Extensión de Cantidades Clásicas a la Teoría de la Información Cuántica

Proyecto de Grado

Laura Marcela Guzmán Rincón
Director: Alonso Botero Mejía

Departamento de Física
Facultad de Ciencias
Universidad de Los Andes

Mayo 2011

Extensión de Cantidades Clásicas a la Teoría de la Información Cuántica

Proyecto de grado para optar al título de Física

Dirigida por: Alonso Botero Mejía

Departamento de Física
Facultad de Ciencias
Universidad de Los Andes

Mayo 2011

A mi mami,
a mi Carino, a mi Juanpis,
a mumitis y a mis abuelitos

Agradecimientos

Primero agradezco a Alonso Botero por asesorar este proyecto y ser parte sustancial de su desarrollo y culminación. Agradezco a la Universidad de Los Andes y al Programa Quiero Estudiar por permitirme acceder a la educación superior de calidad y brindarme los conocimientos necesarios para realizar mis proyectos y, a futuro, aportar al país. Agradezco a mi mami, que su incondicional apoyo ha hecho que mi vida tome el rumbo que he elegido, agradezco por siempre apoyarme sobre todas las cosas y querernos infinitamente. Te quiero mucho! Agradezco a mis hermanos Juanpis y Carol por compartir mi vida y ser parte fundamental de ella, porque en cada día es una fortuna recordar que los tengo, a mumitis, al papacito y a la mamita por su incondicional apoyo y permanente entrega en todos los proyectos que vamos teniendo. Agradezco a las personas con las que he compartido mi tiempo en la Universidad. A Juani porque ha sido mi compañera y sobre todo amiga desde el primer día que llegué a la Universidad. A todos los demás que ellos saben que son parte importante de esta étapa de la vida y siempre los tendré en los mejores recuerdos. Agradezco a los poderes que están fuera de mi alcance por darme tantas oportunidades y ayudarme a tener éxito en los proyectos que me he propuesto en la vida.

Resumen

La teoría de la información cuántica se ha desarrollado como una extensión de su contraparte clásica, extendiendo los conceptos clásicos a un excenario regido por las propiedades de la mecánica cuántica. Se presenta entonces, una revisión de los conceptos fundamentales en la teoría de la información clásica y los teoremas que caracterizan el procesamiento de la información. Luego, se introduce la entropía de von Neumann como una extensión de la entropía de Shannon que caracteriza la información proveniente de una fuente. Posteriormente se derivan las demás cantidades clásicas sustituyendo directamente la entropía de Shannon por la entropía de von Neumann. Por último se presenta una medida que caracteriza el enredamiento de un estado cuántico.

Índice

Índice de figuras

Capítulo 1

Introducción

La Teoría de la Información tiene como objetivo el estudio de la información y lo concerniente a su almacenamiento y procesamiento. A mediados del siglo XX Claude E. Shannon introduce la entropía como una cantidad que cuantifica la información, a partir de la cuál inicia el desarrollo de la teoría. Posteriormente se introducen nuevas cantidades que permiten la formulación rigurosa de la teoría y no carecen de interpretación en términos de procesos. La información proveniente de una fuente, el envío de datos a través de canales y la posibilidad de comprimir son algunos de los avances que la teoría de la información a logrado durante su desarrollo. Asimismo, a partir de los resultados que se han obtenido son múltiples las aplicaciones en computación y criptografía, entre otros campos. Sin embargo, con el avance de la Mecánica Cuántica y su ineludible importancia, la necesidad de extender los logros la teoría de la información al nuevo escenario dan inicio a la Teoría de la Información Cuántica. Los resultados presentados por Shannon respecto al envío de información por canales o la compresión de datos encuentran un análogo cuántico considerando las propiedades que este escenario posee. De esa forma las preguntas sobre el almacenamiento y procesamiento de datos y la definición de cantidades equivalentes a las definidas clásicamente, son actualmente objeto de estudio.

Considerando el impacto que ha alcanzado la formulación de la teoría cuántica, este proyecto analiza la extensión de las cantidades clásicas a un enfoque regido por la Mecánica Cuántica. Tiene como objetivo principal entender las ambiguedades y problemas al extender conceptos, como la entropía, a la teoría de la información cuántica. A partir de ello analiza el significado operacional que adquiere como consecuencia de dichas discrepancias, en términos de tareas asintóticas.

Capítulo 2

Teoría de la Información Clásica

La teoría de la información cuántica se ha desarrollado como una extensión de la versión clásica de la teoría de la información a un escenario cuántico. El planteamiento cuántico requiere la extensión de los conceptos desarrollados previamente en la teoría clásica. Sin embargo, los conceptos extendidos requieren de tareas asociadas que les brinden una interpretación operacional, análogo al caso clásico. ¿Cuáles son las tareas asociadas a dichas cantidades clásicas?

La teoría de la información clásica fue desarrollada por Shannon en el siglo XX, construyendo un formalismo base para el entendimiento de la información y facilitar los procesos de su almacenamiento y procesamiento. Como base para esta construcción Shannon planteo el concepto de entropía asociada a una variable aleatoria y, a partir de sus características, surge la entropía relativa, entropía condicional e información mutua. Clásicamente cada una de estas cantidades está bien establecida y adicionalmente tiene asociada una tarea específica que le da una interpretación operacional. A continuación se presentarán cada una de estas cantidades de acuerdo al planteamiento ya establecido, enfocado a su sentido operacional, para el distribuciones discretas.

2.1. Entropía de Shannon

Una de las preguntas fundamentales en la construcción de la teoría de la información es cómo cuantificar la cantidad (almacenamiento) de información de un estado. Esta cantidad está asociada con la probabilidad de que el estado tome ciertos valores. Para entender eso se define X como una variable aleatoria que tiene asociada la distribución de probabilidad $\{p(x_i)\}_{i\in I}$. Intuitivamente la cantidad de informaición disminuye al aumentar la pro-

babilidad de que ocurra dicho evento, por lo tanto se busca una cantidad que aumente inversamente a $p(x_i)$. Adicionalmente para dos eventos independientes la cantidad de información es aditiva, teniendo en cuenta que $p(x_i, y_j) = p(x_i)p(y_j)$. De esta forma surge naturalmente que el contenido de información h tiene la forma $h \sim log[1/p(x_i)]$.

A partir de los resultados anteriores se define el *contenido de información de Shannon* como

$$h(x_i) := log[1/p(x_i)],$$

donde $x_i \in X$, cuantificando la cantidad de información aportada por la variable X si el valor tomado es x_i. La unidad de información depende de la base elegida. En particular, si la base del logaritmo es 2, la unidad se conoce como *bit* RR. Si se quiere conocer la cantidad media de información que una variable X aporta entonces se calcula el valor esperado $\sum_i p(x_i)log[1/p(x_i)]$ para todo $x_i \in X$. El anterior resultado se conoce como *Entropía de Shannon*:

$$S := \sum_{i \in I} p(x_i)log[1/p(x_i)] = -\sum_{i \in I} p(x_i)log[p(x_i)], \tag{2.1}$$

definiendo $0log0 := 0$ dado que $\lim_{n \to 0} nlog[n] = 0$. Análogamente, para dos variables aleatorias X y Y con sus distribuciones respectivas asociadas se extiende el concepto de entropía:

$$\begin{aligned} H(X, Y) &:= \sum_{ij} p(x_i, y_j)log[1/p(x_i, y_j)] \\ &= -\sum_{i \in I} p(x_i, y_j)log[p(x_i, y_j)], \end{aligned} \tag{2.2}$$

donde $p(x_i, y_j)$ es la probabilidad conjunta de que $X = x_i$ y $Y = y_j$.

Si un emisor desea enviar cierta información X proveniente de una fuente se puede interpretar la entropía como la cantidad de información promedio que se está enviando. Similarmente el receptor cuantifica en la entropía la incertidumbre asociada a la variable X. A partir de esta definición intuitiva de entropía se pueden entender las propiedades que se derivan de (2.1):

- $H(X)$ es una función continua porque a pequeños cambios en la probabilidad hay pequeños cambios en la información contenida.
- $H(X) \geq 0$.
- $H(X)$ es máximo si $p(x_i) = p(x_j)$ para todo i, j. Cuando la distribución es uniforme la incertidumbre sobre X es máxima.
- Si $p_i = 1$ para algún i entonces $H(X) = 0$. Si existe total certeza de la ocurrencia de un evento, la incertidumbre sobre X es 0.

- $H(X,Y) \leq H(X)+H(Y)$, con la igualdad cuando X y Y son independientes. Esta propiedad se conoce como *subaditividad* de la entropía de Shannon.

La entropía conjunta de dos variables aleatorias X y Y no supera la información de ambas variables por separado. Como caso particular de la entropía de Shannon está la *Entropía Binaria* , definida para toda variable aleatoria con dos posibles resultados con probabilidades p y q:

$$H_2(X) = -plog(p) - qlog(q).$$

La entropía siempre es mayor a 0, $H_2(X) = 0$ si $p = 1$ o $q = 1$ y $H_2(X) = 1$ si $p = q = 1/2$, como lo muestra la figura 2.1:

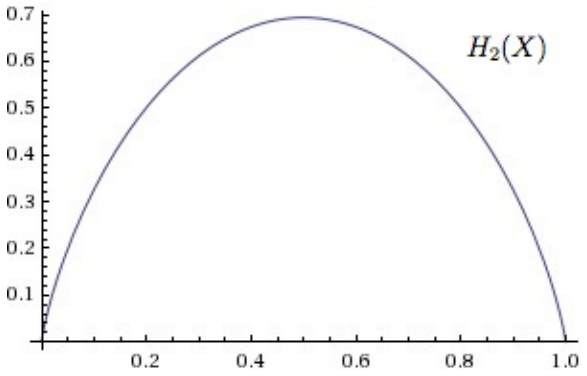

Figura 2.1: Entropía Binaria

Canal de Comunicación

Una de las preguntas fundamentales en la teoría de información es cómo llevar a cabo el envío de información de una fuente a un destinatario. Shannon introduce el concepto de *canal de comunicación* Q como el medio por el cual se envia al receptor un mensaje convertido en señal, que posteriormente es convertido en el mensaje inicial. Este protocolo de envío es formalizado definiendo los conceptos de *transmisor* y *recpetor*. El esquema general se muestra en la figura 2.2.

Teorema de la Fuente de Shannon y Compresión

Si $H(X)$ es la entropía de una fuente, el primer teorema de Shannon [1] establece que $H(X)$ determina la capacidad del canal requerida para enviar información de la fuente con la codificación óptima.
El teorema dice que para un canal con capacidad C, una fuente con entropía H y algún $\epsilon > 0$ existe una forma de codificación de la fuente tal que

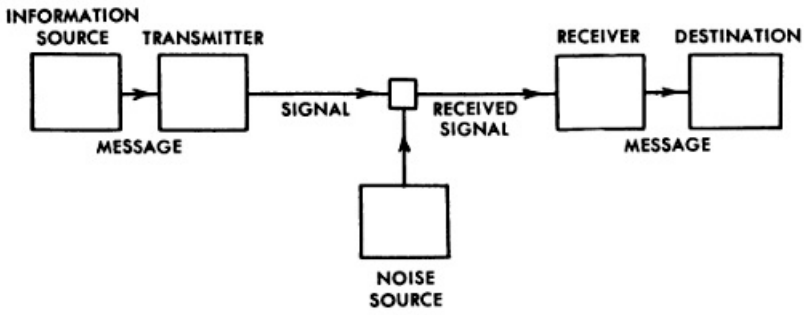

Figura 2.2: Representación de un sistema de comunicación [1]

se pueden trasmitir en promedio $\frac{C}{H} - \epsilon$ símbolos en promedio. El teorema ratifica que no es posible trasmitir símbolos en una rata promedio superior a $\frac{C}{H}$, estableciendo un límite para la codificación de datos.

Con la definición de entropía de Shannon se pueden definir nuevas cantidades que identifiquen tareas asintóticas. En las siguientes secciones se presentará la entropía relativa y la entropía condicional.

2.2. Entropía Relativa

La entropía de Shannon está definida para una variable aleatoria X cuya distribución es conocida $\{p(x_i)\}_i$. Sin embargo si se estima erróneamente que la distribuión correspondiente es $\{q(x_i)\}_i$, entonces hay una discrepancia entre la cantidad de información realmente contenida y la estimada. Esta diferencia se define como *Entropía Relativa* o *Divergencia de Kullback-Leibler* estudiada por S. Kullback y R. A. Leibler en 1951 [5]. La distribución real $\{p(x_i)\}_i$ tiene entropía $H(X) = -\sum_i p(x_i)log[p(x_i)]$. Si se estima erróneamente que la distribución es $\{q(x_i)\}_i$ entonces la información promedio que se calcularía en ese caso sería $-\sum_i p(x_i)log[q(x_i)]$. El déficit de información será entonces:

$$\begin{aligned} D(p\|q) &= -\sum_i p(x_i)log[q(x_i) - H(\{p(x_i)\}) \\ &= -\sum_i p(x_i)log[q(x_i)] + \sum_i p(x_i)log[p(x_i)\} \\ &= \sum_i p(x_i)log\frac{p(x_i)}{q(x_i)}. \end{aligned}$$

Por lo tanto se define la entropía relativa como:

$$D_{KL}(p\|q) := \sum_i p(x_i) log \frac{p(x_i)}{q(x_i)}, \tag{2.3}$$

conocida también como la distancia entre distribuciones.

