado del sistema es disentangled, es nuevamente separable, por medio de la compuerta $J^\dagger$, evolucionando al estado ψ_f que contiene la información probabilística de la asignación canal-usuario. En lo que sigue daremos un ejemplo de como esto funciona.

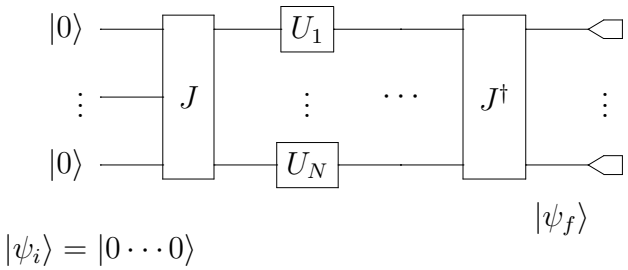

Figura 5.6: Circuito de acceso al canal

Nuevamente consideremos que hay dos usuarios (A y B) y dos canales (0 y 1). La entrada al sistema son dos qubits en estado $|0\rangle$. Luego de aplicar la compuerta , el sistema queda en el estado $\psi_1 = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B)$. Se puede verificar fácilmente que existe una estrategia que conduce a un estado óptimo del sistema cuando ambos usuarios hacen uso de ella. Como se muestra en Fig. 5.6, cuando se aplica $U = H$,

siendo H la compuerta Hadamard definida anteriormente, el estado final resulta:

$$\psi_f = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)^{\otimes 2} \cdot \frac{(|00\rangle - |11\rangle)}{\sqrt{2}} = \frac{(|01\rangle - |10\rangle)}{\sqrt{2}} \tag{5.6.2}$$

De este estado final surgen dos situaciones favorables e igualmente probables para ambos usuarios, esto es: que el usuario A transmita en el canal 0 mientras B utiliza el canal 1 ($|01\rangle$), or que el usuario A elija transmitir en 1 mientras B elige el canal 0 ($|10\rangle$). Bajo estas condiciones, se evita el peor caso, logrando que ambos usuarios transmitan de manera satisfactoria con certeza.

$$U_i(\theta, \phi, \gamma) = \begin{pmatrix} e^{i\phi}\cos(\theta/2) & e^{i\gamma}\sin(\theta/2) \\ e^{i\gamma}\sin(\theta/2) & e^{i\phi}\cos(\theta/2) \end{pmatrix} \tag{5.6.3}$$

5.6.2. Control de acceso para N usuarios

En lo que respecta al caso de N jugadores presentamos aquí dos modelos decisión. Al igual que en el modelo del farol [94], el primer modelo considera que los usuarios, tienen 2 opciones, que en este caso son: acceder o no acceder a un único canal de comunicaciones. Mientras que en un segundo modelo, N usuarios deben elegir entre k canales en los cuales se permite acceso solo a un usuario por intervalo de tiempo. En el modelo que aquí presentamos, los usuarios no hacen uso de conocimientos adquiridos con anterioridad. La elección clásica "1" corresponde a que el usuario en cuestión decide transmitir en el canal y por el contrario "0" implica que decide no transmitir en ese momento.

Supongamos ahora que N usuarios deciden transmitir en un canal dado con capacidad limitada. Como no todos pueden transmitir al mismo tiempo, tendrán que

decidir en cada momento si transmitir o no. Mientras menor sea la cantidad de usuarios usando el canal, mejor resultará la transmisión, lo que da a las claras que estamos frente a un problema de las minorías, que a diferencia de planteo iterativo clásico, los usuarios tienen una sola oportunidad de elegir, es decir de aplicar su estrategia U_i. Las estrategias $U_i(\theta, \phi, \gamma)$ se muestran en (5.6.3) y un posible circuito para la compuerta que genera el estado entangled se muestra en la figura 5.7. El estado entangled generado GHZ se presenta a continuación y lleva su nombre debido a que fue estudiado por primera vez en 1989 por D. Greenberger, M.A. Horne y Anton Zeilinger en 1989 [95].

