La Caminata Cuántica

en el contexto del procesamiento cuántico de la información

Dr. Gonzalo Abal
Instituto de Física – Facultad de Ingeniería
Universidad de la República

Trabajo propuesto en el marco del concurso de méritos y pruebas para el cargo de Profesor Agregado de Física.

Montevideo
30 de Marzo de 2007

Índice general

Las secciones indicadas por (*) *incluyen contribuciones originales desarrolladas en colaboración con nuestro grupo en Montevideo. Las indicadas* (**) *incluyen ideas y propuestas de trabajo actualmente en desarrollo.*

Este trabajo está dedicado a la memoria de Anibal Sicardi.

Capítulo 1

Introducción

El procesamiento cuántico de la información es un área multidisciplinaria, reciente y muy dinámica. Desde el punto de vista de sus aplicaciones, podemos distinguir tres grandes áreas de interés: comunicaciones seguras basadas en distribución cuántica de claves, simulación eficiente de sistemas cuánticos (moléculas, dispositivos microelectrónicos o nanotecnológicos) y el procesamiento algorítmico de información. Esta última área esta potenciada por la posibilidad real de realizar tareas relevantes de forma más rápida que una computadora clásica. El tema convoca a especialistas en Lógica, Matemáticas, Teoría de la información, Física, Ingeniería, Química... trabajando a niveles teórico, experimental y aplicado. Como en otras áreas del conocimiento, existe una sinergia entre los desarrollos teóricos y los avances experimentales que permiten implementarlos. Desarrollos teóricos como la teleportación, el codificado denso, los protocolos criptográficos o los algoritmos de Grover y de Shor, han estimulado y hecho posible la realización de diversos experimentos diseñados para llevarlos a la práctica. Es característico de ésta área, que el proceso predicción-verificación tenga lugar en pocos años, no decenios.

Una carencias importante, es la falta de nuevos algoritmos que aprovechen la ventaja cuántica en situaciones de importancia práctica. Los procesos markovianos han servido de base para la gran familia de algoritmos estocásticos [MR96]. El análogo cuántico de un caminante al azar, es la caminata cuántica (QW). Este protocolo ha despertado un considerable interés en los últimos años ya que, debido a las correlaciones cuánticas, se propaga con mayor rapidez que un caminante al azar clásico y puede explorar un espa-

cio en menor número de pasos que su correspondiente clásico. En ciertas topologías, esta ventaja llega a ser exponencial. Se espera que el QW pueda conducir (como ya lo ha hecho en el caso de los algoritmos de búsqueda) a nuevos algoritmos cuánticos más rápidos que sus correspondientes clásicos. Este trabajo se centra en las realidades y potencialidades de éste protocolo en lo relativo al procesamiento cuántico de la información.

El trabajo está organizado en cinco capítulos. En las siguiente secciones de éste capítulo damos un breve panorama histórico del área, introducimos la notación que usaremos en este trabajo y presentamos los primeros conceptos relativos a la Caminata Cuántica (QW), un protocolo de evolución que es central en éste trabajo. Las correlaciones cuánticas (enredo) son un elemento esencial en el procesamiento cuántico de información.

El capítulo 2 esta dedicado a la caracterización del enredo en sistemas puros y en mezclas estadísticas, en el contexto general del QW con una o dos partículas. Mostraremos aquí algunos resultados propios que hacen posible la caracterización analítica del nivel de enredo a tiempos largos entre los grados de libertad de un caminante cuántico. La Teoría de Juegos proporciona un lenguaje para tratar situaciones entre dos o más agentes que compiten por un recurso con intereses conflictivos. A nivel cuántico, el mismo lenguaje se puede utilizar para aprender sobre el efecto de las medidas sobre estados enredados desde una perspectiva diferente a la de la evolución dinámica. Al final del capítulo 2, damos un ejemplo donde el enredo cuántico es esencial para tener alternativas no existentes en juegos clásicos. Luego mostramos como es posible cuantizar una clase de juegos clásicos (técnicamente, juegos bi-partitas de suma no nula) usando el protocolo del QW con dos o más partículas.

El talón de Aquiles del procesamiento cuántico de la información es la relativamente escasa producción de algoritmos cuánticos que realicen tareas significativas en forma sustancialmente más rápida que sus contrapartes clásicos. En el capítulo 3 discutimos algunos algoritmos cuánticos basados en la técnica de amplificación de amplitud y realizamos un relevamiento de los algoritmos basados en el QW, que no detallamos por razones de espacio. Después de presentar algunas nociones de complejidad algorítmica, consideramos la perspectiva de cuantizar uno de los mejores algoritmos clásicos para resolver una clase de problemas considerados “duros” (NP-completos), para los cuales no se conocen algoritmos eficientes.

Uno de los mayores obstáculos para el procesamiento cuántico de la información es la tendencia de las superposiciones coherentes a degenerar en estados "clásicos" (decoherencia), debido a la interacción inevitable de un sistema cuántico real con su entorno. En el capítulo 5, analizamos diversas manifestaciones de la decoherencia en el QW, desde el punto de vista analítico y numérico y presentamos algunos resultados propios. Finalmente, en el capítulo 6 presentamos nuestras conclusiones y perspectivas.

Por razones de espacio, el enfoque de éste trabajo será fundamentalmente descriptivo, omitiendo todos detalles y demostraciones que no sean necesarios para la comprensión de los conceptos involucrados.

1.1. Procesamiento cuántico de la información

1.1.1. Perspectiva histórica

La idea de que la Mecánica Cuántica podría usarse provechosamente para procesar información fue una de las últimas contribuciones realizadas por R.P. Feynman antes de su muerte en 1988 [Fey82, Fey86]. Esta idea estaba adelantada a su tiempo y en el momento en que fue formulada no tuvo gran impacto, fuera de un pequeño grupo de pioneros entre los que se encontraba Charles Bennet de IBM. En la década del 90, Bennet fue el precursor de la Teleportación, el codificado denso, el primer (y el más usado) protocolo de criptografía cuántica (ver Refs. más adelante). Fue además uno de los primeros en considerar al enredo como un recurso y propuso la medida de enredo actualmente en uso para estados puros. Siendo un físico teórico por formación, Bennet estuvo involucrado en muchos de los experimentos realizados para confirmar sus propuestas teóricas. En 1992 Deutsch y Josza demuestran, a través de un algoritmo concreto [DJ92], que el paralelismo cuántico permite determinar una propiedad global de una función binaria $f(x)$ de argumento entero, exponencialmente más rápido que el mejor algoritmo clásico. Si bien este resultado[1] no resuelve aún un problema práctico, el mismo demuestra el potencial del paralelismo cuántico para procesar información.

[1] La función binaria f esta restringida a ser de dos clases: o es constante o es balanceada, es decir de suma nula. La "propiedad global" consiste en determinar a que clase pertenece. Clásicamente, esto requiere $\mathcal{O}(2^n)$ evaluaciones de $f(x)$, donde n es el tamaño (número de bits) del argumento x. Cuánticamente, se obtiene la misma información con la aplicación de una operación unitaria que evalúa f *simultáneamente en todos los valores de su argumento.*

Poco después Peter Shor formula un algoritmo [Sho97], basado en la transformada cuántica de Fourier, que permite, entre otras cosas, la factorización eficiente[2] de grandes números enteros. Este problema es de gran aplicación práctica, ya que la dificultad para factorizar enteros grandes es la base del protocolo criptográfico RSA, comúnmente usado en la actualidad. A partir del resultado de Shor, se dispara un gran nivel de actividad en el área, tanto a nivel teórico como experimental.

A nivel teórico, se formulan los primeros algoritmos de búsqueda basados en la amplificación de amplitud [NC00], el más conocido de los cuales es debido a Luv Grover [Gro97], el cual esencialmente adiciona la amplificación de amplitud a un protocolo de Deustch-Josza ligeramente modificado. Típicamente, este tipo de algoritmos es capaz de encontrar un ítem particular entre N elementos desordenados, en $\mathcal{O}\left(\sqrt{N}\right)$ pasos, lo cual representa una mejora cuadrática[3] con respecto al caso clásico, que requiere $\mathcal{O}(N)$ pasos.

Los primeros logros experimentales se han producido en el área de la encriptación de información y distribución segura de claves. Protocolos de encriptación cuánticos, como el BB84 (Bennet y Brassard, [BB84]) y el de Eckert [Eke91], han sido implementados usando pares de fotones distribuidos por distancias de varios kilómetros por fibra óptica [MZG96]. Recientemente, se ha demostrado en China el protocolo BB84 sobre una distancia de 15 km usando fotones transmitidos por aire [PBZ$^+$05] y hace un mes se reportó una experiencia similar entre dos de las Islas Canarias, a través de 144 km [Urs06]. Existen dispositivos de encriptación segura, basados en el protocolo BB84, en fase comercial hace un par de años[4].

En 1993 Charles Bennet y colaboradores plantean la posibilidad de utilizar las correlaciones cuánticas (entanglement o enredo), asistido por un canal de comunicación clásico, para *teleportar* estados cuánticos [BBC$^+$93]. La teleportación se concretó por primera vez en 1997, en un experimento con fotones polarizados [BPM$^+$97]. Recientemente, se logró teleportar en forma

[2]En el contexto algorítmico, una determinada tarea se realiza en forma "eficiente" si el número de pasos requeridos crece como un polinomio $\mathcal{O}(x^n)$ con el tamaño n de la entrada. El tamaño de la entrada se asimila, por ejemplo, al número de bits necesarios para representarla.

[3]Los algoritmos cuánticos de búsqueda $\mathcal{O}\left(\sqrt{N}\right)$ son óptimos, es decir que no es posible obtener una ganancia exponencial a partir de técnicas de amplificación de fase.

[4]Véase, por ejemplo, los productos ofrecidos por la compañía suiza *ID Quantique* http://www.idquantique.com/home.htm

determinista estados codificados en partículas masivas (iones de Calcio y Berilio) usando trampas de iones en el NIST [BCS+04] e independiente y simultáneamente en Innsbruck [RHR+04]. En éstos experimentos, que siguen de cerca el protocolo propuesto originalmente por Bennet et al., la distancia es pequeña (una fracción de mm) y se obtiene una fidelidad del orden de 75 % entre el estado original y el teleportado. El año pasado en el Instituto Nils Bohr en Dinamarca [SKO+06] se logró teleportar un estado codificado en luz laser a un ensemble de $\sim 10^{12}$ átomos de Cesio sobre una distancia de ~ 50 cm. Esto representa un logro importante, ya que la información se codifica en fotones para su transmisión, pero se almacena en un soporte material (átomos, iones, spines, o similar). Poder transformar, minimizando pérdidas, un qubit lógico entre ambos tipos de soporte físico[5] (fotones y átomos) es una habilidad esencial para el procesamiento cuántico de la información. En el Apéndice B describimos en detalle un ejemplo sencillo de teleportación y así como del protocolo de codificado denso (también debido a Bennet y colaboradores) que permite enviar dos bits de información usando un sólo qubit usando el enredo.

En los últimos años se han ensayado diversas tecnologías escalables[6] (como las trampas de iones, sistemas con fotones o puntos cuánticos en materia condensada) orientadas a la preparación, manipulación y preservación de estados cuánticos coherentes. Un resumen de las fortalezas y debilidades de las distintas tecnologías candidatas para realizar un computador cuántico se encuentra en la "Hoja de Ruta" de Computación Cuántica, elaborada por un panel de expertos [Hug04]. Actualmente, es posible durante un tiempo limitado preparar y manipular en forma controlada unos pocos qubits[7] y se espera lograr en los próximos años el control coherente de decenas de qubits, lo cual haría posible los primeros ensayos de protocolos cuánticos de corrección de errores, un elemento esencial de cualquier dispositivo práctico para el procesamiento cuántico de información.

[5] A veces se habla, en lenguaje muy gráfico, de qubits voladores y qubits fijos.

[6] Es decir, con el potencial de ser extendidas a decenas o centenas de qubits.

[7] Muy recientemente, la compañía D-Wave lanzó al mercado una máquina con procesador cuántico, basado en pares superconductores, que opera a temperaturas de Helio líquido con la intención declarada de alquilar tiempo de máquina a la industria para simulaciones cuánticas eficientes (Vea http://www.dwavesys.com/ por más detalles). Esta propuesta es limitada, controvertida y no se apoya en trabajo divulgado anteriormente por los canales usuales de la comunidad científica.

1.1.2. Algunos conceptos preliminares

El bit, la unidad de información clásica, se codifica en un sistema físico con dos estados bien diferenciados. En forma similar, la unidad de información cuántica (el qubit) se codifica en un sistema cuántico de dos estados ortogonales. Típicamente, se denomina a estos estados $|0\rangle, |1\rangle$ independientemente de su naturaleza física. Símbolos como $|\cdot\rangle$ representan vectores en un espacio de Hilbert y pueden referirse a los niveles electrónicos internos de un ion en una trampa de iones, a la dirección de polarización de un fotón, a la orientación del spin de un electrón, o a la presencia o no de corriente en un circuito superconductor, entre otros ejemplos. En el Apéndice A, que complementa a esta Sección, damos una versión resumida de los postulados de la Mecánica Cuántica, introducimos con cierto detalle la notación de Dirac (de uso corriente en el contexto de la información cuántica y adoptada en este trabajo) y sentamos las bases de la descripción cuántica de estados de uno o varios qubits en sistemas cuánticos cerrados o abiertos.

Es interesante observar que la especificación de un qubit arbitrario, $|\Psi\rangle = \cos\theta\,|0\rangle + e^{i\varphi}\sin\theta\,|1\rangle$, requiere de dos parámetros reales (θ, φ) y por lo tanto de infinitos bits. Al medir un qubit, el resultado es no determinista. De acuerdo con las reglas de la Mecánica Cuántica, obtenemos una de las alternativas "clásicas": $|0\rangle$ con probabilidad $\cos^2\theta$ y $|1\rangle$ con probabilidad $\sin^2\theta$. Como ya mencionamos, uno de los mayores obstáculos para un dispositivo de computación cuántica real, es la tendencia de las superposiciones cuánticas, como $|0\rangle + |1\rangle$, a decaer hacia las alternativas clásicas ($|0\rangle$, $|1\rangle$) como consecuencia de interacciones con el entorno.

Las transformaciones reversibles de un qubit se llevan a cabo a través de operaciones unitarias. Es usual referirse a estas operaciones (por analogía con el caso clásico) como "compuertas cuánticas". Una compuerta importante es la compuerta de Hadamard que actúa superponiendo uniformemente los kets de entrada

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{1.1}$$

En la representación canónica[8], $|0\rangle \to (1,0)^T$ y $|1\rangle \to (0,1)^T$, la matriz

[8]Usamos el supraíndice T para indicar el transpuesto.

asociada al operador H es

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{1.2}$$

Cuando se consideran estados de más de un qubit, aparecen nuevas propiedades sin análogo clásico. Consideremos primero un estado de n qubits, todos en el estado $|0\rangle$. Este estado se describe por el producto tensorial $|0\rangle^{\otimes n}$. Si se aplica una operación unitaria U sobre n qubits, el nuevo estado es $U|0\rangle^{\otimes n}$. Por ejemplo, si esta operación consiste en $U = H^{\otimes n}$, el resultado es la superposición uniforme de las $N = 2^n$ alternativas clásicas,

$$H^{\otimes n}|0\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \|j\rangle. \tag{1.3}$$

En la expresión anterior, los kets $|j\rangle$ describen estados de n qubits expresados en notación compacta[9]. El estado (1.3) corresponde a una superposición de los primeros 2^N enteros no negativos. La Fig. 1.1 muestra gráficamente la acción de esta compuerta.

Este tipo de superposiciones permite aprovechar las ventajas del paralelismo cuántico. Por ejemplo, una operación U_f que implemente un oráculo[10] $f(x)$, actuaría simultáneamente en los 2^n valores del argumento x. Esto es lo que se hace, por ejemplo, en el algoritmo de Grover, discutido en la Sección 3.1.1.

Existen compuertas que representan operaciones controladas y no pueden descomponerse en productos de compuertas de un qubit. El C-NOT (NOT controlado) es una compuerta de dos qubits que actúa invirtiendo el segundo qubit si el primero esta activo, pero no afecta el segundo qubit si el primero esta inactivo. Se puede expresar en forma simple usando la suma binaria $\oplus$,

$$C|a, b\rangle = |a, a \oplus b\rangle \tag{1.4}$$

donde a y b representan dígitos binarios del primer y segundo qubit, respec-

[9] Por ejemplo, un estado de dos qubits $\|3\rangle = |11\rangle = |1\rangle \otimes |1\rangle$. En general, esta claro a partir del contexto si un ket esta expresado en notación compacta o en notación binaria. Cuando haya posibilidad de confusión usaremos la notación $\|\cdot\rangle$ para identificar a los estados de varios qubits expresados en notación compacta.

[10] En informática teórica se designa así a una función binaria con dominio entero.

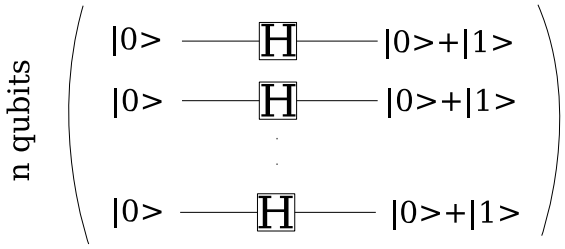

Figura 1.1: Diagrama mostrando la acción de la compuerta $H^{\otimes n}$ sobre el n-qubit $|0\rangle^{\otimes n}$. Se omiten los factores de normalización en las salidas de un qubit. La salida es la superposición uniforme (1.3).

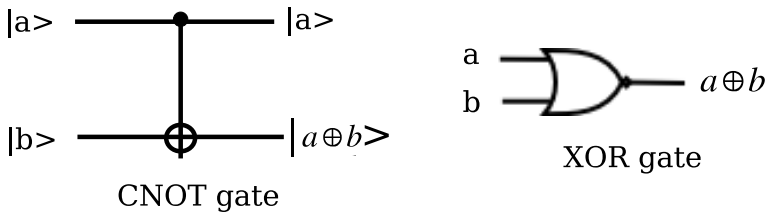

Figura 1.2: Diagramas mostrando la acción de las compuertas CNOT (cuántico) y XOR (clásico). Los símbolos a y b representan dígitos binarios.

tivamente. En forma explícita,

$$\begin{aligned} C|00\rangle &= |00\rangle \\ C|01\rangle &= |01\rangle \\ C|10\rangle &= |11\rangle \\ C|11\rangle &= |10\rangle \end{aligned} \tag{1.5}$$

En la representación canónica de dos qubits, $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, la matriz 4x4 de la compuerta CNOT es

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} I & 0 \\ 0 & \sigma_x \end{pmatrix}$$

donde I es la identidad 2x2, 0 la matriz nula y σ_x la matriz de Pauli que representa la inversión, $\sigma_x|0\rangle = |1\rangle,\ \sigma_x|1\rangle = |0\rangle$. La acción de esta compuerta es similar (a primera vista) a la de la compuerta clásica XOR (OR exclusivo)

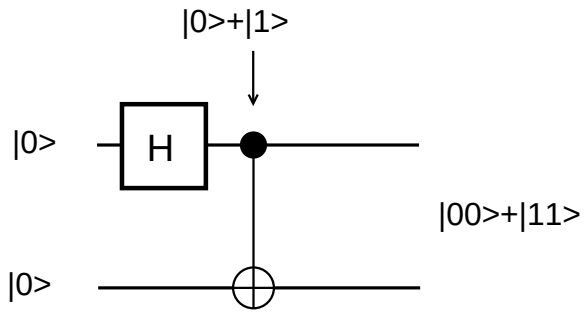

Figura 1.3: Una compuerta CNOT controlada por una superposición genera puede enredar los estados de entrada. Se omiten factores de normalización.

que tiene dos entradas binarias a y b y una salida $a \oplus b$. La compuerta XOR opera de acuerdo a la tabla de la verdad de la suma binaria,

$a\backslash b$	0	1
0	0	1
1	1	0

(1.6)

Sin embargo, existen diferencias fundamentales entre estas compuertas. En primer lugar, la compuerta clásica XOR es una operación irreversible: dada su salida $a \oplus b$, no se puede saber cuales eran los valores de entrada que le dieron origen. En cambio, dada la salida (1.5) de la compuerta CNOT es inmediato saber cual fue la entrada: la compuerta CNOT es (como toda compuerta cuántica) reversible porque se preserva la información del canal de control. En la Figura 1.2 se representa esquemáticamente la acción de ambas compuertas. La otra gran diferencia entre los CNOT clásicos y cuánticos tiene que ver con el hecho de que la compuerta cuántica puede estar controlada por una superposición $\alpha|0\rangle + \beta|1\rangle$. Como lo muestra la Fig. 1.3, en este caso la compuerta puede generar enredo entre los estados de entrada. Por otra parte, compuertas cuánticas que son un producto de compuertas de un qubit, como $H^{\otimes 2}$, no afectan a las correlaciones cuánticas.

La compuerta CNOT es un ingrediente esencial de cualquier dispositivo de procesamiento cuántico de información. Una compuerta CNOT más el conjunto completo de compuertas de un qubit (por ejemplo, las matrices de Pauli y la identidad) conforman un conjunto *universal* de compuertas. Es decir, una operación unitaria arbitraria sobre n qubits se puede implementar en base a éstas compuertas [NC00].

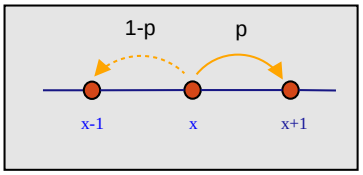

Figura 1.4: En su versión básica unidimensional, un caminante al azar da un paso a la derecha con probabilidad p o (excluyente) a la izquierda con probablilidad $1-p$.

1.2. La Caminata Cuántica

En una cadena de Markov o caminata al azar, la posición del caminante en un instante dado t queda determinada por su posición anterior, en $t-1$, donde t es una variable discreta no negativa. En el caso unidimensional más sencillo, el caminante da pasos iguales (a la derecha o a la izquierda) con probabilidad p y $1-p$, respectivamente. Ocupa sitios discretos uniformemente distribuidos en una línea, que inidicamos por enteros $x = 0, \pm 1, \pm 2, \ldots$ (vea la Fig. 1.4). El desplazamiento es condicional al valor de una variable aleatoria binaria. La caminata al azar es un paradigma para procesos difusivos en general y como tal encuentra múltiples aplicaciones en Ciencia y Tecnología. En particular, las cadenas de Markov han servido de base para diversos algoritmos de optimización que requieren la exploración de espacios multidimensionales. Por ejemplo, como se muestra en el Capítulo 3, algunos de los mejores algoritmos para resolver problemas NP-completos son estocásticos y se basan en la caminata al azar.

La caminata cuántica (QW) [Kem03] es un análogo de una cadena de Markov, en el cual el componente estocástico (un bit de información obtenido, digamos, como resultado de arrojar una moneda) se reemplaza por una operación unitaria aplicada sobre un qubit. Si este qubit se mide a cada paso, se destruye la coherencia y el proceso es markoviano. Pero si se le deja evolucionar en forma unitaria, y se realiza el desplazamiento condicional se obtiene un proceso coherente con características propias. Por ejemplo, la "moneda" cuántica, a diferencia de su contraparte clásica, puede existir en superposiciones de las alternativas clásicas y en ese caso el caminante se

desplaza simultáneamente a derecha e izquierda. La evolución resultante es reversible, como lo requiere la Mecánica Cuántica, y por lo tanto la caminata cuántica *no es un proceso estocástico*[11]. Si bien el desplazamiento condicional es un elemento común a ambos enfoques, el punto de vista cuántico es muy diferente del de un proceso clásico. Al cabo de cierto número de pasos, el caminante cuántico se encuentra en una *superposición de varias posiciones* (y estados de moneda). Sólo cuando se realiza una medida, se obtiene una posición concreta y se destruye el estado previo en el proceso. Además, la propia evolución va generando correlaciones cuánticas entre la moneda y la posición, de modo que – por ejemplo – una medida de la moneda afecta drásticamente la distribución de probabilidad de la posición. En su versión a tiempo discreto, el QW fue propuesto originalmente por Y. Aharonov, L. Davidovich y N. Zagury [ADZ93].

1.2.1. Formalismo básico del QW

El espacio de Hilbert de la caminata cuántica (QW) es de la forma $\mathcal{H} = \mathcal{H}_p \otimes \mathcal{H}_c$ donde $\otimes$ indica un producto tensorial, $\mathcal{H}_p$ es el espacio de posición y $\mathcal{H}_c$ un espacio auxiliar de un qubit (al cual nos referiremos como el espacio de la "moneda"). El espacio de posiciones es generado por el conjunto ortonormal $\{\|x\rangle\}$ donde los enteros $x = 0, \pm 1, \pm 2 \ldots$ están asociados a sitios en la línea. El espacio de moneda es generado por los estados $\{|0\rangle, |1\rangle\}$, de modo que un estado genérico del caminante es descrito por

$$|\Psi\rangle = \sum_{x=-\infty}^{\infty} [a_x|0\rangle + b_x|1\rangle] \otimes \|x\rangle, \tag{1.7}$$

donde a_x, b_x son coeficientes complejos que satisfacen la condición de normalización[12] $\sum_x |a_x^2| + |b_x|^2 = 1$. Un paso de la caminata cuántica se da al aplicar el operador de evolución,

$$U = \sum_x \left(\|x+1\rangle\langle x\| \otimes |0\rangle\langle 0| + \|x-1\rangle\langle x\| \otimes |1\rangle\langle 1| \right) \cdot (I_p \otimes U_c), \tag{1.8}$$

donde I_p es la identidad en el espacio de posición, U_c una operación unitaria en el espacio de un qubit, $\mathcal{H}_c$. Este operador actúa primero haciendo evolucionar la moneda bajo U_c y luego aplica una traslación condicional a

[11] Es bastante común encontrar en la literatura la expresión "quantum random walk" asociada a este proceso, lo cual es claramente un abuso de lenguaje.

[12] En lo que sigue, quedan implícitos los límites de la suma sobre sitios en la línea.

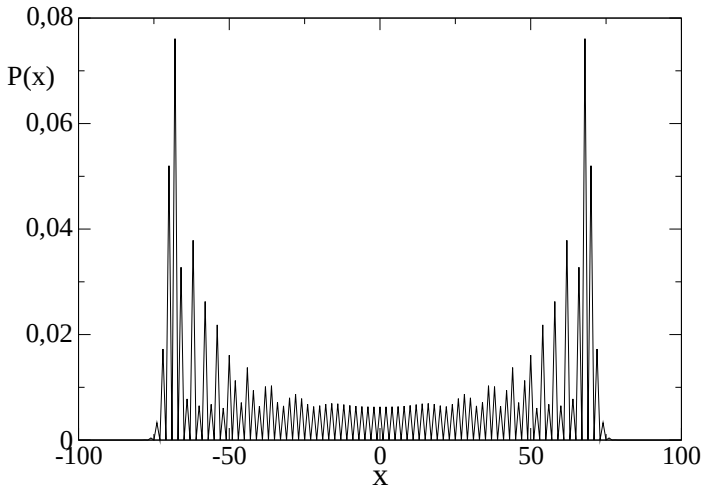

Figura 1.5: Distribución de probabilidad del caminante cuántico, ec. (1.10), después de $t = 100$ pasos. La distribución no guarda ninguna semejanza con la de un caminante al azar con $p = 1/2$, que es una gaussiana centrada en el origen.

las amplitudes de los estados de la moneda. De manera que, a cada paso, el caminante cuántico avanza *simultáneamente* en ambas direcciones. El hecho de que la traslación sea condicional al estado de la moneda, implica que en la evolución se generan correlaciones cuánticas (enredo) entre la posición y la moneda. Trataremos en detalle estas correlaciones y su valor a tiempo largos en el capítulo 2.

Después de t pasos (t es una variable discreta y positiva), un estado inicial $|\Psi(0)\rangle$ evoluciona a

$$|\Psi(t)\rangle = U^t|\Psi(0)\rangle. \tag{1.9}$$

Si se realiza una medida, la partícula será encontrada a cierta distancia del orígen de orden $\sim n$. Más específicamente, la distribución de probabilidad de encontrar la partícula en el sitio x es

$$P(x,t) = \langle\Psi_t| \left(\|x\rangle\langle x\| \otimes I_c\right) |\Psi_t\rangle = |a_x(t)|^2 + |b_x(t)|^2. \tag{1.10}$$

Es muy común usar la operación de Hadamard, introducida en la sección 1.1.2, como operación de moneda ya que la misma al aplicarse sobre $|0\rangle$ (o $|1\rangle$) genera superposiciones uniformes de ambas alternativas, vea la ec. (1.1). Usando $U_c = H$, en la ec. (1.9) y asignando un estado inicial, por ejemplo uno localizado en el origen,

$$|\Psi(0)\rangle = \frac{|0\rangle + i|1\rangle}{\sqrt{2}} \otimes \|0\rangle \tag{1.11}$$

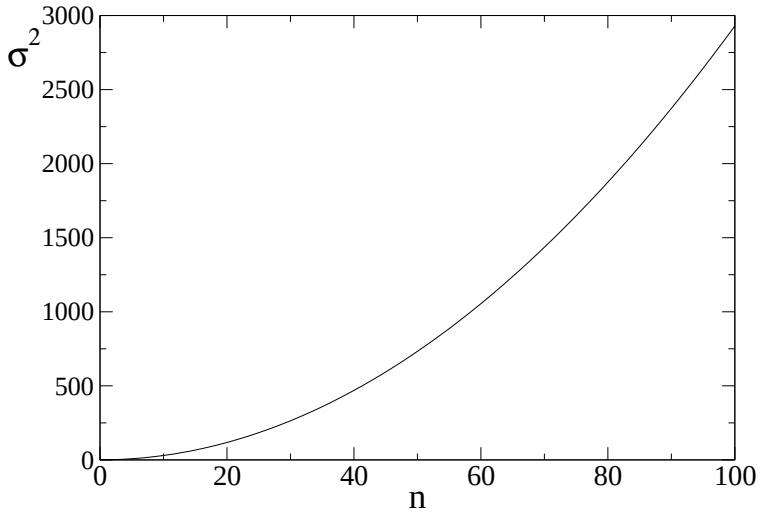

Figura 1.6: Varianza de la distribución $P(n,t)$ en función del número de pasos, t, para una evolución de Hadamard. El crecimiento es balístico independientemente de las condiciones iniciales.

se obtiene una evolución concreta. A partir de la misma se puede evaluar la distribución de probabilidad $P(x,t)$, luego de cierto número de pasos, por ejemplo $t = 100$. El resultado, Fig. 1.5, muestra los efectos de la interferencia entre ondas de materia. Para ésta condición inicial, la evolución de Hadamard es simétrica y se cumple[13] $P(x,t) = P(-x,t)$. Los picos en los extremos avanzan como $x \approx \pm t/\sqrt{2}$. La regla de evolución (1.8) es tal que, partiendo del origen $x = 0$, solo se ocupan sitios con la misma paridad que el número de pasos t. Esto es, para $t = 0, 2, 4 \ldots$, $P(x,t) = 0$ si x impar. Similarmente, a tiempos impares solo se ocupan sitios impares.

La varianza de esta distribución,

$$\sigma^2(t) \equiv \sum_x x^2 \, P(x,t) \tag{1.12}$$

se muestra en la Fig. (1.6) como función del número de pasos. A diferencia del caminante clásico, cuya varianza crece como $\sim t$, en éste caso la varianza crece como t^2 para todas las condiciones iniciales. Este resultado ha sido demostrado por varios autores[14] usando diversas técnicas analíticas [TM02, NV, Kon02a, RSSS$^+$04]. De modo que, en el mismo número de

[13] Esto no es así para condiciones iniciales arbitrarias. Para $U_c = H$ y un inicio localizado, la condición para una evolución simétrica es una moneda inicial $a_0|0\rangle + b_0|1\rangle$ equilibrada ($|a_0| = |b_0|$) y con $\Re(a_0^* b_0) = 0$ [KNS04].

[14] Entre los cuales se cuenta nuestro grupo de Montevideo.

pasos, el caminante cuántico es capaz de explorar una porción significativamente mayor del espacio accesible que el caminante clásico. El crecimiento cuadrático de σ^2 esta directamente relacionado con la interferencia entre ondas de materia y depende de una evolución coherente. Sin embargo, en el Cap. 4 mostramos que en presencia de niveles de ruido moderados, la caminata cuántica es significativamente más rápida que su correspondiente clásica, aún a tiempos largos [RSA$^+$04].

No es posible en general, obtener en forma cerrada la dependencia temporal de los coeficientes $a_x(t), b_x(t)$ definidos en la ec. (1.7). Sin embargo, realizando una transformada de Fourier para expresar el problema en el espacio de número de onda, es posible obtener expresiones aproximadas, válidas para $t \gg 1$ y para una condición inicial dada. En el capítulo siguiente mostramos como, a través del análisis de Fourier, es posible caracterizar el nivel de enredo asintótico entre la moneda y la posición, que en este sistema alcanza valores bien definidos [ADRS06].

1.2.2. Implementación física

En los últimos años se han realizado propuestas para implementar el QW usando diversos sistemas físicos: cavidades con fotones (cavity QED) [SB03], trampas de iones [TM02], átomos neutrales en redes ópticas (optical lattices) [DKB02, EMBL05], resonancia magnética nuclear (NMR) [DLS$^+$03] o usando fotones polarizados y óptica lineal [ZDY$^+$02, PA06, KLM01].

Para implementar el protocolo del QW, es necesario contar con un procesador cuántico capaz de manejar en forma coherente algunos qubits por tiempo suficiente (digamos, $t \approx 10$) para aplicar varias operaciones unitarias. Esto no es una tarea fácil con la tecnología actual, pero tampoco es imposible. De las numerosas propuestas mencionadas, recientemente se ha reportado la realización de dos de ellas. Una se realizó usando el procesador cuántico (basado en Resonancia Magnética Nuclear, NMR) de la Universidad de Waterloo por Ryan et al [RLBL05]. En esta tecnología, los qubits se codifican en ensembles de diferentes tipos de moléculas en solución. El sistema esta a temperatura ambiente y el estado cuántico es una mezcla estadística que debe ser descrita por un operador densidad. Es relativamente fácil implementar compuertas cuánticas de uno y dos qubits usando pulsos de radio frecuencia para interactuar con los spin nucleares de variedades específicas que codifican un qubit dado. Sin embargo, es difícil preparar el

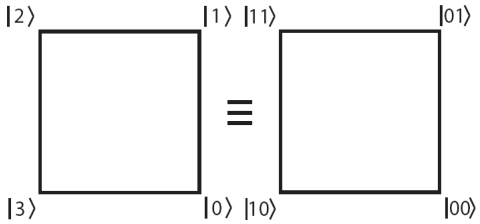

Figura 1.7: La implementación de Ryan et al usa 3 qubits. Con 2 qubits se etiquetan los vértices de un cuadrado. El qubit restante se usa para la moneda. Figura tomada de [RLBL05].

estado inicial deseado y, más importante, la tecnología no es escalable mas allá de sistemas de pocos (7 u 8) qubits [Hug04]. En el experimento de Ryan et al., el procesador cuántico tiene 4 qubits: 2 qubits se usan para describir 4 posiciones, 1 qubit se usa como moneda y el restante, que no participa de la dinámica, es necesario para preparar el estado inicial.

El QW que se reproduce tiene lugar en una geometría cerrada (un cuadrado) en vez de una línea abierta. La distribución de probabilidad de un QW en una cadena cerrada de N nodos, es la misma que la del QW en la línea si el número de pasos es $t \lesssim N$. Para $t \sim N$ aparecen efectos de interferencia entre los dos "extremos" de la función de onda que afectan a la distribución de probabilidad, haciéndola recurrente. Para $t \gg N$ la distribución de probabilidad tiende a ser uniforme en toda la circunferencia. En el caso $N = 4$, luego de $t = 8$ pasos se recupera la distribución de partida, es decir $U^8 = I$. Ryan et al. consideran una operación de moneda de Hadamard y miden el operador densidad (por tomografía cuántica) luego de cada paso $n = 1, 2 \ldots 8$. Obtienen fidelidades del orden de 90 % con respecto al valor teórico. En particular, luego de 8 pasos, la fidelidad con el estado inicial es de $87\,\% \pm 4\,\%$. Finalmente, introducen ruido en forma controlada en la operación de moneda y observan que la distribución de probabilidad tiende a los valores clásicos, como es de esperar.

Implementación con óptica lineal

La otra realización experimental del QW [DSB$^+$05] se basa en una propuesta realizada en 2003 [DLX$^+$03] que utiliza la polarización y la dirección de propagación de fotones junto con elementos de óptica lineal para codificar el QW sobre una "línea dinámica" abstracta. Esta propuesta ha sido

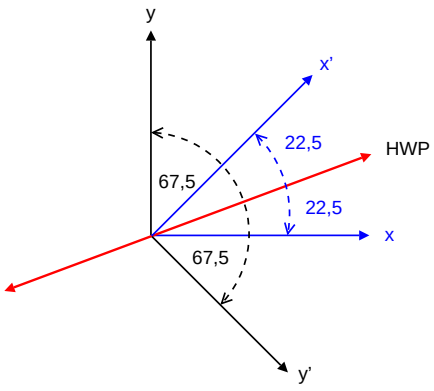

Figura 1.8: Geometría para la acción de la placa de media onda que simetriza las direcciones de polarización en torno a su eje principal (línea roja). Cuando el mismo se orienta formando un ángulo de $22,5^o$ con x, esta dirección de polarización se transforma en x' y la dirección ortogonal y en y', lo cual corresponde a la transformación de Hadamard, ec. (1.13).

recientemente extendida a pares de fotones [PA06], lo cual permite implementar un QW con dos partículas. Este esquema puede ser la base para una implementación de juegos cuánticos iterados (Sección 2.3.2), por lo que será expuesto en cierto detalle.

El qubit de moneda se codifica usando los estados de polarización lineal (x, y) de un fotón. La posición en una línea abstracta se codifica de una forma algo más compleja que explicamos más adelante, pero los grados de libertad relevantes son dos direcciones de propagación (h, v) del fotón en una mesa óptica bidimensional. El estado del fotón en un momento determinado es un estado de dos qubits $|\varphi\rangle \in \mathcal{H}_2$, donde asociamos el primero a la dirección de propagación y el segundo a la polarización de modo que $|\varphi\rangle = |t, p\rangle = |t\rangle|p\rangle$.

Establecemos contacto con el protocolo del QW a través de las asociaciones

$$t \begin{cases} h & \leftrightarrow & 0 \\ v & \leftrightarrow & 1 \end{cases} \qquad \text{y} \qquad p \begin{cases} x & \leftrightarrow & 0 \\ y & \leftrightarrow & 1. \end{cases}$$

De este modo, el ket $|01\rangle$ representa a un fotón que se propaga en dirección h con polarización y y el ket $|t\,p\rangle$ con t, p binarios representa un estado de la base computacional de dos qubits.

Los elementos de óptica lineal requeridos para implementar un QW son una placa de media onda (HWP, Half-Wave Plate) y un separador de haz

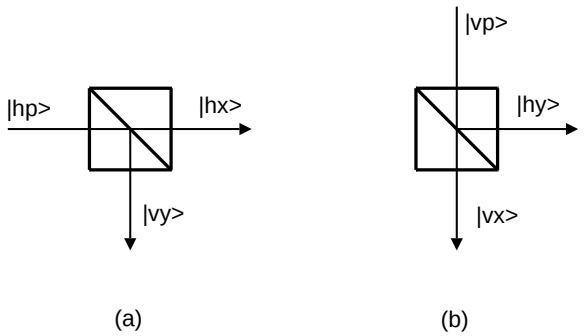

Figura 1.9: A PBS transmits the x component and reflects the y component of polarization. When a photon enters the PBS in a superposition polarization state $|p\rangle = \alpha|x\rangle + \beta|y\rangle$, its propagation direction is shifted only for the polarization component y. This conditional operation implements a polarization-controlled CNOT gate, as discussed in the text.

por polarización (PBS, Polarizing Beam Splitter). Este elemento simetriza las componentes de polarización con respecto a la dirección de su eje principal. Orientando el mismo para que forme un ángulo de $22,5^o$ con la dirección de polarización x, como se muestra en la Fig. 1.8, implementa una transformación de Hadamard sobre la polarización,

$$H|x\rangle = \frac{1}{\sqrt{2}}(|x\rangle + |y\rangle), \qquad H|y\rangle = \frac{1}{\sqrt{2}}(|x\rangle - |y\rangle). \tag{1.13}$$

El cubo PBS transmite la componente x de polarización, pero refleja la componente y, cambiando la dirección de propagación en forma condicional a la polarización, como se muestra en la Fig. 1.9. Esto representa una operación CNOT sobre la dirección de propagación (codificada en el primer qubit) controlada por la polarización (codificada en el segundo qubit).

Estos elementos básicos se intercalan como se muestra en la Fig. 1.10. Un fotón sale de un PBS moviéndose en dirección h o v con polarización arbitraria. Si sale en la dirección h se considera que dio un paso a la derecha en una línea imaginaría (llamada "línea dinámica") en la cual tiene lugar el QW lógico. Si sale del PBS con dirección v se considera que da un paso a la izquierda en la línea dinámica. La posición n en la línea dinámica (esto es, el número de pasos horizontales menos el número de pasos verticales) se puede incluir en la descripción del caminante. Un estado del mismo pasa a estar dado por $|n, t, p\rangle$, donde $|t, p\rangle$ representa los estados genéricos asociados a la dirección de propagación y la polarización, pero $|n\rangle$ representa un registro

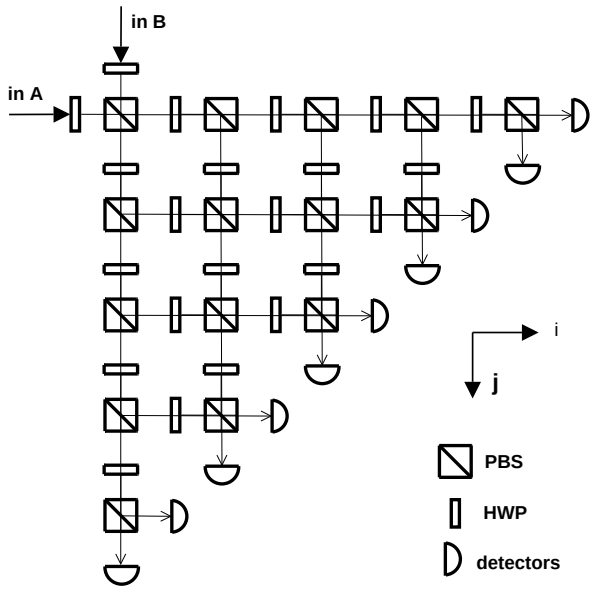

Figura 1.10: Optical arrangement that produces a QW with one or two photons. The input ports are labelled A and B. In this example, the detectors are placed so that the positions of the photons are measured after $N = 5$ iterations.

de varios qubits asociado a la posición en la línea dinámica. La acción del PBS se representa en este espacio por

$$C = \sum_n \left[\left(\sum_t |n,t,x\rangle\langle n,t,x| \right) + |n,v,y\rangle\langle n,h,y| + |n,h,y\rangle\langle n,v,y| \right]$$

Recordemos que esta operación condicional sobre la dirección de propagación es controlada por la polarización. Al salir de un cubo PBS se aplica un operador traslación S que modifica la posición en la línea dinámica en ± 1 en forma condicional a la dirección de propagación,

$$S = \sum_{n,p} \left(|n+1,h,p\rangle\langle n,h,p| + |n-1,v,p\rangle\langle n,v,p| \right)$$

donde p representa un estado genérico de polarización. En este espacio, un paso de la evolución queda dado por un operador unitario

$$U = S \cdot C \cdot (I \otimes H).$$

Partiendo de un estado inicial, luego de pasar por t cubos PBS, se obtiene $|\Psi_t\rangle = U^t|\Psi_0\rangle$ y se realiza la medida de la posición y dirección de propagación n, d a través de la detección (y destrucción) del fotón en alguno de los detectores del array.

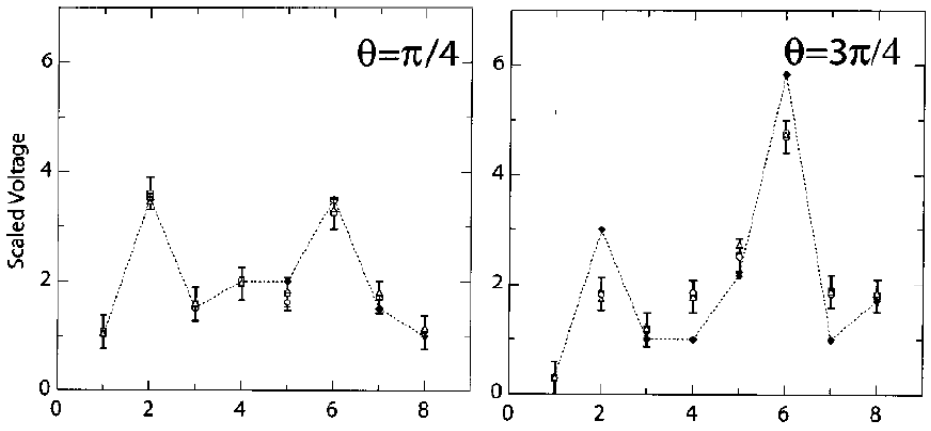

Figura 1.11: Resultados de 4 experimentos midiendo la posición del QW en la línea dinámica luego de pasar por $t = 5$ compuertas PBS-H. El eje horizontal corresponde al número del detector, es decir a sitios en la línea dinámica ($n = 0$ corresponde al detector # 4). El eje vertical es proporcional a la intensidad observada en cada sitio. El ángulo θ fija la polarización inicial con respecto a x, como se discute en el texto. Figura tomada de [DSB$^+$05].

El aparato puede operarse en régimen de baja intensidad, de modo que un único fotón este presente a la vez en el mismo. En este caso, el fotón interfiere consigo mismo en los diferentes caminos hacia uno de los detectores. En el experimento de [DSB$^+$05], se usó como estado inicial $|\Psi_0\rangle = |n = 0\rangle \otimes |v\rangle \otimes |p\rangle$, donde la polarización forma un ángulo θ con la dirección x, es decir $|p\rangle = \cos\theta|x\rangle + \sin\theta|y\rangle$. Los resultados (esperados vs. observados) luego de pasar por $N = 5$ PBS y para varios valores de θ se muestran en la Fig. 1.11. Los efectos de interferencia son visibles, pese a que solo son cinco pasos.