El hecho de que $D_{KL}(p\|q) \geq 0$ es conocido como *desigualdad de Gibbs* sin embargo $D_{KL}(p\|q)$ no se debe confundir con una métrica, pues $D_{KL}(p\|q)$ no es simétrica: $D_{KL}(p\|q) \neq D_{KL}(q\|p)$. Adicionalmente, cuando $\{p_i\}_i = \{q_i\}_i$ entonces $D_{KL}(p\|q) = 0$.

2.3. Entropía Condicional

La entropía condicional es un concepto que se construye a partir de las probabilidades condicionales entre dos variables aleatorias X y Y. La expresión $p(x_i|y_i)$ cuantifica la probabilidad de que ocurra x_i dado que y_i se cumple. La entropía condicional se define entonces como la incertidumbre sobre X dado cierto algún valor de $Y = y_i$:

$$H(X|y_i) = -\sum_j p(x_j|y_i) log[p(x_j|y_i)],$$

para todo i. A partir de este resultado se define la entropía de X dado Y como:

$$\begin{aligned} H(X|Y) &= -\sum_i p(y_i) H(X|y_i) \\ &= -\sum_i p(y_i) \left[\sum_j p(x_j|y_i) log[p(x_j|y_i)] \right]. \end{aligned} \tag{2.4}$$

$H(X|Y)$ se interpreta entonces como la incertidumbre promedio sobre la variable X cuando se conoce el estado de Y. Intuitivamente $H(X|Y)$ está asociada a la información extra que posee X respecto a Y y a la información que ambas variables comparten. Se introduce entronces la *regla de la cadena* para la entropía, análogo a la regla de la cadena para la probabilidad conjunta $p(x, y) = p(x|y)p(y)$:

$$H(X|Y) = H(X, Y) - H(Y). \tag{2.5}$$

Considere el caso en el cual un receptor que tiene total conocimiento sobre la variable Y desea conocer el estado de un posible emisor con conocimiento sobre X. Para conocer el estado total de X, el emisor debe enviar

la información faltante, es decir, la información que el receptor ignora, que viene dada por la diferencia entre la información conjunta de X y Y y el prior $H(Y)$. Por lo tanto la cantidad de *bits* (en el caso del logaritmo en base 2) es $H(X,Y) - H(Y)$ que, por (2.5) es igual a la entropía condicional $H(X|Y)$. Según esto, la entropía condicional cuantifica la incertidumbre de Y respecto a X.

Intuitivamente la entropía condicional en este caso partícular es siempre no-negativa:

$$H(X|Y) \geq 0$$

es decir, $H(X,Y) \geq H(Y)$ porque, intuitivamente la cantidad de información conjunta entre X y Y es mayor o igual a la cantidad de información asociada a Y únicamente. En partícular, $H(X|Y) = 0$ cuando $H(X,Y) = H(Y)$, es decir, conocer el estado de Y permite inmediatamente conocer el estado de X. Si X y Y son variables independientes entonces $H(X|Y) = H(X,Y) + H(Y) = H(X) + H(Y) - H(Y) = H(X)$. En este caso conocer el estado de Y no aporta información sobre el conociemento de X.

A continuación se define la información mutua, definida en términos de la entropía condicional anteriormente definida.

2.4. Información Mutua

Sean X y Y variables aleatorias. Si están correlacionadas existe cierta información conocida por ambas variables. La *información mutua* se introduce para cuantificar esa información y se defeine como:

$$I(X;Y) := H(X) - H(X|Y). \tag{2.6}$$

Intuitivamente (2.6) cuantifica la información que no se obtiene de X al conocer Y. Por lo tanto se espera que $I(X;Y) := H(Y) - H(Y|X)$. Por (2.5):

$$\begin{aligned} I(X;Y) &= H(X) - H(X|Y) \\ &= H(X) - (H(X,Y) - H(Y)) \\ &= H(X) + H(Y) - H(X,Y) \\ &= H(Y) - H(X,Y) + H(X) \\ &= H(Y) - H(Y|X). \end{aligned}$$

Del resultado anterior tenemos que para todo X y Y $I(X;Y) = I(Y;X)$.
La figura 2.3 muestra gráficamente la relación entre las entropías de X y Y, la entropía condicional y la información mutua.

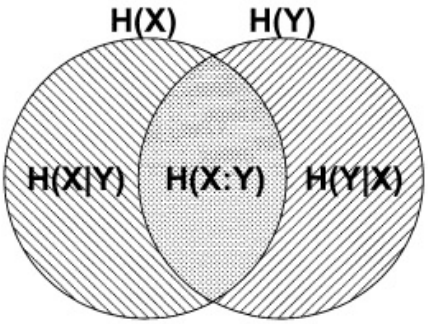

Figura 2.3: Entropía condicional con respecto a $H(X)$ y $H(Y)$. [2]

Si se toman las definiciones (2.1) y (2.4) a la información mutua se obtiene:

$$\begin{aligned} I(X;Y) &= H(X) - H(X|Y) \\ &= -\sum_i p(x_i) log[p(x_i)] + \sum_j p(y_j) \sum_i p(x_i|y_j) log[p(x_i|y_j)] \\ &= -\sum_{ij} p(x_i, y_i) log[p(x_i)] + \sum_{ij} p(x_i, y_j) log \frac{p(x_i, y_j)}{p(y_j)} \\ &= \sum_{ij} p(x_i, y_j) log \frac{p(x_i, y_j)}{p(x_i)p(y_j)} = D_{KL}(p(x_i, y_j) \| p(x_i)p(y_j)). \end{aligned}$$

Por lo tanto la información mutua es siempre positiva:

$$I(X;Y) = D_{KL}(p(x_i, y_j) \| p(x_i)p(y_j)) \geq 0. \tag{2.7}$$

La cantidad definida previamente es utilizada por Shannon [1] para determinar el límite de información que se puede enviar por un canal.

Capacidad de Canal

La información mutua cumple un papel fundamental en la determinación de la capacidad de un canal, asignándole una interpretación operacional en términos del envío de señales. No es sorprendente que la capacidad de envío este relacionada con la capacidad de trasmitir la información proveniente de una fuente aleatoria.La capacidad C se asocia entonces a la cantidad de bits (si está en base 2) por unidad de tiempo, teniendo en cuenta que C no es la cantidad de símbolos por segundo. De manera que C se establece como la mínima cota superior de información que puede enviarse por medio del canal respecto a las distribuciones de probabilidad posibles P_X:

$$\begin{aligned} C(Q) &:= \max_{P_X}(H(X) - H(X|Y)) \\ &= \max_{P_X} I(X;Y). \end{aligned} \tag{2.8}$$

Como la capacidad está ligada a la medida de información que el canal puede trasmitir, Shannon introduce el Teorema de la Codificación de Canal [1] donde prueba que C es la rata a la que se pueden comunicar señales con una pequeña probabilidad de error [2].

Segundo Teorema de Shannon

Sea C la capacidad de un canal discreto y H la entropía por segundo que genera la fuente. El segundo teorema de Shannon establece que existe un sistema de codificación tal que la información proveniente de la fuente puede enviarse con una pequeña probabilidad de error a través del canal en el caso que $H \leq C$.

La prueba del teorema justifica la definición de C en (2.8). Para un canal ruidoso, la cantidad $H(X|Y)$ se asocia al ruido proveniente del canal. Por lo tanto la máxima rata de envío de bits, sin pérdida de generalidad, es la diferencia entre la entropía de la fuente y la entropía condicional propia del canal. Al enviar una señal por el canal, el ruido genera una pérdida de información en la señal recibida. Esa pérdida se asocia con incertidumbre sobre la fuente dada la señal de llegada, es decir, $H(X|Y)$. Por tanto la información mutua determina la rata de datos que se envían por el canal ruidoso, teniendo en cuenta la información faltante.

Durante el capítulo se han definido las cantidades básicas desarrolladas por la teoría de la información clásica y su significancia operaciona. Asimismo se han presentado los teoremas asociados al almacenamiento y envío de información. A continuación se introducirán las cantidades análogas a las anteriormente definidas, pero en el marco de la mecánica cuántica.

Capítulo 3

Entropía de Von Neumann

Uno de los problemas fundamentales de la Teoría de la Información es cómo cuantificar el almacenamiento de información proveniente de una fuente. Clásicamente la entropía de Shannon, como se describió en el capítulo anterior, mide esa cantidad. ¿Existe una contraparte de la entropía de Shannon como medida de información en la Mecánica Cuántica? En 1927, John von Neumann asoció el concepto de entropía a operadores estadísticos dando a conocer su famosa fórmula para la entropía cuántica. Inicialmente él buscaba una conexión entre la entropía termodinámica y la Mecánica Cuántica, sin embargo más adelante se le asociaría una interpretación operacional como medida de información.

En este capítulo se desarrollarán los formalismos alrededor de la entropía de von Neumann. Inicialmente se introducirá a la noción de Operador Densidad, luego se definirá formalmente la entropía de von Neumann y sus propiedades. Adicionalmente, se discutirán las interpretaciones que se asocian a esta cantidad. Por último se estudiará la extensión del teorema de la fuente de Shannon al marco de la Mecánica Cuántica.

3.1. Operador Densidad

La Mecánica Cuántica tiene un formalismo bien definido para sistemas que se describen con vectores de estados. Sin embargo cuando el estado de un sistema no puede conocerse, existe una nueva formulación basada en el *Operador Densidad* o *Matríz densidad* del sistema. Si un sistema puede estar en el estado $|\psi_i\rangle$ con probabilidad p_i, entonces el *Operador Densidad* se define como:

$$\rho := \sum_i p_i |\psi_i\rangle\langle\psi_i|, \tag{3.1}$$

donde cada $|\psi_i\rangle$ es una función de onda pura y $|\psi_i\rangle\langle\psi_i|$ la proyección sobre dicho estado. Un sistema que deba describirse con más de un estado puro

se conoce como *mezcla estadística* y no se le puede asignar un único estado puro. En caso contrario, si el el operador densidad es $\rho = |\psi_i\rangle\langle\psi_i|$, el sistema se identifica mediante la función $|\psi_i\rangle$ y se considera un estado puro.

A partir de (3.1) se observa que ρ es un operador positivo, hermítico cuya traza siempre es igual a 1: $\mathrm{tr}(\rho) = 1$. Además $\mathrm{tr}(\rho^2) \leq 1$ con la igualdad si y sólo si ρ describe un estado puro. Además, sean A y B sistemas descritos por ρ^A y ρ^B respectivamente. Si son sistemas no correlacionados, entonces:

$$\rho^{AB} = \rho^A \otimes \rho^B. \tag{3.2}$$

3.1.1. Operador Densidad Reducido

Para describir sistemas cuánticos compuestos por varios sistemas físicos, se define el *Operador densidad reducido*. Por ejemplo, si un sistema está descrito por la matríz densidad ρ^{AB}, el operador densidad del subsistema A viene dado por la traza parcial sobre B:

$$\rho^A := \mathrm{tr}_B(\rho^{AB}). \tag{3.3}$$

Para ρ^B se define análogamente.

El operador densidad de un estado es herramienta fundamental en la formulación de las cantidades y teoremas que se presentarán de acá en adelante. En general, es un concepto básico para el desarrollo de la teoría de la información cuántica.

3.2. Entropía de von Neumann

Con el operador densidad definido, von Neumann define la versión cuántica de la entropía de Shannon, sustituyendo la distribución de probabilidad de un sistema por la matríz densidad del sistema cuántico.

$$S(\rho) := -\mathrm{tr}(\rho \log \rho) \tag{3.4}$$

$$:= -\sum_i \lambda_i \log \lambda_i, \tag{3.5}$$

donde λ_i son los valores propios de ρ, el logaritmo es en base 2 por convención y, al igual que en el caso clásico, se define $0 \cdot \log 0 := 0$.

Si se relaciona la matríz densidad ρ con ausencia de información del sistema (se desconoce el estado en el cuál se encuentra), es natural asociarle una medida de incertidumbre [6], justificando la definición de la ecuación (3.4). Como los estados puros representan situaciones de mínima ignorancia

entonces la entropía de von Neumann de dichos estados es igual a 0. Análogo al caso clásico, se define la *entropía conjunta*. Sean A y B sistemas descritos por ρ^A y ρ^B respectivamente, entonces:

$$S(A,B) = -\mathrm{tr}(\rho^{AB} \log \rho^{AB}) \tag{3.6}$$

A partir de (3.4) se definen igualmente la entropía relativa y la información mutua que se discutirán en los cápitulos 4 y 5.

3.2.1. Propiedades de la Entropía de von Neumann

A partir de las anteriores definiciones se demostrarán algunas propiedades relevantes de la entropía de von Neumann, y se realizarán algunas observaciones [7]. Sea ρ y σ operadores densidad de dos sistemas físicos:

- **No-negatividad**

  $$S(\rho) \geq 0, \tag{3.7}$$

  con la igualdad si A está en un estado puro. La información asociada a un estado no tendría sentido operacional si fuera negativo.