$$|GHZ\rangle = \frac{|0\rangle^N + |1\rangle^N}{\sqrt{2}} \tag{5.6.4}$$

En el caso clásico el equilibrio es trivial, ya que el mejor pago esperado que obtienen los usuarios resulta cuando sus decisiones se basan en el lanzamiento de una moneda equilibrada. Por su parte, en el juego cuántico el equilibrio más favorable para los usuarios se obtiene cuando el número de éstos es par. Benjamin y Hayden [93] demostraron por ejemplo para el caso de $N = 4$ que existe una estrategia $U_i(\pi/2, -\pi/16, \pi/16)$ que si es aplicada por todos los usuarios conduce a un equilibrio óptimo, y con un pago esperado para cada usuario igual al doble del que podría obtener un usuario clásico. Esto se traduce en el problema que tratamos aquí, en el que los usuarios cuánticos tendrán éxito en la transmisión con una probabilidad mayor, ya que podrán evitar colisiones con más frecuencia. Esta optimización es producto de la eliminación de los estados para los cuales ninguno de los usuarios gana, esto es aquellos donde todos los usuarios hacen la misma elección o la elecciones están balanceadas. Esto solo es posible gracias al estado inicial entangled del sistema, que

claramente no es posible en el caso clásico. Se puede demostrar que las estrategias para N par mayor que 4 tienen la forma $U_i(\pi/2, -\delta, \delta)$ con $\delta = \frac{\pi}{4N}$, [92].

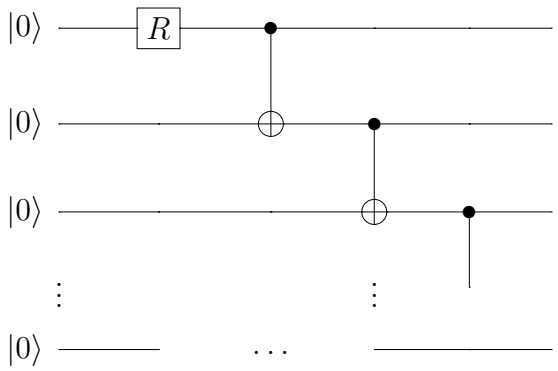

Figura 5.7: *Posible circuito para generar el estado entangled GHZ*

Por último planteamos aquí otro problema muy interesante que es el que involucra a N usuarios que desean transmitir información, a través de N canales a una estación base, por ejemplo. Lo cierto es que varios usuarios pueden elegir el mismo canal, siempre que no superen la capacidad del sistema. Dado que ninguno de los nodos de la red conoce la intención del otro, deben elegir en qué canal transmitir de manera aleatoria. El pago, como una medida de la fiabilidad de la comunicación, dependerá de cuántos usuarios seleccionen el mismo canal. Mientras más lo elijan, menor será el pago obtenido. El peor caso es cuando todos eligen el mismo canal. La probabilidad de que esto ocurra, en el caso clásico, esta dada por

$$p_w = \frac{N}{N^N}.$$

En cambio, el mejor caso, que es cuando todos los usuarios eligen canales diferentes, ocurre con una probabilidad dada por

$$p_b = \frac{N!}{N^N}$$

Sean $i = 0...N-1$ los índices correspondientes a los posibles canales que los usuarios pueden utilizar para transmitir, mientras $j = 1...N-1$ denotan los índices correspondientes a los usuarios de la red. Si el usuario 0 elige transmitir a través del canal i_0, el usuario 1 elige el canal i_1 y el usuario $N-1$ elige i_{N-1} el estado del sistema se describe $|i_0, i_1, ..., i_{N-1}\rangle$. El sistema comienza en $|00..,0\rangle$ y mediante una compuerta el transformación se crea el estado inicial entangled $|\psi_i\rangle$ de la ecuación 5.6.5, que no es otra cosa que la aplicación de la transformada cuántica de Fourier (QFT).

