Introducción a la teoría de la información cuántica

Francisco J. Gálvez

10 de diciembre de 2008

Índice

1. Introducción

Hasta hace muy poco, la información se ha considerado siempre en términos clásicos. La mecánica cuántica, en el campo de la información ha jugado tan solo un papel auxiliar en el diseño de los dispositivos físicos utilizados para el procesado de la información.

Actualmente el desarrollo de una teoría cuántica de la información ha demostrado su aplicabilidad en algunos campos tales como la criptografía, y también ha mostrado el potencial que podrían tener ordenadores cuánticos en la resolución de ciertos problemas matemáticos complejos. Estás nuevas posibilidades están basadas en propiedades totalmente cuánticas tales como: Incertidumbre, Interferencia y Entrelazamiento (Entanglement).

Todo apunta a que una teoría de la información basada en principios cuánticos puede extender y completar la teoría clásica de la información de la misma forma que los números complejos extienden el campo de los números reales.

La nueva teoría cuántica de la información contiene generalizaciones cuánticas de conceptos clásicos tales como: Fuente, Canal y Código, y además complementa dos tipos de información cuantificable como son información clásica y entrelazamiento cuántico.

2. El Procesado Clásico

Un sistema de comunicación clásico está compuesto esencialmente por tres bloques que son:

1. Fuente: Genera símbolos de un determinado conjunto finito, alfabeto, a intervalos regulares y de manera aleatoria e independiente de los símbolos generados con anterioridad.
2. Canal: Transmite los símbolos de un determinado conjunto, que denominamos alfabeto de entrada, y genera otros símbolos que pertenecen a otro conjunto que denominamos alfabeto de salida. Si ambos alfabetos no coinciden se hace necesario un proceso adicional de codificación y/o decodificación. Normalmente, el canal no es un sistema ideal, lo cual se traduce en la existencia de una probabilidad de error que hace que la información recibida pueda diferir de la enviada.
3. Receptor: Tiene como misión recuperar la información original con el máximo nivel de fidelidad.

La unidad de información en la teoría clásica es el bit. Un bit clásico consiste generalmente en un sistema macrocópico en el que se definen claramente y de forma arbitraria dos estados físicos del sistema que representan los estados lógicos 0 y 1.

Un número n de bits puede representar 2n estados lógicos, descritos por el rango de valores $[000\ldots0, 111\ldots1]$. Además de almacenar la información en formato binario, un sistema de procesamiento clásico puede manipularla. La manipulación de información binaria se realiza mediante una secuencia de operaciones booleanas, que al actuar sobre uno o dos bits simultáneamente pueden realizar cualquier transformación con resultado determinista.

Con el fin de estudiar la relación entre los recursos necesarios para representar información y las fuentes de información, es necesario introducir una medida de la cantidad de información que emite una determinada fuente. Dicha medida fue sugerida por C. E. Shannon, y se denomina ."Entropía"por analogía con la mecánica estadística. La entropía de una fuente de información con distribución de probabilidad p es:

$$H(p) = -\sum_x p(x) log\, p(x)$$

La entropía de una fuente es, intuitivamente, la cantidad de información que produce en promedio dicha fuente. Tambien se puede entender como la incertidumbre que tiene un observador frente a la próxima salida de la fuente (se

puede definir la entropía para fuentes más complejas como aquellas que pueden ser representadas por cademas de Markow).

En el clásico trabajo de Shannon sobre la teoria de la comunicación, se plantean una serie de propiedades razonables sobre la magnitud $H(p)$. La entropía de Shannon juegan un papel muy relavante en la teoría de la información clásica. En esta pequeña exposición sobre Información Cuántica no entraremos nos centraremos más (aunque no todo lo profundamente que se debiera) en su homólogo cuántico "La entropía de Von Neumann".

3. El Procesado Cuántico

En la teoría de la información cuántica los operadores densidad permiten describir estados cuánticos aleatorios de forma similar a las distribuciones de probabilidad para la información clásica. Es decir, una fuente de información cuántica puede verse como una secuencia de operadores densidad. En definitiva, una fuente de información cuántica se describe mediante un espacio de Hilbert H y un operador densidad ρ.

Los conceptos de Fuente, Canal y Receptor expuestos anteriormente se mantienen, pero con algunas puntualizaciones.