Finalmente, mencionamos que se ha "simulado" un QW usando interferencia entre señales luminosas coherentes [KRS03b, JPK04] aunque en este caso, no es posible reproducir algunos aspectos esenciales ya que la "caminata" se realiza en frecuencia y la información se codifica en modos clásicos del campo electromagnético. Como consecuencia, no hay enredo entre la posición y la "moneda" [KRS03a].

1.2.3. La Caminata Cuántica a tiempo continuo

Existe una versión de la caminata cuántica basada en una descripción Hamiltoniana con tiempo continuo, introducida en 1998 por Fahri y Gutmann [FG98]. Esta versión produce resultados similares a la de tiempo discreto, pero presenta algunas diferencias. Por ejemplo, no requiere un grado de libertad de moneda. Algunos resultados algorítmicos interesantes [CCD$^+$03, CG04] se han formulado en base a la caminata a tiempo continuo, por lo que la definiremos aquí y daremos algunas características básicas de la misma.

La idea es considerar sitios en un grafo definido por un conjunto de vértices $\mathcal{V} = \{1, 2, \dots v\}$ y un conjunto de conexiones entre ellos. Las conexiones pueden definirse por una matriz de conectividad A, de dimensión $v \times v$ talque $A_{ij} = 1$ si los vértices (i, j) están conectados y $A_{ij} = 0$ de otro modo. La diagonal de A es nula.

Se considera el espacio de Hilbert generado por los estados $|x\rangle$, donde x es un vértice del grafo, $x \in \mathcal{V}$. Un estado genérico se representa por

$$|\Psi(t)\rangle = \sum_x a_x(t)|x\rangle. \tag{1.14}$$

La evolución está dada por la ecuación de Schrödinger (usamos $\hbar = 1$),

$$i\frac{d}{dt}\langle x|\Psi(t)\rangle = \sum_y \langle x|H|y\rangle\langle y|\Psi(t)\rangle \tag{1.15}$$

donde el hamiltoniano se define proporcional a la matriz de conectividad[15], $H = -\gamma A$ y γ es la probabilidad por unidad de tiempo de que tenga lugar una transición entre dos vértices. Si escribimos la solución formal de la ecuación de Schrödinger,

$$|\Psi\rangle = e^{-i\gamma At}|\Psi(0)\rangle \tag{1.16}$$

se ve el parecido con el QW a tiempo discreto con la identificación $U = e^{-i\gamma A}$.

Nos interesa el caso particular de la caminata a tiempo continuo en una línea. En este caso, un sitio x solo conecta con sus vecinos $x \pm 1$. El Hamiltoniano se reduce a

$$H|x\rangle = -\frac{1}{2}\left(|x-1\rangle + |x+1\rangle\right) \tag{1.17}$$

[15]Para grafos bidireccionales, como los considerados aquí, $A_{ij} = A_{ji}$ y el Hamiltoniano es hermítico.

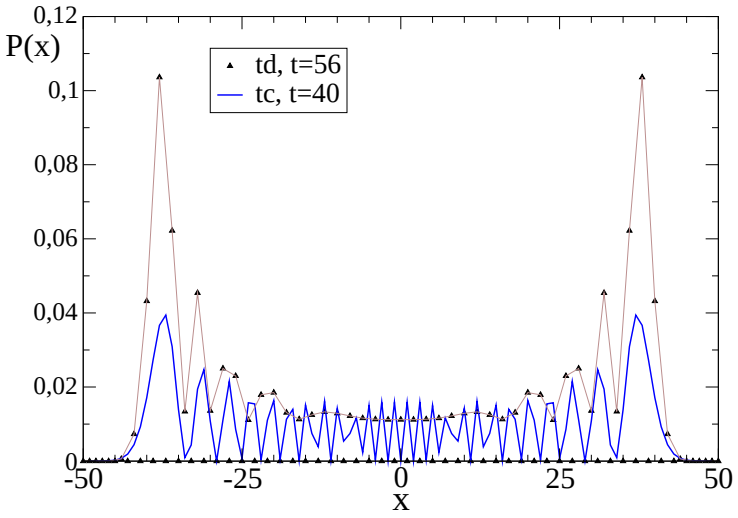

Figura 1.12: Comparación entre las distribuciones de probabilidad generadas por (i) la caminata a tiempo discreto en marrón, obtenida a partir de la ec. (1.19), con $t = 56$ (se grafican los sitios pares, pero los triángulos indican todos los puntos) y (ii) a tiempo continuo con $t = 40$ en azul. La condición inicial es localizada en $x = 0$ y en el caso de la caminata a tiempo discreto la moneda es $(|0\rangle + i|1\rangle)/\sqrt{2}$.

es decir, una matriz con las dos diagonales vecinas de la principal con valores constantes. Hemos fijado $\gamma = 1/2$ para que la probabilidad de ir a derecha o a izquierda sea 1 y la probabilidad de permanecer en el sitio x, cero.

La solución de (1.15) en este caso es inmediata. Los coeficientes $a_x(t)$, definidos en la ec. (1.14), satisfacen

$$i\frac{d}{dt}\,a_x = -\frac{1}{2}\left[a_{x+1}(t) + a_{x-1}(t)\right]. \tag{1.18}$$

Para una condición inicial localizada en el origen, $a_x(0) = \delta_{x0}$, la solución de esta ecuación es proporcional a la función de Bessel cilíndrica,

$$a_x(t) = (-i)^x J_x(t), \tag{1.19}$$

de modo que la distribución de probabilidad es simplemente $P(x,t) = J_x^2(t)$.

En la Fig. 1.12 se muestra esta distribución para $t = 40$. La distribución del QW a tiempo discreto para $t = 56$ se muestra en el fondo y la semejanza es evidente. La razón por la cual es necesario usar tiempos de evolución diferentes en la comparación es que la velocidad de dispersión de la caminata a tiempo continuo es algo mayor que la de tiempo discreto. En ambos casos, la varianza asociada a la distribución $P(x,t)$ crece cuadráticamente con el tiempo.

La relación formal entre ambos procesos (tiempo discreto, tiempo continuo) era un problema en abierto hasta que se estableció detalladamente la forma de pasar del QW discreto al continuo, el año pasado [Str06]. Pese a que ambos espacios de Hilbert son diferentes (uno tiene un qubit de moneda que el otro no tiene) tomando el límite de tiempo continuo del QW discreto produce dos caminatas a tiempo continuo, una para cada grado de libertad de la moneda. En este trabajo nos ocuparemos principalmente de la caminata a tiempo discreto, ya que esta propuesta es más cercana al modelo de compuertas lógicas usado en la búsqueda de nuevos algoritmos.

Capítulo 2

Correlaciones cuánticas

El enredo es una de las características que distinguen a la Mecánica Cuántica de una descripción clásica. Si dos partículas comparten un estado enredado, el estado de cada una depende del estado de la otra, aunque se encuentren espacialmente separadas y sin interacción mutua. Las medidas de observables asociados a cada una de ellas estarán correlacionadas entre si, de una forma que excluye a las explicaciones clásicas basadas en el realismo local.

Estas correlaciones cuánticas (o enredo, para abreviar) son un recurso esencial para el procesamiento cuántico de información. El enredo puede ser creado, transformado de diversas maneras y consumido para realizar determinadas tareas. Los protocolos cuánticos de corrección de errores, un componente esencial de cualquier dispositivo real, requieren de grandes cantidades pares de estados enredados.

La teleportación cuántica es una de las aplicaciones mas importantes de los estados enredados. Por ejemplo, la teleportación más las operaciones de un qubit conforman un conjunto universal de operaciones [GC99]. En la actualidad, la teleportación tiene un rol importante en la transformación de la información codificada en un qubit lógico con soporte físico en fotones (y por lo tanto móvil) a un soporte material para su almacenamiento o procesamiento. Por ejemplo, experimentos recientes teleportan información de pulsos luminosos a ensembles de $\sim 10^{15}$ átomos de Cesio [SKO$^+$06, JSC$^+$04]. En el ejemplo elemental del Apéndice B, mostramos que para teleportar un qubit se consume cierta cantidad (un e-bit) de enredo.

Las aplicaciones criptográficas constituyen otro ejemplo de la impor-

tancia de la capacidad de manipular correlaciones cuánticas. Existen desde hace tiempo protocolos de distribución segura de claves basados en estados enredados [Eke91], y han sido implementados usando pares de fotones distribuidos por distancias de decenas de kilómetros por fibra óptica [MZG96] y por aire [PBZ+05]. Una forma de extender el alcance de estas técnicas es usar "repetidores cuánticos", capaces de recibir un fotón de un par enredado y re-transmitir otro fotón con las mismas características que el primero [BDCZ98]. Esto debería realizarse además con suficiente fidelidad como para no estropear la información transmitida. Las exigencias técnicas para un repetidor cuántico operativo son formidables. Pese a ello, se ha reportado recientemente un gran avance en esta dirección [YZC+06] usando la técnica de "Entanglement swapping"[1].

Por todo lo anterior, es importante aprender a cuantificar el nivel de enredo en un sistema cuántico. La cuantificación del enredo esta bien establecida en el caso de enredo bipartita entre estados puros. No obstante, el caso de las mezclas estadísticas (típicas de sistemas cuánticos abiertos) es el más relevante desde el punto de vista de las aplicaciones y en este caso existen múltiples medidas de enredo con propiedades diferentes. En el caso de enredo multipartita, la situación es aún más compleja. En este trabajo nos limitaremos al caso de enredo bipartita.

La caminata cuántica en la línea, con una partícula, presenta enredo entre los estados de posición y de moneda. Este enredo se genera durante la evolución. Cuando se consideran dos partículas, pueden aparecer diversos tipos de enredo (entre ambas posiciones, entre ambas monedas, etc.). Ciertas operaciones de moneda generan enredo entre las partículas, otras lo preservan. En este capítulo intentamos dar un panorama de como se puede caracterizar y cuantificar el enredo en el QW de una y dos partículas. Finalmente, dado que el enredo es una de las características que distingue a los juegos cuánticos de sus correspondientes clásicos, hemos incluido una sección sobre juegos cuánticos, especialmente los juegos iterados que hemos propuesto recientemente, basados en el QW.

[1] En esencia, esta técnica consiste en lo siguiente: dado un par enredado A-B con A y B alejados entre si, es posible hacer que B interactue con una tercer partícula C y generar enredo B-C. Una medida (usualmente destructiva) de B, deja el par A-C en un estado mutuamente enredado, aunque A y C nunca han interactuado directamente! La partícula B ha servido de mediadora para generar enredo entre A y C.

2.1. Estados enredados

Los estados enredados están implícitos en el Principio de Superposición, aplicado a estados de más de una partícula. Por ejemplo, un estado genérico del sistema compuesto más simple, un estado arbitrario de dos qubits en el espacio de Hilbert $\mathcal{H}_2$, tiene la forma

$$|\Psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle. \tag{2.1}$$

Como mencionamos en el Apéndice A, a menos que se verifique la relación (A.48) entre los coeficientes, no es posible descomponer este estado en un producto de dos estados de un qubit. En $|\Psi\rangle$, el estado de una partícula depende del estado de la otra. Los estados producto, $|\Psi_p\rangle = |\varphi_A\rangle \otimes |\varphi_B\rangle$, en los cuales cada subsistema (A,B) esta en un estado bien definido, son estados especiales de $\mathcal{H}_2$.

Los llamados "estados de Bell"[2]

$$\begin{aligned} |\Phi^{\pm}\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle \pm |11\rangle\right) \\ |\Psi^{\pm}\rangle &= \frac{1}{\sqrt{2}}\left(|01\rangle \pm |10\rangle\right) \end{aligned} \tag{2.2}$$

forman una base ortonormal en $\mathcal{H}_2$ y son estados máximamente enredados: una medida de uno de los qubits, permite predecir *con certeza* el valor del otro. El enredo de uno de éstos pares de Bell es una unidad adecuada para medir este recurso y recibe el nombre de "e-bit" (entanglement-bit o unidad de enredo).

Enredo parcial

Un estado de más de un qubit puede estar parcialmente enredado, como por ejemplo

$$|\Psi(\theta)\rangle = \cos\theta|00\rangle + \sin\theta|11\rangle \tag{2.3}$$

donde $\theta \in [-\pi/2, \pi/2]$. Supongamos que ambos qubits se separan y Alice mide el primero en tanto Bob mide el segundo, en una experiencia tipo EPR. Para comprender la naturaleza del enredo parcial, supongamos por simplicidad que $\theta \in [0, \pi/4]$ y consideremos dos situaciones:

[2] La nomenclatura se justifica por su rol central en las experiencias tipo EPR vinculadas a verificaciones experimentales de violaciones a las desigualdades de Bell.

i) Si Alice no hace nada, Bob observa $|0\rangle$ con probabilidad $p_B(0) = \cos^2\theta$ y $|1\rangle$ con probabilidad $p_B(1) = \sin^2\theta$.

ii) Alice mide su qubit y digamos que obtiene $|0\rangle$. Después de la medida, el sistema conjunto esta en $|00\rangle$. En general, la realidad de Bob se ve afectada por la medida ya que ahora tiene probabilidades $p'_B(0) = 1$ y $p'_B(1) = 0$.

La magnitud del cambio en la realidad de Bob depende de θ. Si $\theta = 0$ no cambió nada, ya que las probabilidades de Bob son iguales antes y después de la medida de Alice; esto coincide con el caso en que el estado $|\Psi\rangle$ es separable y no hay enredo. En cambio, si $\theta = \pi/4$, el cambio es máximo: antes de la medida de Alice ambos resultados son equiprobables para Bob (mínima información). Después de la medida de Alice, Bob sabe con certeza que su medida resulta en $|0\rangle$ (máxima información). Esto coincide con el caso en que (2.3) es un estado de Bell, máximamente enredado. En los casos intermedios, la medida de Alice afecta la realidad de Bob en una proporción que depende del valor de θ. Estas correlaciones reflejan el carácter no local de la Mecánica Cuántica.

Enredo y el operador densidad

En general, en el contexto del procesamiento cuántico de información es necesario trabajar con el formalismo de operador densidad (en la Sección A.3, enumeramos sus propiedades más relevantes) que representa la mezcla estadística resultante cuando se cuenta con información incompleta sobre el sistema.

Existe una correspondencia entre los estados en el espacio de Hilbert $\mathcal{H}$ y los operadores densidad ρ en el espacio asociado $\mathcal{D}(\mathcal{H})$. Recordamos que el operador densidad se define como

$$\rho = \sum_{i=1}^{n} p_i |\Psi_i\rangle\langle\Psi_i| \tag{2.4}$$

donde las probabilidades p_i satisfacen los requisitos usuales, $0 \leq p_i \leq 1$ y $\sum_i p_i = 1$. Dado un operador densidad ρ que describe un estado de un sistema compuesto, $\mathcal{H} = \mathcal{H}_\mathcal{A} \otimes \mathcal{H}_B$, diremos que un estado bipartita ρ es separable si es posible expresarlo como una mezcla de estados producto,

$$\rho = \sum_{i=1}^{n} p_i \rho_i^{(A)} \otimes \rho_i^{(B)} \tag{2.5}$$

donde $\rho_A \in \mathcal{D}(\mathcal{H}_A)$ y similar para B, son operadores locales a los subespacios $\mathcal{H}_A$ o $\mathcal{H}_B$.

Dado un operador compuesto ρ, no es obvio si el mismo es separable. Por ejemplo, dado el estado

$$\rho = \begin{pmatrix} \frac{3}{24} & i\frac{\sqrt{2}}{24} & 0 & i\frac{\sqrt{2}}{12} \\ -i\frac{\sqrt{2}}{24} & \frac{1}{4} & -i\frac{\sqrt{2}}{12} & 0 \\ 0 & i\frac{\sqrt{2}}{12} & \frac{5}{24} & -i\frac{\sqrt{2}}{24} \\ -i\frac{\sqrt{2}}{12} & 0 & i\frac{\sqrt{2}}{24} & \frac{5}{12} \end{pmatrix}$$

en la representación canónica de dos qubits, $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ (vea el Apéndice A), no es evidente que puede expresarse como una mezcla de la forma (2.5) y es separable.

Un testigo de enredo (entanglement witness) es cualquier cantidad, computable a partir de ρ o medible en el laboratorio, que permita distinguir estados enredados de estados producto. El parámetro de Bell, S, asociado a las correlaciones entre medidas de observables conjugados de un par de partículas, es un testigo de enredo que se determina experimentalmente. Un testigo de enredo responde la pregunta sobre si un estado es separable, pero en caso negativo no nos dice cuanto enredo contiene (en términos de e-bits), por lo que es de utilidad limitada.

2.2. Medidas de enredo

Para cuantificar el enredo se requiere una cantidad que refleje la intensidad de las correlaciones cuánticas (EPR) entre ambas partículas, pero que no sea crezca debido a otro tipo de correlaciones. Usamos la notación usual para el espacio de Hilbert $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ compuesto por dos subsistemas A y B. Los operadores densidad ρ, ρ_A, ρ_B pertenecen a los correspondientes espacios asociados. En general, una medida de enredo es un funcional E que asocia un real no negativo a cada operador densidad $\rho \in \mathcal{D}(\mathcal{H})$. Existen algunos requisitos que una medida de enredo "útil" debe satisfacer [SM95, HHH96, VPRK98]:

1. Testigo de enredo. $E(\rho) = 0$ si y solo si, el estado ρ es separable.

2. Normalización. $E(\rho)$ es máximo cuando ρ está completamente mezclado. En particular, para dos subespacios de dimensión d, el estado má-

ximamente enredado $|\Phi_d^+\rangle = \sum_{i=1}^{d}(|i\rangle_A \otimes |i\rangle_B)/\sqrt{d}$, donde $|i\rangle_A$ ($|i\rangle_B$) es una base ortonormal en $\mathcal{H}_A$ ($\mathcal{H}_B$), tendrá un enredo $E(|\Phi_d^+\rangle\langle\Phi_d^+|) = \log_2 d$. Para el caso de enredo entre dos qubits, $d = 2$, $|\Phi_2^+\rangle$ es un estado de Bell y el máximo es $E = 1$.

3. Monotonía bajo operaciones LOCC. El enredo (correlaciones entre partes distantes de un mismo sistema) no puede generarse[3] a partir de operaciones locales, aunque se disponga de un canal de comunicación clásica que permita coordinar las operaciones de A y B. Este conjunto de operaciones – mediante las cuales es imposible generar enredo – recibe el nombre LOCC (Local operations and Classical Communications). Cuando hablamos de "operaciones locales" nos referimos a Medidas Generalizadas (vea el Apéndice A) restringidas a cada uno de los subespacios A,B (operaciones unitarias locales y/o medidas proyectivas locales). Una buena medida de enredo debe ser monótona decreciente bajo LOCC. Es decir, no puede aumentar bajo LOCC. En base a este requisito, a veces se denomina a la medida de enredo un "monótono de enredo" (entanglement monotone). Si denotamos por $\mathcal{E}_{A,B}$ las respectivas LOCC,

$$\rho \to \rho' = [\mathcal{E}_A \otimes \mathcal{E}_B](\rho)$$

entonces $E(\rho) \geq E(\rho')$.

4. Convexidad. El enredo de una mezcla es menor o igual que la mezcla del enredo de sus componentes. Es decir que las correlaciones clásicas de una mezcla estadística no aumentan el nivel de enredo,

$$E\left(\sum_i p_i \rho_i\right) \leq \sum_i p_i E(\rho_i).$$

Existen además algunos requisitos de segundo orden, de carácter más técnico (como el que tiene que ver con la sub-aditividad del enredo) que no serán detallados aquí. En líneas generales, se pueden dividir las medidas de enredo en dos grandes clases: las medidas de tipo "operacional" y las medidas "computables".

[3]De hecho, podría definirse el enredo como el tipo de correlaciones que no es posible generar via LOCC.

Hay varias medidas de enredo en uso, que satisfacen estas condiciones total o parcialmente. Para estados puros, la situación es mas simple ya que existe un teorema de unicidad y se usa casi exclusivamente la entropía de enredo. Para mezclas estadísticas hay una multitud de medidas en uso, de las cuales sólo mencionaremos algunas. En particular, la Concurrencia [Woo98] es especialmente interesante debido a que se ha mostrado recientemente [WSRD$^+$06] que es directamente observable en el laboratorio. En este trabajo, por simplicidad, limitamos la discusión al caso de enredo bipartita.

2.2.1. Estados puros – Entropía de enredo

La cuantificación del enredo en el caso de un estado puro bipartita, con $|\Psi\rangle \in \mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$, se ve facilitada por que estos estados describen sistemas sin correlaciones clásicas. Para un estado puro enredado, el estado de cualquier subsistema componente es una mezcla. En este caso, el grado de "mezcla" o la falta de información sobre cual es el estado del subsistema, se puede tomar como un indicador fiable del enredo.

Un ejemplo ayudará a aclarar la situación. El estado de Bell $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ esta representado por el operador densidad

$$\rho = \frac{1}{2}\left(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|\right) \tag{2.6}$$

que evidentemente describe un estado puro, ya que $tr(\rho^2) = 1$. Para representar el estado del qubit en $\mathcal{H}_A$ (el primer qubit desde la izquierda), aplicamos la traza parcial sobre el otro subespacio[4] y obtenemos el operador densidad en $\mathcal{D}(\mathcal{H}_A)$,

$$\rho_A = tr_B(\rho) = \frac{1}{2}I \tag{2.7}$$

donde I es la identidad en el espacio de un qubit $\mathcal{H}_A$. Este estado describe una mezcla estadística ya que $tr(\rho_A^2) = 1/2 < 1$ y es un estado de mínima información: una medida del primer qubit resulta en $|0\rangle$ o $|1\rangle$ con probabilidad 1/2. Esto es una manifestación del enredo presente en $|\Phi^+\rangle$, ya que la traza parcial representa una media sobre todos los estados de B.

La falta de información en un estado ρ puede cuantificarse adecuadamente usando la entropía de von Neumann, S

$$S(\rho) \equiv -tr(\rho \log \rho) = -\sum_i \lambda_i \log \lambda_i \tag{2.8}$$

[4]La situación es completamente idéntica si se busca expresar el estado del segundo qubit tomando la traza con respecto al primero.

donde los λ_i son los autovalores de ρ. En el caso de un estado puro, como (2.6), la entropía es nula. Pero en el caso de la mezcla (2.7) la entropía es máxima (y el contenido de información, mínimo). En efecto, es fácil verificar directamente que $S(\rho_A) = 1$, si se usa el logaritmo base 2.

De modo que, para estados puros, puede usarse la entropía asociada a la matriz reducida como una medida de enredo. Esta entropía verifica las propiedades que hemos enunciado en la sección anterior y se conoce como "Entropía de enredo",

$$S_E(\rho) \equiv -tr_A(\rho_A \log \rho_A) = -\sum_{i=1}^{d_A} \lambda_i \log_{d_A} \lambda_i \tag{2.9}$$

donde $\rho_A = tr_B(\rho)$ y d_A es la dimensión de $\mathcal{H}_A$. En realidad, es una materia de conveniencia si la entropía se calcula tomando la traza sobre el subespacio A o el B ya que los autovalores de la matriz reducida son los mismos[5].

A modo de ejemplo, consideramos el estado puro con enredo parcial definido en la ec. (2.3). El operador densidad reducido es diagonal, con autovalores $\lambda_1 = \cos^2\theta$ y $\lambda_2 = \sin^2\theta$, de modo que la entropía de enredo es

$$S_E(\theta) = -\cos^2(\theta)\log_2\left[\cos^2(\theta)\right] - \sin^2(\theta)\log_2\left[\sin^2(\theta)\right].$$

Esta función, de período $\pi/2$, se gráfica en la Fig. 2.1. El grado de enredo varía entre 0 (estado producto) y 1 (estado máximamente enredado). La entropía de enredo permite cuantificar en forma simple las situaciones de enredo parcial, como la descrita en el apartado anterior.

Existe un teorema de unicidad para la entropía de enredo. Este resultado establece que, para estados puros, cualquier medida de enredo que satisface los criterios (1-3) antes enunciados más algunas otras condiciones razonables relativas a la aditividad y continuidad debe coincidir con la entropía de enredo [DHR02]. De modo que, en los últimos años, esta es la medida de enredo que se ha usado, en casi todos los casos, para cuantificar el enredo para estados puros. Sin embargo, no es adecuada para mezclas estadísticas, ya que no distingue entre correlaciones cuánticas y clásicas. Las siguientes secciones describen trabajo recientemente publicado, realizado en colaboración con nuestro grupo, donde usamos esta medida de enredo para cuantificar

[5]Este resultado se prueba usando la descomposición de Schmidt para expresar el estado puro en la forma $|\Psi\rangle = \sum_{k=1}^{min(d_A,d_B)} \mu_k |a_k\rangle \otimes |b_k\rangle$, de donde resulta que los operadores reducidos tienen los mismos autovalores μ_k^2.

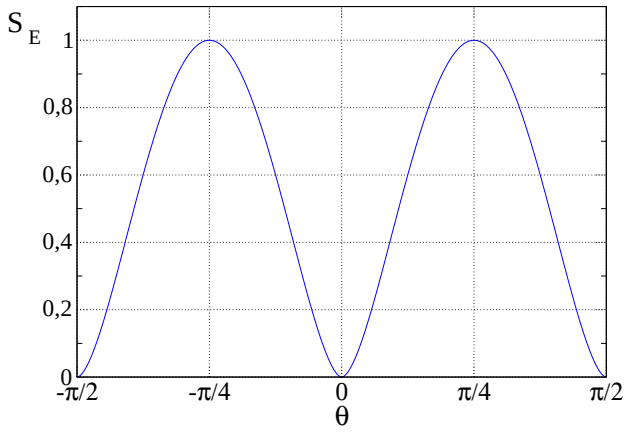

Figura 2.1: Entropía de enredo para el estado puro definido en la ec. (2.3), como función del parámetro θ.

el nivel de enredo a tiempos largos en la caminata cuántica con una y dos partículas.

2.2.2. Enredo asintótico en el QW (*)

El objetivo de esta sección es evaluar el nivel de enredo entre la posición y el grado de libertad de "moneda", para una caminata cuántica en la línea, a tiempo discreto (QW). Para una evolución coherente, este enredo se cuantifica usando la entropía de enredo, S_E, que hemos introducido en la sección anterior. Si bien a tiempos intermedios S_E es oscilante, a tiempos largos la amplitud de las oscilaciones decae y el enredo converge a un valor estable que depende de las condiciones iniciales. Estos resultados, que aclaran y extienden consideraciones previas basadas en observaciones numéricas [ClX$^+$05], han sido publicados en [ASRR06].

Recordando el formalismo introducido en la sección 1.2.1, los dos subsistemas son los subespacios de posición $\mathcal{H}_p$ y de moneda $\mathcal{H}_c$. El operador de evolución del QW, ec. (1.8), implica una *traslación condicional* al estado de la moneda, lo cual genera enredo entre ambos grados de libertad. El estado puro (1.7) esta asociado a un operador densidad

$$\rho = |\Psi\rangle\langle\Psi|.$$

Para calcular la entropía de enredo, es necesario reducir ρ a uno de los dos subespacios tomando la traza parcial con respecto al otro. Es más convenien-

te tomar la traza respecto de la posición[6] de modo que el operador reducido resultante, ρ_c, actúa en $\mathcal{H}_c$, un espacio de dimensión 2. En la representación canónica $\{|0\rangle, |1\rangle\}$, este operador es

$$\rho_c = tr_p(\rho) = \begin{pmatrix} A & B \\ B^* & C \end{pmatrix}, \tag{2.10}$$

donde

$$A \equiv \sum_x |a_x|^2, \qquad B \equiv \sum_x a_x b_x^*, \qquad C \equiv \sum_x |b_x|^2. \tag{2.11}$$

La normalización de $|\Psi\rangle$ implica que $\mathrm{tr}(\rho) = A + C = 1$. Los autovalores reales, positivos de ρ_c son

$$\lambda_{1,2} = \frac{1}{2}\left[1 \pm \sqrt{1 + 4(|B|^2 - AC)}\right] = \frac{1}{2}\left[1 \pm \sqrt{1 - 4\Delta}\right]. \tag{2.12}$$

en términos del discriminante $\Delta = AC - |B|^2$. Estos autovalores determinan la entropía de enredo

$$S_E(\rho) = -\lambda_1 \log_2 \lambda_1 - \lambda_2 \log_2 \lambda_2. \tag{2.13}$$

El enredo S_E depende exclusivamente del discrimante Δ. La dificultad para evaluar esta cantidad consiste en que la dependencia temporal de los coeficientes a_x, b_x que evolucionan bajo la operación U, vea la ec. (1.9) es complicada y no se puede obtener analíticamente. Sin embargo, es posible avanzar trabajando en la representación de número de onda (transformada de Fourier de la posición) y tomando el límite de tiempos largos.

Representación k

El método de trabajar en el espacio transformado de Fourier para obtener la dependencia a tiempos largos del vector de estado del QW fue utilizado por primera vez en [NV]. El espacio dual de la posición $\mathcal{H}_k$ es generado por los kets transformados $|k\rangle = \sum_x e^{ikx}|x\rangle$, donde el número de onda k es un real en $[-\pi, \pi]$. El vector de estado en esta representación es

$$|\Psi\rangle = \int_{-\pi}^{\pi} \frac{dk}{2\pi} |k\rangle \otimes \left[\tilde{a}_k|0\rangle + \tilde{b}_k|1\rangle\right] \tag{2.14}$$

[6] $\mathcal{H}_p$ es un espacio de n qubits y dimensión 2^n, donde n depende de la máxima posición L que se desea representar. Para representar los $2L+1$ sitios entre $[-L, L]$, se requieren $n \geq log_2(L+1)$ qubits.

donde las amplitudes en k $\tilde{a}_k = \langle k, 0|\Psi\rangle$ and $\tilde{b}_k = \langle k, 1|\Psi\rangle$ se relacionan con la posición por

$$\tilde{a}_k = \sum_x e^{-ikx} a_x \qquad \text{and} \qquad \tilde{b}_k = \sum_x e^{-ikx} b_x. \tag{2.15}$$

El operador traslación en (1.8) es diagonal en esta representación[7] Un paso de la evolución se expresa a través del operador U_k, que actúa no trivialmente en $\mathcal{H}_c$,

$$|\Phi_k(t+1)\rangle = U_k|\Phi_k(t)\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} e^{-ik} & e^{-ik} \\ e^{ik} & -e^{ik} \end{pmatrix} |\Phi_k(t)\rangle \tag{2.16}$$

donde $|\Phi_k\rangle = \langle k|\Psi\rangle$ es el spinor $(\tilde{a}_k, \tilde{b}_k)^T$. Usando la representación espectral del operador U_k es posible evaluar U_k^t. Este operador tiene valores y vectores propios $|\varphi_k^{(1,2)}\rangle$ dados por

$$|\varphi_k^{(1)}\rangle = \alpha_k \begin{pmatrix} u_k \\ v_k \end{pmatrix} \qquad |\varphi_k^{(2)}\rangle = \beta_k \begin{pmatrix} u_k \\ w_k \end{pmatrix} \tag{2.17}$$

donde α_k y β_k son las funciones reales, positivas,

$$\begin{aligned} \alpha_k &\equiv \frac{1}{\sqrt{2}} \left[1 + \cos^2 k - \cos k \sqrt{1 + \cos^2 k}\right]^{-1/2} \\ \beta_k &\equiv \frac{1}{\sqrt{2}} \left[1 + \cos^2 k + \cos k \sqrt{1 + \cos^2 k}\right]^{-1/2} \end{aligned} \tag{2.18}$$

y las funciones u_k, v_k y w_k son

$$u_k \equiv e^{-ik}, \quad v_k = \sqrt{2} e^{-i\omega_k} - e^{-ik}, \quad w_k = -\sqrt{2} e^{i\omega_k} - e^{-ik}. \tag{2.19}$$

Las frecuencias ω_k, definidas por

$$\sin \omega_k \equiv \frac{\sin k}{\sqrt{2}} \qquad \omega_k \in [-\pi/2, \pi/2], \tag{2.20}$$

determinan los valores propios, $\pm e^{\mp i\omega_k}$, de U_k. Usando la descomposición espectral para U_k, la evolución temporal de un spinor inicial se puede expresar como

$$|\Phi_k(t)\rangle = U_k^t|\Phi_k(0)\rangle = e^{-i\omega_k t}\langle\varphi_k^{(1)}|\Phi_k(0)\rangle\ |\varphi_k^{(1)}\rangle + (-1)^t e^{i\omega_k t}\langle\varphi_k^{(2)}|\Phi_k(0)\rangle\ |\varphi_k^{(2)}\rangle. \tag{2.21}$$

[7]Esto es debido a que los "pasos" del QW son todos iguales y por lo tanto involucran un único valor de k. Esto no es cierto en QW más generales, como el que usamos más adelante para implementar estrategias cuánticas en el contexto de teoría de juegos.

Si se intenta anti-transformar esta expresión al espacio de posición para obtener $a_x(t), b_x(t)$ resultan integrales complicados que sólo pueden evaluarse numéricamente. Es posible obtener resultados aproximados, válidos a tiempos grandes, usando la aproximación de fase estacionaria [NV]. Evitamos estas dificultades técnicas evaluando la entropía de enredo, ec. (2.13), *directamente en el espacio de Fourier* sin anti-transformar al espacio de posiciones.

Los elementos del operador densidad reducido, ρ_c, que conducen al discriminante Δ, se pueden calcular en el espacio $\mathcal{H}_k$ como

$$\begin{aligned} A &\equiv \sum_x |a_x|^2 = \int_{-\pi}^{\pi} \frac{dk}{2\pi} |\tilde{a}_k|^2 \\ B &\equiv \sum_x a_x b_x^* = \int_{-\pi}^{\pi} \frac{dk}{2\pi} \tilde{a}_k \tilde{b}_k^* \\ C &\equiv \sum_x |b_x|^2 = \int_{-\pi}^{\pi} \frac{dk}{2\pi} |\tilde{b}_k|^2. \end{aligned} \tag{2.22}$$

De modo que para evaluar S_E, resta obtener A y B, $(C = 1 - A)$ los valores medios en k de $|\tilde{a}_k|^2$ y $\tilde{a}_k \tilde{b}_k^*$ respectivamente. La ecuación de evolución (2.21) se puede reescribir más explícitamente como

$$\begin{aligned} \tilde{a}_k(t) &= \alpha_k^2 F_k v_k e^{-i\omega_k t} + (-1)^t \beta_k^2 G_k w_k e^{i\omega_k t} \\ \tilde{b}_k(t) &= \alpha_k^2 F_k u_k e^{-i\omega_k t} + (-1)^t \beta_k^2 G_k u_k e^{i\omega_k t}. \end{aligned} \tag{2.23}$$

donde la dependencia en la s condiciones iniciales esta contenida en las funciones complejas

$$\begin{aligned} F_k &\equiv u_k^* \tilde{a}_k(0) + v_k^* \tilde{b}_k(0) \\ G_k &\equiv u_k^* \tilde{a}_k(0) + w_k^* \tilde{b}_k(0). \end{aligned} \tag{2.24}$$

Las expresiones (exactas) para $|\tilde{a}_k|^2, |\tilde{b}_k|^2$ y $\tilde{a}_k \tilde{b}_k^*$ son

$$\begin{aligned} |\tilde{a}_k(t)|^2 &= \alpha_k^4 |F_k|^2 |v_k|^2 + \beta_k^4 |G_k|^2 |w_k|^2 \\ &\quad + (-1)^t 2\alpha_k^2 \beta_k^2 \mathrm{Re}\left[F_k G_k^* v_k w_k^* e^{-2i\omega_k t}\right] \\ |\tilde{b}_k(t)|^2 &= \alpha_k^4 |F_k|^2 + \beta_k^4 |G_k|^2 \\ &\quad + (-1)^t 2\alpha_k^2 \beta_k^2 \mathrm{Re}\left[F_k G_k^* e^{-2i\omega_k t}\right] \\ \tilde{a}_k(t)\tilde{b}_k^*(t) &= \alpha_k^4 |F_k|^2 v_k u_k^* + \beta_k^4 |G_k|^2 w_k u_k^* \\ &\quad + (-1)^t \alpha_k^2 \beta_k^2 \left[F_k G_k^* v_k e^{-2i\omega_k t} \right. \\ &\qquad \left. + F_k^* G_k w_k e^{2i\omega_k t}\right] u_k^*. \end{aligned} \tag{2.25}$$

No es posible evaluar los promedios en k de estas expresiones en forma exacta. Sin embargo, a tiempos largos la contribución de los términos dependientes del tiempo cae como $t^{-1/2}$ [NV] y los valores asintóticos $\bar{A}, \bar{B}$ and $\bar{C}$ pueden obtenerse de las expresiones independientes del tiempo,

$$\begin{aligned} \bar{A} &= \int_{-\pi}^{\pi} \frac{dk}{2\pi} \left(\alpha_k^4 |F_k|^2 |v_k|^2 + \beta_k^4 |G_k|^2 |w_k|^2\right) \\ \bar{C} &= \int_{-\pi}^{\pi} \frac{dk}{2\pi} \left(\alpha_k^4 |F_k|^2 + \beta_k^4 |G_k|^2\right) \\ \bar{B} &= \int_{-\pi}^{\pi} \frac{dk}{2\pi} \left(\alpha_k^4 |F_k|^2 v_k u_k^* + \beta_k^4 |G_k|^2 w_k u_k^*\right), \end{aligned} \tag{2.26}$$

válidas para $t \gg 1$ y condiciones iniciales arbitrarias. En este punto es necesario parametrizar la condición inicial antes de continuar.

Posición inicial localizada

El nivel de enredo asintótico depende de la elección inicial del qubit de moneda, lo cual contradice afirmaciones iniciales basadas en simulaciones numéricas que exploran solo una porción limitada del espacio de condiciones iniciales [ClX$^+$05]. Consideramos como condición inicial un autoestado de posición[8] y un estado genérico en $\mathcal{H}_c$ como moneda inicial, de modo que

$$|\Psi(0)\rangle = \|0\rangle \otimes \frac{1}{\sqrt{2}} \Big(\cos\alpha |0\rangle + e^{i\beta} \sin\alpha |1\rangle\Big) \tag{2.27}$$

con α, β dos ángulos reales, en términos de los cuales, los coeficientes transformados (2.15) son

$$\begin{aligned} \tilde{a}_0(0) = a_0(0) &= \cos\alpha \\ \tilde{b}_0(0) = b_0(0) &= e^{i\beta} \sin\alpha. \end{aligned} \tag{2.28}$$

A partir de las expresiones (2.24), para esta clase de condiciones iniciales se obtiene

$$\begin{aligned} |F_k|^2 = F_e(k) + F_o(k) &= \cos^2\alpha + |v_k|^2 \sin^2\alpha + \sin(2\alpha)\,\mathrm{Re}\left[u_k^* v_k e^{-i\beta}\right] \\ |G_k|^2 = G_e(k) + G_o(k) &= \cos^2\alpha + |w_k|^2 \sin^2\alpha + \sin(2\alpha)\,\mathrm{Re}\left[u_k^* w_k e^{-i\beta}\right]. \end{aligned}$$

[8] Que tomamos como $x = 0$ sin pérdida de generalidad.

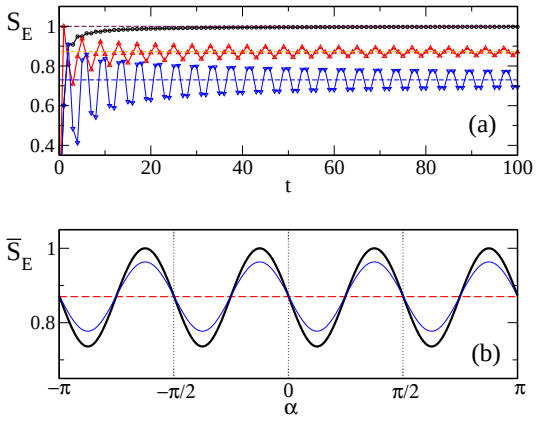

Figura 2.2: (a) Evolución de la entropía de enredo para tres condiciones iniciales localizadas con monedas $|\chi\rangle$ parametrizadas por la ec. (2.27): para $\alpha = -\pi/8$ y $\beta = \pi$, en negro (nivel máximo de enredo asintótico), $\beta = \pi/2$ en rojo, (nivel intermedio de enredo asintótico) y $\beta = 0$, en azul (nivel mínimo de enredo asintótico). El enredo asintótico varía en forma discontinua con el número de pasos t. Las líneas se incluyen sólo para guiar la vista. (b) Enredo asintótico $\bar{S}_E$ vs. α en la ec. (2.27) para $\beta = 0$ (línea negra gruesa), $\beta = \pi/4$ (línea fina azul) y $\beta = \pm\pi/2$ (línea roja a trazos).

donde las partes pares (e) e impares (o) son las funciones reales

$$\begin{aligned} F_e(k) &\equiv \cos^2\alpha + |v_k|^2 \sin^2\alpha - \left(1 - \sqrt{2}\cos(\omega_k - k)\right)\sin(2\alpha)\cos\beta \\ F_o(k) &\equiv -\sqrt{2}\sin(\omega_k - k)\sin(2\alpha)\sin\beta \\ G_e(k) &\equiv \cos^2\alpha + |w_k|^2 \sin^2\alpha - \left(1 + \sqrt{2}\cos(\omega_k + k)\right)\sin(2\alpha)\cos\beta \\ G_o(k) &\equiv -\sqrt{2}\sin(\omega_k + k)\sin(2\alpha)\sin\beta. \end{aligned} \tag{2.29}$$

Usando estas expresiones en (2.26) obtenemos

$$\begin{aligned} \bar{C} &= c_1 + (c_2 - c_1)\sin^2\alpha + c_3\sin(2\alpha)\cos\beta \\ \bar{B} &= b_1 + (b_2 - b_1)\sin^2\alpha + \sin(2\alpha)\left(b_3\cos\beta + ib_4\sin\beta\right) \end{aligned} \tag{2.30}$$

donde las constantes b_i, c_i están dados por integrales en k que es posible evaluar exactamente. Los detalles son algo engorrosos (vea el Apéndice en [ASRR06]). Como resultado el discriminante, se puede expresar como

$$\Delta = \Delta_0 - 2b_1^2\cos\beta\sin(4\alpha) \tag{2.31}$$

con $b_1 = (2 - \sqrt{2})/4$ y $\Delta_0 = (\sqrt{2} - 1)/2$. A partir de esta expresión se calculan los valores propios (2.12) y la entropía de enredo en función de la moneda inicial. El resultado se muestra en la Fig. 2.2. Para $\sin\alpha = 0, \pi$ o

$\beta = \pm\pi/2$, el discriminante se reduce a Δ_0 y esto resulta en un nivel de enredo intermedio $S_E \approx 0{,}872\ldots$. Para una condición inicial localizada en posición, el nivel de enredo asintótico oscila entre $0{,}736\ldots$ y un máximo muy cercano a 1.

La pregunta inmediata es si es posible "sintonizar.otros niveles de enredo asintótico considerando condiciones iniciales no locales.

Posición inicial distribuida

Consideramos ahora el caso de posiciones iniciales no localizadas, ya que un trabajo previo muestra que hay diferencias con el caso local [ADRS06]. En particular, consideramos posiciones iniciales en el subespacio de posición $\mathcal{H}_{p1}$ generado por $|\pm 1\rangle$. El estado de moneda se fija en $|\chi\rangle = (|0\rangle + i|1\rangle)/\sqrt{2}$, que genera una evolución simétrica, $P_t(x) = P_t(-x)$, cuando se inicial en $x = 0$. El estado inicial es de la forma,

$$|\Psi(\theta,\varphi)\rangle = \left(\cos\theta\, \||-1\rangle + e^{-i\varphi}\sin\theta\, \||1\rangle\right) \otimes |\chi\rangle. \tag{2.32}$$

Los ángulos $\theta \in [-\pi/2, \pi/2]$ y $\varphi \in [-\pi, \pi]$ parametrizan la posición inicial. Las amplitudes iniciales transformadas son $\tilde{b}_k(0) = i\tilde{a}_k(0)$ y $\tilde{a}_k(0) = \left(e^{ik}\cos\theta + e^{-i(k+\varphi)}\sin\theta\right)/\sqrt{2}$, por lo tanto,

$$|\tilde{a}_k(0)|^2 = |\tilde{b}_k(0)|^2 = \frac{1}{2}\left[1 + \sin(2\theta)\cos(2k+\varphi)\right]. \tag{2.33}$$

Para esta clase de condiciones iniciales, las ecs. (2.26) resultan en

$$\bar{C} = \int_{-\pi}^{\pi} \frac{dk}{2\pi} |\bar{b}_k|^2 \equiv \int_{-\pi}^{\pi} \frac{dk}{2\pi} Q(k) |\tilde{a}_k(0)|^2 \tag{2.34}$$

donde $Q(k)$ es una función de distribución

$$\begin{aligned} Q(k) &= 4\left[\alpha_k^4\left(1 - \cos(k - \omega_k + \pi/4)\right)\right. \\ &\quad \left. + \beta_k^4\left(1 + \cos(k + \omega_k + \pi/4)\right)\right] = 1 + \frac{\sin k \cos k}{1 + \cos^2 k} \end{aligned} \tag{2.35}$$

que satisface $Q(k) > 0$ and $\int_{-\pi}^{\pi} \frac{dk}{2\pi} Q(k) = 1$. A partir de ésta expresión se obtiene

$$\begin{aligned} \bar{C} &= \frac{1}{2} + \sin(2\theta)\sin(\varphi)\int_{-\pi}^{\pi} \frac{dk}{2\pi}\, Q(k)\sin(2k) \\ &= \frac{1}{2} - B_+ \sin(2\theta)\sin(\varphi) \end{aligned} \tag{2.36}$$

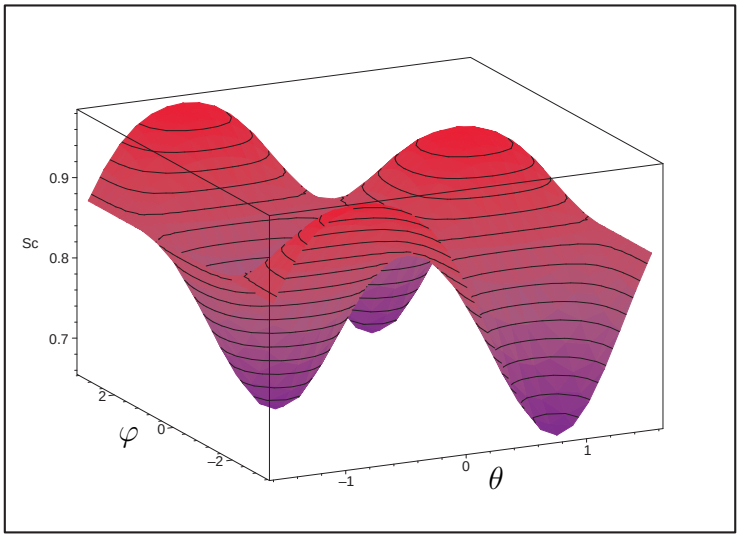

Figura 2.3: Entropía de enredo $\bar{S}_E(\theta,\varphi)$ como función del estado inicial en el subespacio de posición $\mathcal{H}_{p1}$, ec. (2.32). La entropía se calcula a partir de las expresiones para $\bar{C}$ y $|\bar{B}|$ dadas por las ecs. (2.36) y (2.39).

con $B_+ = (\sqrt{2}-1)/2$. El valor asintótico de $\bar{B}$ es imaginario puro y se expresa como

$$\mathrm{Im}\left[\bar{B}\right] = \mathrm{Im}\left[\int_{-\pi}^{\pi} \frac{dk}{2\pi}\, \overline{a_k b_k^*}\right] \equiv \int_{-\pi}^{\pi} \frac{dk}{2\pi} R(k)\ |\tilde{a}_k(0)|^2 \tag{2.37}$$

con [ADRS06]

$$\begin{aligned} R(k) &\equiv 4\sqrt{2}\left\{\alpha_k^4\left[1-\cos(k-\omega_k+\pi/4)\right]\sin(k-\omega_k)\right. \\ &\qquad \left. -\beta_k^4\left[1+\cos(k+\omega_k+\pi/4)\right]\sin(k+\omega_k)\right\} \\ &= \frac{\sin^2 k}{1+\cos^2 k}. \end{aligned} \tag{2.38}$$

Usando esta expresión para $R(k)$ se evalúa la ec. (2.37) y resulta en

$$\mathrm{Im}\left[\bar{B}\right] = B_0 - B'\sin(2\theta)\cos(\varphi), \tag{2.39}$$

con coeficientes $B_0 = \frac{\sqrt{2}-1}{2}$ y $B' = \frac{3\sqrt{2}-4}{2}$. El máximo de ésta expresión, $|B| = B_0 + B'$, resulta en el menor enredo asintótico y esto ocurre para $(\theta,\varphi) = (-\pi/4, 0)$ o $(\theta,\varphi) = (\pi/4, \pm\pi)$. Ambos casos corresponden a superposiciones equilibradas de ambas posiciones con fase relativa $\pm\pi$,

$$|\Psi_-\rangle \equiv \frac{|-1\rangle - |+1\rangle}{\sqrt{2}}.$$

El mínimo, $|B| = B_0 - B'$, que se obtiene para $(\theta, \varphi) = (\pi/4, 0)$ o para $(\theta, \varphi) = (-\pi/4, \pm\pi)$, genera el máximo enredo asintótico. Corresponde a una superposición equilibrada con igual fase,

$$|\Psi_+\rangle \equiv \frac{|-1\rangle + |+1\rangle}{\sqrt{2}}.$$

Para $\theta = 0, \pm\pi/2$ (condición inicial localizada) se obtiene el valor intermedio B_0, que genera un enredo asintótico $\bar{S}_0 \approx 0{,}872$, consistente con el resultado de la sección anterior.