$$|\psi_i\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega_N^k |kk...k\rangle \tag{5.6.5}$$

donde $\omega_N = e^{2\pi i/N}$. Se considera aquí que como todos los usuarios tienen como fin común el bienestar de la red, se presenta una situación equitativa y todos eligen la misma estrategia U. Los elementos de la matriz que representa al operador U tienen la forma

$$u_{ij} = \frac{1}{\sqrt{N}} (\omega_N)^{i.j} \tag{5.6.6}$$

donde $i, j = 0, 1, ..., N-1$ Se puede demostrar que si todos los usuarios aplican U, la transformación realizada sobre el estado entangled hará que las amplitudes de probabilidad asociadas a los estados más desfavorables se desvanezcan, y por lo tanto aumenten las otras amplitudes. Esto logra no solo evitar el caso más desfavorable para los usuarios de la red que se produce cuando todos eligen el mismo canal, sino que también la probabilidad de tener un transmisión con la mayor calidad esta dada por la expresión

$$p_b^Q = N.\frac{N!}{N^N}.$$

Si lo comparamos con el caso clásico es N veces mayor. Este fenómeno de amplificación

selectiva de las amplitudes de probabilidad comparte las mismas características del utilizado en el mercado de citas, cuando utilizamos el algoritmo de Grover como método de búsqueda.

5.7. Conclusiones del capítulo

Las investigaciones en computación cuántica y comunicaciones cuánticas han crecido rápidamente en estos últimos años. Al mismo tiempo, se han desarrollado algoritmos basados en la teoría de la mecánica cuántica para los propósitos más variados y en diversas áreas, tales como Economía, Sociología, Biología e Ingeniería, entre otras. Por otra parte, las investigaciones relacionadas con la teoría de juegos han demostrado que puede ser usada para analizar la interacción competitiva de los usuarios que actúan en las redes inalámbricas reales. Asimismo, algunos modelos de juego conocidos han sido utilizados como soluciones de problemas de acceso al medio en redes de comunicaciones clásicas. En este capítulo la atención está centrada en los sistemas de comunicaciones inalámbricas multiusuario. En primer lugar se analizó el problema del manejo de los recursos a nivel de la capa física de la estructura del protocolo. Los problemas de interferencia, de asignación de potencia y la distribución equitativa del espectro, son, como se ha detallado al principio de este capítulo, temas de suma importancia. Tomando como base un juego de interferencia, se definió un modelo cuántico para el problema de asignación de potencia de múltiples usuarios. Se presentó un caso de dos usuarios en el cual surge el problema del prisionero y se demostró que se puede obtener una mejor administración de la energía si se utilizan las propiedades de la mecánica cuántica. Quedó planteada la extensión del problema para múltiples usuarios, que si bien es una tarea compleja, resulta interesante en pos

de poder encontrar el equilibrio del problema.

Luego, presentamos una propuesta de solución a nivel de acceso al medio, relacionando su optimización con un problema de juego de la minoría cuántico. La cuantización del juego de las minorías permite, en muchos casos, obtener resultados que mejoran el máximo rendimiento que se puede obtener en el caso tradicional. En el caso $N = 2$ los usuarios pueden hacer una transmisión exitosa, marcada por un pago promedio 1, mientras que en el juego los jugadores clásicos sólo se puede llegar a un pago máximo promedio igual a $\frac{1}{2}$. En este caso, la recompensa debe ser entendida como la probabilidad de una transmisión con éxito. Para el caso de $N > 2$ el mejor de los casos no se alcanza, lo que significa que cuando todos los dispositivos decide transmitir al mismo tiempo no se puede evitar. Sin embargo, los pagos esperados superan al caso clásico cuando el número de usuarios, N, es un número par, y es igual cuando el número de usuarios es impar. Por último, para el caso en el que existan N usuarios intentando transmitir en N canales se presentó una solución cuántica que no solo evita que el peor caso se produzca, sino que también se mejore la probabilidad de que a los usuarios se le presente el mejor caso.

5.8. Trabajo Futuro

Nuestra intención es seguir desarrollando nuestros conocimientos en el área de los algoritmos cuánticos, sobre todo en lo que respecta a las aplicaciones relacionadas con las comunicaciones modernas, no solo como un aporte a las comunicaciones cuánticas del futuro sino también a las comunicaciones clásicas emergentes. Por otra parte, es necesario considerar que mientras no existan computadoras cuánticas sobre las cuales

volcar toda la batería de software existente, resulta necesario que se desarrolle hardware que sea capaz de emular el comportamiento de éstas. Como hemos mencionado en su oportunidad, la tecnología de arreglos de compuertas programables en campo (FPGA) cuentan con una serie de ventajas que las hacen apropiadas para esta tarea, es por eso parte de nuestra investigación estará dirigida al diseño de hardware que emulen circuitos cuánticos con ésta tecnología.