- Al símbolo generado por la fuente se le asocia un estado cuántico, descrito por un operador densidad, que se define sobre un espacio de estados n-dimensional.
- El alfabeto de entrada del canal pertenece a un estado de Hilbert bidimensional (qubits), con lo que se hace necesaria una codificación de la fuente que asigne a cada estado-simbolo una representación en qubits.
- Cualquier proceso relacionado con la transmisión de información que altere el estado asociado a la misma viene caracterizado por la acción de un superoperador, pero se suele incluir el comportamiento ruidoso del canal, debido a la interacción del sistema con su entorno, en el alfabeto fuente. En los canales libres de errores se asocia con cada símbolo un estado puro, mientras que en los ruidosos se suele emplear una mezcla estadística. Tenemos por tanto sistemas cuánticos cerrados, compuestos por subsistemas asociados a la información (sistemas abiertos) y al entorno ruidoso.
- En el procesado cuántico, la calidad de la comunicación se mide en el receptor mediante la función Fidelidad.

El elemento básico de representación de la información cuántica es el qubit. Un bit cuántico o qubit, puede representar un conjunto continuo de estados, que matemáticamente serían vectores unitarios en un espacio vectorial complejo bidimensional (espacio de Hilbert H_2).

En una base ortonormal representada por $|0\rangle$, $|1\rangle$ la forma más general de expresar un qubit sería de la forma:

$$|\psi\rangle = a_0|0\rangle + a_1|1\rangle$$

siendo a_0 y a_1 números complejos que verifican la propiedad de completitud:

$$|a_0|^2 + |a_1|^2 = 1$$

En un marco clásico tendriamos dos estados lógicos, el estado lógico 0 asociado al estado físico $|0\rangle$ o bien el estado 1 asociado al estado físico $|1\rangle$, es decir, un bit contiene una información claramente determinada. Sin embargo, una medida que proyecte un qubit sobre la base $|0\rangle, |1\rangle$ siempre proporciona un resultado basado en probabilidades, y tan solo se obtiene una medida estable si uno de los dos coeficientes complejos a_0 o a_1 es igual a cero. Además de los diferentes valores que pueden tomar los módulos de los coeficientes a_0 y a_1, hay que tener también en cuenta su desfase o interferencia, de lo cual se entrevee que el qubit no puede ser tratado unicamente desde una perspectiva de probabilidad clásica.

Los estados del qubit tienen su correspondencia con un sistema cuántico real, tal como un átomo, el spin de un nucleo o fotones polarizados. Los estados lógicos 0 y 1 vendrán dados por un par de estados distinguibles del sistema cuántico. Sin embargo, el sistema tambien genera una continuo de estados de superposción, que matemáticamente se representan como vectores unitarios en el espacio de Hilbert H_2. Dos estados cuánticos son realmente distinguibles si y solo si sus representaciones vectoriales son ortogonales.

4. Implicaciones Fundamentales

El procesado de información con sistemas cuántico conlleva tres propiedades: Impredecibilidad, indistinguibiliddad y no clonabilidad.

4.1. Impredecibilidad

No hay ningún estado cuántico tal que a la hora de realizar una medida, se pueda establecer probabilidad uno a algún dato. En los sistemas cuánticos, información maximal no es lo mismo que información completa. Se dice que una medida es maximal cuando consta del número máximo de proyectores ortogonales. En un espacio de Hilbert de dimensión $\mathcal{D}$, el número de proyectores mutuamente ortogonales es precisamente $\mathcal{D}$.

Dada una medida maximal con proyectores $\Pi_d = |\psi_d\rangle\langle\psi_d|$, la representación espectral del estado cuántico asignado al sistema será:

$$\rho = \sum_i \lambda_i |\lambda_i\rangle\langle\lambda_i|$$

La probabilidad $p(d)$ de adquisición del dato d se evalúa mediante $tr(\rho\Pi_d)$, con lo cual se puede escribir:

$$p(d) = \sum_i \lambda_i \left|\langle\lambda_i|\psi_d\rangle\right|^2 \leq \left|\langle\lambda_i|\psi_d\rangle\right|^2 = 1$$

Como ρ es un operador densidad, la igualdad solo se alcanzará cuando el estado cuántico ρ sea unidimensional, e igual al proyector Π_d, es decir cuando el propio estado cuántico sea uno de los elementos de la medida maximal. Por lo tanto, en un contexto de adquisición de datos mediante medidas maximales, se puede disponer de certeza en cuanto a un dato, solo si se asigna al sistema un estado cuántico también maxiimal, incluido en la propia medida.

