



Redes de comunicación cuántica a grandes escalas

Marco Méndez y Alfredo Villegas

noviembre 2022

Universidad Simón Bolívar

Resumen

La codificación de redes cuánticas de gran escala, en inglés: Large-scale quantum network coding (LQNC) Es un método pensado para distribuir qubits entrelazados por redes de comunicación cuántica de grandes escalas que soportan la teleportación y la distribución de claves cuánticas.

El proceso consta de un procedimiento de codificación para distribuir pares entrelazados de qubits entre los pares de usuarios emisor-receptor conectados por una ruta troncal de N saltos. El tipo de red propuesta se conoce como red mariposa. El sistema propuesto es entonces comparado con los sistemas basados en el entrelazamiento de intercambio para resaltar los beneficios.

1. Resumen
2. Codificación de redes cuánticas
3. Esquema general de la red de comunicación cuántica
4. Conclusiones

Codificación de redes cuánticas

Redes de comunicación cuántica

Las **redes de comunicación cuántica** abarcan el caso en el que se tienen más de dos nodos, estableciendo así topologías diversas en donde se tiene como objetivo transmitir qubits desde usuarios fuentes hacia usuarios objetivos vía teleportación.

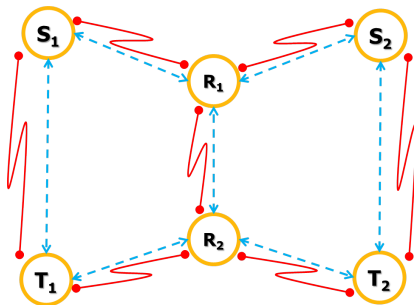


Figura 1: Ejemplo de red cuántica tipo mariposa.

Codificación de redes cuánticas

El método más eficiente para establecer entrelazamiento entre usuarios de una red separados por nodos repetidores es la [codificación de redes cuánticas](#).

El método consiste en realizar operaciones no unitarias sobre los estados entrelazados de los nodos con el fin de obtener un entrelazamiento entre los nodos deseados.

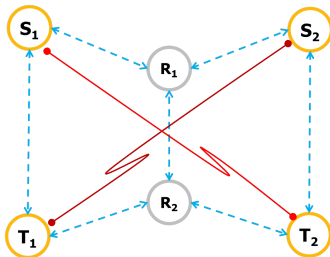


Figura 2: Red cuántica luego de la codificación

Operaciones no unitarias de la codificación de redes

Las operaciones no unitarias de codificación están basadas en **circuitos cuánticos** compuestos por operaciones unitarias y de medida. Estas son:

- Connect
- Removal
- Fanout
- Add
- RemAdd

Estas operaciones son *no unitarias*, debido a que no preservan la cantidad de particiones del estado de entrada y de salida.

Dado que estas operaciones se realizan en redes cuánticas es **importante** observar que las particiones de los estados entrelazados se encuentran físicamente en **nodos distantes**.

Operación Connect

Los estados $|AB\rangle$ y $|CD\rangle$ son estados máximamente entrelazados, como por ejemplo los estados de Bell, el circuito transforma estos dos estados y los **conecta** descartando una de las particiones para así tener un estado entrelazado de tres particiones a la salida.

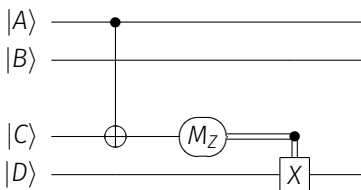


Figura 3: Diagrama de circuito cuántico de la Operación Connect

El estado a la salida es un estado tripartito máximamente entrelazado. Por ejemplo el estado GHZ.

$$|\psi_{out}\rangle = \frac{1}{\sqrt{2}}(|000\rangle_{ABD} + |111\rangle_{ABD})$$

Operación Removal

La operación está concebida para **remove** un qubit de un estado entrelazado, aplicando la compuerta Hadamard y luego midiendo ese qubit en la base “+” (también llamada base Z), el resultado de esa medida controla la compuerta Z en la partición “B”, de esta forma se evita una posible pérdida de información.

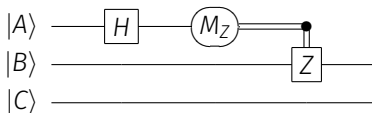


Figura 4: Diagrama de circuito cuántico de la Operación Removal

Operación Add

Esta operación es muy similar a Connect, la diferencia radica en la compuerta CNOT adicional con otro par EPR.

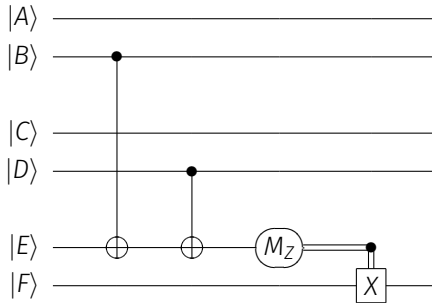


Figura 5: Diagrama de circuito cuántico de la Operación Add

Operación FanOut

Esta operación es equivalente a realizar la operación Connect dos veces, tomando el mismo qubit de control y aplicarlo a otro par entrelazado, conectando así el control a dos pares entrelazados.