Bibliografía

[1] O.G. Zabaleta and C.M Arizmendi. Quantum search for the dating market. *Special Issue of Advances and Applications in Statistical Sciences (AASS)*, (4091034-SS59):162–167, August 2009.

[2] O.G. Zabaleta and C.M Arizmendi. Quantum dating market. *Physica A*, 389:2858–2863, 2010.

[3] O.G. Zabaleta and C.M Arizmendi. Quantum decision theory on a dating market. *Special Issue of Advances and Applications in Statistical Sciences (AASS)*, 2011.

[4] C. M. Arizmendi and O. G. Zabaleta. Stability of couples in a quantum dating market. *special IJAMAS issue "Statistical Chaos and Complexity*, 26:143–149, 2012.

[5] C. M. Arizmendi, J. P. Barrangu, and O. G. Zabaleta. A 802.11 MAC Protocol Adaptation for Quantum Communications. In *Distributed Simulation and Real Time Applications (DS-RT), 2012 IEEE/ACM 16th International Symposium on*, pages 147 –150, oct. 2012.

[6] C. M. Arizmendi and O. G. Zabaleta. *Advances in QUANTUM MECHANICS, Chapter Name: Quantum Dating Market.* Intech, Croatia, 2013.

[7] Richard Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21:467–488, 1982.

[8] C. Negrevergne, R. Somma, G. Ortiz, E. Knill, and R. Laflamme. Liquid-state nmr simulations of quantum many-body problems. *Phys. Rev. A*, 71:032344, Mar 2005.

[9] D. Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. 400:97–117, 1985.

[10] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *arXiv:quant-ph/9508027v2*, 1996.

[11] L.K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings, 28th Annual ACM Symposium on the Theory of Computing (STOC)*, pages 212–219, May 1996.

[12] A. Galindo and Martín-Delgado M. A. Information and computation: Classical and quantum aspects. *Rev. Mod. Phys.*, 74:347–423, 2002.

[13] P. Kaye, R. Laflamme, and Michele Mosca. *An Introduction to QuantumComputing*. Oxford University Press, 2007.

[14] Y. Kanamori, S. M. Yoo, W. D. Pan, and Sheldon S.T. A short survey on quantum computers. *International Journal of Computers and Applications*, 28:97–117, 2006.

[15] K. C. Lee, M. R. Sprague, B. J. Sussman, J. Nunn, N. K. Langford, X.-M. Jin, T. Champion, P. Michelberger, K. F. Reim, D. England, D. Jaksch, and I. A. Walmsley. Entangling macroscopic diamonds at room temperature. *Science*, 334(6060):1253–1256, 2011.

[16] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47(10):777–780, May 1935.

[17] James D. F. V. and P. G. Kwiat. Quantum state entanglement. *Los alamos Science*, 27:52–57, 2002.

[18] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Omer, M. Furst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger. Entanglement-based quantum communication over 144 km. *Nature Physics*, 3(7):481–486, 2007.

[19] D. Deutsch. Quantum computational networks. *Proc. R. Soc. Lond. A*, 425:73–90, 1989.

[20] W. K. Wootters and W. Zurek. *Nature*, 299:802, 1982.

[21] P. W. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52:2493–2496, 1995.

[22] A.M Steane. Error correcting codes in quantum theory. *Phys. Rev. Lett*, 77:793–797, 1996.

[23] A. R. Calderbank and P. W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54:1098–1105, 1996.

[24] James D. F. V. and P. G. Kwiat. Quantum state entanglement. *Los alamos Science*, 27:188–225, 2002.

[25] L. De Micco, Zabaleta O.G;, C. M. González, C. M. Arizmendi, and Larrondo H. A. Implementación en fpga de un generador de ruido coloreado. In *IBERCHIP XIV Workshop*, February 2008.