En cuanto a medidas no maximales, sí es posible disponer de certeza con respecto a algunas de ellas aun en el caso de un estado cuántico no maximal. Si se considera un medida no maximal con proyectores Π_d, a la adquisición del dato d se le puede asociar la probabilidad:

$$p(d) = tr(\rho\Pi_d) = \sum_i \lambda_i \langle\lambda_i|\Pi_d|\lambda_i\rangle$$

La probabilidad $p(d)$ solo alcanza la unidad cuando lo hacen todos los factores $\langle\lambda_i|\Pi_d|\lambda_i\rangle$, para los cuales $\lambda_i \neq 0$. Esta condición es equivalente a $\Pi_d|\lambda_i\rangle = |\lambda_i\rangle$, es decir $|\lambda_i\rangle$ debe pertenecer al soporte del proyector Π_d. La condición final es que el soporte $\mathcal{S}_\rho$ del estado cuántico esté contenido en el soporte del proyector, $\mathcal{S}_{\Pi_d}$. Por lo tanto, el proyector correspondiente al dato sobre el que se desea tener certeza ha de ser de la forma:

$$\Pi_d = \sum_{i|\lambda\neq 0} |\lambda_i\rangle\langle\lambda_i| + \ldots$$

donde Π_d puede incluir otros proyectores unidimensionales y ortogonales. Esta condición también puede expresarse como:

$$\Pi_d\rho = \rho\Pi_d = \rho$$

Por lo tanto, dado un estado cuántico no maximal, se puede disponer de certeza sólo y cuando la medida sea a su vez no maximal y el soporte del estado cuántico esté contenido en el de alguno de los proyectores de la medida.

En el ámbito del procesado cuántico se utiliza la denominación de estados cuánticos de información maximal. En base a lo expuesto en este punto, se infiere que esta denominación está relacionada con la certeza en la adquisición de datos.

La condición necesaria y suficiente para disponer de certeza ante una medida consiste en que el soporte del estado cuántico esté contenido en el de alguno de los proyectores de aquella. En el caso de que la medida sea maximal, ello supone que el estado cuántico coincida con uno de los proyectores, y por tanto, que sea un operador densidad unidimensional. Entonces, un operador densidad unidimensional es un estado cuántico maximal en el sentido de qu provee de

certeza para algunas medidas correspondientes a un número máximo de alternativas, igual a la dimensión del espacio de Hilbert. Por el contrario, en el caso de operadores de densidad estrictamente multidimensionales, se puede disponer de certeza solo para medidas con un número de alternativas menor que el máximo. En particular, siendo $\mathcal{S}_\rho$ el soporte del estado cuántico ρ, si se denota como N el número de alternativas para la medida, la condición de certeza implica la siguiente desigualdad:

$$N \leq D - dim(\mathcal{S}_\rho)$$

Por lo tanto el número máximo de alternativas es estrictamente menor que el máximo $\mathcal{D}$. La estructura de la mecánica clásica admite estados que, en principio, permite disponer de certeza en torno a la adquisición de datos en cualquier contexto experimental admisible para el sistema dado. La estructura de la teoría es por tanto determinista, y de tales estados se dice que son de información completa. La estructura de la teoría cuántica es indeterminista. En un escenario cuántico, el análogo de lo estados clásicos deterministas viene dado por los estados cuánticos maximales, ya que son los únicos que permiten disponer de certeza para algunos conjuntos de contexto de adquisición en un número máximo de alternativas o de máxima capacidad resolutiva. Ya que ningún estado cuántico aporta certeza para todos estos contextos se puede decir que en lo que respecta al procesado con sistemas cuánticos, información maximal no es información completa.