- **Valor máximo**

  Si d la dimensión del espacio de Hilbert entonces $S(\rho) \leq \log d$ con la igualdad si ρ es un estado máximamente mezclado, es decir, $\rho = (1/d)\mathbb{I}_d$, análogo al caso clásico de distribuciones uniformes.

- **Aditividad**

  $$S(\rho \otimes \sigma) = S(\rho) + S(\sigma).$$

  Para un producto de estados, la información asociada es la suma de la entropía de cada estado.

- **Concavidad**

  Si el operador se escribe como $\rho = \sum_i p_i \rho_i$ entonces

  $$S(\rho) \leq \sum_i p_i S(\rho_i).$$

Sean A, B,C sistemas físicos descritos por ρ^A, ρ^B y ρ^C respectivamente, donde $S(\rho^A, \rho^B) := S(\rho^{AB})$:

- **Subaditividad**

  $$S(\rho^A, \rho^B) \leq S(\rho^A) + S(\rho^B)$$

- **Desigualdad triangular**

$$S(\rho^A, \rho^B) \geq |S(\rho^A) - S(\rho^B)|.$$

- **Subaditividad fuerte**

$$S(\rho^A, \rho^B, \rho^C) + S(\rho^B) \leq S(\rho^A, \rho^B) + S(\rho^B, \rho^C).$$

  Las dos últimas propiedades son ciertas a pesar que, a diferencia del caso clásico, $S(\rho^A) \leq S(\rho^A, \rho^B)$ (ver capítulo 5), tratándose de una propiedad fundamental en la teoría de la información cuántica.

La prueba de las anteriores propiedades es demostrada en el Apéndice A.1.

En adelante, la expresión $S(A)$ hace referencia, por convención, a $S(\rho^A)$ y $S(\rho^A, \rho^B)$ a $S(A, B)$.

3.2.2. Continuidad de la Entropía de Von Neumann

El cambio en la entropía de von Neumann tiene una cota demostrada por la *desigualdad de Fannes*. La distancia entre la entropía de dos matrices densidad está acotada por una función de la distancia de la traza. Sean ρ y σ matrices densidad en un espacio de Hilbert de dimensión d. La distancia de la traza (*trace distance*) se define como:

$$T(\rho, \sigma) = \frac{1}{2}|\rho - \sigma|. \tag{3.8}$$

Como 3.8 es simétrica y cumple la desigualdad triangular entonces es considerada una métrica y usada como distancia entre estados cuánticos. La desigualdad de Fannes para dos estados tales que $T(\rho, \sigma) \leq 1/e$ se define como [7]:

$$|S(\rho) - S(\sigma)| \leq T(\rho, \sigma) \log d - T(\rho, \sigma) \log T(\rho, \sigma). \tag{3.9}$$

3.3. Interpretación Operacional

Aunque se define como una extensión natural de su contraparte clásica, la entropía de von Neumann no debe carecer de sentido operacional. A continuación se discutirán los posibles significados que dicha entropía adquiere bajo tareas asintóticas.
Inicialmente se presentará como la extensión del concepto de *entropía termodinámica* asignandole un significado estadístico. Luego se asociaá la entropía de von Neumann como la información de una fuente. Por último, se presentará el *Teorema de Schumacher*.

3.3.1. Significado Estadístico

Von Neumann construyó el concepto de entropía de una matríz densidad a partir de la entropía termodinámica, con le fin de extender la mecánica estadística a la mecánica cuántica. De ahí se puede extender el significado estadístico de la entropía definida en 3.4.

Sea ρ la matríz densidad que describe un sistema cuántico en un espacio de Hilbert. Si se hacen N mediciones al sistema entonces, para N muy grande se obtendrán $Np(x_i)$ veces cada estado $|x_i\rangle$. ¿Cómo entender estadísticamente el significado de entropía asociado a esas mediciones? Para ello se calcula la entropía termodinámica $s = k_B \ln W$ haciendo el conteo del número de microestados correspondientes W_N a las N mediciones. Cada posible grupo de mediciones, que pertenece a $\mathcal{H}^{\otimes N}$, puede interpretarse como un microestado posible ($Np(x_i)$ veces cada estado $|x_i\rangle$). Por lo tanto el número de microestados es ($k_B = 1$):

$$W_N = \frac{N!}{\prod_i (Np(x_i))!}. \tag{3.10}$$

Si se introduce en la definición de entropía termodinámica se obtiene:

$$\begin{aligned} S &= \ln W_N \\ &= \ln \left(\frac{N!}{\prod_i (Np(x_i))!} \right), \end{aligned}$$

para N muy grande y usando la aproximación de Stirlng:

$$S \approx -\sum_i p(x_i) \ln p(x_i), \tag{3.11}$$

coincidiendo con la definición de entropía de von Neumann en (3.4).

La entropía de von Neumann se puede interpretar como la generalización de la entropía termodinámica a la mecánica cuántica, desde una perspectiva estadística, cuantificando el caos o incertidumbre asociado al sistema medido [8].

3.3.2. Información de la Fuente

La entropía de Shannon cuantifica la incertidumbre asociada a la distribución de probabilidad de una fuente. La entropía de von Neumann se puede entender de la misma forma, definiendo previamente el significado de

una fuente de estados cuánticos. Una *fuente cuántica i.i.d* o fuente de estados cuánticos independientes e idénticamente distribuidos está determinada por una matriz ρ actuando en un espacio de Hilbert $\mathcal{H}$ y que hace parte de un estado puro. La matríz ρ actúa como distribución de probabilidad conteniendo la información sobre el sistema: $\rho = \sum_i p(x_i)|x_i\rangle\langle x_i|$.

Con las anteriores consideraciones se demuestra que la entropía de von Neumann cuantifica la información proporcionada por una fuente, demostrando que cumple con las condiciones para ser una medida de información:

- No puede ser una cantidad negativa.
- Debe ser continua. A pequeños cambios en el estado, pequeños cambios en la información.
- Para un estado máximamente mezclado $\rho = (1/d)\mathbb{I}_d$ debe ser máxima (equiprobables).

Estas propiedades fueron demostradas en las secciones (3.2.1) y (3.2.2) y permiten entender la entropía de von Neumann como una medida de información.

3.3.3. Compresión y Teorema de Schumacher

En la teoría de la información clásica Shannon enuncia el *Teorema de codificación sin ruido* (sección (2.1)). Con esta restricción, la entropía de Shannon adquiere una nueva interpretación: existe un límite de la eficiencia en la que se puede almacenar la información proveniente de una fuente. ¿Existe un análogo a este teorema en el marco de la mecánica cuántica? En 1995, Benjamin Schumacher prueba el *Teorema de codificación cuántica sin ruido* y, al igual que la entropía de Shannon, la entropía de von Neumann adquiere una nueva interpretación operacional.

La tarea consiste en producir N estados de una fuente con ρ asociada, como se introdujo en la sección (3.3.2). Si se trata cada estado cuántico como información, el anterior esquema correspondería a una fuente cuántica. Suponga ahora que

$$\rho = \sum_i p(x_i)|x_i\rangle\langle x_i|,$$

donde $|x_i\rangle \in \mathcal{H}$ son los estados propios (ortonormales) de ρ con sus respectivas probabilidades y

$$s(\rho) = -\sum_i p(x_i)\log p(x_i),$$

de acuerdo con la ecuación (3.4). La fuente produce una secuencia de N estados:

$$|x\rangle = |x^{(1)}\rangle \otimes \cdots \otimes |x^{(N)}\rangle. \tag{3.12}$$

Como cada estado $|x_i\rangle$ tiene asociada una probabilidad $p(x_i)$ entonces se espera que para N grande la fuente haya producido $Np(x_i)$ veces el estado x_i. Por lo tanto,

$$p(|x\rangle) \approx p(\prod_i p(x_i)^{Np(x_i)}),$$

entonces

$$\begin{aligned} \log p(|x\rangle) &= \sum_i Np(x_i) \log p(x_i) \\ &= Ns(\rho), \end{aligned}$$

obteniento para N grande:

$$p(|x\rangle) \approx 2^{-Ns(\rho)}. \tag{3.13}$$

A medida que N aumenta las secuencias que se aproximan al resultado obtenido en (3.13) forman un conjunto típico. Por lo tanto, codificar la información proveniente de la fuente para N muy grande requiere menos bits que si se tienen en cuenta las secuencias típicas y atípicas. El anterior esquema se formaliza en el *Teorema de secuencias típicas* y el *Teorema de Schumacher*.

Teorema de las Secuencias Típicas

Para presentar y demostrar el *Teorema de las secuencias típicas* se define primero una secuencia típica y un subespacio típico respecto a una fuente descrita por una matriz $\rho = \sum_i p(x_i)|x_i\rangle\langle x_i|$. Se toman n copias del estado $\rho^{\otimes n}$ que produce secuencias de estados:

$$|x\rangle := |x^{(1)}\rangle \otimes \cdots \otimes |x^{(n)}\rangle, \tag{3.14}$$

donde cada $|x^{(i)}\rangle$ pertenece al conjunto $X = \{|x_i\rangle\}$ asociado a ρ. El conjunto de todas las posibles secuencias $|x\rangle^{\otimes n}$ es:

$$X(n) := \{|x^{(1)}\rangle \otimes \cdots \otimes |x^{(n)}\rangle \mid |x^{(i)}\rangle \in X\}. \tag{3.15}$$

Sea $\epsilon > 0$. Análogo al caso clásico, una secuencia $x^{(1)}, ..., x^{(n)}$ es *secuencia ϵ-típica* si cumple la siguiente propiedad:

$$2^{-n(S(\rho)+\epsilon)} \leq p(x^{(1)}, ..., x^{(n)}) \leq 2^{-n(S(\rho)-\epsilon)}. \tag{3.16}$$

Se dice entonces que $|x\rangle_T := |x^{(1)}\rangle \otimes \cdots \otimes |x^{(n)}\rangle$ es un *estado ϵ-típico* si $x^{(1)}, ..., x^{(n)}$ es una secuencia ϵ-típica. Por último, el *subespacio ϵ-típico* se define como:

$$T_\epsilon(n) = \text{span}\{\ |x\rangle \in X(n) \mid |x\rangle \text{ es estado } \epsilon\text{-típico }\}. \tag{3.17}$$

Con las definiciones previas se enuncia el *teorema de las secuencias típicas* [7].

Teorema 3.3.1 (Teorema de las secuencias tipicas)

(a) Sea $\epsilon > 0$. $\forall \delta > 0$, $\exists N \in \mathbb{N}$ *tal que:*

$$tr(P_\epsilon(N)\rho^{\otimes N}) \geq 1 - \delta. \tag{3.18}$$

(b) Sea $\epsilon > 0$. $\forall \delta > 0$, $\exists N \in \mathbb{N}$ *tal que:*

$$(1-\delta)2^{n(S(\rho)-\epsilon)} \leq |T_\epsilon(n)| \leq 2^{n(S(\rho)+\epsilon)}. \tag{3.19}$$

(c) Sea $\delta > 0$, $R \leq S(\rho)$ *y* $S(n) \subset X(n)$. *Si* P_S *es el proyector asociado a* $S(n)$, *con dimensión* $d \leq 2^{nR}$, *entonces:*

$$tr(P_S\rho^{\otimes N}) \leq \delta. \tag{3.20}$$

La parte (a) del teorema 3.3.1 indica que para cualquier ϵ y δ mayores que 0 existe un N tal que se pueden hacer N copias del estado, de tal forma que la probabilidad de encontrar un estado típico es muy cercano a 1. La parte (b) del teorema indica que el tamaño del subespacio típico puede aproximarse a una cota que depende de $S(\rho)$ tanto como se quiera: (δ). Por último, la parte (c) del teorema dice que la probabilidad de obtener un estado de un subconjunto, de $X(n)$ de dimensión menor a $nS(\rho)$, se desvanece a 0.

Teorema de Schumacher

El *teorema de codificación cuántica sin ruido* presentado por Schumacher es una consecuencia del teorema 3.3.1 de secuencias típicas. El teorema es una versión al teorema de la fuente de Shannon, dando una condición para que la compresión de los datos producidos por una fuente cuántica sea posible.

Teorema 3.3.2 (Teorema de Schumacher) *Considere una fuente de estados* Q *descrita por el operador* ρ *actuando en* $\mathcal{H}$ *y considere un esquema de compresión cuya rata viene dada por* R. *Por lo tanto, si* $S(\rho) < R$ *entonces la compresión es posible, de lo contrario, para* $S(\rho) > R$ *no es realizable.*

El teorema de Schumacher da una condición para que la comunicación por un canal sea realizable, es decir, para ratas superiores a la entropía de la fuente [7].

El esquema general de los siguientes capítulos se extenderán las cantidades clásicas sustituyendo la entropía de Shannon por la entropía de von Neumann definida en (3.4).