[26] O. G. Zabaleta, L. De Micco, C. M. González, C. M. Arizmendi, and Larrondo H. A. Generador de ruido estocástico coloreado mediante fpga. In *Proceedings of*

Designer's Forum. IV Southern Programmable Logic Conference(SPL08), pages 69–73, 2008.

[27] L. De Micco, Zabaleta O.G, C. M. González, C. M. Arizmendi, and Larrondo H. A. Ruido 1/fd implementado en fpga. In *IBERCHIP XV Workshop*, March 2009.

[28] G. Negovetic, M. Perkowski, M. Lukac, and A. Buller. Evolving quantum circuits and an fpga-based quantum computing emulator. In *Proc. Intern. Workshop on Boolean Problems*, pages 15–22, 2002.

[29] A. U. Khalid, Z. Zilic, and K. Radecka. Fpga emulation of quantum circuits. In *Proceedings of the IEEE International Conference on Computer Design*, pages 310–315, 2004.

[30] D. C Marinescu and M. M. Marinescu. *Approaching Quantum Computing*. Pearson Prentice Hall, United states of America, 2005.

[31] E. Bernstein and U. Vazirani. Quantum complexity theory. In *Proc. 25th Annual ACM Symposium on Theory of Computing, ACM*, pages 11–20, 1993.

[32] R. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21:120–126, 1978.

[33] A. Eckert and R. Jozsa. Quantum computation and Shor's factoring algorithm. *Rev. Mod. Phys.*, 68:733–753, 1996.

[34] M. Boyer, G. Brassard, P. Hoeyer, and Tapp A. Tight bounds on quantum searching. *Fortsch.Phys*, 46:493–506, 1998.

[35] D. H. Wolpert, K. Tumer, and J. Frank. Using collective intelligence to route internet traffic. *arXiv:cs/9905004v1*, 1999.

[36] Zhen K., Yu-Kwong K., and Jiangzhou W. Game theoretic packet scheduling to combat non-cooperativeness in wireless mesh networks. In *Distributed Computing*

Systems Workshops, 2008. ICDCS '08. 28th International Conference on, pages 162–167, june 2008.

[37] I. Koutsopoulos, L. Tassiulas, and L. Gkatzikis. Client and server games in peer-to-peer networks. In *Quality of Service, 2009. IWQoS. 17th International Workshop on*, pages 1–9, 2009.

[38] Li, Changja Chen, and Lei Li;. Evaluating the latency of clients by player behaviors in client-server based network games. In *3rd International Conference on Innovative Computing Information and Control, 2008. ICICIC '08.*, page 375, August 2008.

[39] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Qishi Wu. A survey of game theory as applied to network security. In *Conference on System Sciences (HICSS), 2010 43rd Hawaii International*, pages 1–10, 2010.

[40] Zeng Jia, Mu Chundi, and Jiang Min. Game theoretic distributed energy control in sensor networks. In *Conference on Computer and Information Technology, 2007. CIT 2007. 7th IEEE International*, pages 1015–1019, 2007.

[41] D.A. Meyer. Quantum strategies. *Phys. Rev. Lett.*, 82:1052–1055, 1999.

[42] Du Jiang-Feng et al. Multi-player and multi-choice quantum game. *Chinese Phys. Lett*, 19:1221, 2002.

[43] A. Iqbal and A.H. Toor. Quantum repeated games. *Physics Letters A*, 300:541–546, 2002.

[44] Esteban Guevara Hidalgo. Quantum games entropy. *Physica A*, 383:797–804, 2007.

[45] M. J. Osborne and A. Rubinstein. *A Course in Game Theory.* The MIT Press Cambridge, Massachusetts, England, 1998.

[46] J. Neel, J. Reed, and R. Gilles. Game models for cognitive radio analysis. *SDR Forum Technical Conference*, 2004.

[47] W. , D. Ernst, C. Moy, and J. Palicot. Multi-armed bandit based policies for cognitive radio's decision making issues. In *Signals, Circuits and Systems (SCS), 2009 3rd International Conference on*, pages 1 –6, nov. 2009.