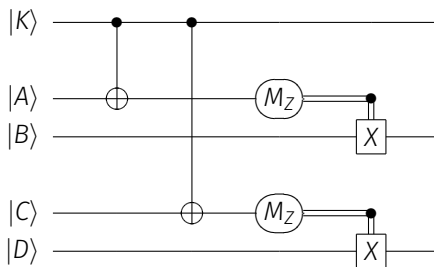


Figura 6: Diagrama de circuito cuántico de la Operación FanOut

Operación RemAdd

Esta operación es similar a Removal, con la salvedad de que existe un control clásico adicional que va a una compuerta Z en la partición “C”.

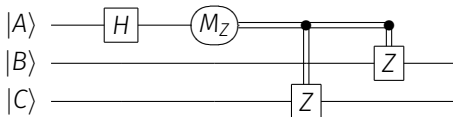


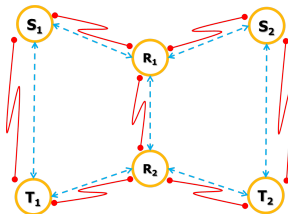
Figura 7: Diagrama de circuito cuántico de la Operación RemAdd

Codificación de una red cuántica para una red troncal simétrica

¿Qué es una red troncal simétrica?

Una red troncal simétrica, conocida también como **“Red mariposa”**, es una red compuesta por una cantidad par de parejas de usuarios fuente-objetivo, que se encuentran conectados entre sí y a su vez a un enlace troncal de repetidores. Las redes mariposa a considerar se diferencian por la cantidad de pares de usuarios M y la cantidad N de enlaces entre las repetidoras de la ruta troncal.

En este tipo de redes, sobre los diferentes nodos de la red se aplican las operaciones de codificación ya descritas en función de M y N .



Codificación de una red cuántica para una red troncal simétrica

Red mariposa $N=1, M=2$

La red mariposa más simple es aquella con $N = 1$ saltos entre repetidoras y $M = 2$ pares de usuarios.

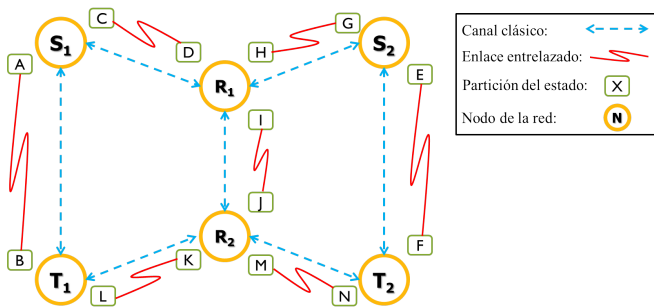


Figura 8: Red cuántica tipo mariposa, luego de distribuir entrelazamiento y antes de la codificación.

Codificación de una red cuántica para una red troncal simétrica

Cuadro 1: Etapas de la codificación de la red tipo mariposa para el caso $N = 1$ y $M = 2$

Fases	Operaciones	Nodos
1	$Con_{C \rightarrow D}^A$ $Con_{G \rightarrow H}^E$	$S_1 \rightarrow R_1$ $S_2 \rightarrow R_1$
2	$Add_{I \rightarrow J}^{D,H}$	$R_1 \rightarrow R_2$
3	$Fan_{K \rightarrow L, M \rightarrow N}^J$	$R_2 \rightarrow T_1, T_2$
4	$CNOT_{L,B}$ $CNOT_{N,F}$	T_1 T_2
5	$Rem_{L \rightarrow J}$ $Rem_{N \rightarrow J}$	$T_1 \rightarrow R_2$ $T_2 \rightarrow R_2$
6	$RemAdd_{J \rightarrow D, H}$	$R_2 \rightarrow R_1$
7	$Rem_{D \rightarrow A}$ $Rem_{H \rightarrow E}$	$R_1 \rightarrow S_1$ $R_1 \rightarrow S_2$

Cálculos de la codificación de redes cuánticas simétricas

Por tratarse de operaciones no unitarias los estados al final de la codificación no se encuentran normalizados, sin embargo conociendo que estos estados finales serán máximamente entrelazados se entiende que al normalizar se obtiene que la amplitud de probabilidad de cada par EPR es de $\frac{1}{\sqrt{2}}$.

Red mariposa $N=1, M=2$

Se muestran los cálculos de la codificación de la red tipo mariposa más simple, donde $M = 2$ representan dos pares de usuarios emisor y receptor, y $N = 1$ representa la cantidad de saltos entre las repetidoras de la línea troncal.