Capítulo 4

Entropía Cuántica Relativa

A partir de la definición de la entropía de von Neumann se pueden reformular las cantidades utilizadas en la teoría de la información clásica en términos de operadores densidad. Se define entonces la entropía relativa cuántica cuya interpretación operacional en términos de tareas asintóticas es conocida. En la sección 4.1 se extiende la entropía relativa definida en el capítulo 2 y se demuestran sus propiedades básicas. En la sección 4.2 se interpreta esta cantidad como la distancia entre dos estados cuánticos y se discute la distinguibilidad de estados. Por último, en la sección 4.3 se asocia la entropía relativa como una medida de enredamiento.

4.1. Entropía Relativa

En el capítulo 2 se definió la entropía relativa de dos distribuciones de probabilidad de una misma variable aleatoria, interpretada como la distancia entre ambas distribuciones. Con el fin de encontrar un análogo cuántico que cuantifique la distancia entre dos estados cuánticos se reescribe la entropía clásica como:

$$\begin{aligned} H(X||Y) &= \sum_i p(x_i) \log p(x_i) - \sum_i p(x_i) \log p(y_i) \\ &= H(X) - \sum_i p(x_i) \log p(y_i). \end{aligned} \tag{4.1}$$

De acuerdo a 3.4 se define la *entropía relativa cuántica* haciendo uso de la entropía de von Neumann:

$$\begin{aligned} S(\rho||\sigma) &= \operatorname{tr}(\rho \log \rho) - \operatorname{tr}(\rho \log \sigma) \\ &= -S(\rho) - \operatorname{tr}(\rho \log \sigma). \end{aligned} \tag{4.2}$$

donde ρ y σ son los operadores densidad asociados a dos estados cuánticos. Para estados clásicos (ver capítulo 2) la definición en (4.2) coincide con (4.1).

Si $\rho\sigma = \sigma\rho$ entonces:

$$S(\rho||\sigma) = \mathrm{tr}(\rho(\log\rho - \log\sigma)) = \mathrm{tr}(\rho\log\rho\sigma^{-1}), \tag{4.3}$$

cumpliendo con el mínimo requerimiento para ser una extensión del caso clásico.

A pesar de la similitud entre ambas definiciones no es evidente que la cantidad definida en (4.2) tenga significado operacional ni que corresponda a una medición de la distinguibilidad de dos estados cuánticos. Sin embargo cumple con dichas afirmaciones. Para demostrarlo, primero se derivan algunas propiedades de la entropía relativa.

4.1.1. Propiedades de la Entropía Relativa

A partir de la definición dada en (4.2) se derivan algunas propiedades. Sean ρ, ρ' y σ, σ' operadores densidad en los espacios de Hilbert $\mathcal{H}_1$ y $\mathcal{H}_2$. Entonces:

- **Desigualdad de Klein**

  $$S(\rho||\sigma) \geq 0. \tag{4.4}$$

  con la igualdad si $\rho = \sigma$. La información asociada a un estado no tendría sentido operacional si fuera negativo.

- **Aditividad**

  $$S(\rho_1 \otimes \rho_2||\sigma_1 \otimes \sigma_2) = S(\rho_1||\sigma_1) + S(\rho_2||\sigma_2).$$

- **Monotonicidad**

  $$S(\rho^{AB}||\sigma^{AB}) \geq S(\rho^{A}||\sigma^{A}).$$

- **Convexidad**

  Si $\rho = p_1\rho_1 + p_2\sigma_2$ y $\sigma = p_1\sigma_1 + p_2\sigma_2$ entonces:

  $$S(\rho||\sigma) \leq p_1 S(\rho_1||\sigma) + p_2 S(\rho_2||\sigma).$$

- **Invarianza bajo operaciones unitarias**

  Si U es un operador unitario entonces:

  $$S(\rho||\sigma) \leq S(U\rho U^{\dagger}||U\sigma U^{\dagger}).$$

La prueba de las anteriores propiedades es demostrada en el Anéxo A.1.

4.2. Distinguibilidad de Estados

Definir la entropía relativa cuántica como una extensión de su contraparte clásica no asigna una interpretación operacional de la nueva cantidad. Sin embargo puede hacerse un tratamiento clásico para demostrar que adquiere la misma significancia: distinguibilidad de estados.

Clásicamente (ver capítulo 2) la probabilidad de confundir una distribución clásica q_i con p_i (definidas sobre la misma variable aleatoria) después de N mediciones (para N grande) es:

$$P_N(q \to p) = 2^{-NH(q||p)}. \tag{4.5}$$

Para justificar que cuánticamente la distinguibilidad tiene el mismo comportamiento se hace un tratamiento clásico a dos estados cuánticos descritos por ρ y σ.

Suponga que se quiere calcular la probabilidad de confundir σ con ρ. Para tratar el problema clásicamente [9],[10] se debe definir una distribución asociada a cada estado de acuerdo con un observable. Para ello sea $\{A_i\}$ un POVM en un espacio de Hilbert $\mathcal{H}$ tal que $\sum_i A_i = \mathbb{1}$. Se definen las distribuciones $\{p_i^{(1)}\}$ y $\{q_i^{(1)}\}$ como los valores esperados de cada observable A_1 para una copia de ρ y σ:

$$p_i^{(1)} := \mathrm{tr}(A_i\rho), \tag{4.6}$$

$$q_i^{(1)} := \mathrm{tr}(A_i\sigma). \tag{4.7}$$

Nótese que $\sum_i p_i^{(1)} = \sum_i \mathrm{tr}(A_i\rho) = \sum_i \mathrm{tr}(\rho) = \mathrm{tr}(\rho) = 1$, igual para $\sum_i q_i^{(1)} = 1$. Con las distribuciones, la distinguibilidad se calcula de acuerdo a (4.1). Sin embargo, como se busca distinguir dos estados entonces se escoge el POVM que maximice la distinguibilidad, es decir, que maximice la entropía relativa. Por lo tanto la entropía del sistema H_1 (una copia) es:

$$H_1 := \sup_{\{A_i\}} H(p_i^{(1)}||q_i^{(1)}) \tag{4.8}$$

$$= \sup_{\{A_i\}} \left(\sum_i p_i^{(1)} \log \frac{p_i^{(1)}}{q_i^{(1)}} \right)$$

$$= \sup_{\{A_i\}} \left(\sum_i p_i^{(1)} \log p_i^{(1)} - \sum_i p_i^{(1)} \log p_i^{(1)} \right)$$

$$= \sup_{\{A_i\}} \left(-H(p_i^1) - \sum_i p_i^{(1)} \log p_i^{(1)} \right). \tag{4.9}$$

Como la probabilidad de confundir los estados está definida en el caso asintótico entonces se debe calcular la entropía relativa para N copias de cada estado. Análogo al caso anterior se introduce la distribución de probabilidad $\{p_i^{(N)}\}$ y $\{q_i^{(N)}\}$:

$$p_i^{(N)} := \mathrm{tr}(A_i \rho^{\otimes N}), \tag{4.10}$$

$$q_i^{(N)} := \mathrm{tr}(A_i \sigma^{\otimes N}), \tag{4.11}$$

obteniendo la entropía relativa para cada copia:

$$H_N : = \sup_{\{A_i\}} H(p_i^{(N)} || q_i^{(N)})/N \tag{4.12}$$

$$= \sup_{\{A_i\}} \left(-H(p_i^1) - \sum_i p_i^{(1)} \log p_i^{(1)} \right) /N \tag{4.13}$$

Como es un tratamiento clásico, la probabilidad de confundir ρ con σ para N grande, de acuerdo con (4.16), es:

$$P_N(\sigma \to \rho) = 2^{-NH_N}. \tag{4.14}$$

Sin embargo, para $N \to \infty$, H_N se comporta como $S(\rho||\sigma)$ definido en (4.2):

$$\lim_{N\to\infty} H_N = S(\rho||\sigma). \tag{4.15}$$

El anterior resultado es demostrado por Hiai et. al. [11]. Por lo tanto, cuando $N \to \infty$:

$$P_N(\sigma \to \rho) \to 2^{-NS(\rho||\sigma)}. \tag{4.16}$$

De la misma forma que para (4.16), la probabilidad de confundir un estado descrito por σ con otro descrito por ρ disminuye al aumentar $S(\rho||\sigma)$, por tanto la entropía relativa cuántica se puede interpretar como una medida de distinguibilidad de estados cuánticos. A mayor entropía relativa mayor distinguibilidad.

4.3. Medida de Enredamiento

En la sección anterior se expone la entropía relativa como un indicador de la distinguibilidad de dos estados cuánticos. Haciendo uso de dicha caracterización se puede definir una medida de enredamiento en términos de la entropía cuántica relativa.

Un estado enredado es aquel que no puede expresarse como producto de estados, es decir, no es separable. Se busca una cantidad $E(\rho)$ que cuantifique el enredamiento de un estado ρ. Vedral et. al., [12],[13], introduce el enredamiento de un operador ρ, $E(\rho)$ como:

$$E(\rho) := \min_{\sigma\in\mathcal{D}} D(\rho||\sigma), \tag{4.17}$$

donde $D(\rho||\sigma)$ es una medida de la distancia entre ρ y un estado separable $\sigma \in \mathcal{D}$ que minimice la distancia. Si se toma $D(\rho||\sigma) = S(\rho||\sigma)$ se cumplen las tres condiciones para la medición de un estado enredado. Por lo tanto $E(\rho)$ definido como:

$$E(\rho) := \min_{\sigma \in \mathcal{D}} D(\rho||\sigma), \tag{4.18}$$

es una medida de apropiada para el enredamiento de un estado ρ. La probabilidad de confundir un estado enredado ρ con uno separable σ, después de N mediciones y para N grande viene dado por (4.16):

$$P_N(\sigma \to \rho) = 2^{-NE(\rho)}. \tag{4.19}$$

De acuerdo a los anteriores resultados, la entropía relativa, definida como extensión de la entropía de Shannon, tiene el mismo sentido operacional de distinguibilidad de estados que su contraparte clásica. Incluso puede ser interpretada como una medida de enredamiento. Sin ambargo, la entropía condicional no tiene esa ventaja al definirla como una extensión, como se presentará en el siguiente capítulo.

Capítulo 5

Entropía Condicional Cuántica

En los capítulos previos ha definido la versión cuántica de cantidades clásicas y discutido su significancia bajo las propiedades que el marco de la mecánica cuántica impone. Como se discutió anteriormente, ¿es posible extender todas las cantidades que clásicamente están definidas al caso clásico? En este capítulo se definirá la extensión de la entropía condicional y se presentarán las discrepancias que surgen. En la sección 5.1 se probarán algunas propiedades que difieren de las clásicas. En la sección 5.2 se presentará la interpretación de la entropía condicional en términos de protocolos. Por último, en la sección 5.3 se planterá una definición alternativa de la entropía condicional, necesaria para la definición de cantidades en el capítulo 6.

5.1. Entropía Condicional

En el capítulo 2 se definió la entropía condicional clásica de la distribución A condicionada por B como:

$$H(A|B) = H(A,B) - H(B). \tag{5.1}$$

Como se hizo para la entropía relativa, se extiende el concepto definido en 5.1 usando la entropía de von Neumann:

$$S(\rho^A|\rho^B) := S(\rho^{AB}) - S(\rho^B), \tag{5.2}$$

donde ρ^{AB} es el operador que describe el estado AB, $\rho^A = \mathrm{tr}_B(\rho^{AB})$, $\rho^B = \mathrm{tr}_A(\rho^{AB})$. Con la convención $S(X) := S(\rho^X)$, (5.2) queda expresada como:

$$S(A|B) := S(A,B) - S(B), \tag{5.3}$$

donde A y B son estados descritos por ρ^A y ρ^B respectivamente.

En la siguiente sección se mostrarán las propiedades de la entropía condicional.

5.1.1. Propiedades de la Entropía Condicional

Sean A, B,C,D estados. Se cumplen las siguientes afirmaciones:

- $S(A|B,C) \leq S(A|B)$.
- $S(A,B|C,D) \leq S(A|C) + S(B|D)$.
- $S(A|B)$ puede ser menor que 0 (para estados enredados)

La prueba de las anteriores propiedades es demostrada en el Apéndice A.1.
A pesar de la similitud en la definición, algunas propiedades de la entropía cuántica difieren de la clásica, como la no-negatividad.

Si A,B son distribuciones clásicas $H(A|B)$ cuantifica la información que requiere B para conocer A, por tanto carecería de sentido obtener $H(A|B)$ negativa. ¿Cómo interpretar la entropía negativa en el caso cuántico? A continuación se planteará un protocolo que le asigna a 5.3 un significado operacional.

5.2. Quantum State Merging

Con la búsqueda de entender la entropía condicional para estados enredados, en los últimos años se ha introducido un protocolo de transferencia óptima de información, M. Horodecki, J Oppenheim y A. Winter enunciaron este procedimiento en [14], llamado *Fusión de Estados Cuánticos* (*Quantum State Merging*), abreviado SM. Dicho protocolo es definido para asignar una interpretación operacional a la entropía condicional cuántica. Clásicamente la entropía definida en 5.1 cuantifica la cantidad de información que debe enviar una fuente A a un receptor B para que este último conozca completamente el estado de A. Sin embargo, como la entropía condicional definida en 5.3 puede adquirir valores negativos, el anterior procedimiento no sería válido, pues la información negativa no tiene ningún sentido operacional. Si se describe el envío de información cuántica en términos del protocolo SM, la entropía condicional adquiere un sentido operacional. A continuación se describirá el protocolo SM y sus implicaciones en la interpretación de cantidades cuánticas.