[48] D. Gale and L.S. Shapley. College admissions and the stability of marriage. *Am. Math. Monthly*, 69:9–15, 1962.

[49] C.M Arizmendi. Paradoxical way for losers in a dating game. In Osvaldo A. Rosso Orazio Descalzi and Hilda A. Larrondo, editors, *Proc. AIP Nonequilibrium Statistical Mechanics and Nonlinear Physics*, pages 20–25, Mar del Plata , Argentina, December 2006.

[50] S. Das and E. Kamenica. Two-sided bandits and the dating market. In Alessandro Saffiotti Leslie Pack Kaelbling, editor, *Proceedings of the Nineteenth International Joint Conference on Artificial Intelligence,IJCAI-2005*, pages 947–952, Edinburgh, Scotland, UK, August 2005.

[51] J. Eisert, M. Wilkens, and M. Lewenstein. Quantum games and quantum strategies. *Phys. Rev. Lett.*, 83:3077–3080, 1999.

[52] L. Marinatto and T. Weber. A quantum approach to static games of complete information. *Physics Letters A*, 272:291–303, 2000.

[53] H. Robbins. Some aspects of the sequential design of experiments. *Bulletin of the American Mathematical Society*, 55:527–535, 1952.

[54] J. C. Gittins. Bandit processes and dynamic allocation indices. *Journal of the Royal Statistical Society. Series B (Methodological)*, 41:148–177, 1979.

[55] G. Parmigiani and L. Y. T. Inoue. *Decision Theory: Principles and approaches*. JOHN WILEY and SONS, 2009.

[56] P. M Allais. Le comportement de l'homme rationnel devant le risque: Critique des postulats et axiomes de l'école americaine. *Econometrica*, 21(4):503–546, 1953.

[57] S.O Hansson. Decision theory: A brief introduction. Department of Philosophy and the History of Technology Royal Institute of Technology (KTH) Stockholm, 1994.

[58] A. Lambert-Mogiliansky, S. Zamir, and H. Zwirn. Type indeterminancy: a model of kt-man. *J. Math. Psych.*, 53:349–361, 2009.

[59] V.I. Yukalov and D. Sornette. Quantum decision theory as quantum theory of measurement. *Physics Letters A*, 372(46):6867–6871, 2008.

[60] T. Temzelides. An uncertainty principle for social science experiments. *Available at http://www.owlnet.rice.edu/ tl5*, 2005.

[61] R. V. Mendes. The quantum ultimatum game. *Quantum Information Processing*, 4(1):1–12, 2005.

[62] A.E. Roth and M. Sotomayor. Two-sided matching: A study in game-theoretic modeling and analysis. *Econometric Society Monograph Series*, 324, 1990.

[63] K.B. Clark. Origins of learned reciprocity in solitary ciliates searching grouped 'courting' assurances at quantum efficiencies. *Biosystems*, 99:27–41, 2010.

[64] Z. Chengshi, Z. Mingrui, Bin S., K. Bumjung, and Kyungsup K. Cooperative spectrum allocation in centralized cognitive networks using bipartite matching. *IEEE "GLOBECOM"2008 proceedings*, pages 1–6, 2008.

[65] A. Berger, Gross J., and Harks T. The k constrained bipartite matching problem: Approximation algorithms and applications to wireless networks. *IEEE INFOCOM 2010 proceedings*, 2010.

[66] P. Laureti and Y.C. Zhang. Matching games with partial information. *Physica A*, 324:49–65, 2003.

[67] C. Zhao, M. Zou, B. Shen, B. Kim, and K. Kwak. Cooperative spectrum allocation in centralized cognitive networks using bipartite matching. In *Proceedings of the Global Communications Conference, 2008. GLOBECOM 2008, New Orleans, LA, USA, 30 November - 4 December 2008*, pages 2998–3003. IEEE, 2008.

[68] M. Hunziker, D. A Mayer, J. Park, J Pommersheim, and M. Rothstein. The geometry of quantum learning. *arXiv:quant-ph/0309059*, 2003.

[69] A. Romanelli. Quantum games via search algorithms. *Physica A*, 379:545–551, 2007.