Los valores propios asintóticos $\bar{\lambda}_{1,2}$ se obtienen de la ec. (2.12),

$$\bar{\lambda}_{1,2}(\theta, \varphi) = \frac{1}{2} \pm \left[\big(B_0 - B' \sin(2\theta)\cos(\varphi)\big)^2 + (B_0 + B')^2 \sin^2(2\theta)\sin^2(\varphi) \right]^{\frac{1}{2}}. \tag{2.40}$$

El valor asintótico de la entropía de enredo $\bar{S}_E(\theta, \varphi)$, resultante de éstos autovalores se muestra en la Fig. 2.3. El gráfico de niveles para esta superficie, Fig. 2.4, muestra que hay dos máximos y dos mínimos (que corresponden a las condiciones iniciales $|\Psi_+\rangle$ y $|\Psi_-\rangle$ respectivamente) para los cuales el enredo asintótico es $\bar{S}_+ \approx 0{,}979$ y $\bar{S}_- \approx 0{,}661$, respectivamente. Las líneas verticales a trazos indican posiciones iniciales localizadas para las cuales el enredo asintótico es $\bar{S}_0 \approx 0{,}872$. Sin embargo, para superposiciones arbitrarias de $|\pm\rangle$, la fase relativa $\varphi = \pm\pi/2$ también resulta en el mismo nivel de enredo asintótico (estos estados se indican por las líneas horizontales a trazos).

Hemos mostrado que (i) una condición inicial localizada resulta en un enredo asintótico que varía entre $\sim 0{,}74$ y 1, como función de la moneda inicial y (ii) con condiciones iniciales distribuidas en el subespacio de posición $\mathcal{H}_{p1}$ (con moneda fija $|\chi_c\rangle$) se obtiene una mayor variación en los niveles de enredo asintótico (entre $\sim 0{,}66$ y $\sim 0{,}98$). Cabe preguntarse si, partiendo de una mayor dispersion en la posición inicial, cualquier nivel de enredo asintótico es posible. El siguiente argumento, basado en la reversibilidad de la dinámica, muestra que en efecto éste es el caso. Si partimos de un estado producto (sin enredo) $|\Psi_1\rangle$ y evolucionamos al estado distribuido $|\Psi_2\rangle = U^t|\Psi_1\rangle$, el movimiento inverso, bajo $U^\dagger$, nos lleva del estado distribuido al estado local $|\Psi_1\rangle = (U^\dagger)^t|\Psi_2\rangle$ que es un estado producto de posición y moneda. El operador $U^\dagger = U^{-1}$ es un operador de QW válido que corresponde simplemente a intercambiar los roles de los estados de moneda $|0\rangle \leftrightarrow |1\rangle$ en la ec. (1.8). Un argumento alternativo, basado en considerar

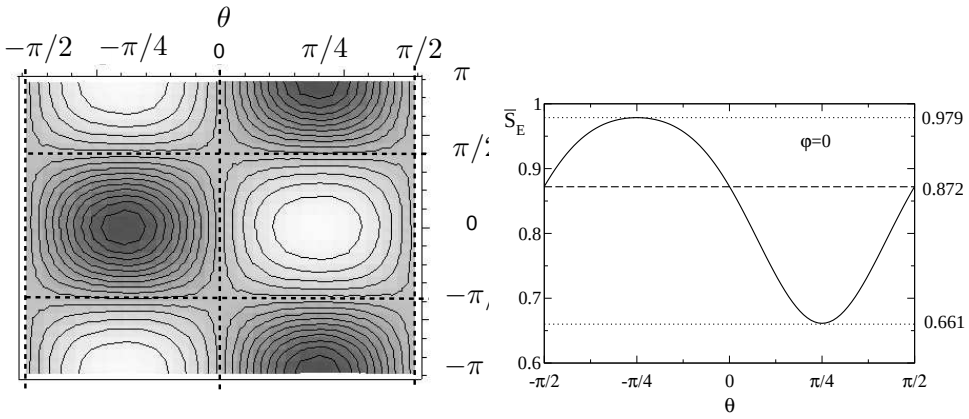

Figura 2.4: (Izq.) gráfico de niveles correspondiente a la superficie de la Fig. 2.3. Las áreas claras indican valores máximos, las áreas oscuras los valores mínimos. (Der.) variación del enredo asintótico con la no localidad de la posición inicial θ para la fase relativa $\varphi = 0$, en la ec. (2.32).

un paquete gaussiano distribuido en posición con un ancho característico σ conduce a la misma conclusión [ADRS06]. De modo que, a las conclusiones que mencionadas más arriba, agregamos: (iii) todo nivel de enredo asintótico es accesible si usamos condiciones iniciales espacialmente distribuidas.

2.2.3. Enredo entre dos QW (**)

Existen algunos trabajos exploratorios sobre las propiedades de dos caminantes cuánticos [ClX$^+$05, OPSB, TFMK03], pero no se ha realizado aún un estudio sistemático de los diversos tipos de correlaciones cuánticas que se presentan en este caso. Los resultados preliminares que presentamos en esta Sección, que son un primer paso en esta dirección, han sido recientemente presentados en el WECIQ'06 y publicados en sus anales [ADF06a].

El espacio de Hilbert para dos partículas (A y B) que realizan un QW es simplemente el producto tensorial de dos espacios de Hilbert de una partícula, que indicamos por $\mathcal{H}_A$ y $\mathcal{H}_B$,

$$\mathcal{H}_2 = \mathcal{H}_A \otimes \mathcal{H}_B.$$

Ambos subespacios son isomorfos con el espacio de una partícula, $\mathcal{H} = \mathcal{H}_c \otimes \mathcal{H}_p$, descrito en la Sección 1.2.1. Indicamos las posiciones de los caminantes a través de las coordenadas discretas (x, y), de modo que un estado puro genérico

de dos partículas $|\Psi\rangle$ es de la forma

$$|\Psi\rangle = \sum_{x,y} \{\alpha_{x,y}|00\rangle + \beta_{x,y}|01\rangle + \gamma_{x,y}|10\rangle + \delta_{x,y}|11\rangle\} \otimes \|x,y\rangle, \qquad (2.41)$$

donde usamos el símbolo $\|\cdot\rangle$ para distinguir los autoestados de posición de los autoestados de moneda. Los coeficientes complejos satisfacen el requisito de normalización

$$\sum_{x,y} \left(|\alpha_{x,y}|^2 + |\beta_{x,y}|^2 + |\gamma_{x,y}|^2 + |\delta_{x,y}|^2\right) = 1. \qquad (2.42)$$

El operador de evolución de dos partículas tiene la misma estructura que (1.8), es decir una operación unitaria U_c en el subespacio de monedas, $\mathcal{H}_c^{\otimes 2}$, seguida de un desplazamiento condicional S en el subespacio de posición,

$$U_2 = S \cdot (I_P \otimes U_C) \qquad (2.43)$$

donde I_p representa la identidad en el subespacio de posición $\mathcal{H}_p^{\otimes 2}$ de dos partículas[9]. El operador de traslación o desplazamiento

$$\begin{aligned} S &= \sum_{x,y} \{|x+1,y+1\rangle\langle x,y| \otimes |00\rangle\langle 00| + |x+1,y-1\rangle\langle x,y| \otimes |01\rangle\langle 01| \\ &+ |x-1,y+1\rangle\langle x,y| \otimes |10\rangle\langle 10| + |x-1,y-1\rangle\langle x,y| \otimes |11\rangle\langle 11|\} \end{aligned} \qquad (2.44)$$

implementa desplazamientos de paso fijo en las coordenadas de cada partícula, condicionales al estado de ambas monedas. Como antes, $|0\rangle$ implica un desplazamiento positivo y $|1\rangle$ un desplazamiento negativo en la coordenada correspondiente.

En este trabajo inicial sobre el tema, nos limitamos al caso de la caracterización de enredo en estados puros. La caracterización de enredo en mezclas es un problema más complejo, sobre el cual damos algunos elementos en la siguiente sección. Un estado inicial puro de dos partículas, caracterizado por un operador densidad $\rho_0 = |\Psi(0)\rangle\langle\Psi(0)|$, evoluciona a

$$\rho_t = U_2^t \, \rho_0 \left(U_2^\dagger\right)^t \qquad (2.45)$$

luego de t pasos (observe que, como antes, t es una variable discreta no negativa).

[9]Este subespacio es generado por los kets ortonormales $\|x,y\rangle = \|x\rangle \otimes \|y\rangle$ con (x,y) enteros.

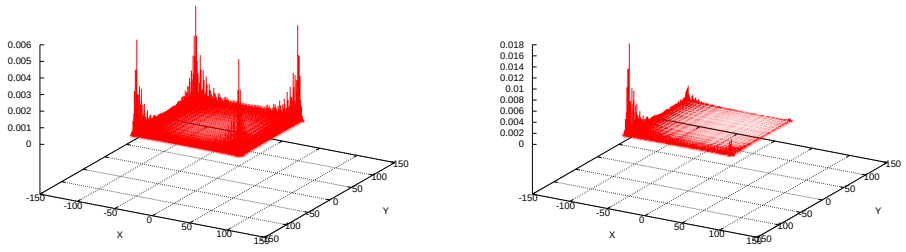

Figura 2.5: Distribución de probabilidad conjunta $P(x, y)$ luego de $t = 100$ pasos con la operación de moneda separable de Hadamard, ec. (2.47). Las posiciones iniciales se localizan en el orígen y, por claridad, se representan las coordenadas de A y de B a lo largo de direcciones ortogonales. (Izq.) Monedas iniciales $|\chi_1\rangle$, eq. (2.48), que resultan en una evolución simétrica, i.e. $P_A(x, t) = P_A(-x, t)$ y $P_B(y, t) = P_B(-y, t)$; (Der.) Monedas iniciales $|\chi_2\rangle$, eq. (2.49). En ambos casos, no hay enredo entre A,B de modo que una medida de una partícula no afecta al estado de la otra.

La distribución de probabilidad conjunta de encontrar A en el sitio x y B en el sitio y es

$$P_2(x, y; t) = tr_C(\rho_t) = |\alpha_{x,y}|^2 + |\beta_{x,y}|^2 + |\gamma_{x,y}|^2 + |\delta_{x,y}|^2. \tag{2.46}$$

Observe que, si ρ describe un estado puro separable (i.e. $\rho = \rho_A \otimes \rho_B$), la distribución conjunta es el producto de dos distribuciones de una partícula, $P_2(x, y; t) = P_A(x, t)P_B(y, t)$. En el caso general, ρ no es separable[10] y una medida de la posición de una partícula afectará drásticamente la distribución en posición de la otra.

Operaciones de moneda separables

En el caso más simple, la operación de moneda U_c, en la ec. (2.43), es separable

$$U_C = U_A \otimes U_B,$$

con U_A y U_B operaciones unitarias de un qubit locales al subespacio $\mathcal{H}_c$. Para esta clase de operaciones de moneda, el enredo entre los subespacios $\mathcal{H}_A$ y $\mathcal{H}_B$ de ambas partículas puede surgir solo de una elección de condiciones iniciales enredadas y es preservado por la evolución.

[10]Es decir, describe un estado en el cual hay enredo entre los subespacios de ambas partículas.

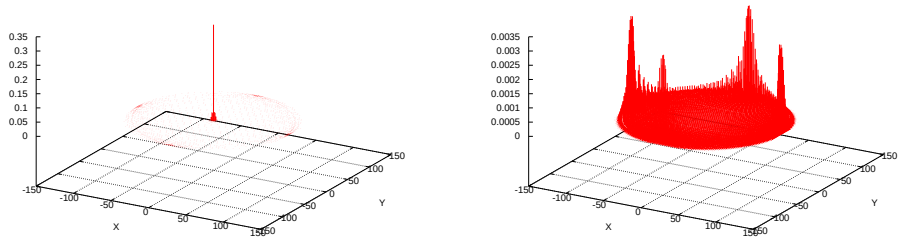

Figura 2.6: Distribución de probabilidad conjunta $P(x, y)$ luego de $t = 100$ pasos con la operación de moneda de Grover, ec. (2.50). (Izq.) Monedas iniciales $|\chi_1\rangle$, ec. (2.48), que resultan en una distribución que permanece altamente concentrada en el origen; (Der.) Monedas iniciales $|\chi_2\rangle$, ec. (2.49), que resultan en la máxima dispersion.

Como un ejemplo sencillo, consideramos la caminata cuántica de dos partículas con monedas de tipo Hadamard.

$$U_c = H \otimes H = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} . \tag{2.47}$$

La Fig. 2.5 muestra la distribución de probabilidad conjunta, luego de $t = 100$ pasos, para dos condiciones iniciales localizadas en el origen de coordenadas con las monedas iniciales

$$|\chi_1\rangle = \frac{1}{2}(|0\rangle + i|0\rangle)^{\otimes 2} = \frac{1}{2}\left[|00\rangle + i|01\rangle + i|10\rangle - |11\rangle\right] \tag{2.48}$$

$$|\chi_2\rangle = \frac{1}{2}(|0\rangle - |0\rangle)^{\otimes 2} = \frac{1}{2}\left[|00\rangle - |01\rangle - |10\rangle + |11\rangle\right] . \tag{2.49}$$

Observe que ambas monedas son separables, de modo que en este caso no hay enredo entre ambas partículas[11].

Operaciones de moneda no-separables

Una situación más interesante se presenta cuando se usa una operación de moneda no separable, que cambia el enredo entre ambas partículas. En

[11] No obstante, de acuerdo a la descripción detallada de la sección anterior, la evolución genera enredo entre la posición y la moneda de cada partícula.

este caso, el enredo entre A y B puede ser introducido por la elección de la condición inicial o (no excluyente) por la operación de moneda.

Existen diversos tipos de enredo, ya que la evolución en cada subespacio enreda la posición y moneda de cada partícula. Si además, la operación de moneda enreda ambas monedas, las posiciones de ambas partículas resultan enredadas en forma indirecta. Este proceso se asemeja al "entanglement swapping" (de interés en estaciones repetidoras para comunicaciones cuánticas por fibra óptica) en el cual, un fotón B previamente enredado con otro A, transfiere su enredo a un tercer fotón C, de modo que A y C quedan enredados sin haber interactuado. En este caso, las posiciones de ambas partículas quedan enredadas por mediación de la operación de moneda no separable.

En lo que sigue nos interesa el enredo entre ambas partículas generado por la operación de moneda U_c, de modo que consideramos las monedas iniciales no enredadas dadas por las ecs. (2.48) y (2.49).

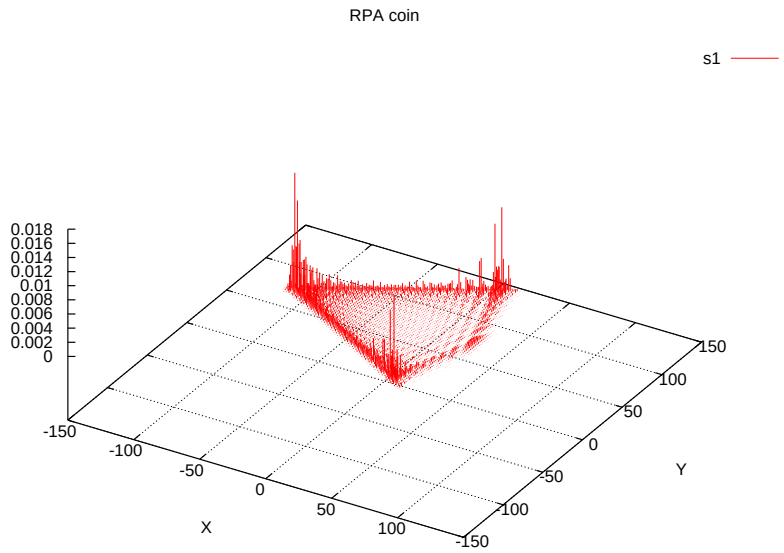

Figura 2.7: Distribución de probabilidad $P(x, y)$ luego de $t = 100$ pasos con esta operación de moneda. El estado inicial es localizado con monedas dadas por $|\chi_1\rangle$, eq. (2.48).

Como primer ejemplo de un operador de moneda no separable, conside-

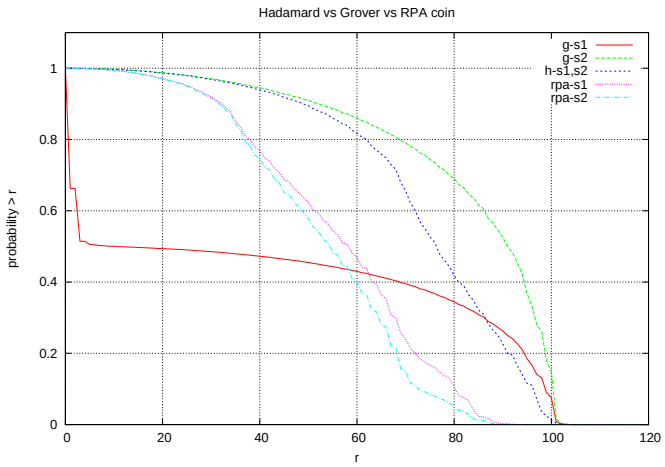

Figura 2.8: Probabilidad de encontrar ambas partículas a una distancia mayor que r del origen al cabo de $t = 100$ pasos, para las operaciones de moneda de Hadamard (h-s1,s2), de Grover (g-s1,s2) y RP (rpa-s1,s2). La condición inicial es localizada en el origen, con las dos monedas iniciales $|\chi_1\rangle$ (s1) y $|\chi_2\rangle$ (s2). La operación de Grover produce las dispersiones extremas (verde y rojo) para estas dos condiciones iniciales.

ramos la operación de Grover dada por

$$G = \frac{1}{2}\begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}. \tag{2.50}$$

Esta operación unitaria tiene un rol central en el algoritmo de búsqueda de Grover [Gro96]. La distribución de probabilidad resultante de esta operación de moneda tiene un pico en el origen para la mayoría de las condiciones iniciales, vea la Fig. 2.6 (Izq.). Sin embargo, para la moneda inicial $|\chi_2\rangle$, ec. (2.49), esta operación resulta en la máxima dispersion [TFMK03], como se muestra en el panel derecho de la misma figura.

Otro caso de interés es el de operaciones de moneda asociadas a estrategias en juegos cuánticos [ADF06b, ADF07] (vea la Sección 2.3). En

particular, la operación de moneda

$$U_C = CNOT \cdot (H \otimes I) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix} \tag{2.51}$$

describe un juego cuántico (RP) en el cual Alice implemente una estrategia al azar (Random), representada por una operación de Hadamard, y Bob responde siguiendo una estrategia tipo Pavlov, a través de una operación condicional CNOT. La operación conjunta, $U_c = CNOT \cdot (H \otimes I)$, genera enredo. De hecho, produce los estados de Bell ecs. (2.3), a partir de los estados de la base computacional de dos qubits. La distribución de probabilidad

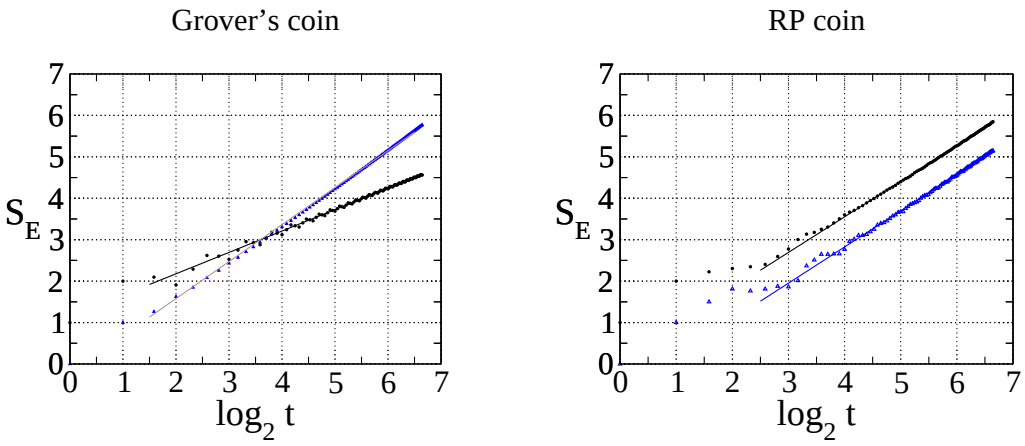

Figura 2.9: Entropía de enredo S_E vs $log_2(t)$ generada por las operaciones de moneda no separables de Grover (Izq.) y RP (Der.). Los estados iniciales son localizados en el origen con monedas $|\chi_1\rangle$ (círculos negros) y $|\chi_2\rangle$ (triángulos azules). Las líneas rectas corresponden a un ajuste, como se discute en el texto.

El enredo bi-partita generado por las operaciones de Grover y RP puede cuantificarse usando la entropía de enredo, S_E, ya que estamos tratando con estados puros y no hay decoherencia. El cálculo de esta cantidad implica diagonalizar la matriz densidad reducida (que actúa en el espacio de 2 qubits y es por lo tanto representado por una matriz de dimensión 4x4). Esto se puede realizar numéricamente a cada paso, para condiciones iniciales dadas.

La dependencia temporal de ésta cantidad se muestra en la Fig. 2.9. En todos los casos considerados, la entropía de enredo aumenta logarítmicamente con el número de pasos t, de forma que $S_E \sim clog_2(t)$, donde c es una constante que depende de la condición inicial y de la operación de moneda. El aumento logarítmico puede entenderse a partir del hecho de que a cada paso, más sitios en el plano son ocupados[12] y pasan a participar del enredo entre A y B. Hemos estimado la constante c usando regresión lineal. Para la operación de Grover, con la moneda inicial $|\chi_1\rangle$ (dispersion mínima), $c = 0{,}52$. En el caso de la moneda $|\chi_2\rangle$ (máxima dispersion) el enredo aumenta más rápido y $c = 0{,}89$. La operación de moneda RP, que produce una distribución en posición bien diferente, genera enredo a una tasa $c = 0{,}87$ para ambas monedas iniciales (Fig. 2.9).

Podemos concluir – tentativamente – que el enredo bipartita entre dos QW con operaciones de moneda no separables crece logarítmicamente con el número de pasos. La relación que muestra la moneda de Grover entre el nivel de enredo y velocidad a la cual el caminante explora el espacio accesible no parece ser de carácter general. Estos resultados son de carácter inicial y se requiere más trabajo para comprender los aspectos multipartitas (moneda1,2 y posición 1,2) del enredo entre dos QW.

2.2.4. Mezclas estadísticas (**)

En sistemas abiertos (en interacción con el ambiente) o en sistemas sobre los cuales poseemos información incompleta, la única descripción adecuada es la del operador densidad. En un sistema abierto, la decoherencia tiende a destruir el enredo. Por otra parte, desde un punto de vista más formal, la decoherencia es resulta del enredo del sistema con los grados de libertad de su ambiente. De modo que existe una relación estrecha entre decoherencia y enredo.

Como caracterizar el enredo bipartita[13] cuando el sistema esta descrito por una mezcla estadística? Recordamos que un estado mezcla es separable

[12] Razonando en una dimensión, para t pasos el registro de la posición requiere n qubits, donde $2^n \sim 2t + 1$ sitios, y por lo tanto el número de qubits involucrados, n, crece logarítmicamente con el número de pasos, $n \sim log_2(t)$.

[13] Limitaremos la discusión al caso más simple de enredo bipartita, aunque mencionado algunas generalizaciones propuestas para el caso de enredo multipartita.

si se puede expresar como una mezcla estadística de estados producto,

$$\rho = \sum_i p_i \rho_A \otimes \rho_B.$$

A diferencia de los estados puros, en el caso de mezclas no se usa (hasta el momento) una única medida de enredo sino que se han propuesto varias posibilidades.

Medidas operacionales de enredo

Históricamente, las medidas operacionales fueron las primeras en ser propuestas y están asociadas con la noción de enredo como un recurso que puede ser creado, destilado y consumido [NC00]. Un ejemplo es el Enredo de Formación (a veces mencionado como "costo de enredo"), E_F. Solamente con LOCC no es posible crear un estado enredado a partir de un estado separable. Pero si se dispone de suficientes copias de estados máximamente enredados, se pueden preparar algunas copias del estado enredado deseado mediante LOCC. El Enredo de Formación (entanglement of formation) es el *menor número de pares máximamente enredados necesarios para preparar el estado deseado mediante LOCC.*

El concepto dual es el Enredo destilable, E_D (distillable entanglement). Dado un cierto número $n \gg 1$ de copias de un estado ρ enredado, es posible mediante LOCC, transformarlo en cierto número $m \leq n$ de estados máximamente enredados, en un proceso que se conoce como "destilación" de enredo. La eficiencia m/n del proceso es el Enredo destilable, E_D. En otras palabras, es el *máximo número de pares máximamente enredados (por copia), obtenibles de varias copias de un estado ρ mediante LOCC.* Ambas medidas son conceptualmente importantes ya que se basan en el enredo como recurso. Sin embargo, son extremadamente difíciles de calcular incluso en los casos mas sencillos, ya que involucran procedimientos de maximización/minimización sobre el enorme conjunto de posibles LOCC's.

Medidas computables de enredo

Las medidas de enredo computables tienden a subsanar el problema de dificultad de cálculo de las medidas operacionales (a veces a expensas de la interpretación física). Sin embargo, no siempre es posible asignar un sentido físico a estas medidas. Mencionaremos aquí a dos de ellas, la Negatividad

$N(\rho)$ y la Concurrencia $C(\rho)$ [Woo98]. Esta última es especialmente relevante ya que se ha mostrado muy recientemente que está asociada a un observable y puede (al menos en el caso de dos qubits) ser determinada experimentalmente, sin necesidad de determinar el estado ρ por tomografía cuántica [FSMDZ06, WSRD$^+$06]. Además, muy recientemente se ha propuesto una generalización de la Concurrencia para el caso de enredo multipartita [MKB05].

Para calcular la negatividad [VW02] se realizan ciertas transformaciones en el estado ρ En primer lugar se obtiene el estado ρ^{T_B} (puede hacerse con respecto a A también) trasponiendo los elementos de ρ correspondientes al subespacio B (operación de trasposición parcial). Luego se calcula la norma definida por $\|\rho\| = \sum_i |\lambda_i|$, es decir la suma del valor absoluto de los valores propios. Si bien la transposición parcial debe hacerse en una representación concreta, los autovalores del resultado (y la norma) son independientes de la representación. La Negatividad se define por, $N(\rho) \equiv \|\rho\| - 1$. Para un estado separable, la trasposición parcial resulta en un operador densidad válido, es decir un operador con valores propios positivos y traza 1. En este caso la norma es 1 y $N = 0$. Como consecuencia del enredo, la trasposición parcial genera un objeto con autovalores negativos (no es un operador densidad) y cuya norma supera 1 en proporción al grado de enredo. Esta medida satisface las propiedades (i-iv) antes enunciadas y es fácil de calcular usando cualquier paquete de diagonalización de matrices. Sin embargo, si se quiere determinar el enredo de un estado ρ obtenido experimentalmente es necesario primero determinar ρ por un proceso relativamente complicado de tomografía cuántica y recién después es posible plantearse si el estado esta enredado. La Negatividad es computable, pero no es directamente observable.

La Concurrencia también se define a través de los autovalores de un operador transformado [Woo98]. Para el caso de enredo entre dos qubits, dado un operador densidad ρ, se calcula el operador transformado

$$\tilde{\rho} = (\sigma_y \otimes \sigma_y)\rho^*(\sigma_y \otimes \sigma_y)$$

donde ρ^* es el conjugado de ρ en cierta representación y σ_y es la matriz de Pauli

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}.$$

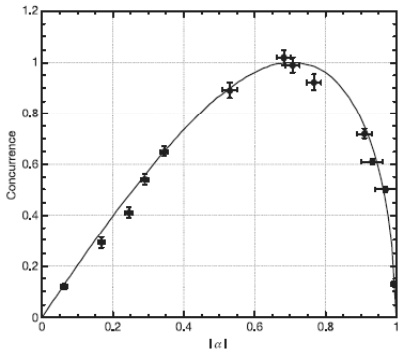

Figura 2.10: Valores de la concurrencia determinados experimentalmente para los estados enredados indicados en el texto. La curva llena corresponde al valor calculado. El máximo enredo corresponde a $|\alpha| = 1/\sqrt{2}$, un estado de Bell. Figura tomada de [WSRD$^+$06].

Se diagonaliza el operador $\rho\tilde{\rho}$ y se ordenan sus autovalores (reales, no negativos) en forma decreciente $\mu_1 \geq \mu_2 \geq \mu_3 \geq \mu_4$. La Concurrencia es la cantidad

$$C(\rho) \equiv \text{máx}\{0, \sqrt{\mu_1} - \sqrt{\mu_2} - \sqrt{\mu_3} - \sqrt{\mu_4}\}. \tag{2.52}$$

Es decir, que la Concurrencia es no nula sólo si la raíz del primer autovalor excede a la suma de las raíces de los otros tres. Esta cantidad, como la Negatividad, es fácil de calcular usando cualquier paquete de diagonalización de matrices. Pero la Concurrencia ofrece una ventaja adicional de gran importancia. Como se mencionó antes, para el caso de dos qubits, se ha mostrado [FSMDZ06] que esta cantidad puede ser determinada experimentalmente. En la Fig. 2.10, se muestran resultados de medidas reportadas recientemente [WSRD$^+$06] para la Concurrencia de estados puros de dos qubits de la forma $\alpha|01\rangle + \beta|10\rangle$ (con $|\alpha|^2 + \beta^2 = 1$) para los cuales $C = 2|\alpha|\sqrt{1-\alpha|^2}$. Los qubits 1 y 2 se codificaron en la polarización y cantidad de movimiento de fotones y las medidas se realizaron usando óptica lineal.

Finalmente, mencionamos al parámetro de Bell S, calculable a partir del estado o medible a partir de las correlaciones entre las medidas de un observable de cada parte de un par de Bell. Para estados enredados $S > 2$ y para estados separables $S \leq 2$.

Perspectivas para el QW

En el QW en presencia de ruido (vea el Cap. 4) coexisten diversos tipos de enredo, ya que hay dos subsistemas A y B con dos grados de libertad

(moneda y posición) diferentes. Un operador de evolución separable, enreda las monedas y posiciones de cada subespacio como se describió en la Sección 2.2.2. Por otra parte, si el operador de moneda es no separable (o si el operador de desplazamiento es más complejo, como en el caso de juegos cuánticos que discutimos a continuación) la evolución puede generar enredo entre los grados de libertad de A y B. Hasta el momento hemos estudado en detalle, usando técnicas analíticas, el enredo asintótico posición-moneda de un QW. En el caso de dos QW con moneda separable (Hadamard), es posible seguir la misma caracterización analítica, y ese trabajo esta medianamente avanzado, aunque los detalles resultan bastante más engorrosos que los presentados en la Sección 2.2.2 para el caso de una partícula. Paralelamente, hemos comenzado a caracterizar numéricamente el enredo bi-partita generado por operaciones de moneda no separables, entre dos QW coherentes. Hemos determinado que el enredo crece logarítmicamente con el número de pasos, como consecuencia de que un número creciente de autoestados de posición participan del mismo a media que los QW's se expanden en el espacio accesible.

Todo lo anterior se realizó usando estados puros y la Entropía de Enredo como cuantificador de correlaciones cuánticas. Si el sistema se coloca en un ambiente ruidoso (vea el Cap. 4), la descripción anterior debe reemplazarse por la de operador densidad y la Concurrencia puede usarse como medida de enredo. Es bien sabido que el enredo es frágil y decae en presencia de ruido, pero existen estados más robustos que otros frente a determinados tipos de ruido. La identificación de éstos estados enredados en sistemas concretos es importante para eventuales aplicaciones que requieran enredo. En el Cap. 4, luego de discutir lo que se sabe sobre el QW en presencia de ruido, realizamos una propuesta concreta en este sentido.

A continuación presentamos un formalismo que hemos desarrollado recientemente, en colaboración con H. Fort y R. Donangelo, que permite implementar juegos cuánticos bipartitas iterados usando dos QW.

2.3. Juegos Cuánticos

La Teoría de Juegos describe situaciones en las cuales cierto número de agentes racionales se enfrenta a decisiones que involucran un conflicto de intereses. La Teoría de Juegos analiza los efectos de implementar diferentes

estrategias, en lo que es, en cierto modo un problema de optimización con aplicaciones prácticas. El "problema de los bienes públicos" (Public Goods issue) es una de las situaciones paradigmáticas en las cuales la Teoría de Juegos es de interés. Instancias de este problema corresponden al pago o evasión de impuestos, a la compra o bajada ilegal de software o música, al pago de una fracción equitativa o no de una cuenta conjunta en un bar, a la relación parásito-huésped en Biología... En todas estas situaciones los agentes enfrentan una disyuntiva entre evadir una responsabilidad colectiva y obteniendo una ventaja individual a corto plazo pero perjudicando el interés común a largo plazo. El esquema de juego involucra en última instancia el procesamiento de información. A través del enredo y el paralelismo cuánticos es posible implementar estrategias y obtener resultados que no son accesibles clásicamente, como mostró por primera vez el matemático D. Meyer a través de un ejemplo elemental [Mey99]. El estudio – por ahora, a nivel teórico – de los juegos regidos por reglas cuánticas es lo que se conoce como Teoría Cuántica de Juegos [Pat07], un nombre algo pomposo para un área hasta el momento incipiente del procesamiento cuántico de la información. En comparación con otras tareas, los juegos cuánticos requieren pocos qubits para su implementación[14]. Existe actualmente un proyecto concreto, en los laboratorios Hewlett-Packard orientado a generar los protocolos y el hardware necesarios para implementar subastas "cuánticas" de contratos públicos, con fines comerciales [Pat07, CHB03].

El Dilema del Prisionero

El problema de bienes públicos entre dos agentes se reduce al "Dilema del Prisionero", una situación de conflicto paradigmática bien conocida en Teoría de Juegos [Flo52] en la cual dos agentes racionales toman una decisión binaria: Cooperar (C) o Delatar (D). El retorno cuando ambos cooperan (R) es superior al retorno cuando ambos delatan (P), pero si uno delata y el otro coopera, el delator recibe el mayor retorno posible (T) y el cooperador el peor retorno posible (S). Los retornos de cada jugador (A,B) se resumen en la siguiente "matriz de pagos" donde $T > R > P > S$ y $2R > T + S$.

[14]Por ejemplo, para implementar el algoritmo de Shor para factorizar enteros grandes y romper claves criptográficas requiere la manipulación de cientos de qubits en forma coherente, una tarea formidable (aunque no imposible) en el futuro cercano.

A/B	C	D
C	(R, R)	(S, T)
D	(T, S)	(P, P)

Cuadro 2.1: Matriz de pagos para el Dilema del Prisionero.

Razonando sobre la base del retorno individual, un agente decide delatar[15]; como el otro agente hace el mismo razonamiento, ambos delatan y acaban perjudicándose con un retorno P inferior a R. El punto D, D es un *equilibrio de Nash*[Nas50], en el cual ninguno de los agentes puede mejorar su retorno realizando un cambio unilateral en su estrategia. Por otra parte el punto C, C es un *Pareto óptimo*, ya que ningún jugador puede mejorar su retorno sin perjudicar al otro. El equilibrio de Nash es preferible desde el punto de vista individual, el óptimo Pareto lo es desde el punto de vista del interés colectivo. El dilema se resume en el hecho de que el equlibrio de Nash y el óptimo Pareto no coinciden. En la versión cuántica de este juego, existen estrategias en las cuales el equilibrio de Nash es un óptimo Pareto y el dilema desaparece. Como veremos, cierto nivel de enredo es un requisito esencial para que esto tenga lugar.

2.3.1. Juegos cuánticos "one-shot"

Eisert y Wilkens realizan una propuesta que permite implementar en forma cuántica el dilema del Prisionero y otros juegos bi-partitas [EWL99a, DXZH02]. El esquema se basa en un sistema de dos qubits preparados en un estado máximamente enredado $|\Psi_{CC}\rangle$ (o simplemente $|CC\rangle$) que especificamos más abajo. Describimops este estado puro por el operador densidad $\rho_{CC} = |\Psi_{CC}\rangle\langle\Psi_{CC}|$. Cada jugador (A o B) aplica una operación unitaria local (U_A, U_B) a su qubit con lo cual se obtiene un estado

$$\sigma = (U_A \otimes U_B)\, \rho_{CC}\, (U_A \otimes U_B)^\dagger .$$

Luego un árbitro realiza una medida generalizada de ambos qubits para determinar el resultado del juego. La medida generalizada (vea la Sección A.5)

[15] En media, es mejor delatar ya que $T + P > R + S$.

esta definida por el conjunto de operadores de Kraus

$$\begin{aligned} \pi_{CC} &= |CC\rangle\langle CC|, & |CC\rangle &= \tfrac{1}{\sqrt{2}}(|00\rangle + i|11\rangle) \\ \pi_{CD} &= |CD\rangle\langle CD|, & |CD\rangle &= \tfrac{1}{\sqrt{2}}(|01\rangle - i|10\rangle) \\ \pi_{DC} &= |DC\rangle\langle DC|, & |DC\rangle &= \tfrac{1}{\sqrt{2}}(|10\rangle - i|01\rangle) \qquad (2.53) \\ \pi_{DD} &= |DD\rangle\langle DD|, & |DD\rangle &= \tfrac{1}{\sqrt{2}}(|11\rangle + i|00\rangle). \end{aligned}$$

(2.54)

El resultado de esta medida proyectiva en la base (2.53) es una de las 4 alternativas $\{CC, CD, DC, DD\}$ del juego clásico, ahora codificadas en éstos cuatro estados enredados. Usando la matriz de pagos (cuadro 2.1), en forma análoga al caso clásico, se obtienen los retornos en cada uno de los resultados posibles. Luego de varias repeticiones del ciclo (Preparación→ Manipulación → Medida) se obtienen los valores medios[16]

$$\begin{aligned} \Pi_A &= R\,tr(\pi_{CC}\sigma) + S\,tr(\pi_{CD}\sigma) + T\,tr(\pi_{DC}\sigma) + P tr(\pi_{DD}\sigma) \\ \Pi_B &= R\,tr(\pi_{CC}\sigma) + T\,tr(\pi_{DC}\sigma) + S\,tr(\pi_{CD}\sigma) + P\,tr(\pi_{DD}\sigma). \end{aligned} \qquad (2.55)$$

En este juego, la participación de cada agente consiste en elegir una operación unitaria sobre un qubit. Clásicamente, un agente solo realiza una elección binaria, lo cual refleja el hecho de que el espacio de estrategias de un juego cuántico es mucho mayor que en su análogo clásico. Las estrategias clásicas

$$C = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad D = i\sigma_y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad (2.56)$$

corresponder a elegir cooperar o delatar. En efecto si ambos usan C, ($U_A = U_B = C = I$), el estado no cambia y $\sigma = \pi_{CC}$, con lo cual la medida final resulta en CC con certeza. Si ambos usan D, ($U_A = U_B = D = \sigma_y$), el estado final es π_{DD}. Si Alice coopera pero Bob no, $\sigma = (C \otimes D)\rho_{CC} = \pi_{CD}$, etc. De modo que las operaciones (2.56) corresponden a la alternativa clásica de cooperar o no.

Sin embargo, la elección de estrategia se puede parametrizar con dos

[16]Recordando que el valor esperado de un operador Hermítico A es $< A >= tr(\rho A)$, donde $tr(.)$ representa la traza. Vea el Apéndice A por más detalles.

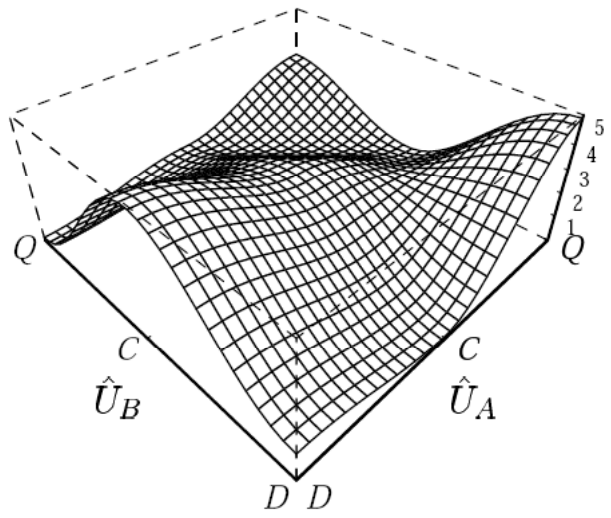

Figura 2.11: Retorno medio de Alice, Π_A definido en la ec. (2.53), para estrategias parametrizadas por parámetros t_A, t_B como se explica en el texto. Cooperación corresponde a $t = 0$, Delación a $t = 1$. Para $t < 0$ se obtienen estrategias sin análogo clásico. La estrategia Q, discutida en el texto, corresponde al caso $t = -1$. Figura tomada de [EWL99a].

parámetros[17] en la forma

$$U(\theta, \phi) = \begin{pmatrix} e^{i\phi}\cos\theta/2 & \sin\theta/2 \\ -\sin\theta/2 & e^{-i\phi}\cos\theta/2 \end{pmatrix}. \tag{2.57}$$

Observe que las estrategias C y D están contenidas en esta parametrización ya que $C = I = U(0, 0)$ y $D = U(\pi, 0)$. Se puede parametrizar una estrategia con un único parámetro real $t \in [0, 1]$, eligiendo

$$U_A = \begin{cases} U(t\pi, 0) & \text{para} \quad t \in [0, 1] \\ U(0, -t\pi/2) & \text{para} \quad t \in [-1, 0). \end{cases}$$

Adoptando la misma parametrización para Bob, con $t_B \in [-1, 1]$, se puede generar una superficie de retornos medios para uno de los jugadores, digamos Alice: $\Pi_A(t_A, t_B)$, y sacar algunas conclusiones. La Fig. 2.11 muestra esta superficie para el conjunto de parámetros $T = 5, R = 3, P = 1, S = 0$.

Esta superficie (en conjunto con otra análoga para el retorno medio de Bob) muestra aspectos nuevos con respecto al juego clásico. El punto (D, D) ya no es un equilibrio de Nash: Alice puede mejorar unilateralmente su

[17] La operación unitaria más general requiere 3 parámetros. Se limita a 2 por simplicidad.

retorno si se aleja de de D. El punto (C, C) tampoco es un óptimo Pareto: ambos jugadores pueden mejorar su retorno desplazándose hacia (Q, Q). En realidad, (Q, Q) es *simultáneamente* un óptimo Pareto y un equilibrio de Nash (el único) con lo cual esta estrategia cuántica debe ser racionalmente elegida y se resuelve el dilema.

La estrategia Q corresponde a $t = -1$ en la parametrización (2.57) de modo que se implementa a través de la operación

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

Cuando ambos jugadores usan esta estrategia, con los parámetros indicados más arriba, obtienen un retorno medio $\Pi_A = \Pi_B = 3$. Si uno de ellos cambia su estrategia unilateralmente, disminuye su retorno. Este juego comenzó con un estado máximamente enredado. Es posible demostrar [DXZH02] que se requiere un mínimo nivel de enredo en el estado inicial para que se resuelva el dilema a través de nuevas estrategias cuánticas. Sin enredo, el estado ρ es en todo momento separable y no hay diferencias con el juego clásico.