5.2.1. Definición

El protocolo SM describe el envío de información de A a B en términos del envío de estados puros $|\psi\rangle_{AB}$ producido por una fuente descrita por ρ^{AB}. El estado bipartito está compuesto por los subsistemas ρ^A y ρ^B que pueden estar correlacionados. Por lo tanto B tiene una información prior sobre el posible estado de A.

Se hacen las siguientes consideraciones:

- La cantidad de información cuántica que A debe enviar a B es la *información parcial cuántica*, donde la comunicación clásica es ilimitada y el envío está descrito por una operación cuántica $\mathcal{M}$.
- El envío de estados debe ser *fiel*, es decir, el estado puro $|\psi\rangle_{AB}$ debe preservarse en el envío. Para ello se introduce un sistema de referencia R tal que el estado tripartito $|\psi\rangle_{ABR}$ coincida con el estado transferido $|\psi\rangle_{B'BR}$ después de n copias del estado (cuando $n \to \infty$), donde B' es la parte enviada por A. A debe mantener la coherencia con R.

  Se introduce entonces un entorno inicial y final que incluya enredamiento, A_0B_0 y A_1B_1 respectivamente, donde A_0A_1 son registros del estado ρ^A y B_0B_1 son registros del estado ρ^B. Si K y L es el rango de Schmidt de A_0A_1 y B_0B_1, entonces los estados máximamente enredados inicial y final son ϕ_K y ϕ_L.

Teniendo en cuenta la última consideración, el estado inicial incluyendo el entorno de enredamiento es:

$$|\psi_i\rangle = \psi_{ABR} \otimes (\phi_K)_{A_0B_0}, \tag{5.4}$$

que debe ser fiel con el estado después de la fusión de estados:

$$|\psi_f\rangle = (\phi_L)_{A_1B_1} \otimes \psi_{B'BR}. \tag{5.5}$$

A partir de las observaciones presentadas anteriormente se define el protocolo SM como una operaión cuántica $\mathcal{M}$, es decir, un mapa completamente positivo que preserva la traza, tal que [15]:

$$\mathcal{M} : AA_0 \otimes BB_0 \to A_1 \otimes B_1B'B, \tag{5.6}$$

que representa el envío de A teniendo en cuenta los estados enredados inicial A_0B_0 y final A_1B_1. Como $\mathcal{M}$ es completamente positivo define una función $\mathcal{M} \otimes Id_R$ tal que:

$$\mathcal{M} \otimes Id_R : \psi_{ABR} \otimes (\phi_K)_{A_0B_0} \mapsto \rho.$$

Por lo tanto, la exigencia de fidelidad en SM con error ϵ arbitrariamente pequeño se puede escribir como:

$$\mathcal{F}\left((\mathcal{M} \otimes Id_R)(\psi_{ABR} \otimes (\phi_K)_{A_0B_0}), |\psi_f\rangle\right) = 1 - \epsilon, \tag{5.7}$$

donde $\epsilon \to 0$ cuando $n \to 0$. Como el enredamiento inicial es $\log K$ y final es $\log L$ entonces el costo de enredamiento o enredamiento consumido durante el protocolo es

$$C_e := \log L - \log K. \tag{5.8}$$

Para n copias es entonces:

$$C_e^n = \frac{1}{n}(\log L - \log K). \tag{5.9}$$

5.2.2. Información Parcial y Entropía Condicional

M. Horodecki et al.demostraron en [15] que SM cumple con las siguientes afirmaciones:

- La información parcial óptima corresponde a $S(A|B)$ por copia del estado, i.e. A debe enviar a B $S(A|B)$ qubits para transferir el estado.
- Si $S(A|B) > 0$: La rata de envío de información es posible si es mayor a $S(A|B)$. El costo de enredamiento es igual a $-S(A|B)$.
- Si $S(A|B) < 0$: La rata de envío de información es posible si es menor a $S(A|B)$ y el envío se puede lograr haciendo uso únicamente de LOCC. Adicionalmente A y B ganan $-S(A|B)$ pares máximamente enredados para futuras comunicaciones.
- La cantidad de comunicaciń clásica que el protocolo requiere está dada por la información mutua cuántica, que se introducirá en el capítulo 6.

Con estas afirmaciones $S(A|B)$ adquiere un sentido operacional, representando el mínimo de pares máximamente enredados para llevar a cabo el protocolo. En el caso de ser negativo y suponiendo que la comunicación clásica es ilimitada, A puede enviar su estado a B sin costo. La discrepancia de la entropía condicional negativa también se puede resolver haciendo uso de mediciones generalizadas, como se mostrará a continuación.

5.3. Mediciones Generalizadas

El protocolo SM también asigna interpretaciones operacionales a otras cantidades, como la *discordia cuántica*, que se discutirán en el siguiente capítulo. A continuación se presentará una definición de la entropía condicional cuántica diferente a la dada en 5.3. No aporta una interpretación operacional pero es útil en las discusiones posteriores respecto a la información mutua y la discordia cuántica. Considere la situación discutida para el protocolo SM: A desea enviar su estado a B. Sea $\{M_i\}$ un conjunto de mediciones generalizadas en el espacio de Hilbert $\mathcal{H}_B$ correspondiente a B, es decir, $\sum_i M^\dagger M = \mathbb{1}_B$. Como el estado del sistema está descrito por ρ^{AB}, se puede introducir la noción de probabilidad de que una medición en B sea j es:

$$\begin{aligned} p(B=j) &= \langle\psi|M_j^\dagger M_j|\psi\rangle \\ &= \mathrm{tr}(\mathbb{1}_A \otimes M_i \rho^{AB}), \end{aligned} \tag{5.10}$$

donde ρ^{AB} es el estado del sistema. Después de la medición el sistema colapsa al estado:

$$\rho_{A|B=j} := \frac{1}{p(B=j)} \mathrm{tr}(\mathbb{1}_A \otimes M_j \rho^{AB}). \tag{5.11}$$

Por lo tanto se puede definir la entropía condicional clásica análoga al caso clásico definiendo

$$\begin{aligned} S(A|B=j) &:= S(\rho_{A|B=j}) \\ &= -\mathrm{tr}(\rho_{A|B=j} \log \rho_{A|B=j}). \end{aligned} \tag{5.12}$$

Entonces, similar al procedimiento seguido para la entropía relativa, la entropía condicional es [16]:

$$S(A|B_c) := \sup_{\{N_i\}} \sum_j p(B=j) S(A|B=j). \tag{5.13}$$

que por definición es siempre positiva.

En el siguiente capítulo se hará uso de la definición obtenida en (5.13), donde se discutirá la extensión de la información mutua clásica.

Capítulo 6

Información Coherente

Con el fin de encontrar una cantidad análoga a la información mutua clásica, se observan las propiedades y características que está cantidad cumple y se busca un equivalente cuántico que cumpla con las mismas propiedades. De igual forma y como se ha hecho con las cantidades presentadas en los capítulos previos, se puede hacer uso de la entropía de von Neumann para extender directamente la definición de información mutua. Sin embargo, dicha cantidad difiere de aquella que cumple con la desigualdad en el procesamiento de datos, conocida como *información coherente*. En este capítulo se presentarán dos cantidades que extienden la información mutua clásica (secciones 6.1 y 6.2) y se discutirá una nueva medida llamada *discordia cuántica* en la sección 6.3.

6.1. Información Coherente

En la teoría clásica, la información mutua cumple un papel fundamental en la caracterización de canales ruidosos. Como se demostró en el capítulo 2, la desigualdad en el procesamiento de datos indica que la información mutua entre la distribución de probabilidad de entrada X y de salida Y no puede aumentar bajo procesos posteriores. Para construir un análogo cuántico, inicialmente se definirá la noción de canal ruidoso, se definirá un proceso de Markov y se demostrará la versión cuántica de la desigualdad en el proceso de datos.

Sea Q un sistema cuántico cuyos estados iniciales están descritos por los operadores ρ^Q. Un canal cuántico es una operación cuántica ε que produce estados finales $\rho^{Q'}$, es decir:

$$\varepsilon(\rho^Q) = \rho^{Q'}, \tag{6.1}$$

y se impone que ε sea un mapa completamente positivo (CP). Como el canal es ruidoso y ρ^Q no son estados puros, entonces se introduce un sistema

de referencia R de tal forma que se determine si la operación ε preserva enredamiento. Por lo tanto se define el sistema QR tal que su estado inicial $|\psi^{QR}\rangle$ sea puro. El estado ρ^Q, que ahora hace parte del sistema QR se puede calcular bajo la traza parcial:

$$\rho^Q = \mathrm{tr}_R(\rho^{QR}), \tag{6.2}$$

donde $\rho^{QR} = |\psi^{QR}\rangle\langle\psi^{QR}|$. Dado que ε es un mapa CP, la evolución del estado ρ^{QR} se puede describir en términos de la función $(\mathbb{I}_R \otimes \varepsilon)$ tal que preserve la traza y la positividad. Por lo tanto representa una evolución cuántica, que se puede escribir como:

$$\rho^{RQ'} = (\mathbb{I}_R \otimes \varepsilon)\rho^{RQ'}. \tag{6.3}$$

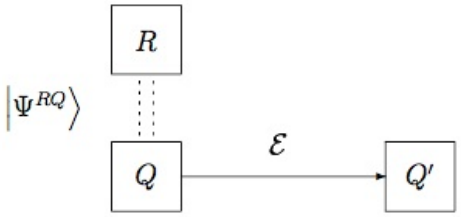

Figura 6.1: Esquema de un canal descrito por ε [3]

Bajo el anterior escenario, descrito en la figura 6.1, se define la *información coherente* de un estado ρ y un canal ε como

$$I_e(\rho, \varepsilon) := S(\rho^{Q'}) - S(\rho^{RQ'}). \tag{6.4}$$

También se puede reescribir como la información coherente entre R y Q' $I_e(R : Q')$.

Suponga que el canal descrito por ε no es ruidoso. Como ρ^{RQ} es un estado puro entonces $\rho^{RQ'}$ lo sería también, es decir, $S(\rho^{RQ'}) = 0$. Por tanto $S(\rho^{RQ'})$, llamada *producción de entropía*, cuantifica el ruido causado por ε y representa la información que permanece en la fuente después del envío. Por consiguiente, la información coherente cuantifica la información transmitible por un canal ruidoso [3]. A continuación se presentarán las propiedades de la información coherente definida en 6.4.

6.1.1. Propiedades de la Información Coherente

Sean A,B estados cuánticos descritos por ρ^A y ρ^B respectivamente. Entonces:

- En general $I_e(A:B)$ no es simétrica, es decir, $I_e(A:B) \neq I_e(B:A)$.
- $I_e(A:B) > 0$ sí y sólo sí AB es un estado enredado.

6.1.2. Desigualdad en el Procesamiento de Datos

A partir de la definición enunciada en la ecuación (6.4) se demuestra una propiedad análoga a la desigualdad en el procesamiento de datos clásicos, que asocia la información coherente como una extensión de la información mutua clásica. Inicialmente se definirá un proceso de Markov para canales cuánticos y, por último se demostrará la desigualdad.

Sea Q un sistema cuántico descrito por la matriz ρ^Q y sean ε_1 y ε_2 operaciones cuánticas que describen la evolución de Q (preservan la traza), es decir,

$$\rho^{Q_1} := \varepsilon_1(\rho^Q), \tag{6.5}$$

$$\rho^{Q_2} := \varepsilon_2(\rho^{Q_1}). \tag{6.6}$$

A partir de las anteriores consideraciones se enuncia el siguiente teorema.

Teorema 6.1.1 (Desigualdad en el procesamiento de datos) *Sean ρ^Q, ε_1 y ε_2 como se definieron previamente. Entonces se cumple que:*

$$s(\rho) \geq I_e(\rho^Q, \varepsilon_1) \geq I_e(\rho^Q, \varepsilon_2 \circ \varepsilon_1). \tag{6.7}$$

Si la operación ε_1 puede revertirse manteniendo la fidelidad con el estado inicial ρ, entonces $s(\rho) = I_e(\rho^Q, \varepsilon_1)$

La prueba de teorema se encuentra en el Apéndice A.2.

Las desigualdades presentadas en el teorema 6.1.1 se hace la siguiente observación. Para un estado inicial y una operación cuántica, la información coherente del esquema no puede aumentar bajo ninguna operación posterior. Si sobre un estado ρ se aplica una operación compuesta $\varepsilon_2 \circ \varepsilon_1$, la información coherente respecto a ε_1 no aumenta al procesar ε_2. Este resultado es equivalente al resultado clásico, razón por la cual se asocia la información coherente a la información mutua clásica. Adicionalmente, de acuerdo a la definición en (6.4), se le puede asignar a la información coherente una interpretación operacional, como se mostrará a continuación.