4.2. Indistinguibilidad

Supongamos un conjunto ortogonal de estados puros, $\{|\psi_x\rangle\}_x$, del cual escogemos el ket $|\psi_x\rangle$ con probabilidad p_x. Para un observador que no conozca la decisión tomada, el sistema se encontrará caracterizado por una mezcla estadística tal como:

$$\hat{\rho} = \sum_x p_x |\psi_x\rangle\langle\psi_x|$$

Si en un instante dado se desea conocer la elección concreta que se efectuó, lo más conveniente será realizar una medida de Von Neumann:

$$\hat{Y} = \sum_y a_y \hat{P}_y$$

donde $\hat{P}_y = |\psi_y\rangle\langle\psi_y|$. Por consiguiente, la obtención como resultado de la medida de un valor a_y determina perfectamente el ket seleccionado, $|\psi_y\rangle$. Sin embargo, ¿que ocurriria si el conjunto sobre el que se escoge el estado no es un conjunto ortogonal? Entonces ya no sería posible determinar con seguridad el estado puro elegido, debido a que para un cierto valor de a_y, siempre habrá varios estados con probabilidad distinta de cero que podrían producir dicho resultado, estos son aquellos estaod $|\psi_x\rangle$ para los que $\langle\psi_x|\psi_x\rangle neq 0$. Ninguna medida permite distinguir o discriminar entre estados cuánticos no ortogonales.

4.3. No Clonabilidad

Podría decirse que copiar un estado cuántico consiste en transferir el estado de un sistema cuántico a otro sistema, preservando el del primero. El esquema de procesado utilizado debe ser válido independientemente del estado cuántico original que se pretenda copiar. Sin embargo una de las grandes diferencias con la Teoría de la Información Clásica es la imposibilidad de copiar un estado cuántico desconocido con total fidelidad. Esto es un corolario del principio de incertidumbre de Heisenberg.

Sean dos espacios de estados bidimensionales representados por $\mathcal{E}_A$ y $\mathcal{E}_B$ y su espacio conjunto:

$$\mathcal{E}_{AB} = \mathcal{E}_A \otimes \mathcal{E}_B$$

Haciendo uso de una puerta cuántica XOR se puede demostrar que siempre es posible encontrar un operador unitario $\hat{U}_{AB}$ que a partir de un conjunto de estados ortogonales de $\mathcal{E}_A$ consiga igualar el estado de $\mathcal{E}_B$ a cualquiera de los kets del conjunto:

$$\hat{U}_{AB} : |0\rangle_A|0\rangle_B \longrightarrow |0\rangle_A|0\rangle_B$$

$$\hat{U}_{AB} : |1\rangle_A|0\rangle_B \longrightarrow |1\rangle_A|1\rangle_B$$

Sin embargo este mismo operador no puede ser empleado cuando el estado de $\mathcal{E}_A$ está descrito pun un ket que no es ortogonal a los estados para los que fue diseñado.

$$\hat{U}_{AB} : (a|0\rangle_A + b|1\rangle_A)|0\rangle_B \longrightarrow a|0\rangle_A|0\rangle_B + b|1\rangle_A|1\rangle_B \neq$$

$$\neq (a|0\rangle_A + b|1\rangle_A) \otimes (a|0\rangle_B + b|1\rangle_B)$$

Por tanto, cuando el estado a copiar es desconocido, normalmente una superposición, no se tiene ninguna garantia de que la operaación de copiar (clonar) vaya a ser realizada con éxito.

A grandes rasgos, cualquier sistema de comunicación puede estructurarse en tres bloques básicos: Emisor, canal y receptor, siendo este último el de mayor complejidad en lo que se refiere al análisis y diseño.

En el contexto de las comunicaciones, el hecho de tomar una decisión sobre un estado cuántico consisten en inferir la asignación que se hizo en el transmisor a partir de la adquisición de algún dato en el receptor.

5. Entropía de Von Neumann

Dada la fuerte analogía que existe entre las fuentes clásicas y las fuentes cuánticas, la entropia de Von Neumann surge como una generalización de la entropía de Shannon. Por la importancia de este concepto en ambas teorías de la información (clásica y cuántica) se concluimos con una breve revisión del mismo.

Supongamos una fuente con un alfabeto de entrada de n elementos que genera, con una probabilidad p_x un símbolo caracterizado por el operador densidad $\hat{\rho}_x$. El estado cuántico proporcionado por la fuente se puede describir por:

$$\hat{\rho} = \sum_x p_x \hat{\rho}_x$$

Definimos la entropia de Von Neumann como la función de $\hat{\rho}$ que viene dada por:

$$S(\hat{\rho}) = -tr(\hat{\rho}\, log\hat{\rho})$$

si se elige una base ortonormal que proporcione una representación matricial diagonal del operador ρ, tal como:

$$\hat{\rho} = \sum_a \lambda_a |a\rangle\langle a|$$

Es fácil ver que la entropia de Von Neumann coincide con la de Shannon al considerar una fuente clásica que genera símbolos a con probabilidad λ_a. Por lo tanto, se pude decir que la entropia de Shannon es una particularización de la entropia de Von Neumann $S(\hat{\rho})$ para un alfabeto fuente compuesto de símbolos ortogonales.