Una de las limitaciones de este tipo de juegos es el hecho de que consisten de una única jugada. No hay posibilidad de desarrollar estrategias en el tiempo, "aprender" de comportamientos fallidos ni "educar" al oponente. Otra gran limitación es el hecho de que los jugadores sólo pueden aplicar operaciones de un qubit. Esto impide aplicar operaciones condicionales que dependan del estado del qubit del oponente. En la siguiente sección mostramos como se puede implementar un juego iterado con estrategias condicionales en forma natural usando el QW. También mostramos que una implementación física de este juego con elementos simples de óptica lineal esta al alcance de la tecnología actual.

2.3.2. Juegos cuánticos iterados (*)

En esta sección mostramos como el formalismo de juegos "one-shot" descrito en la Sección anterior puede ser extendido a juegos iterados usando un QW con dos partículas. Este trabajo fue realizado en Montevideo en colaboración con los H. Fort y R. Donangelo [ADF06b, ADF07].

Cuando el Dilema del Prisionero se juega en forma repetida, cada jugador tiene la posibilidad de recompensar (castigar) a su oponente por haber

cooperado (delatado) en la jugada anterior, de modo que los juegos iterados permiten desarrollar estrategias condicionales. En este contexto clásico, las estrategias posibles se parametrizan por cuatro probabilidades condicionales, $[p_R, p_S, p_T, p_P]$, donde p_i es la probabilidad de cooperar habiendo recibido un retorno $i = R, S, T$ or P respectivamente en la jugada anterior. Por ejemplo, la estrategia de *Pavlov* [KK89], representada por las probabilidades $[1, 0, 0, 1]$, implica cambiar de estado cuando el retorno anterior es insatisfactorio (P, S) o permanecer igual fue satisfactorio (T, R). Una estrategia puede ser determinista, en cuyo caso $p_i = 0, 1$ o puede ser no determinista. Por ejemplo, la estrategia no sesgada de cooperar al azar esta representada por $[\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}]$, de modo que se coopera con probabilidad $1/2$ independientemente del retorno anterior. Otra estrategia importante es la TFT (Tit-for-Tat) que corresponde a copiar la jugada previa del otro jugador y se representa por las probabilidades $[1, 0, 1, 0]$.

Usando el formalismo del QW con dos partículas, descrito en la Sección 2.2.3, es posible formular juegos cuánticos iterados bastante generales. Como veremos, el espacio de estrategías es más amplio que en el caso clásico, de modo que una estrategia clásica, parametrizada por probabilidades $[p_R, p_S, p_T, p_P]$, puede dar origen a *una familia* de estrategias cuánticas relacionadas, aunque no todas las estrategias clásicas pueden ser implementadas como operaciones unitarias. Finalmente, mencionaremos como la conexión entre QW y juegos cuánticos puede ayudar a viabilizar la implementación física éstos últimos usando elementos de óptica lineal.

Comenzamos generalizando la regla de evolución , ec. (2.43), para adaptarla a un juego cuántico. El operador de evolución del QW implica una operación de moneda U_c en el espacio de dos qubits, seguida de una traslación condicional S, ec. (2.44), que en todos los casos era de un paso (hacia adelante o hacia atrás). Para que el desplazamiento condicional pueda incorporar la tabla de retornos de un juego concreto (como el Cuadro 2.1) es necesario considerar desplazamientos diferentes para los diferentes estados de las dos monedas, lo cual puede hacerse a través del operador de despla-

zamiento generalizado $\|x_A, x_B\rangle \equiv \|x_A\rangle \otimes \|x_B\rangle$ as

$$\begin{aligned}\Omega \equiv \sum_{x_A,x_B} \Big\{ & \|x_A + s_A^{(0)}, x_B + s_B^{(0)}\rangle\langle x_A, x_B\| \otimes |00\rangle\langle 00| + \\ & \|x_A + s_A^{(1)}, x_B + s_B^{(1)}\rangle\langle x_A, x_B\| \otimes |01\rangle\langle 01| + \\ & \|x_A + s_A^{(2)}, x_B + s_B^{(2)}\rangle\langle x_A, x_B\| \otimes |10\rangle\langle 10| + \\ & \|x_A + s_A^{(3)}, x_B + s_B^{(3)}\rangle\langle x_A, x_B\| \otimes |11\rangle\langle 11| \Big\}. \end{aligned} \tag{2.58}$$

Los 8 parámetros enteros $s_{A,B}^{(i)}$ para $i = 0, 3$ determinan la magnitud de cada desplazamiento y serán especificados más adelante. Por conveniencia, en este contexto adoptamos una notación ligeramente diferente a la de la Sección 2.2.3. Las posiciones de las partículas (x, y) ahora serán registros que acumulan los retornos de cada jugador A,B y se indican por (x_A, x_B). Estas coordenadas siguen siendo enteras, como antes y las sumas en (2.58) son sobre todos los sitios en el plano. El operador de desplazamiento Ω no es separable con respecto a los subespacios $\mathcal{H}_A$ y $\mathcal{H}_B$ a menos que se satisfagan las relaciones,

$$s_A^{(0)} = s_A^{(1)}, \quad s_A^{(2)} = s_A^{(3)}, \quad s_B^{(0)} = s_B^{(2)}, \quad s_B^{(1)} = s_B^{(3)}. \tag{2.59}$$

La observación esencial es que el operador Ω conecta estados particulares de la moneda conjunta con los correspondientes retornos $s_{A,B}$ especificados en una matriz de pagos. Las variables $x_{A,B}$ se usan como registros para almacenar los pagos acumulados de cada jugador. Con este esquema, se pueden construir juegos cuánticos donde la estrategia depende de la operación de moneda aplicada por cada jugador, como definimos más abajo. La variedad de juegos que se puede implementar en base a este esquema es enorme. Para mostrar la potencia de este formalismo desarrollamos a continuación el ejemplo concreto del Dilema del Prisionero, ya introducido en Secciones anteriores, pero teniendo presente que el esquema básico es bastante más general.

Dilema del Prisionero iterado

Los dos agentes A (Alice) y B (Bob) que se oponen en el juego se rigen por tres reglas sencillas:

i. Los estados de moneda de cada agente son interpretados como $|0\rangle \to C$ (cooperación) y $|1\rangle \to D$ (delación) respectivamente.

ii. Cada agente puede actuar sobre su qubit de moneda con una operación unitaria (su estrategia) U_A o U_B en $\mathcal{H}^{\otimes 2}$. Si bien esta operación tiene lugar en el espacio de dos qubits, *no puede modificar el estado de moneda de su oponente.*

iii. El subespacio de posición se usa como un registro cuántico en el cual se acumulan los retornos de cada agente. Si X_A es el operador de posición para Alice, $X_A \, \|x_A\rangle = x_A \, \|x_A\rangle$, su retorno promedio es $\bar{x}_A = \mathrm{tr}(\rho X_A)$ y lo mismo para Bob.

Los registros de posición se actualizan luego de cada operación en el espacio de moneda, de acuerdo con la ec. (2.58), con las identificaciones siguientes (vea el Cuadro 2.1)

$$\begin{aligned} s_A^{(0)} &= s_B^{(0)} = R, \qquad & s_A^{(1)} &= s_B^{(2)} = S, \\ s_A^{(2)} &= s_B^{(1)} = T, \qquad & s_A^{(3)} &= s_B^{(3)} = P. \end{aligned} \tag{2.60}$$

Estas relaciones, junto con las desigualdades implícitas en los parámetros del Cuadro 2.1, implican que el operador de desplazamiento no es separable con respecto a los subespacios A y B.

Asumimos que ambos jugadores comienzan en el autoestado de posición $|x_A, x_B\rangle = |0,0\rangle$ con un estado de moneda inicial arbitrario $|c_0\rangle \in \mathcal{H}_c^{\otimes 2}$. Un estado puro inicial $\rho_0 = \|0,0\rangle\langle 0,0\| \otimes |c_0\rangle\langle c_0|$ evoluciona a $\rho_N = U^N \rho_0 (U^\dagger)^N$ luego de N iteraciones (o jugadas), con U dado por la ec. (2.43). Al cabo del juego, una medida de los observables de posición $X_{A,B}$ determina el retorno final de cada jugador. Alternativamente, el retorno medio o esperable, $\bar{x}_{A,B} = \langle X_{A,B} \rangle$ puede usarse como indicador de suceso. Si realizan medidas parciales de la moneda a cada paso, se destruye la coherencia y se recupera el juego clásico.

Estrategias condicionales

La elección de estrategias se realiza en el espacio de operaciones unitarias *sobre dos qubits* sujetas a la restricción de la regla (ii) definida más arriba. Las operaciones U_A y U_B pueden representar estrategias clásicas, pero también pueden describir nuevas opciones no disponibles clásicamente.

Asumiendo que, en estados como $|01\rangle \equiv |0\rangle \otimes |1\rangle$, el primer qubit desde la izquierda corresponde a Alice y el segundo a Bob, las estrategias disponibles

para Alice, son las operaciones unitarias en el espacio de dos qubits, que no afectan al segundo qubit.

$$\begin{aligned} U_A &= [a_0|00\rangle + a_1|10\rangle]\langle 00| + [a_2|01\rangle + a_3|11\rangle]\langle 01| + \\ &\quad [a_4|00\rangle + a_5|10\rangle]\langle 10| + [a_6|01\rangle + a_7|11\rangle]\langle 11|, \end{aligned} \tag{2.61}$$

donde los coeficientes complejos a_i satisfacen los requerimientos para la unitariedad de U_A. En forma similar, las posibles estrategias disponibles para Bob, son las operaciones unitarias de dos qubits que no alteran el primer qubit,

$$\begin{aligned} U_B &= [b_0|00\rangle + b_1|01\rangle]\langle 00| + [b_2|00\rangle + b_3|01\rangle]\langle 01| + \\ &\quad [b_4|10\rangle + b_5|11\rangle]\langle 10| + [b_6|10\rangle + b_7|11\rangle]\langle 11| \end{aligned} \tag{2.62}$$

donde los b_i son coeficientes complejos que satisfacen los requerimientos para la unitariedad de U_B.

Estrategias Sequenciales

A través de estas operaciones unitarias se pueden implementar estrategias condicionales donde la acción de un jugador depende del estado previo de *ambos* oponentes. Las estrategias incondicionales (como las discutidas en la Sección anterior) también se pueden implementar usando operaciones locales, $U_A = I \otimes E_A$ y $U_B = E_B \otimes I$, donde $E_{A,B}$ actúan localmente en los respectivos subespacios. En el caso general, $[U_A, U_B] \neq 0$, y el orden en que se realiza la jugada hace una diferencia ya que la operación de moneda en la eq. (2.43) puede construirse como $U_B \cdot U_A$ si Alice juega primero, o como $U_A \cdot U_B$ en otro caso. Llamamos *Juegos Secuenciales* a estos juegos, en los que las operaciones de moneda se aplican en un orden determinado. Otra alternativa, que ambos agentes apliquen sus operaciones simultáneamente, da origen a los *Juegos Simultáneos*. En este caso, la operación de moneda, una operación unitaria U_c en $\mathcal{H}_c^{\otimes 2}$, refleja la opción estratégica de ambos jugadores. Un juego secuencial con operaciones de moneda separables es idéntico al correspondiente juego secuencial. Sin embargo, en el caso de operaciones de moneda no separables, los juegos simultáneos no se pueden jugar en forma secuencial y, recíprocamente, los juegos secuenciales no se pueden implementar en forma simultánea. Las operaciones separables son las más interesantes, por su capacidad de generar enredo entre los subespacios A y B, como mostramos en la Sección 2.2.3. Discutimos primero el

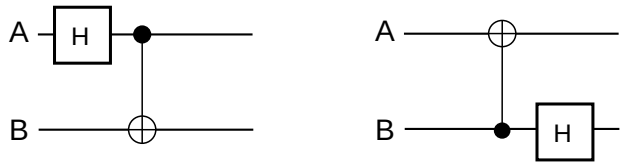

Figura 2.12: Circuitos representando la operaciòn de moneda de un juego cuántico iterado donde se oponen estrategias Pavlov vs. Aleatórea. Izq.: Alice juega Aleat. y Bob responde Pavlov. Der.: Alice juega Pavlov y Bob responde Aleat. Estos circuitos mapean estados de la base computacional en los estados de Bell (máximamente enredados).

caso de los Juegos Secuenciales, que es más cercano al planteo de la Sección anterior y es más sencillo de visualizar.

El vínculo con las estrategias clásicas se logra a través de una parametrización adecuada de las operaciones $U_{A,B}$. En el caso de Alice, operaciones unitarias de la forma (2.61) se parametrizan, en términos de cuatro parámetros reales $[p_R, p_S, p_T, p_P]$ con $p_i \in [0,1]$ como

$$\begin{array}{ll} a_0 = e^{i\varphi_R}\sqrt{p_R} & a_1 = e^{i\theta_R}\sqrt{1-p_R} \\ a_2 = e^{i\varphi_S}\sqrt{p_S} & a_3 = e^{i\theta_S}\sqrt{1-p_S} \\ a_4 = e^{i\varphi_T}\sqrt{p_T} & a_5 = e^{i\theta_T}\sqrt{1-p_T} \\ a_6 = e^{i\varphi_P}\sqrt{p_P} & a_7 = e^{i\theta_P}\sqrt{1-p_P} \end{array} . \tag{2.63}$$

Las fases $\varphi_i, \theta_i \in [-\pi, \pi]$ son nuevas variables con respecto al caso clásico. Una estrategia clásica, definida por valores concretos de $[p_R, p_S, p_T, p_P]$, genera una familia de estrategias cuánticas cuyos integrantes se distinguen por la elección de las fases. Una parametrización similar rige para los coeficientes b_i que determinan las estrategias accesibles para Bob, ec. (2.62). La unitariedad implica que

$$p_R + p_T = p_S + p_P = 1. \tag{2.64}$$

además de las condiciones sobre las fases

$$\left.\begin{array}{rcl} \varphi_T - \varphi_R & = & \theta_T - \theta_R \\ \varphi_P - \varphi_S & = & \theta_P - \theta_S \end{array}\right\} \mod \pi. \tag{2.65}$$

De modo que sólo aquellas estrategias clásicas que satisfacen (2.64) pueden ser implementadas a través de operaciones unitarias. En estos casos, además

de una fase global, una estrategia queda completamente determinada por *siete parámetros reales*.

Por ejemplo, la familia de estrategias de Pavlov, para las cuales $[p_R, p_S, p_T, p_P]$ es $[1, 0, 0, 1]$, cuando es jugada por Alice es de la forma

$$U_A^P = |00\rangle\langle 00| + e^{i\nu_1}|11\rangle\langle 01| + e^{i\nu_2}|10\rangle\langle 10| + e^{i\nu_3}|01\rangle\langle 11| \tag{2.66}$$

en términos de tres fases arbitrarias ν_j. Si se elige $\nu_j = 0$, U_A^P se reduce a una operación CNOT (inversión controlada), [NC00]) en la cual el qubit de control es el de Bob. En forma similar, si es Bob quien aplica Pavlov, la operación es de la forma

$$U_B^P = |00\rangle\langle 00| + e^{i\mu_1}|01\rangle\langle 01| + e^{i\mu_2}|11\rangle\langle 10| + e^{i\mu_3}|10\rangle\langle 11|, \tag{2.67}$$

y para fases $\mu_j = 0$, se reduce a una operación CNOT controlada por el qubit de Alice[18]. Estos son ejemplos de estrategias condicionales basadas en operaciones no separables, en las cuales el orden de aplicación hace una diferencia.

Como ejemplo de una estrategia separable, consideramos el operador de Hadamard definido en la ec. (1.2). Como allí se mostró, este operador genera superposiciones equilibradas de ambos los estados de la base computacional. Esta propiedad lo hace útil para representar una versión cuántica de la estrategia aleatoria $\left[\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}\right]$. De modo que, en cierto modo abusando del lenguaje, si Bob aplica la operación local $U_B = H \otimes I$ diremos que su estrategia es "Aleatoria" por similitud con el caso clásico correspondiente, aunque es claro que la operación realizada es determinista y reversible. Un juego en el cual Alice juega Pavlov y Bob responde con la estrategia aleatoria se describe, para una elección de fases particular, por la operación $U_c = (I_1 \otimes H) \cdot U_A^P$, representada en el circuito de la Fig. 2.12 (Der.).

Para ver que nuevas posibilidades aparecen cuando se consideran estrategias cuánticas, consideramos un espacio de estrategias restringido en el cual suplementamos la condición de unitariedad (2.64) por $p_R + p_S = 1$. De este modo, una estrategia queda determinada (además de la elección de fases) por un único parámetro $\xi \in [0, \pi/2]$ definido por $p_R \equiv \cos^2 \xi$. Para $\xi = 0$ ($p_R = 1$) se obtiene Pavlov y para $\xi = \pi/4$, ($p_R = 0{,}5$) se obtiene una estrategia aleatoria. Valores de $\xi \in [0, \pi/4]$ resultan en estrategias intermedias entre Pavlov y Random. Si se adopta la misma parametrización

[18] Esta es la forma en la cual la operación fue introducida en la ec. (1.5).

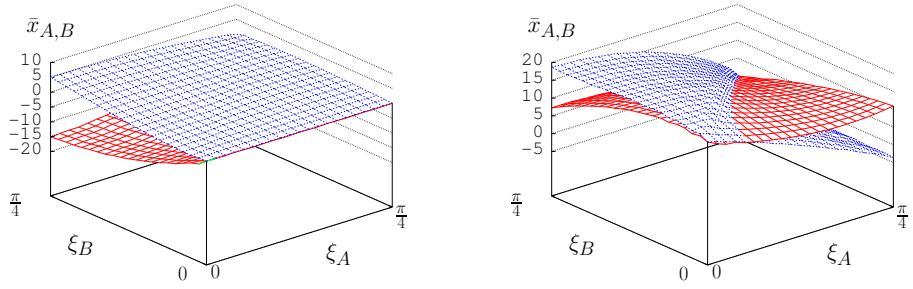

Figura 2.13: Retorno medio de Alice (rojo) y Bob (azul) luego de $N = 50$ jugadas, como función de ángulos $\xi_{A,B} \in [0, \pi/4]$ definidos en el texto. Las condiciones iniciales son equilibradas (vea el texto por detalles).

para la estrategia de Bob, la operación resultante es $U_c = U_B(\xi_B) \cdot U_A(\xi_A)$, suponiendo que Alice juega primero.

Los retornos medios luego de $N = 50$ iteraciones se muestran en la Fig. 2.13 para dos estados iniciales equilibrados: el estado producto $(|00\rangle + i|01\rangle + i|10\rangle - |11\rangle)/2$ (Izq.) y el estado máximamente enredado $(|00\rangle + |11\rangle)/\sqrt{2}$ (Der.). Estos resultados son para los valores de los parámetros $R{=}{-}P{=}1$ and $T{=}{-}S{=}2$. En el caso clásico, al confrontar estas estrategias se obtiene un empate. Esta situación es excepcional en el caso cuántico, donde además los resultados dependen fuertemente de las condiciones iniciales.

Otra forma de ver como se desempeñan ambos jugadores es comparar sus retornos, ($\bar{x}_A$ vs. $\bar{x}_B$), al modo de los economistas. En estos diagramas, la diagonal representa un empate. La Fig. 2.14 muestra estos resultados para los dos estados iniciales equilibrados $(|00\rangle + |11\rangle)/\sqrt{2}$ y $(|01\rangle + |10\rangle)/\sqrt{2}$. Independientemente de la estrategia elegida por Bob, Alice debe jugar Pavlov ($\xi_A = 0$) para maximizar su retorno (vea el panel (a)). Por otra parte, Bob obtiene el máximo retorno cuando adopta una estrategia intermedia con $\xi_B \simeq \pi/20$ si Alice juega Pavlov (vea el panel (b)). El punto P $(\xi_A, \xi_B) = (0, \pi/20)$ es un equilibrio de Nash que también es un óptimo Pareto. Como se muestra en los paneles (c) y (d), la misma estrategia Pavlov puede resultar en un retorno máximo o mínimo, dependiendo de la elección estratégica de Bob.

Debe resistirse la tentación de extraer conclusiones generales a partir del ejemplo aquí mostrado, ya que el mismo corresponde a un espacio de estrategias restringido y a condiciones iniciales particulares. Sin embargo,

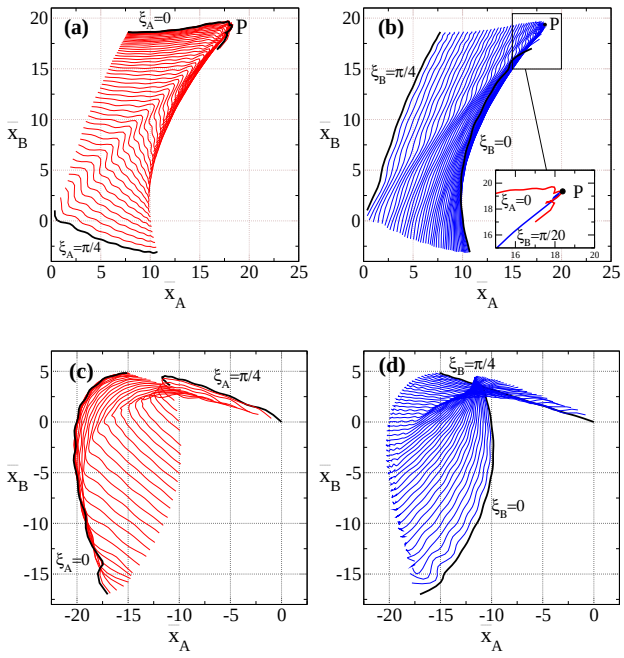

Figura 2.14: Retornos medios ($\bar{x}_A$ vs. $\bar{x}_B$) luego de 50 iteraciones para diferentes condiciones iniciales. En los paneles (a,b) la moneda inicial es $(|00\rangle + |11\rangle)/\sqrt{2}$ y en (c,d) es $(|01\rangle + |10\rangle)/\sqrt{2}$. Los paneles (a, c) muestran líneas de ξ_A constante (en rojo). Los paneles (b,d) muestran líneas de ξ_B constante (en azul). Los valores extremos de ξ_A y ξ_B se indecan por líneas gruesas. En ambos casos, el otro parámetro varía de 0 (Pavlov) a $\pi/4$ (aleatórea). El recuadro en el panel (b) muestra las líneas $\xi_A = 0, \xi_B = \pi/20$ que se intersectan en el punto P en el cual ambos agentes maximizan su retorno simultáneamente.

queda claro que la riqueza de alternativas que se pueden presentar es mucho mayor que en el caso clásico. Como se discutió antes, no todas las estrategias clásicas pueden ser implementadas en un juego cuántico secuencial, debido a la restricción (2.64). Una importante estrategia clásica que no cumple esta restricción es TFT, que consiste en copiar la jugada anterior del oponente. Sin embargo, el espacio de estrategias puede ser extendido considerando que ambos jugadores aplican su operación simultáneamente. En este caso, TFT pasa a ser una opción posible.

Estrategias simultáneas

El caso de jugadas simultáneas es más cercano al Dilema del Prisionero clásico. Supongamos que Alice va a aplicar una estrategia de la familia $[p_R^A, p_S^A, p_T^A, p_P^A]$ y Bob una con parámetros $[p_R^B, p_S^B, p_T^B, p_P^B]$. Una jugada si-

multánea involucra una operación unitaria en el espacio de dos qubits, que puede parameterizarse por

$$\begin{bmatrix} e^{i\varphi_{11}}\sqrt{p_R^A p_R^B} & e^{i\varphi_{12}}\sqrt{p_R^A \bar{p}_R^B} & e^{i\varphi_{13}}\sqrt{\bar{p}_R^A p_R^B} & e^{i\varphi_{14}}\sqrt{\bar{p}_R^A \bar{p}_R^B} \\ e^{i\varphi_{21}}\sqrt{p_S^A p_T^B} & e^{i\varphi_{22}}\sqrt{p_S^A \bar{p}_T^B} & e^{i\varphi_{23}}\sqrt{\bar{p}_S^A p_T^B} & e^{i\varphi_{24}}\sqrt{\bar{p}_S^A \bar{p}_T^B} \\ e^{i\varphi_{31}}\sqrt{p_T^A p_S^B} & e^{i\varphi_{32}}\sqrt{p_T^A \bar{p}_S^B} & e^{i\varphi_{33}}\sqrt{\bar{p}_T^A p_S^B} & e^{i\varphi_{34}}\sqrt{\bar{p}_T^A \bar{p}_S^B} \\ e^{i\varphi_{41}}\sqrt{p_P^A p_P^B} & e^{i\varphi_{42}}\sqrt{p_P^A \bar{p}_P^B} & e^{i\varphi_{43}}\sqrt{\bar{p}_P^A p_P^B} & e^{i\varphi_{44}}\sqrt{\bar{p}_P^A \bar{p}_P^B} \end{bmatrix}$$

donde $e^{i\varphi_{kl}}$ son factores de fase y $\bar{p}_i^{A,B} \equiv 1 - p_i^{A,B}$. En el caso particular de U_c real, $e^{i\varphi_{kl}} = \pm 1$, y la unitariedad implica

$$\begin{aligned} (p_R^A - \bar{p}_S^A)(p_R^B - \bar{p}_T^B) &= (p_R^A - \bar{p}_T^A)(p_R^B - \bar{p}_S^B) = 0, \\ (p_R^A - \bar{p}_P^A)(p_R^B - \bar{p}_P^B) &= (p_S^A - \bar{p}_T^A)(p_S^B - \bar{p}_T^B) = 0, \\ (p_S^A - \bar{p}_P^A)(p_T^B - \bar{p}_P^B) &= (p_T^A - \bar{p}_P^A)(p_S^B - \bar{p}_P^B) = 0. \end{aligned}$$

En el caso general se pueden obtener restriccione análogas que involucran las fases φ_{kl}. Por ejemplo, un juego en el que Alice juega Pavlov $[1, 0, 0, 1]$ y Bob simultáneamente responde con TFT $[1, 0, 1, 0]$, se implementa con

$$U_c^{PT} = |00\rangle\langle 00| + e^{i\lambda_1}|10\rangle\langle 01| + e^{i\lambda_2}|11\rangle\langle 10| + e^{i\lambda_3}|01\rangle\langle 11|,$$

en términos de tres fases arbitrarias λ_i. En la versión clásica de este juego, si ambos agentes comienzan jugando C con probabilidad $1/2$, luego de N iteraciones tienen un retorno nulo en promedio, $N(R + P) = 0$. En el juego cuántico, comenzando con el estado de Bell mencionado antes, los retornos medios son ambos positivos y diferentes ente si.

En la misma forma, es posible confrontar otras estrategias clásicas en forma secuencial, con la limitación (2.68). Por ejemplo, no se pueden confrontar en forma simultánea dos estrategias Pavlov, pero si se puede hacer en forma secuencial. En el Cuadro 2.2 consideramos tres estrategias clásicas e indicamos cuales de ellas pueden confrontarse en forma secuencial o simultánea. Los juegos confrontando TFT vs aletoria, no pueden realizarse en ninguno de los dos esquemas. Estos juegos podrían ser implementados en sistemas abiertos, usando el formalismo más general de operaciones cuánticas.

2.3.3. Resumen y Perspectivas (**)

Hemos centrado nuestra atención en el Dilema del Prisionero, por ser un juego paradigmático a nivel clásico. Se están actualmente realizando ensayos

	Aleatóreo	Pavlov	TFT
Aleatóreo	1, 2	1,2	no unitario
Pavlov	1,2	1	2
TFT	no unitario	2	2

Cuadro 2.2: Algunas estrategias clásicas que generan familias de estrategias cuánticas que se pueden confrontar entre si en el esquema secuencial (1) y simultáneo (2) de juegos cuánticos.

con sujetos humanos no entrenados en Mecánica Cuántica, a los cuales se les presenta una versión del Dilema del Prisionero cuántico simulada con una computadora [CH06]. Luego de una etapa inicial de entrenamiento en la cual aprenden de sus errores, los sujetos son capaces de aprovechar – en forma práctica – las ventajas de las estrategias cuánticas para tener un mejor desempeño, en forma análoga a como un niño atrapa una pelota en el aire sin realizar cálculos de trayectoria basados en los principios de la Mecánica Newtoniana.

Hemos relacionado en forma general los juegos bi-partita iterados de suma no nula con el QW de dos partículas. Los juegos iterados propuestos son los primeros en los cuales la estrategia es una operación condicional sobre dos qubits. Varias estrategias clásicas pueden ser confrontadas, ya sea en forma secuencial o simultánea. Se han obtenido las condiciones que deben ser satisfechas por una estrategia clásica para poder ser implementada a través de operaciones unitarias. Cada estrategia clásica que satisface estas condiciones da lugar a una familia de estrategias cuánticas cuyos integrantes difieren en la elección de las fases. El espacio de estrategias cuánticas es extremadamente grande (especificar completamente una estrategia secuencial requiere 7 parámetros reales). A través de ejemplos hemos mostrado que en los juegos cuánticos se obtienen resultados nuevos con respecto a sus correspondientes clásicos.

En los juegos cuánticos "one-shot" [EWL99b, DXZH02], se requiere preparar (externamente) el estado inicial con cierto nivel mínimo de enredo para tener acceso a las posibilidades cuánticas, i.e. resolver el Dilema del Prisionero alcanzando un equilibro de Nash que es a su vez un óptimo Pareto. En nuestra propuesta iterada, el enredo puede ser generado dinámicamente

por las operaciones no separables utilizadas por los participantes. Hemos cuantificado el enredo entre los subespacios de ambos jugadores en un juego que confronta estrategias Pavlov vs Aleatórea, usando la entropía de enredo (vea la Fig. 2.9). En este y otros casos no separables, el enredo crece logarítmicamente con el número N de jugadas. El espacio de estrategias puede extenderse usando operaciones generalizadas (vea el Apéndice A), de modo que además de las operaciones unitarias, los jugadores puedan realizar medidas parciales de su moneda. Esta medida afectaría al estado del oponente de una forma que depende del nivel de enredo, que pasaría a tener un rol central en el resultado del juego.

El esquema que hemos presentado para juegos bi-partita, se puede adaptar en forma evidente a juegos multi-partitas, como el problema de "distribución de bienes públicos" o *Public Goods problem*, un asunto de interés práctico en diversos ámbitos. Se ha sugerido que las nuevas alternativas emergentes de una versión cuántica del problema [CHB03] pueden ayudar a resolver problemas concretos de distribución equitativa de recursos y asignación equitativa de responsabilidades.

Culminamos este (algo extenso) capítulo mencionando la posibilidad de la implementación física de juegos cuánticos del tipo aqui presentado usando elementos de óptica lineal, usando un esquema similar al mencionado en la Sección 1.2.2, adaptado al caso de dos fotones [PA06] y complementado por la operación condicional CNOT entre estados de moneda codificados en la polarización de *dos fotones*, implementada ópticamente [OPW$^+$03]. Hemos comenzado a analizar la viabilidad de esta propuesta en conjunto con S. Barreiro del IFFI y H. Fort del IFFC.

Capítulo 3

Algoritmos Cuánticos

3.1. Algoritmos cuánticos de búsqueda

Los algoritmos cuánticos de búsqueda pueden encontrar un ítem en una base no indexada de N items en $\mathcal{O}\left(\sqrt{N}\right)$, lo cual es una mejora con respecto a algoritmos clásicos, en general $\mathcal{O}(N)$. Se puede demostrar que un algoritmo cuántico de búsqueda de orden $\mathcal{O}\left(\sqrt{N}\right)$ es óptimo [NC00, # 6.6], de modo que no hay perspectivas de mejorar en este aspecto. Los algoritmos de búsqueda cuánticos no cambian la complejidad del problema de búsqueda, que sigue siendo polinomial. Es poco probable que, por si solos, justifiquen el costo de desarrollar y operar un procesador cuántico. Sin embargo, son interesantes como un ejemplo concreto de que, a través del paralelismo cuántico, es posible resolver problemas relevantes más rápido de lo que los mejores métodos clásicos permiten. Además, como discutiremos en la siguiente sección, la técnica de amplificación de fase usada en el contexto de los problemas NP-Completos, permite lograr la solución más eficiente conocida para esta clase de problemas (considerados los mas "duros" desde el punto de vista computacional).

Dividimos los algorítmos de búsqueda en aquellos "tipo Grover", basados en la amplificación de amplitud y otros basados en el QW (el centro de atención en éste trabajo), aunque todos ellos son óptimos y probablemente equivalentes entre si.

3.1.1. Algoritmos basados en amplificación de amplitud

El algoritmo de Grover [Gro97] ataca el problema de encontrar un elemento en una base no estructurada de N elementos y lo hace en $\mathcal{O}\left(\sqrt{N}\right)$ pasos. Clásicamente, no hay nada mejor que recorrer secuencialmente los elementos uno a uno hasta encontrar el buscado, un proceso que lleva en media $N/2$ consultas y es por tanto $\mathcal{O}(N)$. El algoritmo de Grover se basa en el paralelismo cuántico y en la técnica de amplificación de fase para llegar al elemento buscado y es el paradigma de los algorítmos de búsqueda cuánticos. La versión que aquí presentamos es desprovista de generalizaciones, pero contiene los elementos esenciales del algoritmo de búsqueda.

Algoritmo de Grover

Consideremos el espacio de Hilbert generado por los N estados[1] $\{\|x\rangle\}$ con $k = 0, 1, \ldots x_0, \ldots N-1$. Suponemos que $N = 2^n$, de modo que usamos un registro de n qubits para representar los estados de la base de búsqueda. Estos estados se suponen ortogonales (es decir, distinguibles entre si) y – por simplicidad – supondremos que existe una y solo una solución al problema de búsqueda: $\|x_0\rangle$.

Tanto a nivel clásico como cuántico es necesaria una forma de distinguir el estado buscado de los demás. Esto se hace a través de un oráculo, que nuestro caso es una función binaria con soporte en los enteros $f(0, 1, \ldots, N-1) \to \{0, 1\}$. El oráculo se define por

$$f(x) = \begin{cases} 0 & \text{si} \quad x = x_0 \\ 1 & \text{si} \quad x \neq x_0. \end{cases} \tag{3.1}$$

En la práctica será necesario implementar esta función a través de una operación unitaria, usando las compuertas cuánticas usuales, pero no entraremos en ese nivel de detalle. La acción de f se parametriza a través de una operación unitaria U_f sobre $n+1$ qubits en la forma

$$U_f \, \|x\rangle \otimes |k\rangle \equiv \|x\rangle \otimes |k \oplus f(x)\rangle. \tag{3.2}$$

La implementación del oráculo requiere de un qubit adicional como espacio de trabajo, de modo que el algoritmo se implementa sobre $n+1$ qubits.

[1] Cuando haya riesgo de confusión, en éste capítulo usaremos la notación $\|\cdot\rangle$ para los estados de n qubits, reservando $|0\rangle, |1\rangle$ para los de un qubit.

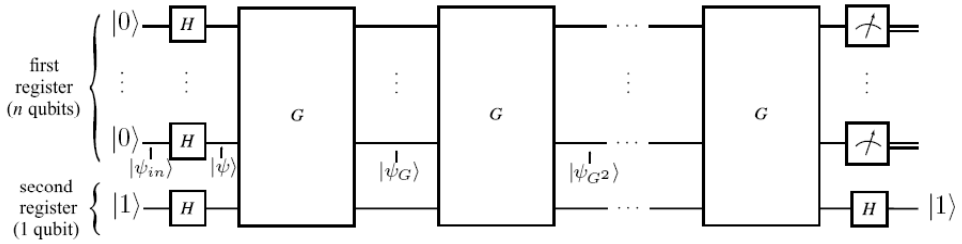

Figura 3.1: Circuito que implementa el algoritmo de Grover. La operación de Grover G incluye al oráculo (corresponde a $\tilde{G} = GU_f$ en el texto) se explica en la Fig. 3.2. Figura tomada de [LMP00].

Trataremos a los n primeros como un registro R que puede contener a los estados de la base (a todos a la vez!) y al último como un qubit auxiliar (*ancilla*, en la jerga).

Se puede resumir el algoritmo de Grover en 4 pasos:

1. Preparación de una superposición uniforme de los estados de la base.
2. Aplicación del oráculo que codifica la información buscada en la fase relativa.
3. Amplificación de amplitud.
4. Medida.

Los pasos 2 y 3 se aplican juntos y se iteran $\sim \sqrt{N}$ veces, hasta que la amplificación es suficiente para tener una razonable chance de éxito al medir. El algoritmo de Grover es no determinista, de modo que puede ser necesario repetir el proceso 1–4 algunas veces hasta encontrar el estado buscado. Estas repeticiones no cambian la complejidad del algortimo, que sigue siendo $\mathcal{O}\left(\sqrt{N}\right)$. Estas etapas se muestran en el esquema de la Fig. 3.1.

1. Preparación.
Partiendo del estado de $n+1$ qubits $\|0\rangle \otimes |0\rangle$, aplicamos una inversión σ_x al último qubit y una operación de Hadamard (como en la ec. (1.3)) para obtener la superposición uniforme

$$|\Psi_0\rangle = H^{\otimes n} \, \|0\rangle \otimes H|1\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \|x\rangle \otimes |-\rangle \tag{3.3}$$

donde $H|1\rangle = |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. El resultado de ésta operación es colocar el registro R en una superposición de todas las alternativas, incluyendo la buscada y preparar el qubit auxiliar en la superposición $|-\rangle$, adecuada para codificar la información en la fase relativa.

2. Oráculo

Se aplica ahora el oráculo sobre ésta superposición, observando que, dado que f es binaria,

$$U_f \, \|x\rangle \otimes |-\rangle = \|x\rangle \otimes \frac{|f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}} = (-1)^{f(x)} \, \|x\rangle \otimes |-\rangle.$$

De modo que este paso codifica la información de $f(x) = 0, 1$ en la fase del estado $\|x\rangle \otimes |-\rangle$. Cuando aplicamos esta operación a la superposición $|\Psi_0\rangle$ dada por la ec. (3.3), el estado buscado adquiere un desfasaje π con respecto al resto,

$$U_f|\Psi_1\rangle = \sum_{x=0}^{N-1} (-1)^{f(x)} \, \|x\rangle \otimes |-\rangle.$$

Aunque la información buscada esta codificada en las fases relativas de éste estado, la misma no es accesible clásicamente ya que el estado sigue siendo una superposición uniforme de todas las alternativas. Si realizamos ahora una medida tenemos una probabilidad despreciable, $1/N \ll 1$, de encontrar el estado x_0... Es necesario, antes de medir, amplificar la amplitud de la componente buscada, usando la técnica de *amplificación de amplitud* [BHMT02].

3. Amplificación de amplitud

Para transformar la información codificada en la fase relativa del estado buscado a su amplitud relativa, se siguen una serie de pasos consistentes en aplicar el oráculo U_f seguido del operador de Grover $G = 2|\Phi_0\rangle\langle\Phi_0| - I$, con respecto al estado de partida. El qubit auxiliar ya no juega ningún rol, de modo que podemos omitirlo y trabajar con los estados de n qubits[2]. La operación de Grover actúa en el espacio de n qubits simetrizando un estado cualquiera $|\Phi\rangle$ con respecto a un estado de referencia $|\Psi\rangle$, como se muestra en la Fig. 3.2 (Izq.).

Para analizar lo que ocurre al aplicar el operador $\tilde{G} = G \cdot U_f$ a la superposición inicial $|\Psi_0\rangle$, lo más conveniente es usar la representación de la

[2]Preservamos los nombres $|\Psi_i\rangle$ anteriores para no recargar la notación

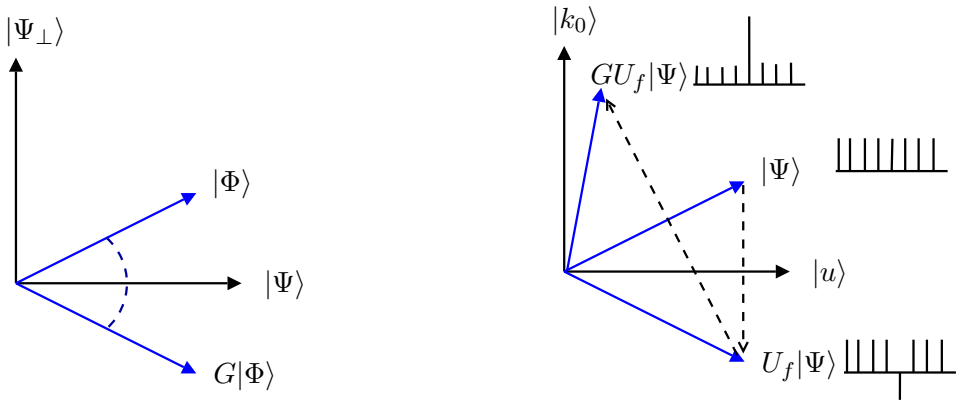

Figura 3.2: Interpretación gráfica de un paso de amplificación de fase. Izquierda: la acción de la operación de Grover, $G = 2|\Psi\rangle\langle\Psi| - I$, sobre un estado arbitrario $|\Phi\rangle$ se visualiza dividiendo el espacio en el estado $|\Psi\rangle$ y el subespacio ortogonal, indicado por $|\Psi_\perp\rangle$. Derecha: la acción del oráculo U_f se visualiza dividiendo el espacio entre el estado buscado, $|k_0\rangle$, y el subespacio ortogonal al mismo, indicado por $|\alpha\rangle$. Al cabo de ambas operaciones, en $GU_f|\Psi\rangle$ el estado buscado aparece con mayor amplitud. Los gráficos de barras muestran, esquemáticamente, las amplitudes a_x.

Fig. 3.2 (Der.), del estado buscado $|x_0\rangle$ y la superposición del resto de los estados $|u\rangle$. La relación es

$$\sqrt{N}|\Psi_0\rangle = \sum_{x=0}^{N-1} |x\rangle = \sqrt{N-1}|u\rangle + |x_0\rangle \tag{3.4}$$

de modo que

$$|\Psi_0\rangle = \cos\theta/2|u\rangle + \sin\theta/2|x_0\rangle \tag{3.5}$$

donde hemos parametrizado las componentes en términos de un ángulo θ como

$$\cos(\theta/2) \equiv \sqrt{1 - \frac{1}{N}}, \quad \text{y} \quad \sin(\theta/2) = \frac{1}{\sqrt{N}}.$$

Este ángulo tiene una interpretación geométrica evidente en la Fig. 3.2 (Der.).

La aplicación del oráculo deja inalterado al estado $|u\rangle$ que no contiene soluciones y cambia la fase de $|x_0\rangle$, de modo que en esta representación,

$$U_f|\Psi_0\rangle = \cos\theta/2|u\rangle - \sin\theta/2|x_0\rangle.$$

A partir de las proyecciones $\langle\Psi_0|x_0\rangle = \sin(\theta/2)$ y $\langle\Psi_0|u\rangle = \cos(\theta/2)$, es fácil ver que la operación de Grover actúa como

$$\begin{aligned} G|u\rangle &= \cos\theta|a\rangle + \sin\theta|x_0\rangle \\ G|x_0\rangle &= \sin\theta|a\rangle - \cos\theta|x_0\rangle. \end{aligned}$$

Por lo tanto una operación (oráculo + Grover) de las indicadas en un bloque G de la Fig. 3.1, actúa como

$$\begin{aligned} |\Psi_1\rangle = \tilde{G}|\Psi_0\rangle &= \cos\frac{\theta}{2}\, G|u\rangle - \sin\frac{\theta}{2}\, G|x_0\rangle \\ &= \cos\left(\frac{3}{2}\,\theta\right)|a\rangle + \sin\left(\frac{3}{2}\,\theta\right)|x_0\rangle \end{aligned} \tag{3.6}$$

Para $N \gg 1$ una expansión de Taylor muestra que $\theta/2 \sim 1/\sqrt{N}$, de modo que la probabilidad de encontrar el estado buscado, si medimos $|\Psi_1\rangle$ es

$$P_1 = \sin^2\left(\frac{3}{2}\,\theta\right) \sim \frac{3}{N}$$

y se ha obtenido una mejora con respecto a $1/N$.

4. Medida

No entraremos aquí en los detalles, pero es posible mostrar que después de k iteraciones del protocolo combinado (oráculo+Grover) el estado resultante es

$$|\Psi_k\rangle = \tilde{G}^k|\Psi_0\rangle = \cos\left(\frac{2k+1}{2}\theta\right)|u\rangle + \sin\left(\frac{2k+1}{2}\theta\right)|x_0\rangle. \tag{3.7}$$

Interesa que en este estado la probabilidad de medir y obtener $|x_0\rangle$ sea alta,

$$P_k = \sin^2\left(\frac{2k+1}{2}\theta\right) \approx 1. \tag{3.8}$$

Esta condición permite estimar el número de iteraciones necesarias antes de realizar la medida. En efecto, usando la aproximación $\theta \approx 2/\sqrt{N}$ para $N \gg 1$, la condición es ($I[\cdot]$ representa la parte entera)

$$\left(k + \frac{1}{2}\right)\theta = \frac{\pi}{2} \Rightarrow k = I\left[\frac{\pi}{4}\sqrt{N}\right].$$

De modo que bastan $\mathcal{O}\left(\sqrt{N}\right)$ iteraciones del protocolo de Grover para encontrar el estado buscado con probabilidad cercana a 1. Como mencionamos en la introducción, esto es óptimo, al menos en lo que concierne a la Mecánica Cuántica.

En los últimos años se han desarrollado muchas variantes del algoritmo de Grover. Una de ellas, desarrollada por integrantes de nuestro grupo [RAD06], usa transiciones resonantes para encontrar el estado buscado. Volviendo al eje de éste trabajo, discutiremos algunos resultados de algoritmos de búsqueda basados en el QW.

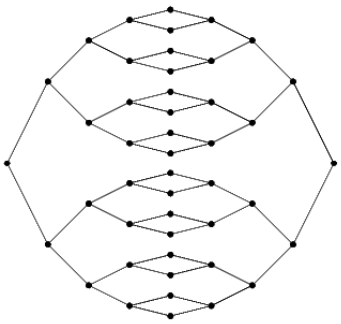

Figura 3.3: Dos grafos binarios de profundidad $N = 4$ conectados por los 2^N nodos del medio. Un caminante clásico tiene que tomar una decisión binaria en cada nodo y lo atraviesa en $\sim 2^N$ pasos. En [CFG02] se muestra que con la caminata cuántica a tiempo continuo requiere $\sim N$ pasos para atravesar el grafo.