6.1.3. Costo de Enredamiento y SM

La información coherente definida en la ecuación (6.4) se puede comparar con la definición de entropía condicional cuántica definida en la ecuación (5.2), obteniendo:

$$I_e(A:B) = -S(A|B). \tag{6.8}$$

Como se presentó en el capítulo 5, $S(A|B)$ tiene asignada una interpretación operacional por medio del protocolo SM. Por lo tanto la información mutua se puede identificar como el número de pares maximamente enredados que se ganan durante el protocolo.

A partir de los resultados obtenidos, se ha demostrado que la información coherente juega un papel aálogo a la información mutua clásica por medio de la desigualdad de procesamiento de datos. Sin embargo hay otras generalizaciones del concepto clásico que se definirán en las siguientes secciones.

6.2. Información Mutua Cuántica

Similar a la entropía de von Neumann, entropía relativa y entropía condicional, la información mutua cuántica puede construirse sustituyendo la entropía de Shannon por la entropía de von Neumann en su definición clásica. Como se definió en el capítulo 2,

$$I(A:B) = H(A) + H(B) - H(A,B).$$

Por lo tanto la versión cuántica de la información mutua se define como:

$$\mathcal{I}(A:B) = S(A) + S(B) - S(A,B), \tag{6.9}$$
$$= S(A) - S(A|B), \tag{6.10}$$

donde $S(A) = S(\rho^A)$ por convención.

6.2.1. Propiedades de la Información Mutua

A partir de la definición de información mutua cuántica derivan las siguientes propiedades. Sea A, B y C estados cuánticos con sus correspondientes operadores ρ^A, ρ^B y ρ^C:

- **No-negatividad**

  $$\mathcal{I}(A:B) \geq 0.$$

  La información asociada a un estado AB nunca es mayor a la suma de la información de los dos subsistemas (subaditividad de la entropía de von Neumann).

- **Simetría**

  $$\mathcal{I}(A:B) = \mathcal{I}(B:A).$$

  A diferencia de la información coherente, $\mathcal{I}(A:B)$ coincide con la simetría de la información mutua clásica.

- **Entropía relativa**

$$\mathcal{I}(A:B) = S(\rho^{AB} \mid\mid \rho^A \otimes \rho^B). \tag{6.11}$$

  La información mutua se puede entender como la distancia entre el estado compuesto AB y el producto de los subsistemas A y B.

- **Subaditividad fuerte**

$$\mathcal{I}(A:B) + \mathcal{I}(A:C) \leq 2S(A).$$

  Es una consecuencia directa de la subaditividad fuerte.

- $\mathcal{I}$ **nunca aumenta al excluir un sistema** [7]

$$\mathcal{I}(A:B) \leq \mathcal{I}(A:B,C).$$

La prueba de las anteriores propiedades es demostrada en el Apéndice A.1.

A partir de la ecuación (6.11) se puede interpretar la información mutua como una medida de distinguibilidad entre el estado del sistema compuesto descrito por AB y el estado $\rho^A \otimes \rho^B$. En otras palabras la información mutua mide la discrepancia que se obtiene al suponer que los subsistemas A y B del sistema compuesto AB no están correlacionados, es decir, se pueden escribir como un estado producto. Por lo tanto reescribir la información mutua en términos de la entropía relativa le asigna una interpretación análoga al caso clásico mostrado en la ecuación (2.7). Sin embargo, usando la entropía condicional definida en la ecuación (5.13), se puede definir la información mutua cuántica respecto a un conjunto de mediciones generalizadas.

6.2.2. Mediciones Generalizadas

La información mutua $\mathcal{I}(A:B)$ considerada hasta ahora en este capítulo est|á definida como la diferencia entre la entropía de un subsistema, A, con la entropía condicional $S(A|B) = S(A,B) - S(B)$, como se muestra en la ecuación (6.10). Sin ambargo existen definiciones alternativas de la entropía condicional, como la presentada en la ecuación (5.13) que induce a una nueva expresión para la información mutua [16]:

$$\begin{aligned}\mathcal{J}(A:B) &= S(A) - S(A|B_c) \\ &= H(A) - \sup_{\{N_i\}} \sum_j p(B=j) S(A|B=j),\end{aligned} \tag{6.12}$$

donde $p(B=j)$ viene dado por la ecuación (5.10) y $S(A|B=j)$ por la ecuación (5.12). Con esta definición son dos las versiones cuánticas de la información mutua. En general se cumple que [16]

$$\mathcal{I}(A:B) \geq \mathcal{J}(A:B). \tag{6.13}$$

Estas expresiones no difieren en el marco clásico, donde $\mathcal{I}_C(A : B) = H(A) + H(B) - HA, B)$ y $\mathcal{J}_C(A : B) = H(A) - H(A|B)$ son idénticas. Esta igualdad clásica sugiere que la diferencia entre ambas cantidades es una medición netamente cuántica. En la siguiente sección se reconoce dicha diferencia como la *discordia cuántica*, cuyas propiedades e interpretación operacional se discutirán a continuación.

6.3. Discordia Cuántica

Como se presentó anteriormente, la diferencia entre $\mathcal{I}(A : B)$ y $\mathcal{J}(A : B)$ induce una nueva cantidad llamada *discordia cuántica* de AB medido por B, que se define como

$$\begin{aligned}\mathcal{D}(A|B) &= \mathcal{I}(A : B) - \mathcal{J}(A : B) \\ &= S(A|B_C) - S(A|B). \end{aligned} \tag{6.14}$$

La discordia cuántica presentada por Zurek et. al. [16] es una medición de las correlaciones no-clásicas presentes incluso en estados separables. La discordia cuántica ha sido de gran utilidad yendo más allá de la clasificación de correlaciones a partir del enredamiento. A pesar de la importancia que $\mathcal{D}(A|B)$ ha adquirido no había sido determinada una interpretación operacional de dicha cantidad. A partir del protocolo SM presentado en 5.2 $\mathcal{D}(A|B)$ adquiere una interpretación como el consumo de enredamiento total durante el protocolo. Esta caracterización será discutida en la sección 6.3.2.

6.3.1. Propiedades de la Discordia Cuántica

A partir de la definición de discordia cuántica se derivan las siguientes propiedades. Sea A y B estados cuánticos con sus correspondientes operadores ρ^A y ρ^B. Entonces:

- **No-negatividad**

$$\mathcal{D}(A|B) \geq 0. \tag{6.15}$$

- **No-simetría**

$$\mathcal{D}(A|B) \neq \mathcal{D}(B|A). \tag{6.16}$$

La prueba de las anteriores propiedades es demostrada en el Apéndice A.1. A continuación se presentará la interpretación operacional de $\mathcal{D}(A|B)$ respecto al protocolo SM.

6.3.2. Protocolo SM Extendido

En la sección 5.2 se presentó el protocolo de fusión de estados SM donde $-S(A|B)$ cuantifica el enredamiento ganado por un estado bipartito AB

después del protocolo. Sin embargo se puede considerar un esquema más general de este protocolo, donde se considera el enredamiento consumido para construir cada copia ρ^{AB} del estado, como se muestra en la figura 6.2. Para ello se hacen las siguientes definiciones del *enredamiento de formación* E_O [17]:

$$\begin{aligned} E_O(|\psi^{AB}\rangle) &:= S(\mathrm{tr}_A(|\psi^{AB}\rangle\langle\psi^{AB}|)) \\ E_O(p_i, |\psi^{AB}\rangle) &:= \sum_i p_i E_O(|\psi^{AB}\rangle) \\ E_O(A\rangle B) &:= \min_{\{p_i, |\psi^{AB}\rangle\}} E_O(p_i, |\psi^{AB}\rangle). \end{aligned} \tag{6.17}$$

La minimización en (6.17) se hace sobre todo los ensambles $\{p_i, |\psi^{AB}\rangle\}$ tales que $\rho = \sum_i p_i |\psi^{AB}\rangle\langle\psi^{AB}|$. Sean A y B estados descritos por ρ^A y ρ^B. El enredamiento de formación cuantifica la cantidad de pares máximamente enredados necesarios para crear una copia de ρ^{AB}, es decir, el consumo de enredamiento por copia del estado.

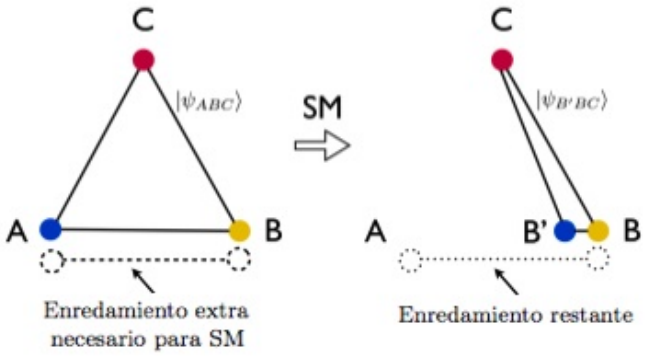

Figura 6.2: Esquema del protocolo SM extendido [4]

El protocolo SM se puede extender tal que entre en consideración el consumo de enredamiento para construir cada copia del estado. Por lo tanto se puede introducir una cantidad que cuantifique la cantidad total de enredamiento $\Gamma(A\rangle B)$ [4]:

$$\Gamma(A\rangle B) = E_O(A\rangle B) + S(A|B). \tag{6.18}$$

La cantidad $\Gamma(A\rangle B)$ es igual al consumo de enredamiento para construir una copia del estado más la pérdida de enredamiento asociada la fusión de estados $S(A|B)$.

Teorema 6.3.1 (Interpretación operacional de la discordia cuántica) *La discordia cuántica de AR medido por el estado de referencia R es igual*

al consumo total de enredamiento en el protocolo SM extendido:

$$\mathcal{D}(A|R) = \Gamma(A\rangle B). \tag{6.19}$$

El teorema 6.3.1 asigna a la discordia cuántica una interpretación operacional como el consumo total de enredamiento en el protocolo SM extendido.

En el capítulo se presentaron varias cantidades que surgen al extender la información mutua cuántica a un escenario cuántico. En el siguiente capítulo no se discutirá ninguna cantidad extendida de la teoría de la información clásica sino mediciones de características válidas únicamente en el marco de la Mecánica Cuántica.

Capítulo 7

Enredamiento Squashed

En los capítulos previos se han definido las cantidades definidas clásicamente en el marco cuántico y se han asignado interpretaciones operacionales a cada una de ellas. Lo anterior con el fin de construir una teoría análoga a la versión cuántica de la teoría de la información. Sin embargo hay propiedades presentes en el escenario cuántico que requieren la introducción de nuevas cantidades. Por ejemplo, la búsqueda de una cantidad fiel que mida el enredamiento de un estado es fundamental en la construcción de la teoría de la información cuántica. En este capítulo se presentará el *Enredamiento Squashed* como una medición fiel del enredamiento de un sistema. Inicialmente en la sección 7.1 se presentarán las condiciones necesarias para ser una medida fiel de enredamientoEn la sección 7.2 se describirá la motivación de la definición del enredamiento Squashed. En la sección 7.3 se definirá esta medida de enredamiento. Por último, en la sección 7.4 se mencionarán las propiedades que hacen del enredamiento Squashed una medida fiel.

7.1. Medidas de Enredamiento

Una cantidad específica $\mathcal{M}$ debe cumplir con algunas propiedades básicas necesarias para que sea una medida de enredamiento. Sea ρ^{AB} un estado bipartito. Si $\mathcal{M}$ es una medida fiel de enredamiento debe:

- Ser aditiva, convexa y continua.
- No aumentar bajo LOCC.
- $\mathcal{M}(A, B) = 0$ si A,B son estados separables.

7.2. Motivación

La subaditividad fuerte cumple un papel fundamental en la teoría clásica y cuántica y hace parte de las motivaciones fundamentales para definir

el enredamiento Squashed. Sea $H(A:B|E)$ la *información mutua condicional* clásica donde E se introduce para enxtender el estado AB. Por la subaditividad se demuestra que $H(A:B|E)$ es siempre mayor o igual a 0:

$$H(A:B|E) \geq 0.$$

Para el caso cuántico se extiende la cantidad $H(A:B|E)$ con la entropía de von Neumann tal que:

$$\begin{aligned} I(A:B|E) &= S(A|E) + S(B|E) - S(A,B|E) \\ &= S(A,E) - S(E) + S(B,E) - S(E) + S(E) - S(A,B,E) \\ &= S(A,E) + S(B,E) - S(E) - S(A,B,E). \end{aligned} \tag{7.1}$$

Por la subaditvidad fuerte mostrada en el capítulo 3 se obtiene que, al igual que $(A:B|E)$:

$$I(A:B|E) \geq 0. \tag{7.2}$$

incluso cuando $S(A|B)$ no es no-negativo en general. esta condición incentiva la definición de una medida de enredamiento en términos de $I(A:B|E)$. Se debe demostrar que, a diferencia de las anteriores cantidades, esta medida de enredamiento cumple con las condiciones necesarias para ser una medida fiel.