[70] G. Brassard, P. Hoeyer, M. Mosca, and Tapp A. Quantum amplitude amplification and estimation. *arXiv:quant-ph/0005055v1*, 2000.

[71] S. Imre and Balazs F. *Quantum Computing and Communications: An Engineering Approach.* John Wiley and Sons, Ltd., England, 2005.

[72] A. Borras, C. Zander, A. R. Plastino, M. Casas, and A. Plastino. *Europhys. Lett.*, 81:30007, 2008.

[73] J. von Neumann. *Mathematische Grundlagen der Quantenmechanik.* Springer-Verlag[translated by R. T. Beyer as Mathematical Foundations of QuantumMechanics (Princeton University Press, Princeton, 1955)], Berlin, 1932.

[74] M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, England, 2000.

[75] V. Auletta, L. Moscardelli, P. Penna, and Persiano G. Interference games in wireless networks. *Lecture Notes in Computer Science*, 5385:278–285, 2008.

[76] J. Mitola and G.Q. Maguire. Cognitive radio: making software radios more personal. *IEEE Personal Communications*, 6:13–18, 1999.

[77] Y. Xiao, X. Shan, and Y. Ren. Game theory models for IEEE 802.11 DCF in wireless ad hoc networks. *Communications Magazine, IEEE*, 43:22–26, 2005.

[78] Charles K. Summers. *ADSL: Standards, Implementation, and Architecture*. CRC Press, 1999.

[79] M. Crisan. *Convergence and Hybrid Information Technologies*. Intech, 2010.

[80] Mohammad Ilyas and Syed A. Ahson. *Handbook of Wireless Local Area Networks*. CRC PressINC, 2005.

[81] William Stallings. *Wireless Communications and Networks.* Pearson Prentice Hall, Upper Saddle River, NJ, 2nd. edition, 2002.

[82] W. Yu, G. Ginis, and J. M. Cioffi. Distributed multiuser power control for digital subscriber lines. *IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS*, 20(5):1105–1115, 2002.

[83] A. Laufer and A. Leshem. Distributed coordination of spectrum and the prisoners dilemma. In *New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005. 2005 First IEEE International Symposium on*, pages 94 –100, nov. 2005.

[84] D. Tse and P. Viswanath. *Fundamentals of Wireless Communication*. Cambridge University Press, England, 2005.

[85] Chao-Yang Pang. Loading N-dimensional vector into quantum registers from classical memory with O(log N) steps. *arXiv:quant-ph/0612061*, 2006.

[86] J. Du, H. Li, X. Xu, X. Zhou, and R. Han. Entanglement enhanced multiplayer quantum games. *Physics Letters, Section A: General, Atomic and Solid State Physics*, 302(5-6):229–233, 2002.

[87] E. Moro. The minority game: An introductory guide. *Advances in Condensed Matter and Statistical Physics, Nova Science Publishers, Inc*, 2004.

[88] D. Challet and Y. Zhang. Emergence of cooperation and organization in an evolutionary game. *Physica A*, 246:407–418, 1997.

[89] P. Mähönen and M. Petrova. Minority game for cognitive radios: Cooperating without cooperation. *Physical Communication*, 1(2):94 – 102, 2008.

[90] E. Rasmusen. *Games and Information: An Introduction to Game Theory*. John Wiley & Sons, 2006.

[91] J. Briet, H. Buhrman, T. Lee, and T. Vidick. Multiplayer xor games and quantum communication complexity with clique-wise entanglement. *arXiv:quant-ph/0911.4007v1*, 2009.

[92] A. P. Flitney and L. C. L. Hollenberg. Multiplayer quantum minority game with decoherence. *Quantum Information and Computation*, 2005.

[93] S.C Benjamin and P. M. Hayden. Multiplayer quantum games. *PHYSICAL REVIEW A*, 64:30301, 2001.

[94] W. B. Arthur. Inductive reasoning and bounded rationality. *American Economic Review*, 84(2):406–11, May 1994.

[95] D.M. Greenberger, M. A. Horne, and A. Zeilinger. Going beyond bell's theorem. *arXiv:quant-ph/0712.0921*, December 2007.