3.1.2. Algoritmos basados en QW

Existen varios protocolos basados en QW que recorren ciertos grafos en forma *exponencialmente* más rápida que en el caso clásico. En lo que respecta al QW a tiempo continuo (vea la Sección 1.2.3), Childs et al. muestran que puede atravesar un grafo consistente en dos árboles binarios de profundidad N conectados entre si (vea la Fig. 3.3) exponencialmente más rápido que en el caso clásico. El proceso se mapea en el QW en una línea y se muestra que un caminante clásico requiere $\sim 2^N$ pasos, en tanto un QW (tiempo continuo) requiere $\mathcal{O}(N)$ pasos [CFG02, CCD$^+$03]. Existe también un algoritmo de búsqueda óptimo ($\mathcal{O}(N)$) basado en resonancias hamiltonianas en un QW a tiempo continuo [CG04].

Propiedades análogas se manifiestan también en el QW a tiempo discreto. En 2002, Julia Kempe mostró que un QW puede atravesar un hipercubo [MR01] de dimensión $d \geq 3$ en un número de pasos exponencialmente menor que el caminante al azar clásico [J.K03]. Existen varios algoritmos de búsqueda basados en el QW. El primero de ellos, debido a Shenvi et al. [SKW03] realiza una búsqueda de un ítem en una base de datos no estructurada de N elementos, usando $\sqrt{N}$ pasos, es decir una búsqueda óptima desde el punto de vista cuántico. Usa para ello un QW en un hipercubo de dimensión $n \approx \log_2 N$. Posteriormente, Ambainis et al. proponen un algoritmo [Amb03] basado en un QW para resolver el problema de determinar si en un conjunto de N elementos, son (o no) todos diferentes (*element distinctenss*) con $\mathcal{O}\left(N^{2/3}\right)$ consultas, lo cual supera (aunque no por mucho)

al mejor algoritmo clásico, que requiere $\mathcal{O}\left(N^{3/4}\right)$. No nos detendremos en éstos algoritmos de búsqueda, en su mayoría variaciones del protocolo de Grover que representan mejoras sobre los algoritmos clásicos pero no cambian la clase de complejidad del problema. Consideramos a continuación los problemas, para los cuales los mejores algoritmos clásicos requieren recursos exponenciales.

3.2. Problemas NP

Los problemas computables se clasifican en clases de complejidad [NC00]. La clase **P** (Polynomial time) comprende aquellos problemas para los cuales se conoce un algoritmo que requiere un tiempo[3] polinomial en el tamaño de la entrada. Una cuantificación adecuada del "*tamaño de la entrada*" puede ser, por ejemplo, el número de bits o de qubits necesarios para codificarla. Los problemas en la clase **P** admiten una solución *eficiente*[4]. Un ejemplo es el protocolo para multiplicar dos números enteros.

Los problemas en la clase NP, son aquellos para los cuales un candidato a solución puede ser verificado en tiempo polinómico. Para estos problemas, en general no se tiene un algoritmo eficiente que encuentre una solución. Un ejemplo de este tipo de problemas es la factorización de enteros. El célebre algoritmo de Shor de 1994 [Sho97], verdadero impulsor del área de la computación cuántica, proporcionó una solución cuántica eficiente para el problema de la factorización de enteros grandes, reduciéndolo a la clase P[5] La importancia del problema de factorización de enteros es que es una de las operaciones "one-way" usadas en criptografía. Uno de los protocolos más comunes (RSA distribución de claves públicas y privadas) se basa en facilidad para multiplicar dos números grandes y la dificultad para luego factorizarlos.

La relación entre las clases **P** y **NP** es uno de los problemas abiertos más importantes[6] en Teoría Informática. La conjetura extendida es que $\mathbf{P} \subset \mathbf{NP}$

[3]En este contexto, "tiempo" significa número de pasos, independientemente de la frecuencia del procesador.

[4]En este contexto, eficiente significa justamente que requieren recursos polinomiales en el tamaño de la entrada.

[5]Aunque, desde un punto de vista práctico continua siendo NP, ya que por el momento no existen procesadores cuánticos de cientos de quits capaces de factorizar enteros grandes en tiempos polinómicos.

[6]Este es uno de los "problemas del Milenio" para el cual existe un premio de un millón

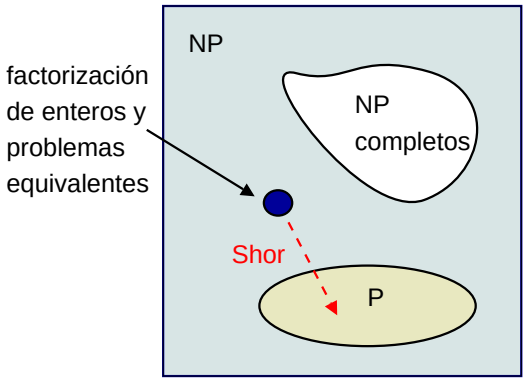

Figura 3.4: Representación gráfica de la conjetura $P \neq NP$. Basada en [Gj99].

en sentido estricto ($\mathbf{P} \neq \mathbf{NP}$); es decir, existirían problemas en **NP** que no admiten solución en tiempo polinomial [Gj99]. La Fig. 3.4 ilustra esta conjetura. Si la conjetura fuera falsa y $\mathbf{P} = \mathbf{NP}$, la existencia de una solución que puede ser verificada en tiempo polinómico implicaría que puede encontrarse dicha solución en forma eficiente.

3.2.1. Problemas NP-completos

Existe un subconjunto de problemas en la clase NP, que son los NP-completos. Este tipo de problemas se caracteriza por la propiedad de que pueden ser mapeados unos en otros en tiempo polinomial. De modo que si uno de estos problemas fuera resuelto eficientemente, se tendría una solución para todos ellos. Existen cientos de problemas NP-completos, vea el Apéndice A de [Gj99] por una lista detallada. En general, son problemas de optimización en espacios de muchas dimensiones con escasa u nula estructura, sujetos a muchos vínculos, lo cual los hace muy difíciles computacionalmente. Algunos de estos problemas son de gran impacto aplicado. Por ejemplo la asignación optima de recursos o tripulaciones en líneas de transporte; el problema del viajante de comercio, en el cual se debe minimizar la distancia o el tiempo empleados para recorrer un determinado número de ciudades, el problema de "simulated annealing" y muchos otros problemas relevantes en lógica, matemáticas, informática, investigación operativa y otras áreas del conocimiento. Lamentablemente, el problema de la factorización de enteros resuelto eficientemente por el algoritmo de Shor, es **NP** (clásicamente)

de dólares del Clay Mathematics Institute, para quien pruebe la relación entre las clases P y NP. Vea http://www.claymath.org/millennium

pero no se ha podido probar que sea **NP-completo**, de modo que su solución eficiente no aporta nada a ésta clase de problemas. Uno de los mejores algoritmos clásicos para resolver estos problemas es estocástico, basado en métodos de búsqueda local y encuentra una solución en tiempo exponencial. Más adelante daremos detallas de este algoritmo, que es muy sencillo. Veremos como usando la técnica de amplificación de fase, como en el algoritmo de Grover, es posible mejorar el tiempo del mejor algoritmo clásico.

Como se prueba usualmente que un problema es **NP-completo**? Existen unos pocos problemas para los cuales se puede demostrar formalmente que pertenecen a esta clase, por ejemplo el problema de satisfabilidad (k-SAT) para $k \geq 3$, que discutimos más adelante. Cualquier otro problema que sea reducible a uno de los primeros en tiempo polinomial esta en la clase **NP**. A través del trabajo pionero de Stephen Cook en 1971 [Coo71] se probó que el problema 3-SAT es **NP-completo**, de modo que si existe un algoritmo eficiente para 3-SAT, toda la clase **NP-completo** se reduciría a **P** y, recíprocamente, si cualquier problema en esta clase es soluble en tiempo polinomial, el 3-SAT también. De algún modo, quizás por precedencia histórica, el problema 3-SAT es el paradigma de los problemas **NP-completos**.

El problema k-SAT

El problema k-SAT se formula en términos de lógica Booleana. Sea $\vec{X} = \{x_1, x_2, \ldots, x_n\}$ un conjunto de $n \geq k$ variables binarias. Consideramos m cláusulas que involucran $k \leq n$ variables cada una, expresadas en la forma estándar CNF[7]. Para una o dos variables , $1, 2 - SAT$, se puede encontrar una solución en tiempo polinómico y el problema esta en la clase de complejidad **P**. Pero para $k \geq 3$, el problema es **NP-completo**. Una demostración de ello se reproduce en [Gj99].

Como los problemas $k - SAT$ con $k > 3$ son reducibles a $3 - SAT$ agregando cláusulas, el problema relevante es con $k = 3$. Damos un ejemplo con $n = 4$ variables (o literales, en este contexto) y $m = 2$ cláusulas:

$$\Omega = (x_1 \vee \bar{x}_2 \vee \bar{x}_3) \wedge (x_1 \vee x_2 \vee x_4).$$

Esta puede ser la formalización de un problema de optimización cualquiera

[7]Conjunctive Normal Form (CNF): una serie de cláusulas unidas por conjunciones AND=$\bigwedge$, donde cada cláusula incluye solo variables, x_i o sus negaciones, $\bar{x}_i$, unidas por disjunciones OR=$\bigvee$. Cualquier proposición lógica puede llevarse a esta forma.

y se trata de encontrar una instancia del vector Booleano $\vec{X}$, que satisface Ω. El espacio de alternativas tiene 2^n elementos, de modo que una recorrida secuencial por este espacio sería un algoritmo exponencial, $\mathcal{O}(2^n)$. Los mejores algoritmos clásicos, estocásticos y basados en búsquedas locales por caminatas al azar, no mejoran mucho esta situación.

Algoritmo de Schöning (**)

En esta sección describimos el algoritmo de Schöning para resolver el problema 3-SAT [Sch99]. Es, hasta donde sabemos, el algoritmo clásico más rápido para resolver este problema, y tiene un costo $\mathcal{O}(1{,}334^n)$, donde n es el número de variables.

La siguiente es la descripción de éste protocolo,

1. Entrada: una fórmula k-SAT Ω con $n \geq k$ variables Booleanas $\vec{X} = \{x_1, x_2, \ldots, x_n\}$.

2. Se asigna un valor *al azar* a $\vec{X}$, eligiendo los valores de cada variable $(0, 1)$ con probabilidad $1/2$.

3. Este paso se repite $3n$ veces:
   Si $\Omega(\vec{X})$ es verdadero, entonces tenemos una solución.
   De lo contrario, sea C una cláusula no satisfecha: se invierte (eligiendo uniformemente al azar) una de las variables en C.

4. Si al cabo de $3n$ repeticiones del paso anterior, no se llegó a una solución se vuelve al paso 2.

Si este algoritmo se visualiza en términos de la distancia de Hamming[8], puede formularse como una cadena de Markov, en la cual la distancia a la solución se va cambia en una unidad, al cambiar un bit en $\vec{X}$. Schöning da una prueba clara, de la cual omitiremos los detalles, de que su algoritmo tiene éxito con probabilidad

$$p \geq \left[\frac{1}{2}\left(1 + \frac{1}{k-1}\right)\right]^n,$$

[8]La distancia de Hamming entre dos números binarios de n bits, es el número $h \leq n$ de bits en que difieren. Por ejemplo, si $z_1 = 001$ y $z_2 = 101$, $|z_1 - z_2|_H = 1$, porque solo difieren en el primer bit.

de modo que repitiendo el protocolo $\mathcal{O}(1/p)$ veces se llega a una solución con certeza. Para el caso $k = 3$, la complejidad del algoritmo es por tanto

$$\left[\frac{1}{2}\left(1+\frac{1}{k-1}\right)\right]^{-n} = \left(\frac{4}{3}\right)^{n} \approx 1{,}333^{n}.$$

No existe, hasta donde sabemos, una versión cuantizada de éste algoritmo. Nos proponemos a estudiar este problema en el futuro cercano.

3.2.2. El aporte cuántico (**)

Es posible, sin entrar en demasiados detalles, ver como las técnica de amplificación de amplitud usada en el contexto del algoritmo de Grover puede servir para superar al algoritmo de Schöning. Estas ideas fueron recientemente formuladas (en forma muy genérica) por Ambainis [Amb05]. En esta sección mostramos que, al menos en principio, podría obtenerse un algoritmo de orden $(4/3)^{n/2} \approx 1{,}155^{n}$, que sería el más eficiente conocido para el problema 3-SAT. Esto es un peor caso, ya que no esta descartada la posibilidad (aunque parece bastante improbable) de que se encuentre un algoritmo que cambie la clase de complejidad del problema 3-SAT y, por extensión, de todos los problemas **NP-completos**.

Supongamos que tenemos una instancia de un problema k-SAT, en la forma $\Omega(x_1, x_2, \ldots x_n)$ y buscamos una asignación $\vec{X}^*$ que haga $\Omega(\vec{X}^*) =$ verdadero. La búsqueda "ingenua" requiere testar 2^n posibilidades. Con una computadora cuántica, podríamos usar el algoritmo de Grover (o uno de sus clones) para buscar el elemento $\vec{X}^*$ entre los $N = 2^n$ posibles. Esto require de $\mathcal{O}\left(\sqrt{N}\right) \approx \mathcal{O}(1{,}414^{n})$ pasos, lo cual ya es comparable al algoritmo de Schöning, el mejor conocido para este problema.

Consideremos un registro R de $N = 2^n$ más un qubit auxiliar (como en la discusión del algoritmo de Grover). Asociemos los 2^n vectores $\vec{X}$ con los números naturales $0, 1, \ldots 2^n - 1$, de los cuales los $\vec{X}$ son la descomposición binaria. Supongamos que contamos con un oráculo capaz de detectar el estado solución. Esto es, una función binaria de argumento entero $f(x)$, tal que

$$f(x) = \begin{cases} 0 & \text{si} \quad \Omega(x) = \text{ falso (no es una solución)} \\ 1 & \text{si} \quad \Omega(x) = \text{ verdadero (es una solución)} \end{cases} \tag{3.9}$$

El oráculo es una operación unitaria en el espacio de $n+1$ qubits que actúa

en la forma usual,

$$U_f \, \|x\rangle \otimes |0\rangle = \|x\rangle \otimes |f(x)\rangle.$$

De este modo es posible codificar la información sobre si un estado $|x\rangle$ es o no una solución, en el qubit auxiliar. Si es $|1\rangle$ tenemos una solución, si es $|0\rangle$, no. Es claro que la operación U_f depende de la instancia particular Ω del problema k-SAT, pero esto no presenta problema alguno. Se puede codificar cualquier instancia k-SAT en forma de oráculo, usando las compuertas lógicas usuales (por ejemplo CNOT y compuertas de un qubit).

Se considera ahora el siguiente protocolo,

1. *Preparación.*
   Se prepara el registro R en una superposición uniforme de los primeros n qubits, dejando el qubit auxiliar en $|0\rangle$.

$$|\Psi_0\rangle = H^{\otimes n} \, \|0\rangle \otimes |0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \|x\rangle \otimes |0\rangle \tag{3.10}$$

2. *Oráculo.*
   Se aplica el oráculo U_f a la superposición $|\Psi_0\rangle$ con el resultado,

$$|\Psi_1\rangle = U_f|\Psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \|x\rangle \otimes |f(x)\rangle.$$

   Ahora tenemos la información sobre el subespacio de soluciones codificada en el valor del último qubit. Suponiendo que hay r (con $N = 2^n > r > 1$) estados que son solución de Ω, podemos re-escribir $|\Psi_1\rangle$ en la forma más conveniente

$$|\Psi_1\rangle = \sqrt{1 - \frac{r}{N}} \, |\Phi_\perp\rangle \otimes |0\rangle + \sqrt{\frac{r}{N}} \, |\Phi\rangle \otimes |1\rangle$$

   donde

$$|\Phi\rangle = \frac{1}{\sqrt{r}} \sum_{x \in \{X^*\}} |x\rangle$$

   es la superposición de las r soluciones y

$$|\Phi_\perp\rangle = \frac{1}{\sqrt{N-r}} \sum_{x \neq x^*} |x\rangle,$$

   es la superposición del resto $(N - r)$ de los estados.

3. *Medida del qubit auxiliar.*
   Con probabilidad $p_s = r/2^n \ll 1$, esta medida resulta en $|1\rangle$ y deja al registro R en una superposición de las r soluciones. Si $r = 1$, tenemos la única solución, de lo contrario una segunda medida *del registro R* proporciona una de las soluciones $|x^*\rangle$ con certeza (perdemos $r - 1$ restantes).

Tenemos por lo tanto un protocolo que produce una solución de Ω con probabilidad $\epsilon = r/2^n \ll 1$. Cuantas veces es necesario repetirlo para tener una probabilidad razonable (digamos 2/3) de llegar a una solución? Clásicamente, la respuesta es $1/\epsilon \sim \mathcal{O}(2^n)$ veces, por lo que no ganamos nada. Podríamos hacer un muestreo uniforme del espacio buscando soluciones.

Cuánticamente, podemos usar el protocolo de amplificación de fase, que hemos detallado para el caso del algoritmo de Grover. Con un número de repeticiones $\mathcal{O}(1/\sqrt{\epsilon})$ logramos una probabilidad de 2/3 de alcanzar una solución [BHMT02]. De manera que la complejidad de éste protocolo es, para $r = 1$,

$$\mathcal{O}\left(\sqrt{2^n}\right) = 1{,}414^n.$$

Si se lograse cuantizar el algoritmo de Schöning, alcanzando *al menos* la misma complejidad $\mathcal{O}(1{,}333^n)$, lo cual no debería ofrecer grandes dificultades, la aplicación posterior de la amplificación de amplitud llevaría la complejidad del protocolo a

$$\mathcal{O}\left(\sqrt{1{,}333^n}\right) \approx 1{,}155^n.$$

Este algoritmo sería el más rápido existente para 3-SAT y, por extensión, para los problemas NP-completos. Es una perspectiva atractiva, aunque y no se disponga, por ahora, de un procesador cuántico de varios qubits para ejecutarlo.

Capítulo 4

Decoherencia

El procesamiento cuántico de la información depende de la habilidad de controlar la evolución coherente de conjuntos de varios qubits durante un tiempo lo bastante largo como para llevar a cabo la tarea propuesta. No existe tal cosa como un sistema aislado. Una vez que aceptamos esta afirmación, la decoherencia debe ser incluida en la descripción de un sistema cuántico.

Supongamos que el sistema de interés, digamos un simple qubit en un estado $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ (con $|\alpha|^2 + |\beta|^2 = 1$), interactua con su entorno. Las interacciones enredan su estado con el entorno y esto genera un decaimiento (en general, muy rápido) de la fase relativa de la superposición $|\Psi\rangle$. En una descripción de matriz densidad, la decoherencia se manifiesta en el decaimiento de los elementos no diagonales. Para el qubit $|\Psi\rangle$, el proceso de decoherencia

$$\rho = |\Psi\rangle\langle\Psi| = \begin{pmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{pmatrix} \longrightarrow \begin{pmatrix} |\alpha|^2 & 0 \\ 0 & |\beta|^2 \end{pmatrix},$$

lleva al estado puro $\rho = |\Psi\rangle\langle\Psi|$ hacia una mezcla estadística[1]. El mecanismo de decoherencia fue estudiado en detalle por Zeh, Zurek, Paz y otros en la década del 80 y es hoy bien comprendido [Zur03]. En particular, nos provee de una elegante explicación de el surgimiento del mundo clásico, en el cual no se observan las superposiciones cuánticas, a partir de una dinámica cuántica subyacente.

[1]Como es característico de una mezcla, $tr(\sigma^2) = |\alpha|^4 + |\beta|^4 < 1$, a menos que $\alpha\beta = 0$ en cuyo caso no hay superposición en el estado de partida.

Existen diversos procesos físicos que atentan contra una evolución coherente. Interacciones no deseadas entre los qubits, interacciones de éstos con su entorno, imperfecciones en la aplicación de las compuertas... son sólo algunos de ellos. La solución elemental de aislar el sistema no es tal, porque se requieren interacciones entre qubits para implementar una compuerta CNOT y se requiere una interacción con el entorno (medida) para preparar el estado inicial y para acceder a los resultados del procesamiento. Las técnicas de corrección cuántica de errores usando codificación redundante y el Teorema Umbral [NC00] dan esperanza a un panorama que de otro modo sería bastante sombrío.

Hay varios formalismos adecuados para tratar sistemas decoherentes. Si se adopta el punto de vista de que la evolución no unitaria resulta del enredo del sistema con el ambiente (en general considerado como una reserva térmica), entonces se puede trabajar sobre la matriz densidad reducida, tomando la traza sobre los grados de libertad de la reserva. La entropía de von Neumann de la matriz densidad reducida crece a medida que progresa la decoherencia y se pierde información sobre el sistema, que pasa a ser descrito por una mezcla estadística.

Una forma fenomenológica de tratar el problema de la decoherencia es a través de una ecuación maestra para el operador densidad. Por ejemplo, si H es el operador Hamiltoniano del sistema y A un observable que esta siendo medido (o, equivalentemente, es directamente afectado por la interacción con el ambiente) la dinámica de la matriz densidad puede ser descrita [Men00] a través de

$$\dot{\rho} = -i\,[H, \rho] - \frac{1}{2}\kappa\,[A, [A, \rho]]\,. \tag{4.1}$$

En esta ecuación, $[A, B] = AB - BA$, es el conmutador de dos operadores. Si $\kappa \to 0$ no hay interacción con el ambiente y resulta la evolución coherente $\dot{\rho} = -i\,[H, \rho]$, que es una forma de la ecuación de Schrödinger. Existen otras ecuaciones de evolución que representan diferentes tipos de interacción sistema-ambiente.

Otra forma de tratar a un sistema abierto es a través del formalismo de superoperadores[2], sumamente poderoso para determinar los efectos de la decoherencia en la dinámica. El lenguaje de superoperadores esta naturalmente relacionado con el de las medidas generalizadas (Apéndice A), los operadores de Kraus y las operaciones cuánticas. Este último formalismo

[2]Así llamados porque actúan sobre el operador densidad.

[NC00] es una alternativa para describir procesos de decoherencia asociados a determinados tipos de ruido (canales) específicos[3]. Tendremos oportunidad de presentar algunos ejemplos concretos[4] de estos enfoques en el curso del análisis del impacto de la decoherencia en el QW.

Como se mencionó en el Cap. 1, debido a la coherencia cuántica el QW en la línea se extiende más rápido que su análogo clásico. Esto se manifiesta en que la varianza σ^2 asociada a la distribución de posición crece cuadráticamente con el tiempo, en vez de linealmente como es el caso en una caminata al azar en una dimensión. En líneas muy generales el efecto del ruido en un QW es que esta ventaja se pierde. La distribución en posición, característica de un fenómeno de interferencia, se hace gradualmente Gaussiana y la varianza pasa a crecer linealmente con el tiempo[5]. Como veremos, este proceso tiene lugar en forma gradual y, si el nivel de ruido no es demasiado grande, a tiempos arbitrariamente largos persisten correlaciones cuánticas que se manifiestan en una tasa de difusión sustancialmente mayor que en el caso clásico.

4.1. Enfoque markoviano (*)

A través del enfoque general [RSAD03], consistente en separar la evolución coherente en una parte markoviana (que toma la forma de una ecuación maestra) y otra que representa los términos de interferencia debidos a las coherencias cuánticas, es posible obtener mucha información sobre el QW en régimen decoherente. Como se verá, este enfoque resulta comparativamente simple, en relación a otros tratamientos de decoherencia basados, por ejemplo, en operaciones cuánticas. Los resultados reseñados en esta sección fueron obtenidos por nuestro grupo en Montevideo hace algunos años [RSSS$^+$04].

4.1.1. Ecuación maestra (*)

El vector de estado del QW, ec. (1.7), se puede expresar como el spinor $|\Psi(t)\rangle \rightarrow [a_x(t), b_x(t)]^T$, donde T indica transposición. Un paso en la evo-

[3]En este modelo, se asume que el impacto del ruido es un proceso determinado en el sistema, por ejemplo la inversión estocástica de uno o varios qubits.

[4]Basados en trabajos recientes realizados por nuestro grupo en Montevideo y en los trabajos más relevantes entre los realizados por otros grupos.

[5]En general, nos referiremos al QW a tiempo discreto, es decir que t es el número de pasos.

lución coherente $|\Psi(t+1)\rangle = U|\Psi(t)\rangle$, donde U esta dado por (1.8), puede expresarse mediante el mapa

$$\begin{aligned} a_x(t+1) &= \frac{1}{\sqrt{2}}\left(a_{x-1} + b_{x-1}\right) \\ b_x(t+1) &= \frac{1}{\sqrt{2}}\left(a_{x+1} - b_{x+1}\right). \end{aligned} \tag{4.2}$$

En lugar de usar las amplitudes de probabilidad, la evolución puede expresarse en términos de la probabilidad de encontrar al caminante en un sitio x, dada por $P_x \equiv |a_x|^2 + |b_x|^2$. El mapa (4.2) implica la ecuación maestra

$$P_x(t+1) = \frac{1}{2}\left[P_{x-1}(t) + P_{x+1}(t)\right] + \beta_{x-1}(t) - \beta_{x+1}(t) \tag{4.3}$$

donde $\beta_x \equiv \Re(a_x b_x^*)$ son los términos de interferencia necesarios para mantener la coherencia de la evolución cuántica. Enfatizamos que las ecuaciones de evolución (1.8), (4.2) y (4.3) son completamente equivalentes entre si.

Si se desprecian las coherencias y se toma el límite contínuo[6] $\Delta t \to 0$ y $\Delta x \to 0$ se obtiene una ecuación de difusión

$$\frac{\partial P}{\partial t} = \frac{D}{2}\frac{\partial^2 P}{\partial x^2}. \tag{4.4}$$

Como se sabe, una distribución gaussiana de probabilidad $P(x,t)$ satisface esta ecuación. La distribución se mantiene gaussiana, con una varianza que crece linealmente con el tiempo, $\sigma^2 = Dt$ con coeficiente de difusión, que en este caso es $D = 1$. Las coherencias β_x no son despreciables, salvo bajo condiciones de ruido extremo. Sin embargo, como veremos, expresar la evolución del sistema en la forma (4.3) es de gran utilidad. Es posible definir un análogo cuántico del coeficiente de difusión clásico. Nos referiremos a esta cantidad como coeficiente de dispersion,

$$D_q \equiv \lim_{t\to\infty} \frac{\partial \sigma^2}{\partial t}.$$

Esta definición esta redactada para tiempo continuo. Se puede usar una versión para tiempo discreto

$$D_q = \lim_{t\gg 1} \frac{\sigma^2(t+\Delta t) - \sigma^2(t)}{\Delta t} \tag{4.5}$$

sin problema, en tanto se evalúe en régimen decoherente y la varianza crezca linealmente con t. Observe que en esta versión no se toma el límite

[6] Hay más de una forma de tomar este límite y según cual se use se obtiene la ecuación del Telegrafista o la ecuación de difusión. Vea [RSSS$^+$04] por más detalles.

$\Delta t \to 0$, pero esta implícito que la dispersion tiene lugar en una escala de tiempo frente a la cual Δt es pequeño. En el límite decoherencia completa, $D_q \to 1$, que el valor correspondiente a una caminata al azar clásica. Como veremos, en general $D_q > 1$ debido a la persistencia de correlaciones cuánticas, aún a tiempos largos.

La evolución de la varianza

$$\sigma^2 = M_2 - M_1^2 = \sum_x x^2 P(x) - \left[\sum_x x P(x)\right]^2 \tag{4.6}$$

se puede obtener a partir de la ec. (4.3). Recordamos que, en el contexto del QW en la línea, las sumas en posición tienen límites implícitos entre $\pm\infty$. Los primeros momentos M_1 y M_2 satisfacen

$$\begin{aligned} M_1(t+1) &= M_1(t) - 2\sum_x \beta_x(t) \\ M_2(t+1) &= [1 + M_2(t)] - 4\sum_x x\beta_x(t). \end{aligned} \tag{4.7}$$

Analizaremos las predicciones de éstas ecuaciones en los casos extremos de decoherencia máxima y de evolución coherente.

Límite difusivo

Cuando las coherencias en (4.7) pueden ser despreciadas, tomando el límite de tiempo continuo, se obtienen las ecuaciones diferenciales acopladas

$$\begin{aligned} \frac{d^2M_1}{dt^2} + 2\frac{dM_1}{dt} &= 0, \\ \frac{d^2M_2}{dt^2} + 2\frac{dM_2}{dt} &= 2. \end{aligned} \tag{4.8}$$

Las soluciones generales son de la forma

$$\begin{aligned} M_1(t) &= C_{11} + C_{12}e^{-2t} \\ M_2(t) &= C_{22} + t + C_{21}e^{-2t} \end{aligned} \tag{4.9}$$

con C_{11}, C_{12}, C_{21} y C_{22} constantes que dependen de la condición inicial. Para $t \gg 1$ los transitorios son despreciables y la varianza (4.6) crece linealmente con el tiempo,

$$\sigma^2 = M_2 - M_1^2 \sim t$$

con pendiente $D = 1$, lo cual es consistente con la ecuación de difusión (4.4) y con el hecho de que no han sido tenidas en cuenta las coherencias cuánticas.

Evolución coherente

En este caso, las sumas en las ecs. (4.7) no son despreciables y debe ser evaluadas. Usando análisis de Fourier, con las definiciones de la Sección 2.2.2, es posible obtener la dependencia temporal de las amplitudes de probabilidad, para condiciones iniciales dadas [NV]. Para una condición inicial localizada en el origen con $a_0(0) = 1$ y $b_0(0) = 0$, las amplitudes son

$$a_x(t) = \frac{1+(-1)^{x+t}}{2} \int_{-\pi}^{\pi} \frac{dk}{2\pi} \left[1 + \frac{\cos k}{\sqrt{1+\cos^2 k}} \right] e^{-i(w_k t + kx)},$$
$$b_x(t) = \frac{1+(-1)^{x+t}}{2} \int_{-\pi}^{\pi} \frac{dk}{2\pi} \left[\frac{e^{ik}}{\sqrt{1+\cos^2 k}} \right] e^{-i(w_k t + kx)}. \tag{4.10}$$

donde $\sin w_k = \frac{\sin k}{\sqrt{2}}$. Usando estas amplitudes es posible evaluar las sumas en (4.7) como

$$\sum_{x=-\infty}^{\infty} \beta_x(t) = A \tag{4.11}$$

$$\sum_{x=-\infty}^{\infty} x\, \beta_x(t) = -At + B. \tag{4.12}$$

donde las constantes (específicas para la condición inicial considerada) son $A = \left(2-\sqrt{2}\right)/4$ y $B = 1 - 5\sqrt{2}/8$. Con este resultado, la ec. (4.7) se reduce al mapa

$$M_1(t+1) = M_1(t) - 2A$$
$$M_2(t+1) = M_2(t) + 4At + (1-4B). \tag{4.13}$$

cuyas soluciones son

$$M_1(t) = -2At + C$$
$$M_2(t) = 2At^2 + (1-4B-2A)t + C', \tag{4.14}$$

con C y C' dos constantes arbitrarias. La varianza es por lo tanto

$$\sigma^2 = M_2 - M_1^2 \approx 2A(1-2A)\, t^2. \tag{4.15}$$

El coeficiente $2A(1-2A) = 1/\sqrt{2} - 1/2 \approx 0{,}207$ es consistente con el obtenido numéricamente para esta condición inicial.

Este resultado muestra que el efecto de las coherencias en la evolución, ec. (4.3), básica es crucial ya que son responsables del crecimiento cuadrático (y no lineal) de la varianza. El mismo resultado ha sido obtenido por otros autores usando diversos métodos: numéricamente [TM02], a partir de análisis de Fourier [NV] o sumas de caminos [Kon02b].

4.1.2. Medidas periódicas de la moneda (*)

En esta Sección describimos los resultados obtenidos en Montevideo a partir de un análisis de ecuación maestra para el caso de medidas periódicas del qubit de moneda [RSA+04].

Se considera un QW con condición inicial localizada en el origen, $\|0\rangle$, con moneda inicial

$$|\chi_{\pm}\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle. \tag{4.16}$$

Con una de estas monedas iniciales, la distribución de probabilidad es simétrica [Kon02b], $P(x,t) = P(-x,t)$, lo cual simplifica la descripción. La medida en el espacio de la moneda se realiza a través del operador de Pauli σ_y cuyos vectores propios son justamente $(1,i)^T$ y $(1,-i)^T$, de modo que la medida preserva la simetría $P(x,t) = P(-x,t)$.

Se realizan medidas de posición y moneda con una periodicidad de T pasos. El estado inicial evoluciona durante $t = T$ de acuerdo a la evolución usual del QW coherente. Cuando se realiza la primer medida, la probabilidad de obtener $|x\rangle$ es

$$q_x \equiv P_x(T)\,. \tag{4.17}$$

donde $P_x = |a_x|^2 + |b_x|^2$ es la distribución de posición del QW coherente a tiempo $t = T$. En general, q_x depende del estado inicial. Sin embargo, como medimos σ_y, luego de la medida el estado de moneda es uno de $|\chi_{\pm}\rangle$ y en $t = 2T$ se vuelve a repetir la misma distribución, centrada en otra posición. Lo mismo ocurre en $t = T, 2T, \ldots \tau T$, donde τ es el número de medidas realizadas. Este proceso se ilustra esquemáticamente en la Fig. 4.1.

La distribución de probabilidad P_x entre medidas satisface la ecuación maestra

$$P_x(t+T) = \sum_{x'=x-T}^{x+T} q_{x-x'} P_{x'}(t), \tag{4.18}$$

donde las probabilidades de transición del sitio x' al sitio x $q_{x-x'}$ se definen en la ec. (4.17). Usando (4.18) calculamos los primeros momentos de la distribución, con el resultado

$$M_1(t+T) = M_1(t) + M_{1q}(T) \tag{4.19}$$

$$M_2(t+T) = M_2(t) + 2M_1(t)M_{1q}(T) + M_{2q}(T) \tag{4.20}$$

donde $M_{1q}(T) = \sum_{x=-T}^{x=T} x q_x$ y $M_{2q}(T) = \sum_{x=-T}^{x=T} x^2 q_x$ son los momentos asociados a la evolución unitaria que tiene lugar entre dos medidas consecu-

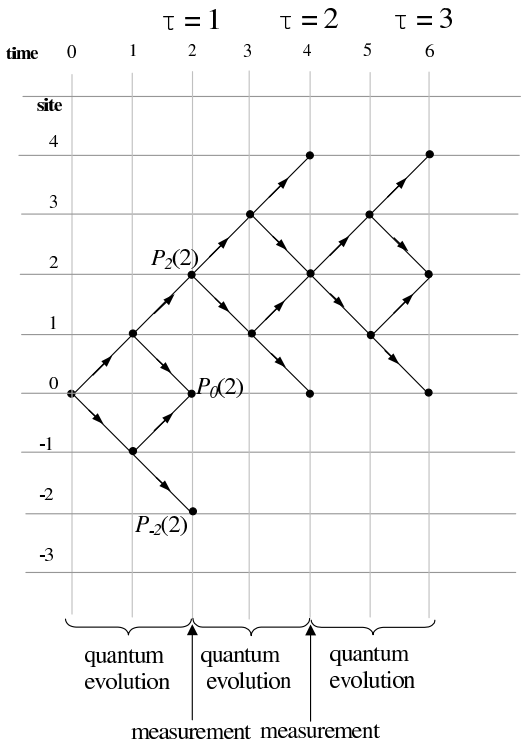

Figura 4.1: Diagrama mostrando la evolución temporal del QW con medidas periódicas (se muestra el caso $T = 2$) de posición y moneda. El estado inicial es localizado en $x = 0$ con una de las monedas descritas en el texto.

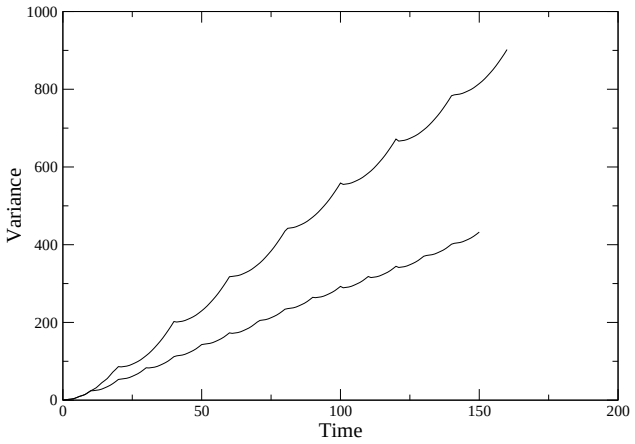

Figura 4.2: Evolución temporal de la varianza del QW con medidas periódicas. Se muestran dos períodos de medida $T = 10$ y $T = 20$. Los segmentos parabólicos corresponden a la evolución unitaria entre medidas.

tivas. La varianza es

$$\sigma^2(t+T) = \sigma^2(t) + \sigma_q^2(T), \tag{4.21}$$

donde $\sigma_q^2(T) = M_{2q}(T) - M_{1q}^2(T)$ es la varianza asociada a la evolución unitaria entre medidas consecutivas. Usando este resultado, el coeficiente de dispersion para medidas periódicas con período T es

$$D_{rm} = \frac{\sigma^2(t+T) - \sigma^2(t)}{T} = \frac{\sigma_q^2(T)}{T}. \tag{4.22}$$

La decoherencia requiere que varias medidas sean realizadas, de modo que este proceso debe verse en una escala temporal del orden de T. Como la varianza del QW coherente es de la forma $\sigma_q^2(T) \sim CT^2$, con C una constante que depende de las condiciones iniciales, resulta un coeficiente de dispersion

$$D_{rm} = CT = C/p \tag{4.23}$$

donde $p = 1/T$ es la frecuencia de eventos decoherentes. La Fig. (4.2) muestra la evolución temporal de la varianza calculada en una simulación con un ensemble de 10^4 trayectorias. La periodicidad no tiene aquí un rol fundamental. Hemos considerado también el caso de medidas frecuentes con intervalos de tiempo al azar entre las mismas y se llega conclusiones similares en cuando al crecimiento lineal del coeficiente de dispersion D con el número de eventos decoherentes [RSA$^+$04].

Los métodos basados en ecuaciones maestras son una herramienta simple para obtener información general sobre una evolución decoherente. No dan sin embargo acceso a los detalles, como por ejemplo que sucede en el régimen de ruido débil o como tiene lugar la transición entre el crecimiento cuadrático y el lineal para la varianza.

4.2. Operaciones cuánticas

El formalismo de operaciones cuánticas es un método poderoso para obtener información detallada del efecto de diversos tipos de ruido en la dinámica. Consideramos el operador densidad en la representación de valores propios de posición y moneda,

$$\rho = \sum_{x,x'} \rho_{x,x'} |x\rangle\langle x| x' \otimes \sum_{c,c'} \chi_{c,c'} |c\rangle\langle c| c' = \sum_{x,c,x',c'} \rho_{xc,x'c'} |x,c\rangle\langle x',c'| \quad (4.24)$$

donde $|x,c\rangle = |x\rangle \otimes |c\rangle$ son los autoestados de posición ($x \in \mathcal{Z}$) y de moneda ($c = 0, 1$), en la notación de [Ken06]. Este operador evoluciona bajo un mapa lineal

$$\tilde{\rho} = \mathcal{E}(\rho) = \sum_j A_j \, \rho \, A_j^\dagger \qquad \text{con} \qquad \sum_{j=1}^{d} A_j^\dagger A_j = I \quad (4.25)$$

donde los operadores de Kraus A_j representan una medida generalizada (vea la Sección A.5), que puede ser una operación unitaria o una medida proyectiva de algún tipo. La segunda condición asegura que el mapa $\mathcal{E}$ preserve la traza (la norma) del estado ρ. La evolución coherente se obtiene si se considera un único operador unitario $A_0 = U$, de modo que la operación cuántica se reduce a la evolución coherente

$$\rho(t) = U^t \rho(0) (U^\dagger)^t.$$

Cuando se introduce decoherencia en la evolución, a cada paso se aplica con cierta probabilidad p la operación decoherente de modo que

$$\rho(t+1) = (1-p)\, U \rho(t)\, U^\dagger + p \sum_{j=1}^{d} K_j \, U \rho(t) \, U^\dagger K_j^\dagger. \quad (4.26)$$

La expresión anterior implica elegir un conjunto de operadores de Kraus $A_0 = \sqrt{1-p}\, U$ con $U^\dagger U = I$ y $A_j = \sqrt{p}\, K_j$ con $\sum_{j=1}^{d} K_j^\dagger K_j = I$ de forma de separar explícitamente la evolución coherente de los eventos decoherentes.

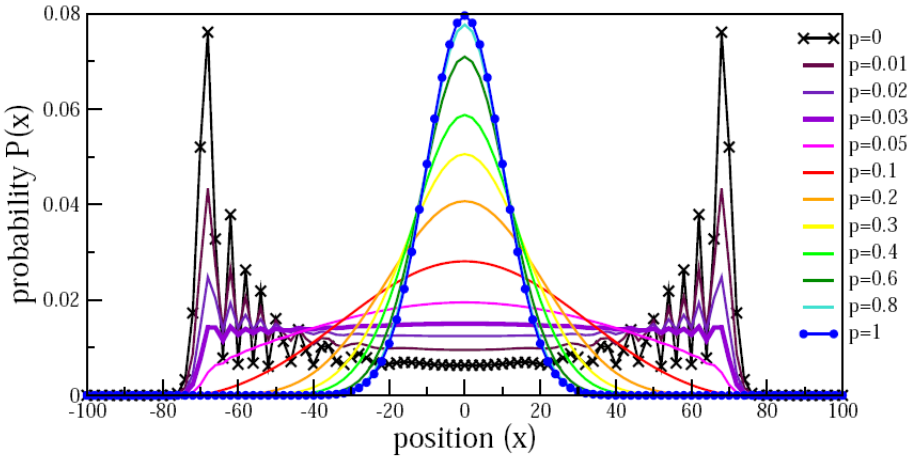

Figura 4.3: Distribuciones de probabilidad en posición, $P(x)$, luego de $t = 100$ pasos para varios niveles de decoherencia según [Ken06]. La decoherencia es debida a medidas completas realizadas (es decir de posición y moneda) realizadas con probabilidad p por unidad de tiempo.

Muchos estudios de decoherencia de QW usan este formalismo obtener información sobre la evolución a tiempos largos. El observable de interés es la varianza asociada a la distribución de posición

$$\sigma^2 \equiv \langle x^2 \rangle - \langle x \rangle^2 = tr(\rho X^2) - [tr(\rho X)]^2. \tag{4.27}$$

Como mencionamos en la Sección anterior, en el caso coherente la varianza crece como t^2. Cuando esta bien establecido el régimen decoherente, la varianza crece como t.

Gran parte del estudio de decoherencia en el QW se basa en versiones de la ec. (4.26) especializadas para distintos tipos de ruido. Se pueden analizar los efectos del ruido sobre el qubit de moneda, del ruido en la posición o de ruido generalizado que afecta ambos grados de libertad. El enfoque es analítico cuando esto es posible, pero en muchos casos se debe recurrir a la simulación numérica de (4.26) para obtener información.

Los primeros resultados basados en simulaciones numéricas [KT03] mostraron que el efecto del ruido en la dinámica es diferente para los distintos grados de libertad. La Fig. 4.3 muestra la distribución de posición luego de $t = 100$ pasos, para diferentes probabilidades de eventos decoherentes (en este caso, medidas de la posición y la moneda). La decoherencia en este caso es debida a medidas de posición y moneda, realizadas con probabilidad p

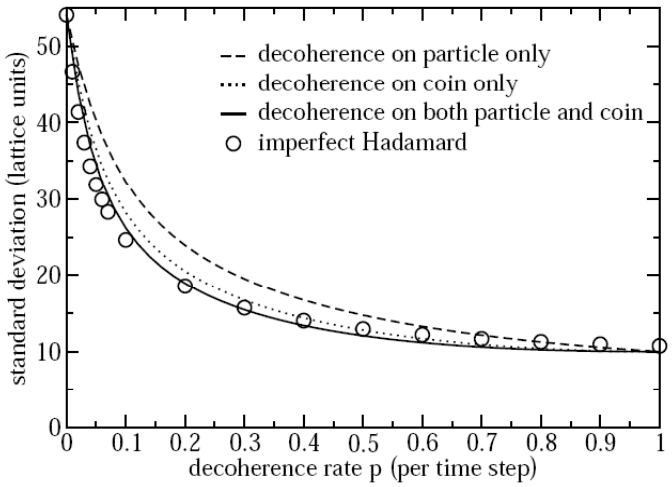

Figura 4.4: Incidencia de diferentes tipos de decoherencia en la evolución del QW de acuerdo a [KT03]. Se muestra la desviación estándar $\sigma(p)$ para $T = 100$ como función de la probabilidad de eventos decoherentes p.

por unidad de tiempo. Cuando el número medio de eventos decoherentes (medidas) es $pT \gg 1$, la distribución adopta claramente la forma gaussiana característica de la difusión clásica. Es particularmente interesante el hecho de que para $PT \approx 3$, la distribución es casi uniforme en toda la región ocupada $[-T/\sqrt{2}, T/\sqrt{2}]$. Como se destaca en [KT03] este puede ser un beneficio de un nivel controlado de decoherencia, ya que esta propiedad puede ser de interés para realizar muestreos uniformes de un subespacio. La distribución cuasi-uniforme no aparece a menos que haya ruido en la posición, lo cual muestra que el impacto de un mismo nivel de ruido puede ser diferente en ambos grados de libertad.

La incidencia de diferentes tipos de decoherencia en la evolución del QW se muestra en la Fig. 4.4, tomada de [KT03]. La figura muestra la desviación estándar $\sigma(p)$ luego de $T = 100$ pasos, para cuatro tipos de decoherencia: medidas de posición, medidas de moneda, medidas completas (posición y moneda) y falla en la aplicación de la operación de Hadamard; en todos los casos el evento decoherente tiene lugar con probabilidad p por unidad de tiempo. Se observa un decaimiento de $\sigma(p)$ con p creciente que es similar en todos los casos, aunque como ya mencionamos, el impacto en la distribución de probabilidad puede ser bien diferente.

En el caso de la decoherencia en la moneda, es posible avanzar con téc-

nicas analíticas, en tanto que en el caso en que el ruido afecta a la posición muchos avances se basan en simulaciones numéricas de la ec. (4.26), por lo que consideramos ambos casos por separado.