7.3. Enredamiento Squashed

A partir de las motivaciones presentadas anteriormente, se define el enredamiento Squashed como la mínima información mutua condicional que se puede obtener respecto a todas las posibles extensiones E [18].

Sea ρ^{AB} un estado bipartito. El *enredamiento Squashed* del estado se define como:

$$E_{Sq}(\rho^{AB}) = \inf_{E}\{\ \frac{1}{2}S(A:B|E)\ \}, \tag{7.3}$$

donde el ínfimo se toma sobre todas las posibles extensiones ρ^{ABE} del estado ρ^{AB}.

7.4. Propiedades del enredamiento Squashed

A partir de la definición de la ecuación (7.3), se derivan las siguientes propiedades que garantizan la fidelidad de E_{Sq} como medida de enredamiento. Las aditividad, monotonicidad y convexidad son demostradas por Christiandl et. al. en [18], la continuidad es demostrada por Alicki et. al. en [19] y el enredamiento para estados separables igual a 0 es demostrada por Brandao et. al. en [20].

- Aditividad
- Convexidad
- Continuidad
- Monotonicidad bajo LOCC
- AB son estados separables sí y sólo sí $E_{Sq}(\rho^{AB}) = 0$

Como se demostró en el capítulo, el enredamiento Squashed es una medida fiel del enredamiento de un estado cuántico bipartito, convirtiendose en una cantidad fundamental en la construcción de la teoría de la información cuántica. Las aplicaciones de esta medida de enredamiento en otros campos, como la teoría de la complejidad presentados en [20], serán caso de estudio en el desarrollo futuro de la teoría de la información.

Capítulo 8

Conclusiones

El desarrollo de la teoría de la información cuántica como una extensión de la versión clásica ha sido objeto de estudio en los últimos años y constituye una herramienta muy útil en el almacenamiento y procesamiento de información. Dentro de este marco, se realizó un análisis de las cantidades cuánticas estudiadas en la teoría de la información cuántica, desde un punto de vista operacional.

En primer lugar se presentó un breve resumén de la teoría de la información clásica con el fin de familiarizarse con las cantidades básicas necesarias para establecer una teoría sólida. Con la posterior introducción de la entropía de von Neumann se dió el primer paso para entender el almacenamiento de información cuántica y permitir la definición de nuevas cantidades. Sin embargo, la definición de medidas cuánticas como la extensión de medidas clásicas, haciendo uso directo de la entropía de von Neumann, dieron lugar a discrepancias. A pesar de ese hecho, se han venido desarrollando protocolos con el fin de asignar interpretaciones a dichas discrepancias, en términos de tareas asintóticas. En particular, la descripción del protocolo State Merging asignó a la entropía condicional cuántica, la información mutua y a la discordia cuántica interpretaciones operacionales válidas, suprimiendo las dificultades que implica no tener sentido operacional. Adicionalmente en el proyecto se reconoció la importancia de las operaciones cuánticas, haciendo uso de sistemas de referencia y otras herramientas matemáticas que ayudan a modelar situaciones y a evidenciar nuevas propiedades.

De los resultados obtenidos se puede concluir que el aprovechamiento de las propiedades de la naturaleza cuántica permiten el desarrollo de metodologías y procedimientos que, comparado con la contraparte clásica, son una ventaja en el almacenamiento y procesamiento de datos. Con la reciente inclusión del enredamiento Squashed como medida fiel del enredamiento de un sistema, la caracterización de correlaciones cuánticas permitirán en un

futuro tomar ventaja para futuras investigaciones. La inclusión de nuevas cantidades, el estudio del enredamiento a mayor profundidad y el desarrollo de la criptografía cuántica entre otras aplicaciones, son estudios posteriores a los tratados en este proyecto. La aparición de discrepancias en la definición de procesos y medidas es fundamental en la búsqueda de nuevas propiedades.

Apéndice A

Pruebas

Resumen: Este apéndice reúne las demostraciones de las propiedades y teoremas que así lo requieren.

A.1. Propiedades

A continuación se demostrarán las propiedades definidas durante el trabajo.

A.1.1. Desigualdad de Klein

En esta sección se demostrará la desigualdad de Klein enunciada en la ecuación (4.4), necesaria para posteriores demostraciones.

Sean $\rho = \sum_i p_i \rho_i$ y $\sigma = \sum_j q_j \sigma_j$ operadores densidad tales que $p_i = |\psi_i\rangle\langle\psi_i|$ y $q_i = |\phi_i\rangle\langle\phi_i|$, entonces:

$$\begin{aligned}
S(\rho||\sigma) &= -S(\rho) - \operatorname{tr}(\sigma \log \sigma) \\
&= -S(\rho) - \sum_i \langle\psi_i|\rho \log \sigma|\psi_i\rangle \\
&= -S(\rho) - \sum_i \langle\psi_i|(\sum_{i'} p_{i'}|\psi_{i'}\rangle\langle\psi_{i'}|) \log \sigma|\psi_i\rangle \\
&= -S(\rho) - \sum_i p_i \langle\psi_i| \log \sigma|\psi_i\rangle \\
&= -S(\rho) - \sum_i p_i \langle\psi_i|(\sum_j \log q_j|\phi_j\rangle\langle\phi_j|)|\psi_i\rangle \\
&= -S(\rho) - \sum_{ij} p_i \log q_j \langle\psi_i|\phi_j\rangle\langle\phi_j|\psi_i\rangle
\end{aligned}$$

$$= \sum_i p_i [\log p_i - \sum_j \log q_j \langle \psi_i | \phi_j \rangle \langle \phi_j | \psi_i \rangle].$$

Por la concavidad del logaritmo:

$$\geq \sum_i p_i \log p_i - p_i \log(\sum_j \langle \psi_i | \phi_j \rangle \langle \phi_j | \psi_i \rangle q_j)$$
$$= -\sum_i p_i \log \left(\frac{\sum_j \langle \psi_i | \phi_j \rangle \langle \phi_j | \psi_i \rangle q_j}{p_i} \right).$$

Como $-\log a \geq 1 - a$:

$$\geq -\sum_i p_i \left(1 - \frac{\sum_j \langle \psi_i | \phi_j \rangle \langle \phi_j | \psi_i \rangle q_j}{p_i} \right)$$
$$= \sum_i p_i - \sum_{ij} \langle \psi_i | \phi_j \rangle \langle \phi_j | \psi_i \rangle q_j \geq 0.$$

Por lo tanto $S(\rho||\sigma) \geq 0$, como se quería. □

A.1.2. Propiedades de la Entropía de von Neumann

En esta sección se demostrarán las propiedades de la entropía de Von Neumann enunciadas en el capítulo 3.

Lema A.1.1 *Si el sistema compuesto determinado por ρ^{AB} está en un estado puro entonces $S(\rho^A) = S(\rho^B)$.*

Prueba. Sea $|\psi_{AB}\rangle$ el estado puro del sistema conpuesto descrito por ρ^{AB} y sea $|\psi_{AB}\rangle = \sum \lambda_j (|\psi_A\rangle_j \otimes |\psi_B\rangle_j)$ la descomposición de Schmidt del estado. Como:

$$\rho^A = \sum \lambda_j^2 |\psi_A\rangle_j$$
$$\rho^B = \sum \lambda_j^2 |\psi_B\rangle_j$$

entonces $S(\rho^A) = -\sum_j \lambda_j^2 \log \lambda_j^2 = S(\rho^B)$, como se quería. □

Lema A.1.2 *Sean ρ^A, ρ^B operadores densidad de los sistemas A, B. Entonces:*

i) $log(\rho^A \otimes \rho^B) = log(\rho^A) + log(\rho^B)$.

ii) $tr(\rho^A \otimes \rho^B) = tr(\rho^A) + tr(\rho^B)$.

Prueba. Sean ρ^A, ρ^B operadores densidad de los sistemas A, B.

La traza del producto tensorial de ρ^A y ρ^B es:

$$\begin{aligned}\mathrm{tr}(\rho^A \otimes \rho^B) &= \sum_i (\rho^A \otimes \rho^B)_i \\ &= \sum_i ((\rho^A)_i \mathrm{tr}(\rho^B)) \\ &= \sum_i (\rho^A)_i \sum_i (\rho^B)_i \\ &= \mathrm{tr}(\rho^A)\mathrm{tr}(\rho^B),\end{aligned}$$

como se quería. □

A partir de los lemas definidos anteriormente se demuestran cada una de las propiedades de la entropía de von Neumann.

- **No-negatividad**

  Sea ρ operador densidad y λ_i los valores propios de ρ. Como $\sum_i \lambda_i = 1$ y λ_i son no negativos entonces $1 \geq \lambda_i \geq 0$. Por lo tanto:

  $$S(\rho) = -\sum_i \lambda_i \log \lambda_i \geq 0,$$

  como se quería. □

- **Valor máximo**

  Sea ρ un operador densidad actuando en el espacio de Hilbert $|\mathcal{H}| = d$. Por la desigualdad de Klein se tiene que $S(\rho||(1/d)\mathbb{I}_d) \geq 0$, entonces:

  $$\begin{aligned}0 &\leq S(\rho||(1/d)\mathbb{I}_d) \\ &= \mathrm{tr}(\rho \log \rho) - \mathrm{tr}(\rho \log((1/d)\mathbb{I}_d)) \\ &= -S(\rho) - \log(1/d)\mathrm{tr}(\rho) \\ &= -S(\rho) + \log(d).\end{aligned}$$

  Por lo tanto:

  $$S(\rho) \leq \log d.$$

  Para el caso en el que ρ sea el operador de un estado puro, entonces $S(\rho) = 0$, como se quería. □

- **Aditividad**

Sean ρ y σ operadores densidad.

$$S(\rho \otimes \sigma) = -\mathrm{tr}((\rho \otimes \sigma)\log(\rho \otimes \sigma)).$$

Por el lema A.1.2:

$$\begin{aligned}
&= -\mathrm{tr}((\rho \otimes \sigma)(\log\rho + \log\sigma)) \\
&= -\mathrm{tr}((\rho\log\rho) \otimes \sigma + \rho \otimes (\sigma\log\sigma)) \\
&= -\mathrm{tr}(\rho\log\rho)\mathrm{tr}(\rho) - \mathrm{tr}(\rho)\mathrm{tr}(\sigma\log\sigma) \\
&= -\mathrm{tr}(\rho\log\rho) - \mathrm{tr}(\sigma\log\sigma) = S(\rho) + S(\sigma),
\end{aligned}$$

como se quería. □

- **Concavidad**

Sea $\rho = \sum_i p_i\rho_i$. Si $\{\lambda_{ij}\}_j$ y $\{|\psi\rangle_{ij}\}_j$ son los valores y vectores propios de ρ entonces $\{p_i\lambda_{ij}\}_j$ son valores propios de ρ_i. Por lo tanto:

$$\begin{aligned}
S(\rho) &= S(\sum_i p_i\rho_i) \\
&= -\sum_{ij}(p_i\lambda_{ij}\log p_i\lambda_{ij}) \\
&= -\sum_{ij}(p_i\lambda_{ij}\log p_i) - \sum_{ij}(p_i\lambda_{ij}\log\lambda_{ij}) \\
&= -\sum_i(p_i\log p_i) + \sum_i p_i S(\rho_i).
\end{aligned}$$

Como $H(p_i) = -\sum_i p_i\log p_i \geq 0$ entonces $S(\rho) \leq \sum_i p_i S(\rho_i)$, como se quería. □

- **Subaditividad**

Sea ρ^{AB} el operador de un sistema AB y sean ρ^A, ρ^B los operadores para cada subsistema. Por la desigualdad de Klein se cumple que:

$$\begin{aligned}
0 &\leq S(\rho^{AB}||\rho^A \otimes \rho^B) \\
&= \mathrm{tr}(\rho^{AB}\log\rho^{AB}) - \mathrm{tr}(\rho^{AB}\log(\rho^A \otimes \rho^B)) \\
&= -S(\rho^A,\rho^B) - \mathrm{tr}(\rho^{AB}(\log\rho^A + \log\rho^B)) \\
&= -S(\rho^A,\rho^B) - \mathrm{tr}(\rho^A\log\rho^A) - \mathrm{tr}(\rho^B\log\rho^B) \\
&= -S(\rho^A,\rho^B) + S(\rho^A) + S(\rho^B).
\end{aligned}$$

Por lo tanto:

$$S(\rho^A, \rho^B) \leq S(\rho^A) + S(\rho^B),$$

como se quería. □

- **Desigualdad triangular**

  Sean ρ^A, ρ^B operadores de los sistemas A,B. Se introduce un sistema de referencia R tal que ρ^{ABR} es un estado puro, por lo tanto, por el lema A.1.1, $S(\rho^B) = S(\rho^A, \rho^B)$ y $S(\rho^R) = S(\rho^{AR})$.