También es interesante ver como $S(\hat{\rho})$ refleja la distinción entre un estado puro y una mezcla estadística. Se constata que tan solo en el caso de estados puros $S(\hat{\rho}) = 0$. Del mismo modo, se podría verificar que la evolución unitaria determinada por la ecuación de Schrödinger no modifica el valor de $S(\hat{\rho})$ (evolución reversible), mientras que la decoherencia producida por la influencia del entorno sí provoca un aumento de la entropía de Von Neumann (evolución irreversible). Se puede decir que mientras un incremento de $S(\hat{\rho})$ está relacionado conla pérdida de información, una reducción de la entropía implica una ganancia de esta.

A continuación se enumeran algunas propiedades útiles dela de la entropía de Von Neumann $S(\hat{\rho})$ donde se ven claramente los aspectos diferenciadores con respecto a la entropía clasica de Shannon:

1. **Rango:** Para cualquier número real, $c \in \mathbb{R}$ y $0 \leq c \leq \infty$ siempre existe un operador densidad $\hat{\rho}$ que verifica $S(\hat{\rho}) = c$

2. **Valor máximo:** Si un operador densidad $\hat{\rho}$ posee N autovalores distintos de cero, entonces:
   $$S(\hat{\rho}) \leq logN$$
   La igualdad solo tiene lugar cuando los N autovalores son iguales.

3. **Invariancia:** Una modificación unitaria del estado no modifica su entropía
   $$S\left(\hat{U}\hat{\rho}\hat{U}^{-1}\right) = S(\hat{\rho})$$

4. **Entropía de una mezcla estadística:** Para un sistema cuántico caracterizado por la mezcla estadística:

$$\hat{\rho} = \sum p_x |\psi_x\rangle\langle\psi_x|$$

Se puede demostrar que:

$$H(X) \geq S(\hat{\rho})$$

donde X es una variable aleatora que toma un valor x con probabilidad p_x y $H(x)$ es la entropia de Shannon. La igualdad solo se verifica si el conjunto es ortogonal. Fisicamente este resultado significa la imposibilidad de distinguir perfectamente estados no ortogonales.

5. **Entropía del resultado de una medida:** Dado un sistema descrito por el operador densidad $\hat{\rho}$ y un obserbable $\hat{A}$:

$$\hat{A} = \sum_n a_n |\psi_n\rangle\langle\psi_n|$$

se cumple que:

$$H(X) \leq S\hat{\rho}$$

donde X representa una variable aleatoria que toma un valor a_n con probabilidad $p_n = \langle a_n|\hat{\rho}|a_n\rangle$ y $H(x)$ es la entropía de Shannon. La igualdad solo es cierta si $[\hat{A}, \hat{\rho}] = 0$. Esta propiedad viene a significar que el resultado de medir una magnitud es menos predecible si su observable asociado no conmuta con el estado cuántico del sistema.

6. **Discontinuidad:** Dado un operador de densidad lineal $\hat{\rho}$ y un número cualquiera $\varepsilon > 0$, siempre existe $\hat{\rho}'$ tal que:

$$tr|\hat{\rho} - \hat{\rho}'| \leq \varepsilon \qquad y \qquad S(\hat{\rho}) = \infty$$

Por tanto, $S(\hat{\rho})$ es claramente, discontinua.

Bibliografia

1. Shannon C. E., .ª Mathematical Theory of Communication", The Bell System Technical Journal, Vol 27, pp.370-423, 1948

2. Charles H. Bennet y Peter W. Shor, "Quantum Information Theory"IEEE Transactions on Information Theory, (Octubre 1998)

3. Nielsen M. A. y Chuan I.L. "Quantum Computation and Quantum Information", Cambridge University Press, ISBN 0-521-63503-9, 2000

4. Marcos Perez-Suarez y David J.Santos, "Procesado de Información con sistemas Cuánticos", Serv. Public. de Univ. de Vigo, ISBN 84-8158-315-4, 2006