4.2.1. Decoherencia en la moneda (*)

Existen diversos trabajos relevantes sobre decoherencia en la moneda, además de los que ya hemos mencionado basados en un enfoque de ecuación maestra. En [LP03], se estudia la dinámica decoherente del QW con medidas de la moneda usando la función de Wigner, logrando visualizar la evolución en el espacio de fases (posición y cantidad de movimiento). En otro trabajo [SBBH03], se estudia el efecto de intercalar (con probabilidad p por unidad de tiempo), una operación unitaria estocástica en el espacio de moneda de la forma e^{iA}, donde A es un operador de un qubit con componentes estocásticas (en términos de las matrices de Pauli). Este tipo de ruido es el que puede tener lugar cuando la operación de moneda no es una operación de Hadamard perfecta, sino que presenta fluctuaciones en torno de la misma. Las conclusiones a las que se llega en este trabajo son similares la las obtenidas a partir de técnicas analíticas. Más adelante presentamos nuestro modelo de ruido topológico (Broken links model), que representa un ruido unitario, que afecta de cierta manera tanto a la posición como a la moneda.

Resultados analíticos

En un trabajo interesante [BCA03b], Brun et al. muestran como se puede usar el formalismo de superoperadores para obtener, analíticamente, el impacto en la dinámica de la decoherencia *de la moneda*. Daremos algunos detalles del método, ya que en la siguiente sección lo aplicamos para determinar el impacto del ruido debido a un canal de bit-flip sobre la dinámica del QW.

La idea principal consiste en representar los efectos de la decoherencia en la moneda a través de un conjunto de operadores de Kraus, como en (4.26), pero que actúan exclusivamente en el espacio de la moneda. Estos operadores satisfacen

$$\sum_i A_i^\dagger A_i = I \tag{4.28}$$

de modo de que preservan la norma. La matriz densidad reducida al espacio de moneda, vea la ec. (4.24), transforma como $\chi_{kk'} \to \sum_i A_i \chi_{kk'} A_i^\dagger$ bajo la

acción de éstos operadores. La matriz densidad de reducida $\chi_{kk'}$ transforma como

$$\chi_{kk'}(t+1) = \sum_n U_k A_n \chi_{kk'}(t) A_n^\dagger U_{k'}^\dagger,$$

donde U_k, dado por la ec. (2.16), representa un paso en la evolución coherente del QW. Dado que toda la acción decoherente tiene lugar en el espacio de moneda, la descripción de la posición en el espacio de Fourier, dada en la Sección 2.2.2, continúa siendo de utilidad. El operador densidad en la representación k, luego de t pasos, se expresa

$$\rho_t = \int_{-\pi}^{\pi} \frac{dk}{2\pi} \int_{-\pi}^{\pi} \frac{dk'}{2\pi} |k\rangle\langle k'| \otimes \chi_{kk'}(t) \tag{4.29}$$

donde

$$\chi_{kk'}(t) = \sum_{i_1, i_2 \ldots i_t} U_k A_{i_t} \ldots U_k A_{i_1} \chi_0 A_{i_1}^\dagger U_{k'}^\dagger \ldots A_{i_t}^\dagger U_{k'}^\dagger. \tag{4.30}$$

Esta ecuación describe una transformación lineal del operador densidad reducido. Esta transformación se puede representar en forma más compacta definiendo un *super-operador* $\mathcal{L}_{kk'}$,

$$\mathcal{L}_{kk'}\left[\chi_{kk'}\right] \equiv \sum_i U_k A_i \chi_{kk'} A_i^\dagger U_{k'}^\dagger \tag{4.31}$$

en términos del cual, la evolución del estado de moneda se expresa en forma compacta $\chi_{kk'}(t) = \mathcal{L}_{kk'}^t\left[\chi_0\right]$.

Los efectos de la decoherencia se manifiestan, principalmente, en la varianza σ^2 de la distribución en posición. Si bien no es posible llegar a una forma analítica para la distribución $P(x,t) = tr(\rho|x\rangle\langle x|) = tr_c\langle x|\rho|x\rangle$, para calcular la varianza se requieren los momentos de primer y segundo orden. Para los tiempos largos $t \gg 1$ de interés (régimen decoherente bien desarrollado) es posible obtener expresiones cerradas para la varianza y, especialmente, para el coeficiente de dispersion.

El momento de orden m de la distribución es[7]

$$\langle x^m \rangle \equiv \sum_x x^m P(x,t) = \sum_x x^m \int_{-\pi}^{\pi} \frac{dk}{2\pi} \int_{-\pi}^{\pi} \frac{dk'}{2\pi} e^{ix(k-k')} tr\left[\chi_{kk'}(t)\right] \tag{4.32}$$

Evaluando la suma sobre posición en términos de derivadas de la función $\delta^{(m)}$ de Dirac, se obtiene

$$\langle x^m \rangle = (-i)^m \int_{-\pi}^{\pi} \frac{dk}{2\pi} \int_{\pi}^{\pi} dk' \; \delta^{(m)}(k-k')\, tr\left[\chi_{kk'}(t)\right]. \tag{4.33}$$

[7]A partir de este punto, la operación traza es con respecto al espacio de moneda, aunque se omita el subíndice.

Al integral por partes, se resuelve la dependencia en la función delta y resultan las expresiones

$$\langle x \rangle = \int_{-\pi}^{\pi} \frac{dk}{2\pi} \sum_{j=1}^{t} tr \left\{ \sigma_z \mathcal{L}_k^j \left[\chi_0 \right] \right\} \tag{4.34}$$

$$\begin{aligned} \langle x^2 \rangle = & \int_{-\pi}^{\pi} \frac{dk}{2\pi} \sum_{j=1}^{t} \left[\sum_{j'=1}^{j} tr \left\{ \sigma_z \mathcal{L}_k^{j-j'} \left(\sigma_z \mathcal{L}_k^{j'} \left[\chi_0 \right] \right) \right\} \right. \\ & \left. + \sum_{j'=1}^{j-1} tr \left\{ \sigma_z \mathcal{L}_k^{j-j'} \left(\left(\mathcal{L}_k^{j'} \left[\chi_0 \right] \right) \sigma_z \right) \right\} \right] \end{aligned} \tag{4.35}$$

para los primeros dos momentos luego de t iteraciones. En esta expresión σ_z es una matriz de Pauli y se ha usado el hecho de que $\mathcal{L}_k$ preserva la traza.

Es posible evaluar estas expresiones para los casos de interés $m = 1, 2$ si se obtiene una expresión limpia para $\mathcal{L}_k^j \left[\chi \right]$. Siguiendo a [BCA03b], parametrizamos la matriz densidad reducida en términos de las matrices de Pauli y la identidad[8],

$$\chi \equiv \sum_{j=0}^{3} r_j \sigma_j = r_0 \, I + r_1 \, \sigma_x + r_2 \, \sigma_y + r_3 \, \sigma_z \tag{4.36}$$

donde I es la identidad 2x2 y las matrices de Pauli son

$$\sigma_1 = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Dado que las matrices de Pauli son de traza nula, $tr(\chi) = 2r_0 = 1$, tenemos $r_0 = 1/2$ y χ se representa por un vector de tres componentes complejas

$$\vec{R} \equiv (r_1, r_2, r_3)^T.$$

La operación lineal $\mathcal{L}_k$ preserva la norma y por tanto no afecta a la componente r_0, que no juega ningún rol. La acción del operador lineal $\mathcal{L}_k$ se representa a través de una matriz 3x3, M_k, que actúa sobre el vector $\vec{R}$,

$$\vec{R}' = M_k \vec{R}, \tag{4.37}$$

donde $\vec{R}'$ representa a las tres componentes no triviales de $\mathcal{L}_k[\chi]$. Para obtener una forma detallada de M_k usando ec. (4.31) es necesario especificar los operadores de Kraus A_i, es decir, definir la operación cuántica.

[8] Todo operador en el espacio de un qubit es parametrizable en esta forma.

Los momentos (4.34) y (4.35) se pueden expresar en términos de la acción de esta matriz M_k. El primer momento requiere la evaluación de $tr\left\{\sigma_z \mathcal{L}_k^j[\chi]\right\}$. En la representación de Pauli (4.34) se reduce a

$$\langle x\rangle = (0\ 0\ 2)\int_{-\pi}^{\pi}\frac{dk}{2\pi}\sum_{j=1}^{t} M_k^j\ (r_1\ r_2\ r_3)^T. \tag{4.38}$$

Si los valores propios λ_i de M_k satisfacen $|\lambda_i| < 1$, para $t \gg 1$ se puede evaluar, con error despreciable, la suma como una serie geométrica de operadores y se obtiene la expresión simple

$$\langle x\rangle = (0\ 0\ 2)\int_{-\pi}^{\pi}\frac{dk}{2\pi}\, G_k\ (r_1\ r_2\ r_3)^T. \tag{4.39}$$

donde

$$G_k \equiv (I - M_k)^{-1} M_k \tag{4.40}$$

y se asume que $I - M_k$ es invertible. Solo la tercer fila de G_k es relevante, debido al producto escalar por (0 0 2). Esta expresión es independiente del tiempo. En efecto en el QW a tiempos largos, con decoherencia ya bien establecida, el valor medio de la posición es constante $< x >= cosnt$ y el segundo momento crece con t.

El cálculo del segundo momento es similar, pero la cuenta es más larga y no la reproduciremos en aquí en detalle. Después de ciertas manipulaciones que no suponen hipótesis adicionales a las incluidas en el cálculo del primer momento, se obtiene

$$\langle x^2\rangle = t + (0\ 0\ 2)\int_{-\pi}^{\pi}\frac{dk}{2\pi}\left[t\, I - (I - M_k)^{-1}\right] G_k\, (0\ 0\ 1)^T. \tag{4.41}$$

Esta expresión, válida a tiempos largos, no depende de las condiciones iniciales, como es el caso para el segundo momento. Debido al doble producto escalar, basta con el elemento $G_k(3,3)$ para calcularla. El coeficiente de dispersion, se puede obtener como la pendiente de (4.41),

$$D_q = 1 + 2\bar{G}_{3,3}. \tag{4.42}$$

La barra superior indica el promedio en el espacio k, i.e. $\bar{G} \equiv \int_{-\pi}^{\pi}\frac{dk}{2\pi}G_k$. El término $\bar{G}_{3,3}$ es el responsable de que la dispersion cuántica sea más rápida que en el caso clásico, donde $D = 1$.

Para tipos particulares de ruido en la moneda, se pueden evaluar las expresiones (4.34) y (4.35) y obtenerse la dependencia de D_q con el nivel del

ruido, por ejemplo. Otra aplicación, consiste en mantener algún parámetro en la evolución y luego evaluar para que valores del parámetro el sistema es más robusto frente a determinado tipo de ruido. A continuación presentamos ejemplos de ambos casos.

Medidas de la moneda

En la Ref. [BCA03b] se usa este método para el caso de ruido debido a medidas en la moneda, en el caso de un QW con operación de moneda de Hadamard. Los operadores de Kraus son

$$A_0 = \sqrt{p}|0\rangle\langle 0|, \quad A_1 = \sqrt{p}|1\rangle\langle 1|, \quad A_2 = \sqrt{1-p}I. \tag{4.43}$$

Esta operación cuántica puede verse, en cierto modo, como si se realizase una medida proyectiva de la moneda con probabilidad p.

Para esta operación cuántica la matriz M_k es

$$M_k = \begin{pmatrix} 0 & -(1-p)\sin 2k & \cos 2k \\ 0 & -(1-p)\cos 2k & -\sin 2k \\ (1-p) & 0 & 0 \end{pmatrix}. \tag{4.44}$$

A partir de esta matriz es posible evaluar los momentos explícitamente, a partir de (4.34) y (4.35). Omitimos los detalles, pero damos el resultado

$$\langle x\rangle = \frac{1-p}{p(2-p)}\left[(1-p)(|\alpha|^2 - |\beta|^2) + 2\Re(\alpha^*\beta)\right] \tag{4.45}$$

para el primer momento, asumiendo una condición inicial localizada en posición con un qubit de moneda genérico $|\chi\rangle = \alpha|0\rangle + \beta|1\rangle$, con α, β complejos satisfaciendo la regla de normalización. El segundo momento, que no depende de la condición inicial, es

$$\langle x^2\rangle = \left(1 + \frac{2(1-p)^2}{p(2-p)}\right) t - \frac{7(1-p)^2}{p^2(2-p)^2} \tag{4.46}$$

Esta última expresión implica el coeficiente de dispersion,

$$D_q = 1 + \frac{2(1-p)^2}{p(2-p)}. \tag{4.47}$$

En el caso coherente ($p = 0$), D_q es singular reflejando el hecho de que la varianza crece cuadráticamente con t. En el otro extremo, $p \to 1$ resulta $D_q \to 1$, como en el caso clásico. Para el caso de ruido débil, $p \ll 1$, $D_q \sim 1 + 1/p \gg 1$ y la dispersion cuántica es mucho más rápida que la difusión clásica, aún a tiempos arbitrariamente largos. Ya habíamos encontrado esta conclusión a partir del enfoque más simple de ecuación maestra.

Canal de bit-flip (**)

En colaboración con F. Severo hemos aplicado el formalismo de superoperadores para el caso del canal de bit-flip para una operación de moneda generalizada de la forma,

$$U_c = \begin{pmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & -\cos\frac{\theta}{2} \end{pmatrix} \tag{4.48}$$

donde $\theta \in [-\pi, \pi]$ is un parámetro real. Para $\theta = \pi/2$, se recupera la operación de Hadamard usual. Esta operación generalizada ya fue utilizada en el contexto de la ecuación maestra [RSSS$^+$04] y la idea es determinar para que valores de θ la dinámica es más robusta frente al ruido. Otra pregunta a responder es si para ruidos diferentes pero de similar intensidad, los resultados finales, por ejemplo en el coeficiente de dispersion varían sustancialmente. Nuestros resultados han sido presentados en un poster en la reunión WECIQ'06 en Brasil, pero son aún de carácter preliminar y aún no han sido enviados a publicar.

El tipo de ruido utilizado corresponde al canal de bit-flip. Este canal fue el primero en tener un protocolo cuántico de corrección de errores [NC00] basado en codificación redundante de $1 \to 3$ qubits. El canal de bit-flip asume que el único efecto del ruido externo es la inversión de un qubit con cierta probabilidad p por unidad de tiempo. Esto se puede describir usando los operadores de Kraus

$$A_0 \equiv \sqrt{p}\,\sigma_x, \quad A_1 \equiv \sqrt{1-p}\,I. \tag{4.49}$$

Estos operadores satisfacen la condición de preservación de la norma.

Con esta definición, la ec. (4.31) se reduce a

$$\chi' = p\,U_k\sigma_x\,\chi\,\sigma_x U_k^\dagger + (1-p)\,U_k\,\chi\,U_k^\dagger \tag{4.50}$$

donde U_k esta dada por la ec. (2.16). En la representación introducida en la sección anterior $\chi = \sum_{j=0}^{3} r_j\sigma_j$, obtenemos

$$M_k(\theta) = \begin{pmatrix} -\cos\theta\cos 2k & q\sin 2k & q\sin\theta\cos 2k \\ -\cos\theta\sin 2k & -q\cos 2k & q\sin\theta\sin 2k \\ \sin\theta & 0 & q\cos\theta \end{pmatrix}. \tag{4.51}$$

con $q \equiv 1 - 2p$. El operador $I - M_k$ es invertible si

$$\Delta \equiv \det(I - M_k) = (1 - q^2)(1 + \cos\theta \cos 2k) \neq 0. \tag{4.52}$$

Nuestro principal interés es obtener la dependencias del coeficiente de dispersion con la probabilidad p. Usando por ejemplo la operación de moneda de Hadamard, $\theta = \pi/4$. La varianza depende únicamente del valor medio en k del elemento G_{33} del operador G_k. En este caso, este elemento es

$$\bar{G}_{3,3} = \frac{q}{1 - q^2} \int_{-\pi}^{\pi} \frac{dk}{2\pi} \frac{(1 + q\cos\theta)\cos 2k + q + \cos\theta}{1 + \cos\theta \cos 2k}. \tag{4.53}$$

El cálculo de ésta expresión se reduce a evaluar dos integrales elementales ($\theta \neq 0, \pm\pi$),

$$\begin{aligned} \int_{-\pi}^{\pi} \frac{dk}{2\pi} \frac{1}{1 + \cos\theta\cos 2k} &= \frac{1}{|\sin\theta|} \\ \int_{-\pi}^{\pi} \frac{dk}{2\pi} \frac{\cos 2k}{1 + \cos\theta\cos 2k} &= \frac{1}{\cos\theta}\left[1 - \frac{1}{|\sin\theta|}\right] \quad \text{ó } 0, \text{ si } \theta = \pi/2. \end{aligned}$$

Los casos singulares $\theta = 0$ y $\theta = \pm\pi$ deben ser discutidos por separado. En cualquier caso, para la moneda de Hadamard, no son casos de interés. A partir de la ec. (4.42) obtenemos la expresión genérica para el coeficiente de dispersion

$$D_q = 1 + \frac{2q}{1 - q^2}\left[\frac{q + \cos\theta}{|\sin\theta|} + \frac{1 + q\cos\theta}{\cos\theta}\left(1 - \frac{1}{|\sin\theta|}\right)\right] \tag{4.54}$$

donde $q = 1 - 2p$, por brevedad. Particularizando para la operación de moneda de Hadamard, $\theta = \pi/2$, el segundo integral es nulo y se obtiene una expresión sencilla,

$$D_q = 1 + \frac{2q^2}{1 - q^2} = 1 + \frac{2(1-p)^2}{p(2-p)} \qquad \text{para } \theta = \pm\pi/2, \tag{4.55}$$

que para ruido débil ($p \ll 1$) es de la forma $1/p$. Notablemente, este resultado coincide con la ec. (4.47), obtenida por Brun et al. para el caso de medidas proyectivas de la moneda. Esto refuerza la hipótesis de que no importa el tipo de medida generalizada que se haga sobre la moneda, sino la frecuencia con se realiza.

Hemos chequeado esta expresión realizando una simulación numérica *independiente* de la caminata en la línea, en la cual el estado de la moneda es invertido con probabilidad p por unidad de tiempo. Para tiempos largos

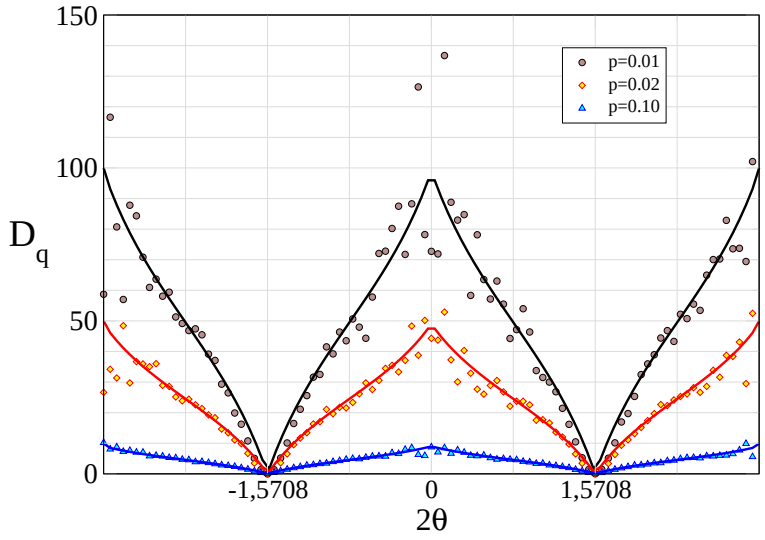

Figura 4.5: Los puntos corresponden a estimativos numéricos del coeficiente de dispersion para un QW con ruido de bit-flip para los tres niveles de ruido ($p = 0{,}01, 0{,}02$, and $0{,}10$ indicados en la clave. Los resultados corresponden a un ensemble de 500 partículas y la dinámica se siguió por 1000 pasos. Las líneas llenas corresponden a la ec. (4.54). [AS06]

comparados con $1/p$ se obtiene la pendiente de la curva $\sigma^2(t)$ por regresión lineal. El resultado es el coeficiente de dispersion como función de p, mostrado en la Fig. 4.5. En esta figura se muestra también la expresión analítica, ec. (4.54), para este coeficiente y el ajuste es notable.

Estos resultados muestran que el efecto del ruido de moneda sobre la distribución en posición es bien diferente que para el caso ruido en posición. Esta observación ya había sido realizada por [KT03] a partir de observaciones numéricas de ruido debido a medidas de la moneda. En [SBBH03], se obtienen distribuciones de probabilidad para el caso de ruido unitario sobre la moneda. El perfil obtenido tiene la misma forma que el de nuestra Fig. 4.5. De modo que cuatro tipos de ruido diferentes sobre la moneda producen distribuciones de probabilidad similares, que son a su vez bien diferentes de las que resultan cuando el ruido afecta directamente a la posición.

4.2.2. Decoherencia en posición

En el caso de decoherencia introducida a través de la posición, el método de superoperadores que hemos expuesto en las secciones anteriores no es fácil

de aplicar y nadie lo ha hecho hasta la fecha. El principal obstáculo es que en este caso el superoperador actúa en un espacio de posiciones y la descripción simple de la dinámica aportada por la transformada de Fourier no puede ser aprovechada.

Kendon y Tregenna han realizado algunos avances usando un método alternativo, basado en la suma de trayectorias [KT03] y calculan analíticamente la varianza $\sigma^2(p,t)$ en el límite $pt \ll 1$ con $t \gg 1$, es decir: ruido débil y también en el caso $p \approx 1$ de decoherencia extrema. En este caso, la decoherencia es debida a medidas proyectivas de posición y moneda,$|c,x\rangle$, realizadas con probabilidad p. La Fig. 4.3 muestra resultados numéricos para este caso.

El método de Kendon y Tregenna es esencialmente una formalización de la suma de caminos mostrada en el ejemplo de la Fig. 4.1. Los detalles son engorrosos y no será reproducido aquí. Llegan al resultado

$$\sigma^2(t,p) \simeq \sigma_q^2(t)\left[1-\frac{\sqrt{2}}{6}pt+p(\sqrt{2}-1)+\mathcal{O}\left(p^2,1/t\right)\right], \tag{4.56}$$

válido en el límite de tiempos largos y ruido débil, $t \gg 1$ con $pt \ll 1$. Los autores validan este resultado a través de simulaciones numéricas usando el valor de la varianza para el caso coherente $\sigma_q^2(t) = (1-1/\sqrt{2})(t-1/t)^2$, obtenido para cierta condición inicial usando el método de Fourier.

Para el caso de ruido fuerte, $p \approx 1$ y $t \gg 1$ obtienen,

$$\sigma^2 \simeq \left[1+(1-p)^4\right]t \tag{4.57}$$

de modo que el coeficiente de dispersion es

$$D_q = 1+(1-p)^4. \tag{4.58}$$

Evidentemente, para $p=1$ se tiene el límite clásico difusivo y para $p<1$, resulta $D_q > 1$, confirmando la persistencia de correlaciones cuánticas. Esta expresión es de limitada utilidad ya que sólo es válida para $p \approx 1$.

4.3. Ruido topológico (Broken links) (*)

En esta Sección describimos un modelo de ruido topológico que hemos desarrollado en los últimos años en Montevideo [RSA+04]. Nuestro modelo ha sido extendido a dos dimensiones en el marco de una tesis doctoral

que esta finalizándose ahora en el Laboratorio Nacional de Computación Científica (LNCC), Petrópolis, Brasil.

Este modelo puede ser presentado como una operación cuántica, pero al tratarse de un ruido en posición y moneda, no se cuenta con las ventajas de las secciones anteriores (para el ruido en el subespacio de moneda) y el problema aún no ha sido resuelto analíticamente. Dado que en última instancia se debe recurrir a la simulación numérica, optamos por presentarlo en términos de mapas condicionales, que es la forma en que fue originalmente formulado. Comenzamos recordando[9] el mapa que da lugar a la evolución coherente del QW en términos de las componentes del spinor $a_x = \langle x, 0|\Psi\rangle$ y $b_x = \langle x, 1|\Psi\rangle$,

$$\begin{aligned} a_x(t+1) &= \frac{1}{\sqrt{2}}\left[a_{x+1}(t) + b_{x+1}(t)\right] \\ b_x(t+1) &= \frac{1}{\sqrt{2}}\left[a_{x-1}(t) - b_{x-1}(t)\right]. \end{aligned} \tag{4.59}$$

En términos de éstas componentes se obtiene, como es usual, la distribución de probabilidad en posición es

$$P(x,t) = |a_x(t)|^2 + |b_x(t)|^2. \tag{4.60}$$

La caminata en la línea se puede ver como un proceso en el cual, a cada paso, se transfiere el flujo de probabilidad de un sitio x a sus vecinos $x \pm 1$, como mostramos en la Fig. 4.6 (a). Consideramos ahora las modificaciones necesarias en el mapa (4.59) cuando uno o ambos de los eslabones que vinculan el sitio x con sus vecinos se han roto de modo que no es posible que ese flujo de probabilidad tenga lugar.

4.3.1. Eslabones rotos en 1D (*)

Si el sitio x no tiene eslabones rotos, como en la Fig. 4.6 (a), se aplica el mapa (4.59) que implica una operación de Hadamard en la moneda seguida de una traslación condicional en posición. Este mapa se genera a partir del operador de evolución (1.8).

[9]Este mapa difiere del usado en la Sección 4.1.1 debido a que en [RSA+04] adoptamos una convención diferente para las componentes del spinor. Aquí la componente a_x esta asociada a traslación a la izquierda y b_x con la traslación hacia la derecha (roles intercambiados con respecto al mapa (4.2). Esto no es un problema, ya que ambas versiones generan la misma dinámica.

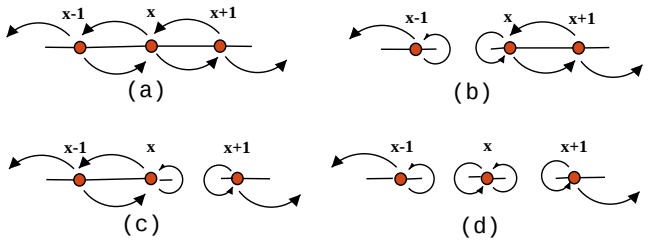

Figura 4.6: Diferentes situaciones que se pueden presentar en un sitio x de la línea: (a) no hay eslabones rotos, (b) esta roto el eslabón de la izquierda, (c) esta roto el eslabón de la derecha, (d) ambos eslabones están rotos. Las flechas indican la dirección del flujo de probabilidad asociado a cada componente superior del spinor.

Cuando un eslabón está roto, esto inhibe el pasaje del flujo de probabilidad. Sin embargo, el flujo de probabilidad es una cantidad conservada, de modo que en estos casos es necesario reorientar el flujo saliente hacia la otra componente del spinor. Si esta roto el link de la izquierda, como en (b) de la Fig. 4.6, la componente superior recibe flujo normalmente de la derecha $(x+1)$ pero no puede entregar flujo hacia la izquierda $(x-1)$. La componente inferior tiene un problema opuesto, ya que entrega pero no recibe. Si suponemos que el flujo saliente de la componente superior es entregado a la componente inferior se restablece el balance de probabilidad en presencia de links rotos. Esto se hace a través del mapa modificado

$$\begin{aligned} a_n(t+1) &= \frac{1}{\sqrt{2}}\left[a_{n+1}(t)+b_{n+1}(t)\right] \\ b_n(t+1) &= \frac{1}{\sqrt{2}}\left[a_n(t)+b_n(t)\right]. \end{aligned} \tag{4.61}$$

Similarmente, si el link roto esta a la derecha de x (Fig. 4.6 (c)), aplicamos el mapa

$$\begin{aligned} a_n(t+1) &= \frac{1}{\sqrt{2}}\left[a_n(t)-b_n(t)\right] \\ b_n(t+1) &= \frac{1}{\sqrt{2}}\left[a_{n-1}(t)-b_{n-1}(t)\right]. \end{aligned} \tag{4.62}$$

Finalmente, si ambos eslabones están rotos y el sitio x se encuentra aislado, como en la Fig. 4.6 (d), la operación de Hadamard es seguida por una inversión y el mapa resultante es

$$\begin{aligned} a_n(t+1) &= \frac{1}{\sqrt{2}}\left[a_n(t) - b_n(t)\right] \\ b_n(t+1) &= \frac{1}{\sqrt{2}}\left[a_n(t) + b_n(t)\right]. \end{aligned} \tag{4.63}$$

La evolución procede de la siguiente forma. A cada paso, la línea tiene todos los eslabones cerrados. Se recorre la línea, rompiendo al azar eslabones con probabilidad p, de modo que una fracción p de ellos esta rota en un momento determinado. Luego, para cada sitio x se aplica una instancia del mapa de evolución, condicionalmente a cual sea su caso (a), (b), (c) o (d). Esta evolución preserva la norma de la función de onda. De hecho, se puede expresar como la serie de operaciones unitarias,

$$|\Psi(t)\rangle = U_t U_{t-1} \ldots U_1 |\Psi(0)\rangle \tag{4.64}$$

donde la forma de cada operador unitario U_k depende de la topología de la línea en ese momento $t = k$. Esto es otro ejemplo de ruido unitario, que afecta a la vez a la posición y a la moneda.

Consideramos la condición inicial $|\Psi(0)\rangle = \frac{1}{\sqrt{2}}(1,i)^T \otimes \|0\rangle$, que lleva a una evolución simétrica en el caso coherente. Centramos nuestra atención en la distribución de probabilidad en posición, ec. (4.3), y en la evolución temporal de la varianza asociada a esta distribución. Consideramos valores de $p < 0{,}50$, ya que para $p \gtrsim 0{,}50$ más la mitad de los eslabones están rotos en media y la propagación en posición se ve impedida.

En presencia de ruido, la distribución de posición tiende gradualmente a una gaussiana como se muestra en la Fig. 4.7. Esto es consistente con observaciones reportadas para otros tipos de ruido, vea la Fig. 4.3. En el caso del ruido topológico que estamos considerando, la transición de un régimen donde domina la coherencia y $\sigma^2 \sim t^2$ a un régimen decoherente donde $\sigma^2 \sim t$ tiene lugar en un tiempo característico

$$t_c = \frac{1}{p\sqrt{2}}. \tag{4.65}$$

Esta observación, que se desprende de un análisis detallado de los resultados mostrados en la Fig. 4.9, es consistente con lo reportado en [SBBH03] para

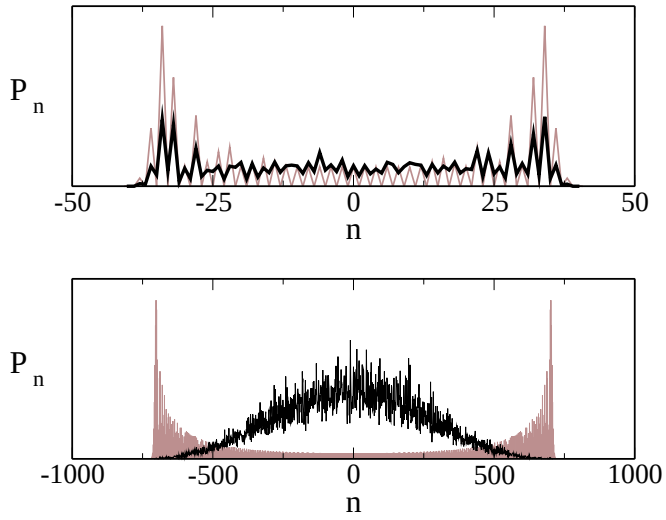

Figura 4.7: Distribución $P(x)$ para $p = 0{,}01$ en dos momentos diferentes, $t = 50$ (panel superior) y $t = 1000$ (panel inferior). Las distribuciones correspondientes al caso coherente ($p = 0$) se muestran en el fondo.

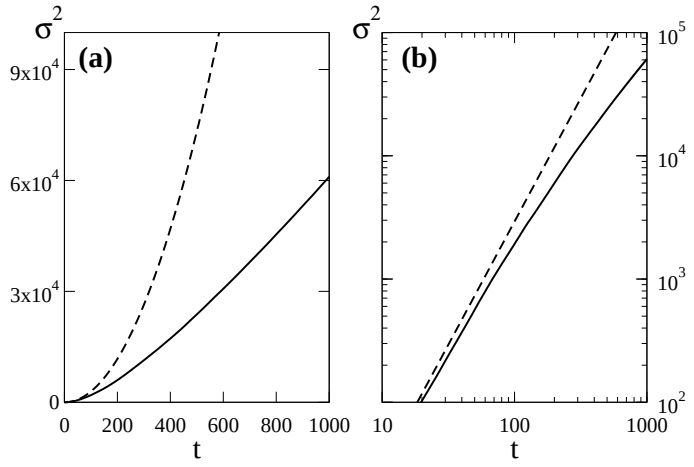

Figura 4.8: (a) Evolución de la varianza, σ^2, para $p = 0{,}01$; en (b) la misma evolución en un a escala logarítmica muestra que la transición entre el crecimiento cuadrático y el lineal es gradual. Las líneas punteadas corresponden al caso coherente, $p = 0$.

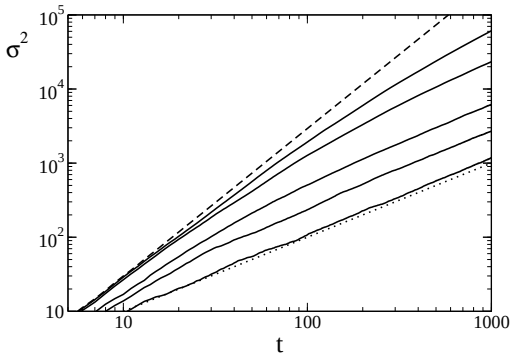

Figura 4.9: Evolución de la varianza con eslabones rotos en una escala log-log. La línea a trazos corresponde al caso coherente $p = 0$ (crecimiento cuadrático con el tiempo). Las líneas llenas corresponden a varios valores de p: 0.01, 0.03, 0.10, 0.20 and 0.40. La línea punteada corresponde a una caminata al azar clásica.

la misma transición en el caso de ruido unitario que actúa exclusivamente sobre la moneda.

En el caso del ruido topológico, existe un argumento sencillo para entender este tiempo característico. En promedio, hay p eventos decoherentes por unidad de tiempo, por unidad de posición. Al principio no hay eventos decoherentes bajo la función de onda, porque la misma esta localizada en posición. Los eventos que tienen lugar fuera de la distribución claramente no afectan la dinámica. La distribución del QW se extiende en ambas direcciones con velocidad constante $1/\sqrt{2}$, de modo que luego de t pasos, el número medio de eventos decoherentes *debajo de la distribución* es $p\sqrt{2}t$. Esta cantidad crece desde cero (evolución coherente) hasta que se hace de orden 1 y afecta apreciablemente a la distribución de probabilidad (vea las Figs.4.7 y 4.8) en el tiempo característico (4.65). La Fig. 4.8 muestra la evolución de la varianza para $p = 0{,}01$, donde el tiempo de coherencia es $t_c \sim 70$. En escala logarítmica se aprecia claramente que la transición entre el crecimiento cuadrático (pendiente 2) y lineal (pendiente 1) es gradual.

A partir de los datos para la evolución de la varianza, mostrados en la Fig. 4.9, se puede se puede calcular (usando datos para tiempos $t \gg t_c$) el coeficiente de dispersion, ec. (4.5), para varios niveles de ruido. La Fig. 4.10

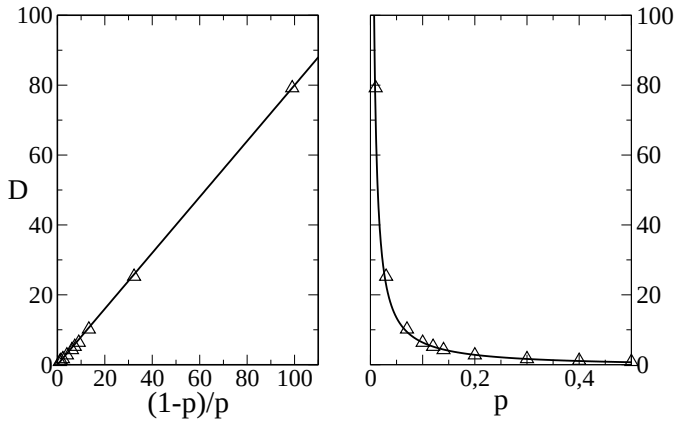

Figura 4.10: Coeficiente de dispersión, ec. (4.5), como función de $(1-p)/p$ (Izq.) y de p (Der). Los triángulos negros se obtienen a partir de los datos de la Fig. 4.9. La línea corresponde al ajuste por regresión lineal, ec. (4.66) con $K = 0{,}40$.

muestra estos resultados, que implican una dependencia lineal con $(1-p)/p$,

$$D_q = K\frac{1-p}{p}. \tag{4.66}$$

Una regresión lineal produce el valor $K \approx 0{,}40$.

La dependencia con $1-p$ se debe al modelo de eslabones rotos y esta presente en el modelo clásico correspondiente. Pero la dependencia dominante en $1/p$, que hemos obtenido también a partir de resultados analíticos de ruido sobre la moneda, es de naturaleza cuántica y muestra que - aún a tiempos arbitrariamente largos - persisten algunas correlaciones cuánticas. Como consecuencia, la dispersion cuántica tiene lugar a una tasa $1/p$ más alta que la difusión clásica. Para niveles de ruido moderados esto puede ser decenas o centenas de veces más rápido.

En la siguiente sección damos evidencia en favor de la persistencia de las correlaciones cuánticas mostrando que si las mismas son despreciadas, los resultados no se ajustan a las observaciones que acabamos de describir.

Correlaciones persistentes (*)

La evolución bajo el modelo de eslabones rotos se ha descrito a través de los mapas (4.59) y (4.61–4.63). Los mismos pueden expresarse en términos

de probabilidades (en vez de amplitud de probabilidad) siguiendo el mismo procedimiento que llevó a la ec. (4.3) en el caso coherente. Como resultado, se obtienen cuatro ecuaciones de evolución que deben aplicarse alternadamente con cierta probabilidad cada una.

$$\begin{aligned} P_x(t+1) &= \frac{1}{2}\left[P_{x+1}(t) + P_{x-1}(t)\right] + \beta_{x+1}(t) - \beta_{x-1}(t) \\ P_x(t+1) &= \frac{1}{2}\left[P_{x-1}(t) + P_x(t)\right] - \left[\beta_{x-1}(t) + \beta_x(t)\right] \\ P_x(t+1) &= \frac{1}{2}\left[P_x(t) + P_{x+1}(t)\right] + \beta_x(t) + \beta_{x+1}(t) \\ P_x(t+1) &= P_x(t). \end{aligned} \tag{4.67}$$

En estas ecuaciones $\beta_x \equiv \Re\left[a_x^* b_x\right]$ y $\Re(z)$ es la parte real de z. Como ya mencionamos, estos términos complementan la descripción de la ecuación maestra para hacerla compatible con la Mecánica Cuántica [RSAD03, RSSS$^+$04].

En el modelo de eslabones rotos, las cuatro situaciones mostradas en la Fig. 4.6 se presentan con probabilidades bien definidas. La probabilidad de que un sitio dado no tenga eslabones rotos es $\Pi_0 = (1-p)^2$. La probabilidad de que tenga uno de los eslabones rotos es $\Pi_1 = p(1-p)$ y la probabilidad de que este aislado, $\Pi_2 = p^2$. Estas probabilidades suman 1. Es posible combinar las cuatro evoluciones en una sola, aplicando estas reglas con las probabilidades respectivas. Si despreciamos el efecto de las correlaciones cuánticas, después de alguna manipulación resulta la ecuación maestra

$$P_x(t+1) = pP_x(t) + \frac{1}{2}(1-p)\left[P_{x+1}(t) + P_{x-1}(t)\right]. \tag{4.68}$$

Esta ecuación describe la evolución de un caminante al azar clásico, en una topología de eslabones rotos y se puede obtener en forma independiente a partir de ese modelo. El proceso es difusivo con coeficiente de difusión, $D_{cl} = 1 - p$. El efecto de los eslabones rotos es obstaculizar la difusión, de modo que si no hay eslabones rotos ($p = 0$), se reduce al caso usual $D = 1$.

El resultado que hemos encontrado en la sección anterior, $D_q \propto (1-p)/p$, implica que los términos que hemos despreciado tienen un impacto importante en la dinámica, aún a tiempos arbitrariamente largos. En otras palabras, salvo para niveles de ruido extremos, el proceso cuántico nunca llega a ser completamente estocástico y eso se manifiesta en un coeficiente de dispersion mayor que el clásico.

Como hemos visto, la misma dependencia $1/p$ de la dispersion cuántica aparece en diferentes modelos de ruido [BCA03a, SBBH03, KT03], de modo que la persistencia de las correlaciones no es una consecuencia del modelo de eslabones rotos. Existe un punto de vista basado en la ecuación de Langevin, y por lo tanto conectado con la ecuación maestra, que aporta una descripción cuantitativa de los resultados obtenidos a partir de nuestro modelo de decoherencia.

Modelo Browniano (*)

La ecuación de Langevin describe el movimiento browniano de una partícula que se mueve en un medio en equilibrio térmico y esta sometida a pequeñas perturbaciones estocásticas [Rei65]. En una dimensión,

$$\frac{dv}{dt} + \gamma v = f(t) \tag{4.69}$$

donde v es la velocidad de la partícula, γ un coeficiente de viscocidad para el medio y $f(t)$ la fuerza impulsiva estocástica (por unidad de masa), que en el modelo original es debida a colisiones con las moléculas individuales del fluido circundante. Se asume que $f(t)$ tiene valor medio nulo de modo que no hay fuerza neta en media. Bajo condiciones de equilibrio térmico con el fluido circundante, y si inicialmente $\overline{x} = \overline{x^2} = 0$, la evolución temporal de la varianza para la posición de esta partícula Browniana es

$$\sigma^2 = \frac{2C}{\gamma}\left[t - \gamma^{-1}\left(1 - e^{-\gamma t}\right)\right], \tag{4.70}$$

donde C es una constante relacionada con la temperatura del baño térmico.

La viscocidad del medio define un tiempo característico γ^{-1} en el cual la varianza tiene una transición entre un crecimiento cuadrático a otro lineal. Para tiempos $t \ll \gamma^{-1}$ se tiene

$$\sigma^2 \simeq Ct^2 \qquad (t \ll \gamma^{-1}). \tag{4.71}$$

Por otra parte, para $t \gg \gamma^{-1}$ los efectos disipativos debidos a las colisiones predominan y resulta

$$\sigma^2 \simeq \frac{2C}{\gamma}t \qquad (t \gg \gamma^{-1}). \tag{4.72}$$

La partícula en este caso experimenta un proceso difusivo, con coeficiente

$$D = \frac{C}{\gamma}. \tag{4.73}$$

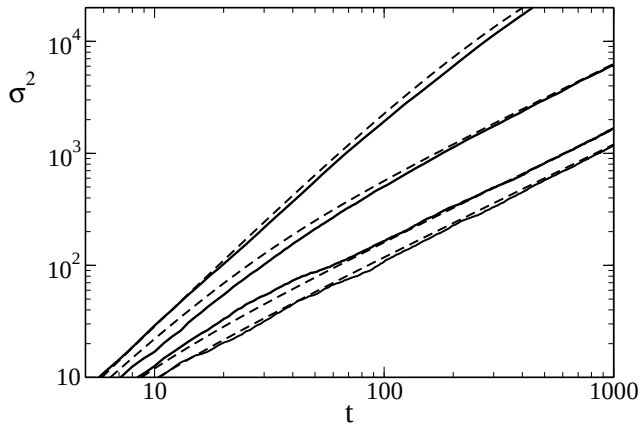

Figura 4.11: Comparación (en escala logarítmica) de la evolución temporal de la varianza de la caminata cuántica con eslabones rotos (líneas llenas) y de una partícula Browniana equivalente ec. (4.70), con $C = 0{,}293$ y γ dado por la ec. (4.74). Los valores de p son (en orden descendiente) $p = 0{,}01, 0{,}10, 0{,}30$ y $0{,}40$.

La constante C es la concavidad de la parábola $\sigma^2(t)$ en el caso coherente. Para las condiciones iniciales que usamos en este trabajo, $C = 0{,}293$.

La tasa de eventos decoherentes p se relaciona con la viscocidad γ, ya que los eslabones rotos funcionan como un obstáculo a la evolución. Una comparación entre los coeficientes de difusión, ecs. (4.4) and (4.66) implica la relación

$$\gamma = 0{,}73\,\frac{p}{1-p}. \tag{4.74}$$

Como se muestra en la Fig. 4.11, este modelo estocástico simple ajusta extremadamente bien la evolución de la varianza del QW con eslabones rotos para un amplia gama de valores de p.

El ajuste entre el movimiento Browniano y la caminata cuántica con eslabones rotos es demasiado bueno para ser casual. El rol de la viscocidad y su equivalente en eslabones rotos es razonable, ya que ambos efectos tienden a obstaculizar el movimiento. Sin embargo, el equilibrio térmico con el medio no tiene un análogo evidente en la caminata cuántica, donde ni siquiera hay definida una temperatura. Se requiere de un formalismo más sofisticado para comprender mejor la relación entre ambos modelos. Un candidato para esto es describir la caminata cuántica abierta con una ecuación maestra para la

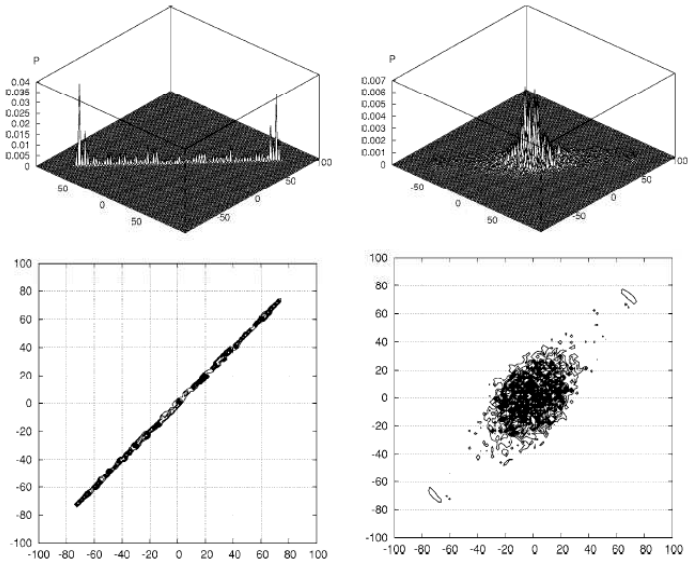

Figura 4.12: Distribución de probabilidad luego de $t = 100$ pasos rompiendo eslabones en 2D en forma anisotrópica. Se usa una operación de Grover con $p_0 = 0$ y $p_1 = 0{,}99$ (Izq.), y $p_0 = 0$ y $p_1 = 0{,}35$ (Der.). Figura tomada de [OPD06].

matriz densidad, en la forma de Caldeira-Legget, por ejemplo.