  Por la subaditividad se cumple que:

$$\begin{aligned} & S(\rho^A, \rho^R) \leq S(\rho^A) + S(\rho^R) \\ \Rightarrow\ & S(\rho^B) \leq S(\rho^A) + S(\rho^{AB}) \\ \Rightarrow\ & S(\rho^{AB}) \geq S(\rho^B) - S(\rho^A). \end{aligned}$$

  Por simetría se obtiene igualmente que $S(\rho^{AB}) \geq S(\rho^B) - S(\rho^A)$, por lo tanto:

$$S(\rho^A, \rho^B) \geq |S(\rho^A) - S(\rho^B)|,$$

  como se quería. □

- **Subaditividad fuerte**

  La demostración de la versión cuántica de la subaditividad fuerte está fuera del alcance de este proyecto. Se recomienda consultar [7].

A.1.3. Propiedades de la Entropía Relativa

En esta sección se demostrarán las propiedades de la entropía relativa enunciadas en el capítulo 4.

- **Aditividad**

  Sean ρ_1, ρ_2, σ_1, σ_2 operadores densidad.

$$S(\rho_1 \otimes \rho_2 || \sigma_1 \otimes \sigma_1) = -S(\rho_1 \otimes \rho_2) - \mathrm{tr}((\rho_1 \otimes \rho_2) \log(\sigma_1 \otimes \sigma_2)).$$

  Por el lema A.1.2 y la aditividad de la entropía:

$$\begin{aligned} &= -S(\rho_1) - S(\rho_2) - \mathrm{tr}((\rho_1 \otimes \rho_2)(\log \sigma_1 + \log \sigma_2)) \\ &= -S(\rho_1) - S(\rho_2) - \mathrm{tr}((\rho_1 \log \sigma_1) \otimes \rho_2 + \rho_1 \otimes (\rho_2 \log \sigma_2)) \\ &= -S(\rho_1) - S(\rho_2) - \mathrm{tr}(\rho_1 \log \sigma_1)\mathrm{tr}(\rho_2) - \mathrm{tr}(\rho_1)\mathrm{tr}(\rho_2 \log \sigma_2) \\ &= -S(\rho_1) - S(\rho_2) - \mathrm{tr}(\rho_1 \log \sigma_1) - \mathrm{tr}(\rho_2 \log \sigma_2) \\ &= S(\rho_1 || \sigma_1) + S(\rho_2 || \sigma_2), \end{aligned}$$

como se quería. □

A.1.4. Propiedades de la Entropía Condicional

En esta sección se demostrarán las propiedades de la entropía condicional enunciadas en el capítulo 5.

- $\mathbf{S(A|B,C) \leq S(A|B)}$

  Sean ρ^A, ρ^B, ρ^C operadores densidad de los estados A, B, C. Por la subaditividad fuerte de la entropía de von Neumann y con la convención $S(\rho^A) = S(A)$ se obtiene:

$$\begin{aligned} S(A|B,C) &= S(\rho^A|\rho^B,\rho^C) \\ &= S(\rho^A,\rho^B,\rho^C) - S(\rho^B,\rho^C) \\ &\leq (S(\rho^A,\rho^B) + S(\rho^B,\rho^C) - S(\rho^B)) - S(\rho^B,\rho^C) \\ &= S(\rho^A,\rho^B) - S(\rho^B) \\ &= S(\rho^A|\rho^B) = S(A|B), \end{aligned}$$

  como se quería. □

- $\mathbf{S(A,B|C,D) \leq S(A|C) + S(B|D)}$

  Sean ρ^A, ρ^B, ρ^C, ρ^D operadores densidad de los estados A, B, C, D. Teniendo en cuenta la convención $S(\rho^A) = S(A)$ se obtiene:

$$\begin{aligned} S(A,B|C,D) &= S(\rho^A,\rho^B|\rho^C,\rho^D) \\ &= S(\rho^A,\rho^B,\rho^C,\rho^D) - S(\rho^A,\rho^C) \\ &= S(\rho^A,\rho^{BD},\rho^C) - S(\rho^A,\rho^C) \end{aligned}$$

  Por la subaditividad fuerte de la entropía:

$$\begin{aligned} &\leq (S(\rho^A,\rho^C) + S(\rho^{BD},\rho^C) - S(\rho^C)) - S(\rho^C,\rho^D) \\ &= S(\rho^A,\rho^C) + S(\rho^B,\rho^C,\rho^D) - S(\rho^C) - S(\rho^C,\rho^D) \end{aligned}$$

  Usando nuevamente la subaditividad fuerte de la entropía:

$$\begin{aligned} &\leq S(\rho^A,\rho^C) + (S(\rho^C,\rho^D) + S(\rho^B,\rho^D) - S(\rho^D)) - S(\rho^C,\rho^D) \\ &= S(\rho^A|\rho^C) + S(\rho^B|\rho^D) = S(A|C) + S(B|D), \end{aligned}$$

  como se quería. □

A.1.5. Propiedades de la Información Mutua

En esta sección se demostrarán las propiedades de la información mutua cuántica enunciadas en el capítulo 6.

- **No-negatividad**

  Sean ρ^A, ρ^B operadores densidad de los estados A, B. Por la subaditividad de la entropía de von Neumann:

  $$S(\rho^{AB}) \leq S(\rho^A) + S(\rho^B)$$

  se obtiene:

  $$\mathcal{I}(A:B) = S(\rho^A) + S(\rho^B) - S(\rho^{AB}) \geq 0,$$

  como se quería. □

- **Simetría**

  La simetriía de la información mutua es una consecuencia directa de la ecuación (6.10). □

- **Entropía relativa**

  Sean ρ^A, ρ^B operadores densidad de los estados A, B. Por el lema A.1.2 se obtiene que:

  $$\begin{aligned}\mathcal{I} &= S(\rho^A) + S(\rho^B) - S(\rho^{AB}) \\ &= -S(\rho^{AB}) - \mathrm{tr}(\rho^{AB}\log\rho^A) - \mathrm{tr}(\rho^{AB}\log\rho^B) \\ &= -S(\rho^{AB}) - \mathrm{tr}(\rho^{AB}(\log\rho^A + \log\rho^B)) \\ &= -S(\rho^{AB}) - \mathrm{tr}(\rho^{AB}\log(\rho^A\otimes\rho^B)) \\ &= S(\rho^{AB}||\rho^A\otimes\rho^B),\end{aligned}$$

  como se quería. □

- **Subaditividad fuerte**

  Sea $ABCR$ un estado puro, donde R es una purificación del sistema ABC. A partir de la subaditividad fuerte se conoce que:

  $$S(\rho^{ABR}) + S(\rho^B) \leq S(\rho^{AB}) + S(\rho^{BR}).$$

  Como $S(\rho^{ABR}) = S(\rho^C)$ y $S(\rho^{BR}) = S(\rho^{AC})$ por ser un estado puro, entonces:

  $$S(\rho^C) + S(\rho^B) \leq S(\rho^{AB}) + S(\rho^{AC}).$$

A partir de los anteriores resultados se demuestra la desigualdad:

$$\begin{aligned}&\mathcal{I}(A:B)+\mathcal{I}(A:C)\\&\quad=S(\rho^A)+S(\rho^B)-S(\rho^{AB})+S(\rho^A)+S(\rho^C)-S(\rho^{AC})\\&\quad\leq 2S(\rho^A)+S(\rho^{AB})+S(\rho^{AC})-S(\rho^{AB})-S(\rho^{AC})=2S(\rho^A),\end{aligned}$$

como se quería. □

- **$\mathcal{I}$ nunca aumenta al exluir un sistema**

  Sean ρ^A, ρ^B, ρ^C operadores densidad de los estados A, B, C.

  $$\mathcal{I}(A:B)=S(\rho^A)+S(\rho^B)-S(\rho^{AB})$$

  Por la subaditividad fuerte:

  $$\begin{aligned}&\leq S(\rho^A)+(S(\rho^{BC})-S(\rho^{ABC}))\\&=\mathcal{I}(A:B,C),\end{aligned}$$

  como se quería. □

A.1.6. Propiedades de la Discordia Cuántica

En esta sección se demostrarán las propiedades de la discordia cuántica enunciadas en el capítulo 6.

- **Asimetría**

  Dado que por definición $S(A|B_C)$ siempre es positiva y $S(A|B)$ puede tomar valores negativos, la diferencia de estas cantidades ($\mathcal{D}(A|B)$) es asimétrica.

A.2. Desigualdad en el Procesamiento de Datos 6.1.1

En esta sección se demostrará la desigualdad en el procesamiento de datos 6.1.1.

Sea ρ^Q un estado cuántico, $\rho^{Q_1}=\varepsilon_1(\rho^Q)$, $\rho^{Q_2}=\varepsilon_2(\rho^{Q_1})$, R, R_1 y R_2 sistemas de referencia asociados a cada sistema y E, E_1 y E_2 entornos. Inicialmente se demuestra la primera desigualdad:

$$I_e(\rho^Q,\varepsilon)=S(\rho^{Q_1})-S(\rho^{RQ_1}).$$

Teniendo en cuenta que el término de producción de entropía para la operación ε_1 se puede escribir como $S(\rho^{Q_1}) = S(\rho^{R_1 E_1'})$ entonces:

$$I_e(\rho^Q, \varepsilon) = S(\rho^{R_1 E_1'}) - S(\rho^{E_1'}).$$

Por la subaditividad de la entropía finalmente se obtiene:

$$\begin{aligned} I_e(\rho^Q, \varepsilon) &\leq S(\rho^{R_1}) + S(\rho^{E_1'}) - S(\rho^{E_1'}) \\ &= S(\rho^R) = S(\rho^Q), \end{aligned}$$

como se quería. □

La estructura de la primera parte de la demostración fue tomada de [7]. En la misma referencia se encuentra la segunda parte, demostración que está fuera del alcance de este proyecto.

A.3. Teorema 6.3.1

En esta sección se demostrará el teorema 6.3.1 y es una versión detallada del procedimiento presentado en [4].

Sea $|\psi^{ABR}\rangle$ un estado puro tripartito donde R es el sistema de referencia. Por definición, la discordia cuántica de AR medido por R es:

$$\mathcal{D}(A|R) = S(A|R_C) - S(A|R)$$

A partir de la relación de Koashi-Winter (tomada de [4]), se tiene que:

$$\begin{aligned} S(B) &= E_F(A:B) + I(B:R_C) \\ &= E_F(A:B) + S(B) - S(B|R_C) \\ &= E_F(A:B) + S(B) - S(A|R_C). \end{aligned}$$

Por lo tanto:

$$S(A|R_C) = E_F(A:B).$$

A partir de la ecuación (6.14) se obtiene:

$$\begin{aligned} \mathcal{D}(A|R) &= S(A|R_C) - S(A|R) \\ &= E_F(A:B) - S(A|R) \\ &= E_F(A:B) - S(AC) + S(C). \end{aligned}$$

Aplicando el resultado del lema A.1.1 a $S(AC)$ y $S(C)$:

$$\begin{aligned} &= E_F(A:B) - S(B) + S(AB) \\ &= E_F(A:B) + S(A|B) = \Gamma(A\rangle B), \end{aligned}$$

como se quería. □

Bibliografía

[1] C. E. Shannon and W. Weaver. *The Mathematical Theory of Communication.* (University of Illinois Press, 1969).

[2] D. J. Mackay. *Information Theory, Inference, and Learning Algorithms.* (Cambridge University Press, Cambridge, 2003).

[3] B. Schumacher and M. D. Nielsen. *Phys. Rev. A*, **54**: 2629, (1996).

[4] D. Cavalcanti, L. Aolita, S. Boixo, K. Modi, M. Piani, and A. Winter. *Phys. Rev. A*, **83**, (2011).

[5] S. Kullback and R. A. Leibler. *Rev. Mod. Phys.*, **22**: 79, (1951).

[6] C. H. Bennett and P. W. Shor. *IEEE Trans. Inf. Theory*, **44**(6): 2724, (1998).

[7] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information.* (Cambridge University Press, Cambridge, 2005).

[8] A. Wehrl. *Rev. Mod. Phys.*, **50**: 221, (1978).

[9] B. Schumacher and M. D. Westmoreland. *arXiv:quant-ph/0004045v1*, (2000).

[10] V. Vedral. *Rev. Mod. Phys.*, **74**: 197, (2002).

[11] Hiai and Petz. *Comm. Math. Phys.*, **143**: 99, (1991).

[12] M.A. Rippin P. L. Knight V. Vedral, M.B. Plenio. *Phys. Rev. Lett.*, **78**: 2275, (1997).

[13] K. Jacobs V. Vedral, M.B. Plenio and P. L. Knight. *Phys. Rev. A*, **56**: 4452, (1997).

[14] M. Horodecki, J. Oppenheim, and A. Winter. *Nature*, **436**: 673, (2005).

[15] M. Horodecki, J. Oppenheim, and A. Winter. *Comm. Math. Phys.*, **269**: 107, (2005).

[16] H. Ollivier and W.H. Zurek. *Phys. Rev. Lett.*, **88**, (2001).

[17] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters. *Phys. Rev. A*, **54**: 3824, (1996).

[18] M. Christandl and A. Winter. *J. Math. Phys.*, **45**: 829, (2004).

[19] R. Alicki and M. Fannes. *J. Phys. A: Math. Gen.*, **37**: L55, (2004).

[20] F. G.S.L. Brandao, M. Christandl, and J. Yard. *arXiv:1010.1750v1*, (2010).