4.3.2. Generalización del modelo a 2D

En un trabajo reciente, Oliveira, Portugal y Donangelo generalizaron el modelo de decoherencia de eslabones rotos a dos dimensiones [OPD06]. En este caso, el caminante cuántico se desplaza en un plano ocupando posiciones discretas (x, y). Usaron operaciones de moneda separables (Hadamard) y no separables (operaciones de Grover y Fourier), observando poco cambio en la evolución de la varianza entre estos casos. Cuando se rompen los eslabones uniformemente con probabilidad p por unidad de tiempo, los resultados son similares al modelo unidimensional. Es decir, se observa una transición desde un regimen de crecimiento cuadrático a otro de crecimiento lineal. La transición tiene lugar en un tiempo característico $\sim 1/p$, como en el caso unidimensional. En el régimen decoherente, el coeficiente de difusión depende de $(1 - p)/p$ como en el caso unidimensional.

Sin embargo, cuando se consideran efectos anisotrópicos en el modelo, aparecen algunas novedades. Por ejemplo es posible romper links a lo largo de

una diagonal y no de la otra, de manera que eventualmente, la propagación se vuelve efectivamente unidimensional, como se muestra en la Fig. 4.3.2. El esquema de eslabones rotos permite (en forma permanente), permite "guiar" el flujo de probabilidad prácticamente a voluntad y es fácilmente generalizable a tres o más dimensiones. Esto genera perspectivas interesantes para estudiar la transmisión a entre regiones de billares abiertos, la percolación cuántica y la propagación en regiones inhomogéneas.

Capítulo 5

Conclusiones y Perspectivas

Las cadenas de Markov, o caminatas al azar, han sido la base de una familia de algoritmos estocásticos muy poderosos [MR96]. Entre ellos se cuentan, entre otros, el Método Monte Carlo, el algoritmo de Metrópolis o el algoritmo de Schöning para el problema 3-SAT, que hemos detallado en este trabajo.

La versión cuantizada de una cadena de markov, la caminata cuántica (QW), resulta ser un protocolo de evolución cuántica tan general como su contraparte clásica. En este trabajo hemos presentado la versión del QW en la línea a tiempo discreto y a tiempo continuo. Para estos casos unidimensionales hay un cuerpo de conocimiento bastante importante, generado en los últimos años y al cual se han realizado algunos aportes desde Montevideo. Debido a la superposición cuántica, el caminante se desplaza simultáneamente a derecha e izquierda. Una de sus características más importantes es que la varianza de la distribución de posición crece cuadráticamente con el número de pasos, de modo que el proceso se extiende más rápidamente que una cadena de Markov clásica, para la cual la varianza crece linealmente con el número de pasos. La operación de desplazamiento condicional genera enredo (correlaciones cuánticas) entre la posición y la moneda del caminante. Este enredo fluctúa, pero tiende rápidamente a un valor límite estable. Hemos mostrado en detalle como es posible obtener expresiones analíticas que permiten conocer el nivel asintótico de enredo entre la moneda y posición como función de la condición inicial[1].

Se han considerado sistemas de dos caminantes cuánticos con diversas

[1] En procesos unitarios la memoria de la condición inicial se mantiene indefinidamente.

operaciones de moneda, separables y no separables. En este último caso, aparece una riqueza considerable en cuanto a las posibilidades de enredo multipartita. En un caso típico, la dinámica involucra operaciones condicionales que enredan las monedas de ambos caminantes. Por otra parte, la traslación condicional de cada uno de ellos enreda su moneda y su posición, de la misma forma que en el caso de una partícula. El resultado es un "enredo indirecto" que vincula a ambas distribuciones de posición. Una medida realizada sobre uno de ellos afectará la distribución del otro, aunque se hallan desplazado en direcciones opuestas y ya no interactuen entre si. Hemos cuantificado el enredo bipartita entre ambos caminantes, para varias operaciones no separables y hemos encontrado un crecimiento logarítmico con el número de pasos. Este crecimiento es probablemente explicable por el hecho de que, a cada paso, la distribución se extiende en el espacio y más autoestados de posición participan de la dinámica. En principio, es posible caracterizar este enredo bipartita a tiempos largos, usando los métodos analíticos que hemos empleado para el caso de una partícula, pero necesitaríamos un estudiante de doctorado para ello...

Como aplicación a la Teoría de Juegos, hemos formulado la primera versión cuantizada del Dilema del Prisionero iterado, en el cual los jugadores pueden implementar varias estrategias clásicas en sus versiones cuánticas. Se han establecido las condiciones para que una estrategia clásica se pueda implementar como una operación unitaria. Cuando se cumplen, una estrategia clásica da origen a una extensa familia de estrategias cuánticas, lo cual abre nuevas posibilidades que aún no fueron exploradas. En particular, el rol del enredo bi-partita y la inclusión de medidas generalizadas u operaciones LOCC por parte de los jugadores. Extensiones a juegos multi-partitas son más o menos inmediatas con el formalismo que hemos desarrollado. También es posible ampliar aún más el espectro de estrategias considerando un sistema abierto y operaciones cuánticas, en lo que podríamos llamar "estrategias no unitarias asistidas por el ruido ambiente". Todas estas posibilidades aparecen en el horizonte.

Cuando el QW se expone al ruido ambiente la ventaja cuántica se pierde gradualmente y la varianza pasa a crecer linealmente con el tiempo. Sin embargo, la tasa de crecimiento cuántica[2], D_q, es mayor (para niveles de ruido

[2]Que hemos llamado coeficiente de dispersion, por analogía con el coeficiente de difusión clásico.

moderados, mucho mayor) que la difusión clásica, $D = 1$. Hemos analizado los resultados de varios estudios numéricos y analíticos, tanto nuestros como de otros investigadores, sobre decoherencia. Se han mostrado en cierto detalle los cálculos basados en la aproximaciones de ecuación maestra y los resultados obtenidos en base al formalismo de operaciones cuánticas. Las fuentes de decoherencia consideradas son bastante diversas: medidas frecuentes de la moneda, de la posición , de ambas, ruido unitario en la moneda, ruido de bit-flip en la moneda, ruido topológico o "eslabones rotos" que pretende simular un ruido térmico que afecta la posición y la moneda, etc. En todos los casos, se observa la regla general de que hay un tiempo característico del orden del inverso de la frecuencia de los eventos decoherentes. Es decir, en este sistema la decoherencia opera a través de un proceso acumulativo. Los detalles como el impacto en la distribución de posición dependen del tipo de ruido considerado.

Esta claro que, para niveles de ruido moderado $p \ll 1$, la dispersion resultante es más rápida que la difusión clásica en un factor $1/p \gg 1$. Hemos mostrado que si se desprecian completamente las correlaciones cuánticas, las ecuaciones de evolución cuántica se reducen a una ecuación de difusión con el coeficiente usual $D = 1$. Lo mismo ocurre en el caso de ruido de eslabones rotos al azar con un coeficiente reducido $D = (1-p)$. Hay indicios fuertes de correlaciones persistentes, aún a tiempos largos, que hacen que la dispersion cuántica en presencia de ruido sea más rápida que la clásica. Creemos que este efecto es inesperado y merece un estudio más profundo. en particular, todos los tipos de perturbaciones que hemos descrito son eso: perturbaciones elegidas para "emular" el efecto de un ambiente. No hay un estudio en el cual se coloca un QW en interacción con un baño térmico de osciladores, por ejemplo, y se calcula su evolución resolviendo la alguna ecuación maestra adecuada, como la de Caldeira-Legget, que agrega un término de viscocidad a la ec. (4.1). En este caso, el efecto sobre el QW sería consecuencia de la interacción propuesta con el baño térmico y no una cosa introducida ad-hoc. En primer lugar, habría que ver si persisten las correlaciones cuánticas en éste caso. En nuestra opinión, este modelo esta fuertemente sugerido por el impresionante ajuste observado numéricamente entre el modelo de eslabones rotos al azar y una partícula Browniana, descrita por una ecuación de Langèvin, que se mueve en un medio viscoso a temperatura T. De modo que este nos parece un tema prioritario, donde hace falta profundizar.

En 1994, el algoritmo de Shor mostró que era posible usar la Mecánica Cuántica para factorizar enteros grandes. Clásicamente, esta tarea requiere recursos exponenciales en el tamaño de la entrada para ser realizada, por lo cual es la base de esquemas muy usados de criptografía, como RSA[3]. El esquema criptográfico continúa en uso, y lo hará por varios años, porque no hay procesadores cuánticos capaces de ejecutar el algoritmo de Shor para cientos de qubits. En 1995 Grover propone su algoritmo de búsqueda. Pese a los cosiderables esfuerzos que se han realizado en esta dirección, no han habido ideas realmente novedosas en el campo de los algoritmos cuánticos desde 1995. La mayoría de los avances producidos se basan en la técnica de transformada cuántica de Fourier que esta detrás de la ganancia exponencial del algoritmo de Shor[4] o en a la técnica de amplificación de fase que se usa en el algoritmo de Grover.

No esta claro aún si el QW puede aportar un nuevo punto de vista algorítmico que destrabe la situación, aunque hay algunos indicios en ese sentido. Hemos mencionado más de un trabajo en el cual un QW (a tiempo discreto o a tiempo continuo) es capaz de atravesar un hipercubo de dimensión $d \geq 3$ (de un vértice al opuesto) en un tiempo polinomial en d cuando un caminante clásico requiere $\mathcal{O}\left(2^d\right)$ pasos. La misma ventaja exponencial ocurre en cierto tipo de grafos (árboles binarios) en el caso del QW a tiempo continuo. Sin embargo, hasta el momento, los algoritmos de búsqueda concretos basados en el QW en hipercubos, sólo han logrado ventajas cuadráticas ($N \rightarrow \sqrt{N}$) con respecto a sus análogos clásicos y, en este sentido, son equivalentes al algoritmo de Grover, que hemos analizado en detalle.

Hemos analizado la clase de problemas NP y NP-completos en cierto detalle. Estos últimos son considerados los problemas más difíciles (dentro de los problemas manejables). El algoritmo de Schöning, el más rápido para problemas 3-SAT (el paradigma de los problemas NP-completos), es un ejemplo moderno del tipo de algoritmos estocásticos basados en cadenas de Markov y es de orden $1{,}333^n$, para un problema de n variables Booleanas.

[3]Hasta fecha, nadie ha logrado factorizar un número de 200 dígitos, pese a que hay recompensas prometidas (desafío RSA).

[4]El reciente algorítmo de Hallgreen [Hal01] es un buen ehjemplo de esta afirmación. Usa la transformada de Fourier cuántica para encontrar soluciones (eficientemente) para un tipo de ecuación diofántica (la ecuación de Pell, uno de los problemas más viejos en teoría de números, $x^2 - dy^2 = 1$ con x, y enteros y d un entero positivo que no es un cuadrado perfecto). Previamente, este problema no tenía solución eficiente conocida.

La cuantización de éste algoritmo no se ha realizado aún (hasta donde sabemos) y no vemos grandes obstáculos para llevarla a cabo. Elaborando sobre ideas previas de A. Ambainis, hemos analizado la posibilidad de reemplazar las repeticiones clásicas del algoritmo de Schöning por iteraciones de amplificación de amplitud. A través de este procedimiento, parece posible obtener un algoritmo cuántico considerablemente más rápido $\sqrt{1{,}333^n} \approx 1{,}155^n$ que el de Schöning, lo cual es un desafío interesante y – al menos en principio – accesible.

La conjetura $P \neq NP$ implica que existen problemas en la clase NP que no están en P. Es decir, problemas para los cuales es imposible encontrar una solución en forma eficiente. Se supone que estos problemas son los NP-completos, ya que se mapean entre si en tiempo polinómico y si se resuelve uno de ellos eficientemente, se resuelven todos. Simplemente, eso parece demasiado bueno para ser cierto, dadas las características comunes a éstos problemas (optimización de varias variables, restringida por muchos vínculos, en espacios grandes y desestructurados). En todo caso, no existe una prueba formal de la conjetura mencionada[5]. Si P=NP, esto significaría que se puede encontrar una solución eficientemente para los problemas NP-completos. En ese hipotético caso, quizás la Mecánica Cuántica, y en particular el modelo QW, tenga algo para aportar en esa dirección. Mientras tanto, los esfuerzos se orientan a problemas NP que no son NP-completos. Como sucedió con el problema de factorización de enteros, éstos problemas podrían ser más accesibles y ser "degradados" a la clase P por un algoritmo cuántico (o clásico!) eficiente.

No se debe olvidar además que el procesamiento cuántico de información es sólo uno de los objetivos del área. La distribución segura de claves cuánticas codificadas en fotones con o sin estados enredados ya esta en la escala de ~ 100 km por fibra óptica [MdRT$^+$04] y también por aire [Urs06] y en este aspecto se producen avances en la escala de meses. El otro uso potencialmente muy importante de un "procesador cuántico" de varios qubits es el de la simulación eficiente de sistemas cuánticos. Las nanotecnologías, la microelectrónica, el diseño de nuevas moléculas, requieren la habilidad de simular sistemas cuánticos de muchos grados de libertad. Una cosa que requiere recursos exponenciales en el número de qubits del sistema. De modo

[5]Pese a que hay hace algunos años un premio de 10^6 dólares esperando a quien la obtenga.

que es posible que el primer uso de un procesador cuántico con algunas decenas de qubits, que hagan posible la implementación de códigos de corrección de errores, sea justamente simular otros sistemas cuánticos eficientemente.

En cualquier caso, aunque nuestra generación nunca llegue a ver procesadores cuánticos de escritorio, en el transcurso de ésta aventura intelectual, habremos aprendido bastante física fundamental y alcanzado un grado de control sin precedentes sobre la materia microscópica.

Apéndices

Apéndice A

Mecánica Cuántica

Este Apéndice contiene información básica sobre los postulados de la Mecánica Cuántica, notación de Dirac y el formalismo del operador densidad. Esta adaptado de los Caps. 2 y 3 del material de apoyo para el curso de Computación Cuántica [AS04] que se dicta (en modalidades de grado y posgrado) en la Facultad de Ingeniería.

A.1. Representación matemática

En esta Sección, repasamos los elementos de álgebra lineal necesaria para trabajar con objetos cuánticos sin intentar ser matemáticamente rigurosos. No repetiremos aquí demostraciones que se encuentran en los textos, salvo cuando contribuyan a aclarar los conceptos presentados. El énfasis esta en la descripción de espacios vectoriales discretos en notación de Dirac.

A.1.1. Funciones de onda

La función de onda $\Psi(\vec{r}, t)$ es una función compleja que contiene toda la información sobre el estado de un sistema físico determinado. De acuerdo a la interpretación de Born, el módulo al cuadrado de la función de onda es una densidad de probabilidad. Es decir que $|\Psi(\vec{r}, t)|^2 dr^3$ es la probabilidad de encontrar una partícula en el elemento de volumen diferencial $(\vec{r}, \vec{r} + dr^3)$. La función de onda debe ser normalizable, $\int dr^3 \, |\Psi(\vec{r}, t)|^2 = 1$, lo cual restringe las funciones de interés a aquellas de módulo cuadrado integrable. Además, desde el punto de vista físico, éstas funciones deben ser bien definidas en todo el espacio, continuas y diferenciables.

Denominaremos $\mathcal{F}$ al espacio vectorial al cual pertenecen. El producto escalar o interno se define por

$$(\Phi, \Psi) \equiv \int dr^3 \Phi^*(\vec{r})\Psi(\vec{r}),$$

y es antilineal con respecto al primer argumento y lineal con respecto al segundo. Un caso particular lo representa el cálculo de la **norma** $||\Psi|| \equiv (\Psi, \Psi)^{1/2}$, que sólo es nula si $\Psi = 0$.

En muchos sistemas cuánticos, una descripción basada en una función compleja de las coordenadas espaciales no es de utilidad. Esta es la situación, por ejemplo, en sistemas de spin, fotones polarizados o sistemas de dos niveles en general, donde la posición espacial no juega un rol relevante. En esta categoría están muchos sistemas de interés para el procesamiento cuántico de la información, por lo que es conveniente usar una descripción abstracta de los estados cuánticos en términos de vectores de estado (o kets) pertenecientes a un espacio vectorial $\mathcal{H}$, llamado indistintamente espacio de estados o espacio de Hilbert. En particular, son de interés los espacios de dimensión finita por lo que en estas notas nos limitaremos a este caso. A continuación introducimos la notación de Dirac, que simplifica enormemente la operativa en éstos espacios.

A.1.2. Notación de Dirac

La notación de Dirac es una de las posibles notaciones para describir espacios lineales. Sin embargo, se adapta especialmente bien para describir el procesamiento cuántico de la información y es la norma aceptada en éste contexto.

Kets

Asociamos a cada función de onda un vector (o ket) en un espacio de Hilbert $\mathcal{H}$,

$$\Psi \rightarrow |\Psi\rangle \tag{A.1}$$

de modo que toda la información sobre el estado cuántico del sistema a describir esta contenida en el mismo. Los espacios $\mathcal{F}$ y $\mathcal{H}$ son isomorfos. Sin embargo, el concepto de espacio de estados es mas general que el de espacio de funciones de onda y se puede utilizar aún cuando los objetos relevantes no sean funciones complejas de posición.

El producto escalar entre dos vectores de $\mathcal{H}$, $|\Psi\rangle$ y $|\Phi\rangle$, es un número complejo que se indica como $\langle\Phi|\Psi\rangle$,

$$(\Psi, \Phi) = \int \Psi^* \Phi \, dr^3 \rightarrow \langle\Psi|\Phi\rangle.$$

De nuevo, el producto escalar es antilineal en el primer argumento y lineal en segundo. Sus propiedades, se escriben en notación de Dirac como

$$\begin{aligned} \langle\Phi|\Psi\rangle^* &= \langle\Psi|\Phi\rangle \\ \langle\lambda_1\Phi_1 + \lambda_2\Phi_2|\Psi\rangle &= \lambda_1^*\langle\Phi_1|\Psi\rangle + \lambda_2^*\langle\Phi_2|\Psi\rangle \\ \langle\Phi|\lambda_1\Psi_1 + \lambda_2\Psi_2\rangle &= \lambda_1\langle\Phi|\Psi_1\rangle + \lambda_2\langle\Phi|\Psi_2\rangle. \end{aligned} \tag{A.2}$$

La norma del ket $|\Psi\rangle$ es el real no negativo, $||\Psi|| \equiv \sqrt{\langle\Psi|\Psi\rangle} \geq 0$, donde, $\langle\Psi|\Psi\rangle = 0 \Leftrightarrow |\Psi\rangle = 0$ (el único vector de $\mathcal{H}$ que no se expresa dentro de corchetes $|\ \rangle$, es el vector nulo).

Bras

El producto escalar se puede interpretar como una regla que asocia a cada ket $|\Psi\rangle \in \mathcal{H}$ un número complejo determinado por otro ket $|\Phi\rangle$. Es decir que a cada ket $|\Phi\rangle \in \mathcal{H}$, le corresponde un **bra**, indicado como $\langle\Phi|$. Un bra es una función lineal que asocia un número complejo a todo ket de $\mathcal{H}$ mediante el producto escalar. Si existe una descripción en términos de funciones, se puede hacer la asociación

$$\int dr^3 \Phi^* \rightarrow \langle\Phi|. \tag{A.3}$$

Los bras son funcionales que pertenecen a un espacio $\tilde{\mathcal{H}}$, llamado **espacio dual** de $\mathcal{H}$.

Representación en $\mathcal{H}$

Hasta el momento no hemos especificado una representación en el espacio de kets $\mathcal{H}$. Supongamos que existe un conjunto de n kets $\{|u_i\rangle\} \in \mathcal{H}$ que satisfacen las relaciones,

$$\langle u_i|u_j\rangle = \delta_{ij} \tag{A.4}$$

$$\sum_{i=1}^{n} |u_i\rangle\langle u_i| = \mathbf{1} \tag{A.5}$$

donde $\delta_{ii} = 1$ y $\delta_{ij} = 0$ si $i \neq j$ (delta de Krönecker). La primera relación expresa que los kets de la base son un conjunto ortonormal. La segunda es la propiedad de clausura. El conjunto $\{|u_i\rangle\}$ es una base ortonormal en $\mathcal{H}$.

A partir de (A.5), es inmediato comprobar que cualquier ket $|\Psi\rangle \in \mathcal{H}$ se puede expresar de forma única como

$$|\Psi\rangle = \sum_{i=1}^{N} a_i |u_i\rangle \tag{A.6}$$

con $a_i = \langle u_i|\Psi\rangle \in \mathcal{C}$. Usualmente se organizan las componentes a_i en un vector columna que representa a $|\Psi\rangle$. La representación de un bra se obtiene en forma similar a partir de la clausura (A.5), (A.6),

$$\langle\Phi| = \langle\Phi| \left[\sum_{i=1}^{n} |u_i\rangle\langle u_i|\right] = \sum_{i=1}^{n} \langle\Phi|u_i\rangle \langle u_i| = \sum_{i=1}^{n} b_i^* \langle u_i| \tag{A.7}$$

con $b_i = \langle u_i|\Phi\rangle$. De modo que la representación del bra $\langle\Phi|$ es el vector fila

$$\langle\Phi| \rightarrow [b_1^*, \ldots, b_n^*].$$

Si $\Psi = \Phi$, decimos que la ec. (A.7) es la "expresión dual" de (A.6). En general, las expresiones duales se obtienen reemplazando bras por kets (o kets por bras), operadores por sus adjuntos y números complejos por sus conjugados. A nivel de representaciones, se obtiene la representación dual trasponiendo y conjugando.

El producto escalar entre un bra $\langle\Phi|$ y un ket $|\Psi\rangle$, se expresa en términos de una representación como

$$\langle\Phi|\Psi\rangle = [b_1^* \ldots b_n^*] \times \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} = \sum_{i=1}^{n} b_i^* a_i. \tag{A.8}$$

En cambio, la expresión $|\Phi\rangle\langle\Psi|$ es **un operador** en $\mathcal{H}$, representado por la matriz $n \times n$,

$$|\Phi\rangle\langle\Psi| = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} \times [a_1^* \ldots a_n^*] = \begin{bmatrix} a_1^* b_1 & \ldots & a_n^* b_1 \\ \vdots & \ddots & \vdots \\ a_1^* b_n & \ldots & a_n^* b_n \end{bmatrix}.$$

En general, $|\Phi\rangle\langle\Psi| \neq |\Psi\rangle\langle\Phi|$ y describen operadores diferentes. Se obtiene la matriz de uno de ellos conjugando y transponiendo la matriz del otro (son conjugados hermíticos).

Operadores en $\mathcal{H}$

Un **operador lineal** A en $\mathcal{H}$ asocia a cada ket $|\Psi\rangle$ otro ket, $|\Psi'\rangle = A|\Psi\rangle \in \mathcal{H}$ en una correspondencia lineal

$$A\left[\lambda_1|\Psi_1\rangle + \lambda_2|\Psi_2\rangle\right] = \lambda_1 A|\Psi_1\rangle + \lambda_2 A|\Psi_2\rangle \quad \forall\lambda_{1,2} \in \mathcal{C}.$$

La acción de un **operador compuesto** AB sobre un ket $|\Psi\rangle$, se define en la forma usual, $A\left[B|\Psi\rangle\right]$. Si los operadores no conmutan entre si, el orden de aplicación hace una diferencia. Se define el **conmutador** de dos operadores como el operador compuesto

$$[A, B] \equiv AB - BA. \tag{A.9}$$

Evidentemente, si $[A, B] \neq 0$ entonces $AB|\Psi\rangle \neq BA|\Psi\rangle$.

Dados dos kets $|\Phi\rangle$ y $|\Psi\rangle$ y un operador A, el **elemento de matriz** del operador entre estos kets es el número complejo $\alpha = \langle\Phi|A|\Psi\rangle$. Un operador lineal A actúa sobre un ket $|\Psi\rangle = \sum_i a_i|u_i\rangle$ produciendo otro ket $A|\Psi\rangle$ al cual le corresponden componentes $b_i = \langle u_i|A\Psi\rangle$ dadas por

$$b_i = \langle u_i|A\Psi\rangle = \langle u_i|A\sum_j a_j|u_j\rangle = \sum_j a_j\langle u_i|A|u_j\rangle = \sum_j \alpha_{ij}\, a_j.$$

Es decir que se obtiene la representación de $A|\Psi\rangle$ en la forma usual, multiplicando su vector columna por la matriz cuadrada de elementos

$$\alpha_{ij} = \langle u_i|A|u_j\rangle. \tag{A.10}$$

Esta matriz compleja es la representación del operador A. Es inmediato obtener una expresión para el operador en términos de la base,

$$A = \left[\sum_{i=1}^{N} |u_i\rangle\langle u_i|\right] A \left[\sum_{j=1}^{N} |u_j\rangle\langle u_j|\right] = \sum_{ij} \alpha_{ij}\, |u_i\rangle\langle u_j|. \tag{A.11}$$

Operador adjunto

Dado un operador lineal A se le asocia otro operador lineal $A^\dagger$ (el adjunto de A) a través de la relación

$$\langle\Phi|A|\Psi\rangle^* = \langle\Psi|A^\dagger|\Phi\rangle. \tag{A.12}$$

Un operador que cumple $A = A^\dagger$ se denomina hermítico o autoadjunto. Los operadores hermíticos son especialmente importantes en Mecánica

Cuántica porque pueden asociarse a magnitudes físicas, de modo que discutiremos sus propiedades por separado.

Es fácil verificar que se obtiene la representación de $A^\dagger$ trasponiendo y conjungando la matriz de A. En particular, un operador hermítico le corresponde una matriz – en cualquier representación – con elementos reales en la diagonal. Esto implica que los autovalores de este operador son reales. La relación de adjunto verifica las propiedades (para cualquier A, B y $\forall\lambda \in \mathcal{C}$),

$$\begin{aligned} \left(A^\dagger\right)^\dagger &= A & \qquad (\lambda A)^\dagger &= \lambda^* A^\dagger \\ (A+B)^\dagger &= A^\dagger + B^\dagger & \qquad (AB)^\dagger &= B^\dagger A^\dagger \end{aligned}$$

Autovalores y autovectores

Un ket $|\Psi\rangle$ es vector propio de un operador A si satisface

$$A|\Psi\rangle = \lambda|\Psi\rangle \tag{A.13}$$

para algún $\lambda \in \mathcal{C}$. Los posibles λ son los valores propios[1] del operador A.

El sistema lineal homogéneo definido por $(A-\lambda I)|\Psi\rangle = 0$ tiene solución no trivial sólo si se satisface la ecuación característica

$$|A - \lambda I| = 0 \tag{A.14}$$

donde $|\cdot|$ indica determinante e I es el operador identidad. Las raíces de ésta ecuación determinan los posibles valores de λ.

Projectores

El operador $P \equiv |\Phi\rangle\langle\Phi|$, aplicado sobre un ket arbitrario $|\Psi\rangle$ resulta en otro ket proporcional a $|\Phi\rangle$,

$$P|\Psi\rangle = \langle\Phi|\Psi\rangle\ |\Phi\rangle$$

Como se muestra en la Figura A.1, esta es la proyección ortogonal de $|\Psi\rangle$ sobre $|\Phi\rangle$.

La propiedad característica de un proyector es

$$\mathbf{P}^2 = \mathbf{P}. \tag{A.15}$$

[1]Si la ec. (A.13) se cumple para una serie de $g_\lambda > 1$ de vectores linealmente independientes $|\Psi_i^\lambda\rangle$ con $i = 1 \ldots g_\lambda$, con el mismo autovalor λ, éste tiene degeneración g_λ. Los autovectores determinan el subespacio propio de λ, $\mathcal{H}_\lambda \subset \mathcal{H}$, en el cual todo ket satisface la ec. (A.13).

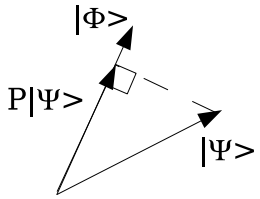

Figura A.1: Acción del proyector $\mathbf{P}\equiv|\Phi\rangle\langle\Phi|$ sobre un ket $|\Psi\rangle$ arbitrario. Observe que si $||\Psi|| = ||\Phi|| = 1$, la proyección $\mathbf{P}|\Psi\rangle$ no esta normalizada.

A partir de ésta propiedad, es inmediato mostrar que los autovalores de un proyector solo pueden ser 0 o 1.

Operadores hermíticos

Los operadores hermíticos ($A = A^\dagger$) son importantes en Mecánica Cuántica porque sus autovalores son reales y se asociar a magnitudes físicas observables.

Proyectando la ec. (A.13) sobre el bra $\langle\Psi|$, es inmediato ver que el autovalor λ se expresa como

$$\lambda = \frac{\langle\Psi|A|\Psi\rangle}{\langle\Psi|\Psi\rangle}. \tag{A.16}$$

La cantidad $\langle\Psi|\Psi\rangle$ (la norma al cuadrado) es siempre real positiva y si el operador A es hermítico,

$$\langle\Psi|A|\Psi\rangle^* = \langle\Psi|A^\dagger|\Psi\rangle = \langle\Psi|A|\Psi\rangle$$

también es real, por lo que el autovalor λ es real.

Los autovectores de diferentes valores propios de un operador hermítico son ortogonales. Supongamos que $\lambda \neq \mu$ son dos autovalores diferentes de un operador hermítico A. Se cumple entonces

$$\begin{aligned} A|\Psi\rangle &= \lambda|\Psi\rangle \\ A|\Phi\rangle &= \mu|\Phi\rangle. \end{aligned}$$

Proyectando la primera ecuación sobre $\langle\Phi|$ y la segunda sobre $\langle\Psi|$ se obtiene, luego de conjugar la segunda,

$$\begin{aligned} \langle\Phi|A|\Psi\rangle &= \lambda\langle\Phi|\Psi\rangle \\ \langle\Phi|A|\Psi\rangle &= \mu\langle\Phi|\Psi\rangle. \end{aligned}$$

La diferencia entre estas ecuaciones implica que los autovectores son ortogonales,

$$(\lambda - \mu)\langle\Phi|\Psi\rangle = 0 \Rightarrow \langle\Phi|\Psi\rangle = 0. \tag{A.17}$$

Este resultado implica que cada observable físico tiene asociados un conjunto de estados mutuamente ortogonales.

Representación espectral

Un operador que conmuta con su adjunto se dice normal: $\mathbf{A}\mathbf{A}^\dagger = \mathbf{A}^\dagger\mathbf{A}$. Los operadores hermíticos son normales. Los operadores normales satisfacen el **Teorema Espectral**[2]:

Un operador normal $\mathbf{A}$ *en* $\mathcal{E}$ *es diagonal en alguna base ortonormal de* $\mathcal{H}$*. Recíprocamente, todo operador diagonalizable en* $\mathcal{H}$ *es normal.*

Otra forma de decir lo mismo es que el conjunto de autovectores de un operador normal es una base de $\mathcal{H}$. Supongamos que $\lambda_1, \lambda_2 \ldots \lambda_N$ son los autovalores de $\mathbf{A}$. Es decir que

$$\mathbf{A}|i\rangle = \lambda_i|i\rangle \qquad \text{para } i = 1, 2 \ldots N.$$

Los autovectores de A, $\{|i\rangle\}$, forman una base ortonormal en $\mathcal{H}$ y satisfacen las ecs. (A.4) y (A.5). En la base propia, la matriz de A es diagonal $\alpha_{ij} = \lambda_i\delta_{ij}$ de modo que la expresión (A.11) se reduce a

$$A = \sum_i \lambda_i|i\rangle\langle i|. \tag{A.18}$$

Esta descomposición se conoce como la **representación espectral** del operador normal A.

Podemos usar la representación espectral para definir la **función de un operador**. Si $f : \mathcal{C} \to \mathcal{C}$ es una función de variable compleja, se puede definir la acción de f sobre un operador A de la siguiente forma:

$$f(A) \equiv \sum_i f(\lambda_i)|i\rangle\langle i|. \tag{A.19}$$

Por ejemplo, el exponencial de un operador es

$$e^A \equiv \sum_i e^{\lambda_i}|i\rangle\langle i|. \tag{A.20}$$

[2]Que aquí solo enunciaremos. Por una demostración ver, por ejemplo [NC00].

Otras funciones de un operador $(\log A, \sin A, \tan A, \sqrt{A}, \ldots)$ se definen en forma similar.

Operadores Unitarios

Un operador unitario se define por la relación

$$\mathbf{U}^\dagger \mathbf{U} = \mathbf{U}\mathbf{U}^\dagger = I. \tag{A.21}$$

Es decir que el operador adjunto de un operador unitario es su inverso.

Una propiedad básica de los operadores unitarios es que preservan la norma dado que

$$\langle \Psi | \Psi \rangle = \langle \Psi | U^\dagger U | \Psi \rangle.$$

Usando (A.21) es fácil comprobar que los autovalores de un operador unitario tienen módulo 1. Es decir que se pueden escribir en términos de fases reales $\varphi \in [0, 2\pi]$ como $e^{i\varphi}$.

La evolución temporal de un sistema cuántico esta asociada a un operador unitario. En particular, las compuertas lógicas por medio de las cuales se actúa sobre un conjunto de qubits están descritas por operadores unitarios.

A.2. Postulados de la Mecánica Cuántica

Para los efectos de éste trabajo, las reglas básicas de la Mecánica Cuántica se pueden resumir en tres postulados: descripción de un sistema físico, medidas y evolución temporal. Los postulados son simples, pero cada uno de ellos tiene una serie de implicancias que intentamos explicitar.

I. Descripción de un sistema físico

La información accesible sobre un sistema físico queda determinada por un vector de estado $|\Psi\rangle$, denominado ket, perteneciente a un espacio de Hilbert $\mathcal{H}$. Una magnitud física (un observable) es descrita por un operador hermítico $A = A^\dagger$ que actúa en $\mathcal{H}$.
Si el sistema es compuesto de n subsistemas en estados $|\Psi_i\rangle$ $(i = 1 \ldots n)$, su espacio de estados es el producto tensorial de los subespacios componentes y el estado del sistema conjunto es

$$|\Psi\rangle = |\Psi_1\rangle \otimes |\Psi_2\rangle \ldots \otimes |\Psi_n\rangle.$$

Al ser $\mathcal{H}$ un espacio lineal, este postulado implica un Principio de Superposición. Si $|\Psi_1\rangle, |\Psi_2\rangle \in \mathcal{H}$, una combinación lineal arbitraria $\lambda_1|\Psi_1\rangle + \lambda_2|\Psi_2\rangle$ con $\lambda_{1,2} \in \mathcal{C}$, es también un ket de $\mathcal{H}$ y representa un posible estado del sistema.

Esto tiene fuertes implicaciones en el procesamiento cuántico de la información. Clásicamente, un sistema de dos estados $|0\rangle$ y $|1\rangle$ puede usarse para representar un bit de información. Cuánticamente, el sistema puede existir además en una superposición de estados. Cuando se describen sistemas de más de un qubit, la superposición de alternativas clásicamente excluyentes da lugar a estados enredados.

II. Medidas

> *El resultado de la medida del observable A solo puede ser uno de sus autovalores reales, a_n. La medida de un observable causa el colapso no determinista del ket $|\Psi\rangle$ en el subespacio asociado al autovalor obtenido. La probabilidad de obtener el resultado a_n esta dada por la proyección del estado del sistema $|\Psi\rangle$, en el instante previo a la medida, en el subespacio propio asociado a ese autovalor.*

Supongamos que el sistema se encuentra en un estado descrito por el ket normalizado $|\Psi\rangle$, de modo que $\langle\Psi|\Psi\rangle = 1$. Si A es un observable, tiene un conjunto de autovalores (reales) y correspondientes autovectores,

$$A|u_n\rangle = a_n|u_n\rangle \tag{A.22}$$

que forman una base en $\mathcal{H}$. El resultado de una medida de A sólo puede ser uno de estos autovalores[3] Dado que A es un observable, se puede expresar el estado antes de la medida como

$$|\Psi\rangle = \sum_n c_n|u_n\rangle \tag{A.23}$$

con $\langle u_n|u_m\rangle = \delta_{nm}$ y $c_n = \langle u_n|\Psi\rangle$. La probabilidad p_n de que la medida resulte en el autovalor a_n es

$$p_n = |c_n|^2 = |\langle u_n|\Psi\rangle|^2. \tag{A.24}$$

[3]Los autovalores a_n pueden o no ser degenerados. Por claridad, discutimos el caso en que no hay degeneración; la generalización es inmediata.

La normalización de $|\Psi\rangle$ implica que $\sum_n p_n = 1$. El resultado de la medida no esta determinado a-priori[4].

En general, un autovalor degenerado puede estar asociado a un conjunto de q kets ortonormales, $|u_1\rangle, |u_2\rangle \dots |u_q\rangle$ que generan un subespacio $\mathcal{H}_q \subset \mathcal{H}$. El proyector sobre este subespacio es $P \equiv \sum_{i=1}^{q} |u_i\rangle\langle u_i|$. La medida resulta en la proyección (normalizada) del estado $|\Psi\rangle$ en el subespacio $\mathcal{H}_q$,

$$\frac{P|\Psi\rangle}{||P|\Psi\rangle||} = \frac{1}{\sqrt{\sum_{i=1}^{q} |c_i|^2}} \sum_{i=1}^{q} c_i |u_i\rangle \qquad \text{con } c_i = \langle u_i|\Psi\rangle.$$

Nos referimos a este proceso como el "colapso" no determinista del estado $|\Psi\rangle$. Es imposible reconstruir el ket $|\Psi\rangle$ a partir del resultado de una medida. En otras palabras, la medida es un proceso irreversible y a diferencia del caso clásico, es imposible observar un estado cuántico sin modificarlo en forma no determinista[5]

Lo anterior describe el formalismo de Medidas Proyectivas tal como se enseña en los cursos de Mecánica Cuántica. Una medida proyectiva es repetible, es decir que si se mide un observable A y se obtiene el autovalor a_n, una medida de A *inmediatamente posterior* resulta con certeza en el mismo valor a_n. Muchas medidas de interés en el procesamiento cuántico de información no son de éste tipo. Por ejemplo, si se mide la polarización de un fotón con un sistema analizador-detector, el fotón es destruido en el proceso y la medida no es repetible. Existe un formalismo de Medidas Generalizadas, que incluye a las medidas proyectivas y es de gran interés para la descripción de sistemas cuánticos abiertos, donde el efecto del entorno debe ser tenido en cuenta. El mismo se presenta en la Sección A.5.

Ensembles

Si se cuenta con un conjunto (o *ensemble*) de muchos sistemas todos preparados en el mismo estado $|\Psi\rangle$, se pueden realizar medidas independientes en cada uno de ellos y obtener una estadística que permita estimar los módulos $|c_n|$. Este proceso se conoce como *tomografía cuántica* del estado Ψ.

[4]Salvo en el caso especial en que el estado del sistema antes de la medida sea un autoestado de A.

[5]Este hecho ha mostrado ser de utilidad comercial en aplicaciones criptográficas seguras. Si se codifica una clave secreta en una serie de estados cuánticos es imposible que un eventual espía acceda a la misma sin alterarla y ser detectado.

En la práctica la tomografía cuántica se aplica a estados descritos por el formalismo de matriz densidad, que introducimos en la Sección A.3.

El valor esperado del observable A, para una serie medidas de sistemas preparados en un estado $|\Psi\rangle$, es el real

$$\langle \mathbf{A} \rangle \equiv \langle \Psi | A | \Psi \rangle = \sum_n |c_n|^2 a_n. \tag{A.25}$$

La dispersion en las medidas se obtiene de la forma usual, a partir de la desviación estándar σ_A, o de su varianza asociada

$$\sigma_A^2 \equiv \langle (\mathbf{A} - \langle \mathbf{A} \rangle)^{\mathbf{2}} \rangle = \langle \mathbf{A^2} \rangle - \langle \mathbf{A} \rangle^2. \tag{A.26}$$

Principio de Incertidumbre de Heisemberg

Las incertidumbres asociadas a un conjunto de medidas de dos observables **A** y **B** que no conmutan satisfacen la relación de incertidumbre de Heisemberg,

$$\sigma_A \sigma_B \geq \frac{1}{2} |i \langle [\mathbf{A}, \mathbf{B}] \rangle|. \tag{A.27}$$

Esta relación, que se demuestra a partir de los postulados [AS04, NC00, Bor57], implica que dos observables conjugados (es decir, que no conmutan) no pueden ser conocidos simultáneamente con precisión arbitraria[6].

El caso mas conocido de la relación de incertidumbre refiere a los observables conjugados de posición $A = x$ y cantidad de movimiento $B = -i\hbar \frac{d}{dx}$. Estas expresiones están en representación de posición en una dimensión. En este caso, $[A, B] = i\hbar$ y (A.27) se reduce a

$$\sigma_x \sigma_{p_x} \geq \frac{\hbar}{2}.$$

Mas adelante en estas notas, pondremos ejemplos de aplicación de la relación de Heisemberg en el espacio de un qubit.

[6]Si los observables conmutan entre si $[A, B] = 0$, resulta la afirmación inocua $\sigma_A \sigma_B \geq 0$. Estos observables se denominan **observables compatibles** y existe una base en $\mathcal{H}$ en la cual ambos son diagonalizables simultáneamente. Se puede determinar su valor simultáneamente con una precisión acotada por las limitaciones del aparato de medida.

III. Evolución

Para un sistema cerrado, la evolución temporal del ket $|\Psi(t)\rangle$ esta dada por la ecuación de Schrödinger

$$i\hbar\frac{d}{dt}|\Psi(t)\rangle = H(t)|\Psi(t)\rangle \tag{A.28}$$

donde H (operador Hamiltoniano) es el observable asociado a la energía total del sistema.

Es decir que la evolución dinámica de un sistema cuántico es determinista y reversible.

La ecuación (A.28) es lineal, de modo que una combinación lineal de sus soluciones también es solución, como lo requiere el Postulado I. La normalización $\langle\Psi|\Psi\rangle = 1$ no fija la fase del ket de modo que dos kets, $|\Psi\rangle$ y $e^{i\varphi}|\Psi\rangle$, que difieren en una fase global $\varphi \in [0, 2\pi]$, representan el mismo estado.

Operador evolución

Existe un operador lineal que aplicado al ket $|\Psi(t_0)\rangle$ resulta en $|\Psi(t)\rangle$. Este operador es el **operador evolución** $U(t_0, t)$ entre t_0 y t. En efecto, se puede integrar formalmente (A.28), expresándola como

$$\frac{d|\Psi\rangle}{|\Psi\rangle} = -\frac{i}{\hbar}H(t)\,dt \tag{A.29}$$

que, luego de integrar, resulta en

$$|\Psi(t)\rangle = e^{-\frac{i}{\hbar}\int_{t_0}^{t} H(t')\,dt'}|\Psi(t_0)\rangle = U|\Psi(t_0)\rangle. \tag{A.30}$$

En general, cuando H depende del tiempo, expresiones como (A.30) sólo tienen interés formal[7]. Si el sistema que se describe es conservativo, su energía es una constante del movimiento y el operador H no depende del tiempo. En este caso, el operador de evolución entre t_1 y t_2 es sencillamente

$$U(t_1, t_2) = e^{-\frac{i}{\hbar}H(t_2 - t_1)}. \tag{A.31}$$

El hecho de que el hamiltoniano es hermítico ($H = H^\dagger$) asegura que el operador de evolución es unitario $U^\dagger U = 1$ y preserva la norma. La evolución unitaria

$$|\Psi(t)\rangle = U_t|\Psi(t_0)\rangle \tag{A.32}$$

[7]Es difícil aplicar $\exp\left[-\frac{i}{\hbar}\int_{t_0}^{t} H(t')dt'\right]$ ya que está implícito un operador de ordenamiento temporal que hace que en el producto de operadores se apliquen primero aquellos que dependen de tiempos menores, pero en general $[H(t'), H(t")] \neq 0$.

es sinónimo de la ecuación de Schrödinger (A.28) e implica **reversibilidad**, ya que siempre existe $U^{-1} = U^{\dagger}$.

Las compuertas cuánticas implementan esta transformación unitaria y sólo pueden ser compuertas reversibles, en contraste con el caso clásico. La lógica Booleana debe reemplazarse por una lógica reversible.

A.3. Operador densidad

Hasta el momento hemos supuesto que se describe un sistema cuántico aislado preparado en un estado $|\Psi\rangle$ conocido perfectamente. En muchos casos de interés, se cuenta con información incompleta sobre el estado del sistema. En éstos casos[8], es conveniente adoptar una descripción alternativa basada en el operador densidad. Supongamos que la preparación de un sistema concreto es el resultado de una medida de cierto observable. En este caso, de acuerdo al Postulado II, el sistema estará en uno de los subespacios asociados a los autovalores del observable. No sabemos cual, sino que tenemos información estadística sobre la probabilidad de que esté en uno u otro estado. Este es un caso en el que el estado del sistema es una *mezcla estadística* y se describe adecuadamente por el operador densidad que definimos a continuación.

Un sistema puede estar en uno de N estados normalizados $|\Psi_i\rangle$ y ortogonales entre si. La restricción de ortogonalidad es físicamente razonable, ya que dos estados no ortogonales no son distinguibles con certeza. Si p_i es la probabilidad de que el sistema esté en el estado $|\Psi_i\rangle$, se define el operador densidad como

$$\rho = \sum_{i=1}^{N} p_i |\Psi_i\rangle\langle\Psi_i| \tag{A.33}$$

donde $p_i \geq 0$ y $\sum_i p_i = 1$. Este operador es hermítico, definido positivo y tiene traza 1, como mostramos más adelante. El formalismo anterior esta contenido en el operador densidad. Si sabemos con certeza que el sistema está en un cierto estado $|\Psi_k\rangle$, entonces $p_i = \delta_{ik}$ y

$$\rho = |\Psi_k\rangle\langle\Psi_k|. \tag{A.34}$$

Nos referimos a éste caso como un *estado puro*. En cambio, el caso general (A.33) describe a una *mezcla estadística*, lo cual implica una referencia a un

[8]Por ejemplo, cuando los efectos del ambiente no son despreciables e introducen ruido en el sistema.

conjunto de sistemas idénticos (un ensemble). Los estados puros pertenecen a un espacio de Hilbert, $|\Psi_i\rangle \in \mathcal{H}$. Existe un espacio asociado $\mathcal{D}(\mathcal{H})$ al cual pertenecen los operadores densidad generados por expresiones como (A.33). La normalización de los estados puros implica que

$$tr(\rho) = \sum_i p_i \, tr(|\Psi_i\rangle\langle\Psi_i|) = \sum_i p_i = 1.$$

Además, ρ es definido positivo ya que, para cualquier vector $|\phi\rangle$, su valor esperado verifica

$$\langle\phi|\rho|\phi\rangle = \sum_i p_i |\langle\phi|\Psi_i\rangle|^2 \geq 0.$$

El valor esperado de un observable es

$$< A > \equiv \sum_i p_i \langle\Psi_i|A|\Psi_i\rangle = tr(\rho A).$$

Existe un criterio simple para distinguir si un operador densidad corresponde a una mezcla o a un estado puro. El operador ρ^2 se expresa

$$\rho^2 = \sum_i p_i^2 |\Psi_i\rangle\langle\Psi_i|$$

y su traza es menor o igual que la traza de ρ,

$$tr(\rho^2) = \sum_i p_i^2 \leq tr(\rho) = 1. \tag{A.35}$$

Dado que siempre $\sum_i p_i = 1$, la igualdad sólo tiene lugar si $p_i = \delta_{ik}$ para algún k, es decir, un estado puro. De modo que la traza de ρ^2 nos indica si ρ describe un estado puro o una mezcla estadística.

Los postulados de la Mecánica Cuántica se pueden enunciar en términos de operadores densidad. Por ejemplo, la evolución de un sistema, ec. (A.32), se expresa en términos del operador densidad como

$$\rho_t = U \rho_0 \, U^\dagger. \tag{A.36}$$

El Postulado II (medidas) se puede expresar en términos de matriz densidad. Supongamos que $a_n^{(i)}$ es un autovalor de $|\Psi_i\rangle$. Con el sistema en el estado puro $|\Psi_i\rangle$, la probabilidad de observar ese autovalor es $\langle\Psi_i|P_n|\Psi_i\rangle = tr(|\Psi_i\rangle\langle\Psi_i|P_n)$ en términos del proyector P_n en el subespacio correspondiente. Con el sistema en un estado mezcla ρ de la forma (A.3), la probabilidad de obtener el autovalor a_n es

$$p(a_n) = \sum_i p_i \langle\Psi_i|P_n|\Psi_i\rangle = tr(\rho P_n).$$

El estado, luego de una medida con el resultado a_n, es

$$\rho \to \rho_n = \frac{\rho P_n}{tr(\rho P_n)}.$$

En el caso de medidas generalizadas, estas expresiones se generalizan en forma inmediata.

A.4. Algunos ejemplos

En este punto, es conveniente ilustrar los postulados a través de ejemplos concretos como la descripción de sistemas de uno y dos qubits.

A.4.1. Sistema de dos estados – qubit

Un sistema clásico de dos estados representa información binaria. Por ejemplo, un transistor conduce corriente o no lo hace. Si representamos, arbitrariamente, estos dos estados por $|0\rangle$ y $|1\rangle$ tendremos una descripción binaria del estado del transistor: un bit de información.

La descripción cuántica para un sistema de dos estados es análoga, pero con una salvedad importante, debida al Postulado I. Las superposiciones también son estados posibles del sistema. Es decir que la forma mas general de una unidad de información codificada en un soporte cuántico es

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad \text{con } |\alpha|^2 + |\beta|^2 = 1 \tag{A.37}$$

y $\alpha, \beta \in \mathcal{C}$. El vector (ket) definido por (A.37) representa un *qubit* de información. El sistema esta en una superposición de ambas alternativas. De acuerdo al Postulado II, una medida colapsaría el ket en forma no determinista al estado $|0\rangle$ con probabilidad $|\alpha|^2$ o al $|1\rangle$, con probabilidad $|\beta|^2$.

Esfera de Blöch

Alternativamente, un qubit puede expresarse, a menos de una fase global sin consecuencias físicas, como

$$|\Psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle \tag{A.38}$$

con $\theta \in [0, \pi]$ y $\varphi \in [0, 2\pi]$ ángulos reales. Los ángulos θ y φ ubican un punto en la superficie de una esfera de radio 1, llamada *esfera de Blöch*. Para $\theta = 0$ se obtiene $|\Psi\rangle = |0\rangle$ y para $\theta = \pi$, resulta $|\Psi\rangle = |1\rangle$. Esta representación

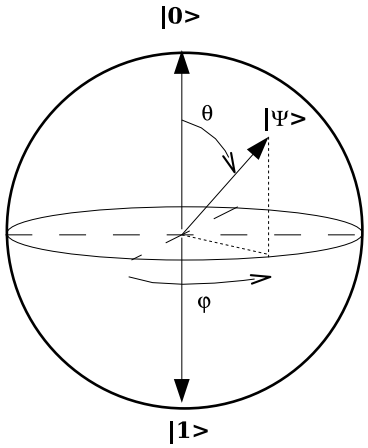

Figura A.2: Esfera de Blöch, mostrando la convención para los estados $|0\rangle$ y $|1\rangle$ y un ket genérico de la forma (A.38).

gráfica (Fig. A.2) permite visualizar las transformaciones lineales que sufre el ket. La utilidad de esta representación se haya limitada por el hecho de que no es extensible a sistemas con más de un qubit.

Para describir un qubit es necesario especificar dos parámetros reales. Esto requiere, en principio, una cantidad infinita de información clásica y puede dar la impresión de que qubit representa una cantidad infinita de información. Esto es sólo aparente, ya que para acceder a la información del ket es necesario realizar una medida y al medir, el qubit colapsa en una de sus dos alternativas clásicas.

La representación canónica para describir un qubit[9] asocia a los estados $\{|0\rangle, |1\rangle\}$, vectores columna

$$|0\rangle \rightarrow \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad |1\rangle \rightarrow \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \tag{A.39}$$

de modo que un qubit genérico se representa por $[\alpha, \beta]^T$, donde T indica transposición.

[9]Esta base ortonormal se denomina *base computacional* en $\mathcal{H}$.

Operador densidad

Una descripción alternativa del estado puro $|\Psi\rangle$ es en términos de su operador densidad que, en la representación canónica, es

$$\rho = \begin{pmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{pmatrix}.$$

Cada punto en la esfera de Blöch corresponde a un estado cuántico. De modo que no es sorprendente que exista una relación que vincule al operador densidad ρ con un punto en la esfera de Blöch,

$$\rho = \frac{I + \vec{r}\cdot\vec{\sigma}}{2} \tag{A.40}$$

donde I es la identidad 2x2, $\vec{r}$ es un vector tridimensional de norma $|\vec{r}| \leq 1$ que ubica un punto en la esfera de Blöch y $\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3)$ es el operador vectorial formado por las matrices de Pauli. Existe una relación entre la traza de ρ^2 y la norma de $\vec{r}$, de modo que se puede demostrar que si $|\vec{r}| = 1$, el estado es puro y si $|\vec{r}| < 1$ el estado es una mezcla estadística. Los estados con información incompleta residen en el interior de la esfera de Blöch. El estado de mínima información $\rho = I/2$ corresponde al centro de la esfera ($\vec{r} = 0$).

A.4.2. Sistemas de dos qubits - Productos tensoriales

El espacio de Hilbert para dos qubits es de dimensión $2^2 = 4$ y se obtiene a partir del **producto tensorial** de los dos espacios de un qubit:
$\mathcal{H}_2 = \mathcal{H}_1 \otimes \mathcal{H}_1 = \mathcal{H}_1^{\otimes 2}$. Sus elementos son productos de kets de la forma $|0\rangle \otimes |0\rangle = |00\rangle$. La base computacional en este espacio esta formada por los kets ortonormales

$$|00\rangle,\ |01\rangle,\ |10\rangle,\ |11\rangle \tag{A.41}$$

y un ket (normalizado) genérico de $\mathcal{H}_2$ se expresa

$$|\Psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle \tag{A.42}$$

donde $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$.

La representación para la base computacional en $\mathcal{H}_2$ esta dictada por las reglas del producto tensorial. Por ejemplo, al ket $|01\rangle = |0\rangle \otimes |1\rangle$ le

corresponde el vector columna

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}. \tag{A.43}$$

Hay que recordar que el producto tensorial de dos matrices $A \otimes B$ se obtiene fácilmente a partir de la regla

$$A \otimes B = \begin{bmatrix} A_{11}B & \dots & A_{1m}B \\ & \ddots & \\ A_{n1}B & \dots & A_{nm}B \end{bmatrix} \tag{A.44}$$

donde A es $n \times m$. La ec. (A.43) se obtiene fácilmente a partir de esta regla. La aplicación de esta regla permite completar inmediatamente la representación de la base computacional en $\mathcal{H}_2$ (A.43),

$$|00\rangle \to \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad |01\rangle \to \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \quad |10\rangle \to \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \quad |11\rangle \to \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}. \tag{A.45}$$

Frecuentemente es conveniente designar un ket de la base computacional por su valor decimal, de modo que

$$|0\rangle \equiv |00\rangle \quad |1\rangle \equiv |01\rangle \quad |2\rangle \equiv |10\rangle \quad |3\rangle \equiv |11\rangle \tag{A.46}$$

y, en notación compacta un ket genérico de $\mathcal{H}_2$ es $|\Psi\rangle = \sum_{i=0}^{3} a_i |i\rangle$. Esta notación compacta se extiende en forma evidente a estados de N qubits.

Estados enredados

El siguiente ejemplo, restringido a sistemas de dos qubits, permite introducir los estados enredados. Supongamos que contamos con dos qubits en estados

$$|\phi_1\rangle = a|0\rangle + b|1\rangle \qquad |\phi_2\rangle = c|0\rangle + d|1\rangle.$$

De acuerdo con el Postulado I, el estado del sistema conjunto es el producto tensorial

$$|\Phi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle = ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle. \tag{A.47}$$

El estado $|\Phi\rangle$ es un **estado producto**, ya que se puede expresar como el producto tensorial de dos estados de un qubit. Como veremos, esto es exepcional. La mayoría de los estados de $\mathcal{H}_2$ no son expresables como un producto de estados de un qubit. Es fácil verificar que la condición necesaria y suficiente para que un estado genérico de $\mathcal{H}_2$, tal como (A.42), sea un estado producto, es

$$\alpha\delta = \beta\gamma. \tag{A.48}$$

Los estados como (A.42) que no son estados producto, $\alpha\delta \neq \beta\gamma$ se denominan **estados enredados** (entangled states). Un conjunto importante de estados enredados son los llamados estados de Bell,

$$\begin{aligned} |\Phi^{\pm}\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle \pm |11\rangle\right) \\ |\Psi^{\pm}\rangle &= \frac{1}{\sqrt{2}}\left(|01\rangle \pm |10\rangle\right) \end{aligned} \tag{A.49}$$

que forman una base ortonormal en $\mathcal{H}_2$. En estos estados, no es posible asignar estados individuales a cada qubit. Al medir, los resultados de las medidas de ambos qubits están máximamente correlacionados.

Por muchos años, los estados de éste tipo han tenido un interés vinculado a las bases de la Mecánica Cuántica. La paradoja EPR (Einstein-Podolsky-Rosen) se formuló en términos de estados enredados y las desigualdades de Bell refieren a cotas superiores que deben satisfacer las correlaciones entre las medidas de cada qubit, de acuerdo a una descripción realista local. La Mecánica Cuántica predice que este tipo estados viola las desigualdades de Bell. Estas predicciones se han visto confirmadas en una larga serie de experimentos que comienza en la década del 70 y llega hasta nuestros dias. Actualmente, el principal interés de los estados enredados esta vinculado a su rol esencial en el procesamiento cuántico de la información (vea el Apéndice B).

A.4.3. Generalización a n qubits

Para representar el número 15 se requieren 4 bits ($2^4 - 1 = 15$). De la misma forma, en una computadora cuántica son necesarios 4 qubits para

representar este número. Sin embargo, con 4 qubits podemos construir estados como $\sum_{n=0}^{1} 4|n\rangle$, una superposición de estados de 4 qubits expresada en notación compacta. Este estado representa de algún modo a todos los enteros entre 0 y 14. En general, con n qubits podemos expresar todos los enteros no negativos menores que $2^n - 1$. Cualquier algoritmo de alguna utilidad debe tratar con sistemas de n qubits. Se estima que una máquina cuántica que supere a sus contrapartes clásicas en tareas realistas, deberá manejar registros con cientos de qubits[10]...

El espacio de Hilbert para n qubits tendrá dimensión 2^n. Es decir que la dimensión del espacio crece *exponencialmente* con el número de qubits, lo cual hace rápidamente inmanejable la simulación de un problema cuántico en una máquina clásica. Por ejemplo, un problema que requiera 100 qubits implica trabajar en un espacio vectorial de dimensión $2^{100} \approx 10^{30}$, generado a partir del producto tensorial de los espacios de 1 qubit, $\mathcal{E}_n = \mathcal{H}_1^{\otimes n}$. Un ket de la base computacional de este espacio es de la forma $|010\ldots110\rangle$, con n dígitos binarios o $|m\rangle$ con $m \in [0, 2^n - 1]$, en notación compacta. La base computacional se compone de los 2^n kets de n qubits

$$|0\rangle, |1\rangle, |2\rangle \ldots |2^n - 1\rangle$$

y un ket genérico (normalizado) de $\mathcal{H}_n$ se representa por

$$|\Psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle \qquad \text{con} \sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1.$$

A.5. Medidas generalizadas

Como mencionamos antes, el formalismo de medidas proyectivas tiene limitaciones y no es adecuado para describir muchas de las interacciones de interés en el procesamiento cuántico de la información. En esta Sección describimos el formalismo de medidas generalizadas, que incluye a las medidas proyectivas como un caso especial. La discusión se basa en [NC00]. Las medidas proyectivas, con el agregado de operaciones unitarias, pasan a ser equivalentes a las medidas generalizadas.

Una medida generalizada se describe por un conjunto de operadores de medida $\{M_m\}$ que actúan en el espacio de estados $\mathcal{H}$ del sistema a medir.

[10] Hasta el momento, se han logrado construir dispositivos de laboratorio que operan, por tiempo limitado, con menos de 10 qubits.

Los posibles resultados de la medida se etiquetan con el índice discreto m. Si el sistema esta en un estado $|\Psi\rangle$ antes de la medida, la probabilidad de observar el resultado m es

$$p_m = \langle\Psi|M_m^\dagger M_m|\Psi\rangle \tag{A.50}$$

Las probabilidades deben cumplir $\sum_m p_m = 1$, de modo que se exige que los operadores de medida satisfagan la condición de completitud,

$$\sum_m M_m^\dagger M_m = I. \tag{A.51}$$

El estado después de una medida con resultado m es

$$|\Psi\rangle \rightarrow |\Psi'\rangle = \frac{M_m|\Psi\rangle}{\sqrt{p_m}}. \tag{A.52}$$

Evidentemente, si los operadores de medida son los proyectores en los subespacios propios de un observable, $M_m = P_m = |m\rangle\langle m|$, el formalismo se reduce al caso de medidas proyectivas[11].

Este formulismo suele utilizarse en el contexto más general de operador densidad. Si el estado (puro o mezcla) se describe en términos de ρ, la probabilidad de medir m es

$$p_m = tr(M_m \rho M_m^\dagger) \tag{A.53}$$

y, luego de la medida, el estado normalizado es

$$\rho \rightarrow \rho' = \frac{M_m \rho M_m^\dagger}{tr(M_m \rho M_m^\dagger)}. \tag{A.54}$$

Este formalismo incluye la posibilidad de aplicar una operación unitaria U como una medida con una única posibilidad de resultado. Si definimos $M_1 = U$, con $U^\dagger U = I$, el estado subsiguiente es

$$\rho' = U\rho U^\dagger$$

ya que la operación unitaria preserva la traza, $tr(U\rho U^\dagger) = tr(\rho) = 1$. Como se mencionó anteriormente, las medidas proyectivas más las operaciones unitarias son equivalentes a una medida generalizada.

A.6. Operaciones Cuánticas

FALTA – ver lo necesario para la parte de decoherencia.

[11] Para un proyector $P_m^\dagger P_m = P_m^2 = P_m$.

Apéndice B

Algunas aplicaciones que consumen enredo

Este Apéndice contiene una descripción breve de dos tareas que requieren (y consumen) cierta cantidad de enredo para ser llevadas a cabo. Esta adaptado del Cap. 4 del material de apoyo para el curso de Computación Cuántica [AS04] que se dicta (en modalidades de grado y posgrado) en la Facultad de Ingeniería.

B.1. Codificado denso

La primer aplicación tiene que ver con la posibilidad de enviar dos bits de información transmitiendo físicamente un único qubit. Esta posibilidad, que requiere de estados enredados, fue propuesta por Bennet y otros [Ben92] y realizada experimentalmente en 1996 [Mat96].

La idea básica es sencilla. Alicia quiere comunicar 2 bits de información clásica a Bob, pero le puede enviar físicamente un solo qubit. Si Alicia y Bob disponen en conjunto de un e-bit[1] de enredo (esto es, comparten previamente un estado máximamente enredado de dos qubits), la tarea puede hacerse, pero el e-bit es consumido en el proceso. Es decir, el codificado denso consume un e-bit por cada 2 bits de información enviado.

Supongamos que el estado de Bell

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left[|00\rangle + |11\rangle\right]$$

[1] El e-bit, o entanglement bit, es la unidad de enredo. Un e-bit equivale al enredo de un par de qubits máximamente enredados, como en los estados de Bell.

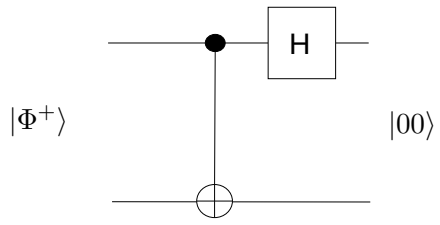

Figura B.1: Circuito usado por Bob para decodificar la información de los estados de Bell. H representa una transformación de Hadamard y el símbolo $\oplus$ representa una operación CNOT sobre el segundo qubit, controlada por el primero. Alimentado por un estado de Bell, se obtiene un estado producto $|ab\rangle$, con a, b binarios, de acuerdo a lo indicado en la tabla más abajo.

es compartido, de modo que Alicia tiene el primer qubit y Bob el segundo[2]. Alicia implementa una de cuatro operaciones unitarias sobre su qubit y luego se lo envía a Bob, quien realiza una medida de ambos qubits en su poder para determinar que estado de Bell tiene. A partir de ello, Bob obtiene los dos bits información que le envió Alicia. Alicia y Bob solo intercambiaron UN qubit.

Los detalles se muestran en la siguiente tabla, donde σ_i representan matrices de Pauli,

Para transmitir	Alicia aplicó	Bob tiene
00	$I\|\Phi^+\rangle$	$\|\Phi^+\rangle = (\|00\rangle + \|11\rangle)/\sqrt{2}$
01	$\sigma_x\|\Phi^+\rangle$	$\|\Psi^+\rangle = (\|10\rangle + \|01\rangle)/\sqrt{2}$
10	$\sigma_z\|\Phi^+\rangle$	$\|\Phi^-\rangle = (\|00\rangle - \|11\rangle)/\sqrt{2}$
11	$i\sigma_y\|\Phi^+\rangle$	$\|\Psi^-\rangle = (\|01\rangle - \|10\rangle)/\sqrt{2}$

Resta mencionar un aspecto del problema: si Bob mide sus qubits en la base computacional, la medida no le revela que estado de Bell tenía. Antes, debe desenredar sus qubits usando el circuito de la figura B.1. Con el, Bob puede transforma cada estado de Bell en uno de los estados producto de la base computacional. Midiendo ambos qubits a la salida de éste circuito, Bob obtiene directamente los valores binarios x, y enviados por Alicia. Para acceder a la información, Bob debe necesariamente destruir el par enredado y consume el e-bit.

[2]Después de establecido el enredo, Alicia y Bob pueden estar cada uno con su qubit separados por una distancia arbitraria.

B.2. Teleportación

La Teleportación es un protocolo para reproducir un estado de un qubit a través de una distancia arbitraria. El proceso requiere de un canal clásico de comunicación y por lo tanto esta limitado por la velocidad de la luz. Los recursos necesarios son: un estado de Bell compartido entre el emisor y el receptor, un canal clásico de comunicación con capacidad de 2 bits (esto es lo que limita la velocidad del proceso) y el qubit que se desea teleportar que es destruido en el proceso. El protocolo consume un e-bit de enredo por qubit teleportado.

La Teleportación cuántica fue propuesta por C. Bennet y colaboradores en 1993 [BBC$^+$93] y realizada experimentalmente por primera vez en 1997 usando qubits codificados en fotones polarizados [BPM$^+$97]. En el 2004, se realizó experimentalmente con trampas de iones usando átomos de Calcio y Berilio [BCS$^+$04, RHR$^+$04]. El qubit lógico que se teleporta puede estar codificado en sistemas físicos bien diferentes. Por ejemplo, muy recientemente se ha usado la teleportación para transferir información codificada en un pulso luminoso que llega por una fibra óptica hacia un qubit codificado en un ensemble de $\sim 10^{12}$ átomos de Cesio [SKO$^+$06]. La información codificada en fotones es útil para un transporte rápido, en tanto que codificada en ensembles mesoscópicos de materia, puede servir como memoria permanente. Este tipo de experimentos ya están siendo realizados [JSC$^+$04].

El emisor Alicia y el receptor Bob comparten previamente cada uno de los qubits de un estado de Bell, es decir disponen de una reserva de enredo de 1 e-bit. Digamos que Alicia tiene el primer qubit y Bob el segundo. Bob se aleja a una distancia arbitraria, pero manteniendo abierta una línea de comunicación clásica. Alicia dispone de un qubit $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ que desconoce y que desea teleportar a Bob[3]. Alicia enreda su qubit $|\Psi\rangle$ con su parte del estado de Bell compartido con Bob y luego mide los dos qubits en su poder. La medida de Alicia afecta instantáneamente el qubit de Bob y es en éste proceso instantáneo, donde la información del qubit $|\Psi\rangle$ pasa a Bob a través de las correlaciones cuánticas. Después de la medida de Alicia, la información del qubit $|\Psi\rangle$ ya esta codificada en el qubit de Bob, pero el no tiene acceso a ella. Alicia envía el resultado de su medida (2 bits) por el

[3]Si Alicia intenta medir su qubit para obtener información de α y β lo destruye sin lograrlo. Incluso si Alicia supiera los valores de α y β, para enviarlos a Bob por un canal clásico perfecto, requeriría un canal con capacidad infinita, ya que son variables continuas.

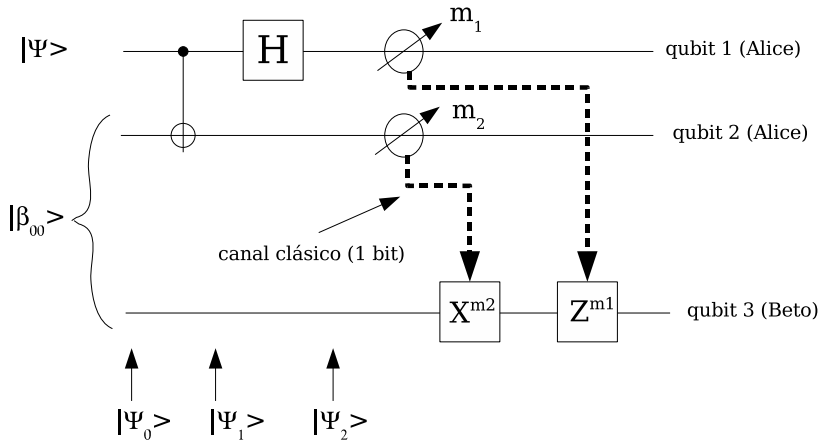

Figura B.2: Circuito para teleportación del estado $|\Psi\rangle$. Detalles en el texto.

canal clásico a Bob. Con esa información, Bob aplica una operación unitaria adecuada a su parte del estado de Bell y reconstruye $|\Psi\rangle$.

Esto se puede hacer con el circuito que se muestra en la Figura B.2 donde los dos canales superiores corresponden a los dos qubits de Alice y el inferior al qubit en poder de Bob. Se supone que el estado de Bell compartido es $|\Phi^+\rangle = \frac{1}{\sqrt{2}}[|00\rangle + |11\rangle]$, con el primer qubit está en poder de Alicia y el segundo en poder de Bob. Estos dos qubits corresponden a los canales medio e inferior en la Figura B.2. Inicialmente, el estado es

$$|\Psi_0\rangle = |\Psi\rangle \otimes |\Phi^+\rangle \tag{B.1}$$

donde $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ (en el canal superior en la Figura B.2) es el qubit que Alicia desea teleportar a Bob. El proceso se realiza en 4 pasos:

1. Alicia enreda el qubit $|\Psi\rangle$ con el estado de Bell compartido, aplicando una compuerta CNOT al qubit compartido controlada por el qubit a teleportar. El resultado de esta operación es

$$|\Psi_1\rangle = \alpha|0\rangle \otimes |\Phi^+\rangle + \beta|1\rangle \otimes |\Psi^+\rangle. \tag{B.2}$$

   donde $|\Psi^+\rangle = \frac{1}{\sqrt{2}}[|01\rangle + |10\rangle]$.

2. Ahora Alicia aplica una operación de Hadamard sobre el qubit a tele-

portar,

$$\begin{aligned} |\Psi_2\rangle &= \frac{1}{\sqrt{2}}\left[\alpha\left(|0\rangle+\beta|1\rangle\right)\otimes|\Phi^+\rangle+\beta\left(|0\rangle-|1\rangle\right)\otimes|\Psi^+\rangle\right] \\ &= \frac{1}{2}\left[|00\rangle\otimes(\alpha|0\rangle+\beta|1\rangle)+|01\rangle\otimes(\alpha|1\rangle+\beta|0\rangle)+\right. \\ &\qquad \left.|10\rangle\otimes(\alpha|0\rangle-\beta|1\rangle)+|11\rangle\otimes(\alpha|1\rangle-\beta|0\rangle)\right]. \quad \text{(B.3)} \end{aligned}$$

3. Alicia mide los dos qubits que están en su poder, lo cual afecta instantáneamente al qubit de Bob, debido al enredo presente en (B.2). En la segunda forma, es evidente que el resultado de la medida de Alicia esta correlacionado con el estado de Bob (luego de la medida de Alicia), como se indica en la tabla (las operaciones X, Y, Z refieren a las matrices de Pauli):

Caso	Alicia mide	Bob tiene	Bob aplica	Bob obtiene
1	$\|00\rangle$	$\alpha\|0\rangle+\beta\|1\rangle$	$\mathbf{I}$	$\|\Psi\rangle$
2	$\|01\rangle$	$\alpha\|1\rangle+\beta\|0\rangle$	X	$\|\Psi\rangle$
3	$\|10\rangle$	$\alpha\|0\rangle-\beta\|1\rangle$	Z	$\|\Psi\rangle$
4	$\|11\rangle$	$\alpha\|1\rangle-\beta\|0\rangle$	Y	$\|\Psi\rangle$

4. Alice comunica a Bob el resultado de su medida por un canal clásico y Bob aplica una operación unitaria, dependiente de esta información, en su qubit.

   Si el resultado de la medida de Alicia es $|00\rangle$ (el caso 1 de la tabla), entonces Bob no necesita hacer nada. En los otros casos, puede obtener $|\Psi\rangle$ aplicando transformaciones unitarias sobre su qubit. Sin embargo, pese a que Bob ya dispone de la información codificada en su qubit, es necesario que Alicia le comunique el resultado de su medida para que el pueda operar en consecuencia y acceder a ella. Este paso requiere el envío de dos bits por un canal clásico y el proceso queda limitado por la velocidad de la luz.

El qubit originalmente en manos de Alicia fue destruido en el proceso, de modo que en la teleportación no se *copia* sino que se *mueve* el estado lógico $|\Psi\rangle$.

Bibliografía

[ADF06a] G. Abal, R. Donangelo, and H. Fort. Long-time entanglement in the quantum walk. In *Anales del 1er Workshop-escola de Computación Cuántica*, pages 189–200. Esc. Inf. UCPel, Pelotas, RGS, Brazil, 2006, versión on-line http://ppginf.ucpel.tche.br/weciq/CD.

[ADF06b] G. Abal, R. Donangelo, and H. Fort. On quantum walk and iterated quantum games. In *Anales del 1er Workshop-escola de Computación Cuántica*, pages 201–210. Esc. Inf. UCPel, Pelotas, RGS, Brazil, 2006, versión on-line http://ppginf.ucpel.tche.br/weciq/CD.

[ADF07] G. Abal, R. Donangelo, and H. Fort. Conditional quantum walk and iterated quantum games. *sometido a J. Quant. Inf. Proc.*, 2007, preprint quant-ph/0607143.

[ADRS06] G. Abal, R. Donangelo, A. Romanelli, and R. Siri. Effects of non-local initial conditions in the quantum walk on the line. *Phys. A*, 371:1–4, 2006, eprint quant-ph/0602188.

[ADZ93] Y. Aharonov, L. Davidovich, and N. Zagury. *Phys. Rev. A*, 48:1687, 1993.

[Amb03] A. Ambainis. Quantum walk algorithm for element distinctness. 2003, preprint quant-ph/0311001.

[Amb05] A. Ambainis. Quantum search algorithms. 2005, preprint quant-ph/0504012.

[AS04] G. Abal and R. Siri. Introducción al procesamiento cuántico de la información. Instituto de Fí-

sica, Facultad de Ingeniería, 2004, Disponibles en http://www.fing.edu.uy/if/cursos/qcomp/extras/notas/qm3.pdf.

[AS06] G. Abal and F. Severo. Quantum walk with spin-flip channel noise. poster en el 1^{er} Workshop-escola de Computación Cuántica, Esc. Inf. UCPel, Pelotas, RGS, Brazil, 9-11 octubre 2006, 2006.

[ASRR06] G. Abal, R. Siri, A. Romanelli, and Donangelo R. Quantum walk on the line: entanglement and initial conditions. *Phys. Rev. A*, 73:042302, 069905(E), 2006, preprint quant-ph/0507264.

[BB84] C.H. Bennet and G. Brassard. Quantum cryptography: public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179. IEEE, New York, 1984.

[BBC+93] C. Bennet, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W.K. Wooters. Teleporting an unknown state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70:1895, 1993.

[BCA03a] T. Brun, H.A. Carteret, and A. Ambainis. Quantum random walks with decoherent coins. *Phys. Rev. A*, 67:032304, 2003, eprint quant-ph/0210180.

[BCA03b] T.A. Brun, H.A. Carteret, and A. Ambainis. Quantum random walks with decoherent coins. *Phys. Rev. A*, 67:032304, 2003, arXiv preprint quant-ph/0210180.

[BCS+04] M.D. Barrett, J. Chiaverini, T. Schaetz, J. Britton, W.M. Itano, J.D. Jost, E. Knill, C. Langer, D. Leibfried, R. Ozeri, and D.J. Wineland. Deterministic quantum teleportation of atomic qubits. *Nature*, 429:738, 2004.

[BDCZ98] H.J. Briegel, W. Dür, J.I. Cirac, and P. Zoller. Quantum repeaters: the role of imperfect local operations in quantum communication. *Phys. Rev. Lett.*, 81:5932, 1998.

[Ben92] S.J. Bennet, C. y Wiesner. Communication via one and two–particle operators on epr states. *Phys. Rev. Lett.*, 69:2881, 1992.

[BHMT02] G. Brassard, P. Hoyer, M. Mosca, and A. Tapp. Quantum amplitude estimation and amplification. *Contemp. Math.*, 305:53–74, 2002.

[Bor57] M. Born. *Atomic Physics*. Hafner, 1957.

[BPM+97] D. Bouwmeester, J. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger. Experimental quantum teleportation. *Nature*, 390:575, 1997.

[CCD+03] A.M. Childs, R. Cleve, E. Deotto, E. Farhi, S. Gutmann, and D. A. Spielman. Exponential algorithmic speedup by quantum walk. In *Proc. 35th ACM Symposium on Theory of Computing (STOC 2003)*, pages 59–68, 2003, preprint quant-ph/0209131.

[CFG02] A.M. Childs, E. Fahri, and S. Gutmann. An example of the difference between quantum and classical random walks. *Quant. Inf. Proc.*, 1:35, 2002, preprint quant-ph/.

[CG04] A. M. Childs and J. Goldstone. Spatial search by quantum walk. *Phys. Rev. A*, 70:022314, 2004, preprint quant-ph/0306054.

[CH06] K. Chen and T. Hogg. How well do people play a quantum Prisioner's Dilemma? *Quant. Inf. Proc.*, 5:43–67, 2006.

[CHB03] K. Chen, T. Hogg, and R. Beausoleil. A practical mechanism for the public goods game. *Quant. Inf. Proc.*, 1:449–469, 2003.

[ClX+05] I. Carneiro, M. loo, X. Xu, M. Gerard, V. Kendon, and P. Knight. Entanglement in coined quantum walks on regular graphs. *New J. Phys.*, 7:156, 2005, preprint quant-ph/0504042.

[Coo71] S. Cook. The complexity of theorem-proving procedures. In *Proc. 3rd Ann. ACM Symp. on theory od Computing*, pages 151–158. Association of Computer Machinery, ACM, New York, 1971.

[DHR02] M.J. Donald, M. Horodecki, and O. Rudolph. The uniqueness theorem for entanglement measures. *J. Math. Phys.*, 43:4252, 2002, quant-ph/0105017.

[DJ92] D. Deutsch and R. Josza. Rapid solution of problems by quantum computation. *Proc. Roy. Soc. London A*, pages 439–553, 1992.

[DKB02] W. Dür, V.M. Kendon, and H.J. Briegel. Quantum random walks in optical lattices. *Phys. Rev. A*, 66:052319, 2002, arXiv preprint quant-ph/052319.

[DLS+03] J. Du, H. Li, M. Shi, J. Wu, X. Zhou, and R. Han. Experimental implementation of the quantum random-walk algorithm. *Phys. Rev. A*, 67:042316, 2003.

[DLX+03] J Du, H. Li, X. Xu, M. Shi, J. Wu, X. Zhou, and R. Han. Experimental implementation of the quantum random-walk algorithm. *Phys. Rev. A*, 67:042316, 2003, preprint quant-ph/0203120.

[DSB+05] B. Do, M.L. Stohler, S. Balasubramanian, D.S. Elliot, C. Eash, E. Fischbach, M.A. Fischbach, and A. Mills. Experimental realization of a quantum quincux by use of linear optical elements. *J. Opt. Soc. Am. B*, 22:499–504, 2005.

[DXZH02] J. Du, X. Xu, X. Zhou, and R. Han. Playing the prisioner's dilemma with quantum rules. *Fluct. Noise Lett.*, 2, 2002, e-print quant-ph/0301042.

[Eke91] A. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67:661, 1991.

[EMBL05] K. Eckert, J. Mompart, G. Birkl, and M. Lewenstein. One- and two-dimensional quantum walks in arrays of optical traps. 2005, arXiv preprint quant-ph/0503084.

[EWL99a] J. Eisert, M. Wilkens, and M. Lewenstein. Quantum games and quantum strategies. *Phys. Rev. Lett.*, 83:3077, 1999.

[EWL99b] J. Eisert, M. Wilkens, and M. Lewenstein. Quantum games and quantum strategies. *Phys. Rev. Lett.*, 83:3077, 1999.

[Fey82] R.P. Feynman. Simulating physics with computers. *Int. J. Theor. Phys.*, 21:467, 1982.

[Fey86] R.P. Feynman. Quantum mechanical computers. *Found. Phys.*, 16:507–531, 1986.

[FG98] E. Fahri and S. Gutmann. Quantum computation and decision trees. *Phys. Rev. A*, 58:915–928, 1998.

[Flo52] M. Flood. Some experimental games. Research Memorandum RM-789, RAND Corporation, 1952.

[FSMDZ06] M. Franca-Santos, P. Milman, L. Davidovich, and N. Zagury. Direct measurement of finite-time disentanglement induced by a reservoir. *Phys. Rev. A*, 73:040305(R), 2006.

[GC99] D. Gottesman and I.L. Chuang. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature*, 402:390, 1999.

[Gj99] M.R. Garey and D.S. johnson. *A guide to the theory of NP-Completeness*. Freeman and Co., Mew York, 1999.

[Gro96] L. Grover. In *Proc. 28th ACM Symposium in the Theory of Computation*, pages 212–219. ACM Press, New York, 1996.

[Gro97] L.K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.*, 79:325, 1997, preprint quant-ph/9706033.

[Hal01] S. Hallgreen. *Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem*. 34th Ann. Symp. on Theory of Computing, Assoc. of Computing Machinery, ACM Press, New York, 2001.

[HHH96] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of mixed states: necesary and sufficient conditions. *Phys. Rev. Lett.*, 223:8, 1996.

[Hug04] R. Hughes. A quantum information science and technology roadmap. 2004, http://qist.lanl.gov/qcomp-map.shtml.

[J.K03] J.Kempe. Quantum random walks hit exponentially faster. In *Proc. of 7th Intern. Workshop on Randomization and Approximation Techniques in Comp. Sc. (RANDOM'03)*, pages 354–69, 2003, eprint quant-ph/0205083.

[JPK04] H. Jeong, M. Paternostro, and M.S. Kim. Simulation of quantum random walks using the interference of a classical field. *Phys. Rev. A*, 69:012310, 2004.

[JSC$^+$04] B. Julsgaard, J. Sherson, I. Cirac, J. Fiurasek, and E.S. Polzik. Experimental demonstration of quantum memory for light. *Nature*, 432:487, 2004.

[Kem03] J. Kempe. Quantum random walks - an introductory overview. *Contemp. Phys.*, 44:307, 2003, preprint quant-ph/0303081.

[Ken06] V. Kendon. Decoherence in quantum walks – a review. 2006, preprint quant-ph/0606016.

[KK89] D. Kraines and V. Kraines. *Theory Decision*, 26:47, 1989.

[KLM01] E. Knill, R. Laflamme, and G.J. Milburn. A scheme for efficient quantum computation with linear optics. 409:46–52, 2001.

[KNS04] N. Konno, T.Ñamiki, and T. Soshi. Symmetry of distribution for the one-dimensional hadamard walk. *Interdisciplinary Information Science*, 10:11–22, 2004.

[Kon02a] N. Konno. *Quant. Inf. Process*, 1:345, 2002, quant-ph/0206053.

[Kon02b] N. Konno. *J. Quant. Inf. Proc.*, 1:345, 2002, quant-ph/0206053.

[KRS03a] P.L. Knight, E. Roldán, and J.E. Sipe. Optical cavity implementations of the quantum walk. *Op. Comm.*, 227:147–157, 2003.

[KRS03b] P.L. Knight, E. Roldán, and J.E. Sipe. Quantum walk on the line as an interference phenomenon. *Phys. Rev. A*, 68:020301(R), 2003.

[KT03] V. Kendon and B. Tregenna. Decoherence can be useful in quantum walks. *Phys. Rev. A*, 67:042315, 2003, eprint quant-ph/0209005.

[LMP00] C. Lavor, L.R.U Manssur, and R. Portugal. Grover's algorithm: quantum database search. 2000, eprint quant-ph/0301079.

[LP03] C.C. López and J.P. Paz. Decoherence in quantum walks: existence of a quantum-classical transition. *Phys. Rev. A*, 68:052305, 2003, eprint quant-ph/0308104.

[Mat96] K. Mattle. Dense coding in experimental quantum communication. *Phys. Rev. Lett.*, 76:4656, 1996.

[MdRT+04] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, M. Legré, and N. Gisin. Distribution of time-bin entangled qubits over 50 km of optical fiber. *Phys. Rev. Lett.*, 93:180502, 2004.

[Men00] M.B. Mensky. *Quantum Measurements and Decoherence*. Kluwer Academic Publishers, Dordrecht, Alemania, 2000.

[Mey99] D. Meyer. Quantum strategies. *Phys. Rev. Lett.*, 82:1052–1055, 1999.

[MKB05] F. Mintert, M. Kus, and A. Buchleitner. Concurrence of mixed multi-partite quantum states. *Phys. Rev. Lett.*, 95:260502, 2005.

[MR96] R. Motwani and P. Raghavan. *Randomized Algorithms*. Cambridge University Press, Cambridge, 1996.

[MR01] C. Moore and A. Russell. Quantum walks on the hypercube. 2001, preprint quant-ph/0104137.

[MZG96] A. Muller, H. Zbinden, and N. Gisin. Quantum cryptography over 23 km in installed under-lake telecom fibre. *Europhys. Lett.*, 33:334, 1996.

[Nas50] J.F. Nash. In *Porc. Natl. Acad. Sci. USA*, volume 36, pages 48–49, 1950.

[NC00] M.A. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 2000.

[NV] A.Ñayak and A. Vishwanath. Quantum walk on the line. preprint quant-ph/0010117.

[OPD06] A.C. Oliveira, R. Portugal, and R. Donangelo. Decoherence in two-dimensional quantum walks. *Phys. Rev. A*, 74:012312, 2006.

[OPSB] Y. Omar, N. Paunkovic, L. Sheridan, and S. Bose. Quantum walk on a line with two entangled particles. arXiv preprint quant-ph/0411065.

[OPW+03] J.L. O'Brien, G.J. Pryde, A.G. White, T.C. Ralph, and D. Branning. Demonstration of all-optical quantum controlled not gate. 426:264, 2003.

[PA06] P.K. Pathak and G.S. Agarwal. Quantum random walk of two entangled qubits. 2006, arXiv preprint quant-ph/0604138.

[Pat07] N. Patel. States of play. *Nature*, 445:144, 2007.

[PBZ+05] C. Peng, X. Bao, J. Zhang, X. Jin, F. Feng, B. Yang, and J. Yang. Experimental free-space distribution of entangled photon pairs over 13 km: towards satellite-based global quantum communication. *Phys. Rev. Lett.*, 94:150501, 2005.

[RAD06] A. Romanelli, A. Auyuanet, and R. Donangelo. Quantum search with resonances. *Phys. A*, 360:274–284, 2006.

[Rei65] F. Reif. *Fundamentals of Statistical and Thermal Physics*. McGraw–Hill Book Co., New York, 1965.

[RHR+04] M. Riebe, H. Haffner, C. F. Roos, W. Hansel1, J. Benhelm, G.P.T. Lancaster, T. W. Korber, C. Becher, F. Schmidt-Kaler, D.F.V. James, and R. Blatt. Deterministic quantum teleportation with atoms. *Nature*, 429:734, 2004.

[RLBL05] C.A. Ryan, M. Laforest, J.C. Boileau, and R. Laflamme. Experimental implementation of discrete time quantum random

walk on an nmr quantum information processor. *Phys. Rev. A*, 72:062317, 2005, preprint quant-ph/0507267.

[RSA+04] A. Romanelli, R. Siri, G. Abal, A. Auyuanet, and R. Donangelo. Decoherence in the quantum walk on the line. *Phys. A*, 347:137–152, 2004, preprint quant-ph/0403192.

[RSAD03] A. Romanelli, R. Siri, G. Abal, and R. Donangelo. Markovian behaviour and constrained maximization of the entropy in chaotic quantum systems. *Phys. Lett. A*, 313:325–329, 2003, preprint quant-ph/0204135.

[RSSS+04] A. Romanelli, A. C. Sicardi Schifino, R. Siri, G. Abal, A. Auyuanet, and R. Donangelo. Quantum walk on the line as a markovian process. *Phys. A*, 338:395–405, 2004, e-print quant-ph/0310171.

[SB03] B.C. Sanders and S.D. Bartlett. Quantum quincux in cavity quantum electrodynamics. *Phys. Rev. A*, 67:042305, 2003, arXiv preprint quant-ph/0207028.

[SBBH03] D. Shapira, O. Biham, A.J. Bracken, and M. Hackett. One-dimensional quantum walk with unitary noise. *Phys. Rev. A*, 68:062315, 2003, eprint quant-ph/0309063.

[Sch99] U. Schöning. A probabilistic algorithm for k-sat and constraint satisfaction problems. In *40th Ann. Symp. Found. Comp. Sci.*, page 410. IEEE, 1999.

[Sho97] P.W. Shor. Polynomial–time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comp.*, page 1484, 1997.

[SKO+06] J.F. Sherson, H. Krauter, R.K. Olsson, B. Julsgaard, K. Hammerer, I. Cirac, and E.S. Polzik. Quantum teleportation between light and matter. *Nature*, 443:557, 2006.

[SKW03] N. Shenvi, J. Kempe, and B. Whaley. Quantum random walk search algorithm. *Phys. Rev. A*, 67:052307, 2003, eprint quant-ph/0210064.

[SM95] J. Schlientz and G. Mahler. Description of entanglement. *Phys. Rev. A*, 52:4396, 1995.

[Str06] F.W. Strauch. *Phys. Rev. A*, 74:030301 (R), 2006, preprint quant-ph/0606050.

[TFMK03] B. Tregenna, W. Flannagan, R. Maile, and V. Kendon. Controlling discrete quantum walks: coins and intitial states. *New. J. Phys.*, 5:83, 2003, preprint quant-ph/0304204.

[TM02] B. Travaglione and G. Milburn. *Phys. Rev. A*, 65:032310, 2002.

[Urs06] R. et al. Ursin. Free-space distribution of entanglement and single photons over 144 km. 2006, eprint quant-ph/0607182.

[VPRK98] V. Vedral, M.B. Plenio, M.A. Rippin, and P.L. Knight. Entanglement measures and purification procedures. *Phys. Rev. A*, 57:1619, 1998.

[VW02] G. Vidal and R.F. Werner. Computable measure of entanglement. *Phys. Rev. A*, 65:032314, 2002.

[Woo98] W. K. and Wootters. Entanglement of formation of an arbitrary state of two qubits. *Phys. Rev. Lett.*, 80:2245–2248, 1998.

[WSRD+06] S. P. Walborn, P. H. Souto Ribeiro, L. Davidovich, F. Mintert, and A. Buchleitner. Experimental determination of entanglement with a single measurement. *Nature*, 440:1022, 2006.

[YZC+06] T. Yang, Q. Zhang, T. Chen, S. Lu, J. Yin, J. Pan, Z. Wei, Z. Tian, and J. Zhang. Experimental synchronization of independent entangled photon sources. *Phys. Rev. Lett.*, 96:110501, 2006.

[ZDY+02] Z. Zhao, J. Du, H.L. Yang, Z. Chen, and J. Pan. Implement quantum random walks with linear optics elements. 2002, arXiv preprint quant-ph/0212149.

[Zur03] W.H. Zurek. Decoherence, einselection and the quantum origins of the classical. *Rev. Mod. Phys.*, 75:715–775, 2003.

Las referencias al archivo bibliográfico Los Alamos se acceden por la ruta http://lanl.arxiv.org/abs/quant-ph/xxxxxxx