Siguiendo la Figura 8 al inicio se tienen siete estados entrelazados entre cada vértice de la red que corresponden al siguiente estado inicial.

$$|\psi_{\text{inicial}}\rangle = |MN\rangle |KL\rangle |IJ\rangle |GH\rangle |EF\rangle |CD\rangle |AB\rangle$$

Cálculos para una red mariposa N=1, M=2

Fase 1: Se aplican las operaciones $Con_{C \rightarrow D}^A$, y $Con_{G \rightarrow H}^E$. Esto resulta en:

$$|\psi_1\rangle = |MN\rangle |KL\rangle |IJ\rangle \left[\frac{1}{\sqrt{2}} (|000\rangle_{EFH} + |111\rangle_{EFH}) \right] \left[\frac{1}{\sqrt{2}} (|000\rangle_{ABD} + |111\rangle_{ABD}) \right]$$

Fase 2: Se aplica $Add_{I \rightarrow J}^{D,H}$. Reescribimos $|\psi_1\rangle$

$$|\psi_1\rangle = |MN\rangle |KL\rangle |IJ\rangle (|000\rangle_{EFH} |000\rangle_{ABD} + |000\rangle_{EFH} |111\rangle_{ABD} + \\ |111\rangle_{EFH} |000\rangle_{ABD} + |111\rangle_{EFH} |111\rangle_{ABD} +$$

Se aplica la operación.

$$|\psi_2\rangle = Add_{I \rightarrow J}^{D,H} |\psi_1\rangle \\ |\psi_2\rangle = |MN\rangle |KL\rangle |000\rangle_{EFH} |000\rangle_{ABD} |0\rangle_J + |MN\rangle |KL\rangle |000\rangle_{EFH} |111\rangle_{ABD} |1\rangle_J \\ + |MN\rangle |KL\rangle |111\rangle_{EFH} |000\rangle_{ABD} |1\rangle_J + |MN\rangle |KL\rangle |111\rangle_{EFH} |111\rangle_{ABD} |0\rangle_J$$

Hasta ahora, se han descartado las particiones “C”, “G”, y “I”.

Cálculos para una red mariposa $N=1, M=2$

Fase 3: Se aplica la operación $Fan_{K \rightarrow L, M \rightarrow N}^J$. Recordando que las operaciones de codificación están compuestas de operaciones unitarias y medidas, separamos esta operación “Fan” en partes.

El circuito cuántico para esta Fase 3 sería el siguiente:

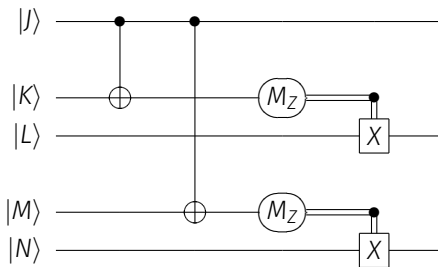


Figura 9: Diagrama de circuito cuántico de la Fase 3

Cálculos para una red mariposa N=1, M=2

Fase 3: Parte a.

Esta parte se refiere a la operación $CNOT_{K,M}^J$ al inicio del circuito, el estado resultante queda así.

$$\begin{aligned} |\psi_{3.a}\rangle = & \left[\frac{1}{2}(|00\rangle_{MN} + |11\rangle_{MN})(|00\rangle_{KL} + |11\rangle_{KL}) \right] |000\rangle_{EFH} |000\rangle_{ABD} |0\rangle_J \\ & + \left[\frac{1}{2}(|10\rangle_{MN} + |01\rangle_{MN})(|10\rangle_{KL} + |01\rangle_{KL}) \right] |000\rangle_{EFH} |111\rangle_{ABD} |1\rangle_J \\ & + \left[\frac{1}{2}(|10\rangle_{MN} + |01\rangle_{MN})(|10\rangle_{KL} + |01\rangle_{KL}) \right] |111\rangle_{EFH} |000\rangle_{ABD} |1\rangle_J \\ & + \left[\frac{1}{2}(|00\rangle_{MN} + |11\rangle_{MN})(|00\rangle_{KL} + |11\rangle_{KL}) \right] |111\rangle_{EFH} |111\rangle_{ABD} |0\rangle_J \end{aligned}$$

Cálculos para una red mariposa N=1, M=2

Fase 3: Parte b.

Esta parte se refiere a la medida en “M”, eliminar el registro y controlar la compuerta X.

$$\begin{aligned} |\psi_{3.b}\rangle = & \left[\frac{1}{\sqrt{2}} |0\rangle_N (|00\rangle_{KL} + |11\rangle_{KL}) \right] |000\rangle_{EFH} |000\rangle_{ABD} |0\rangle_J \\ & + \left[\frac{1}{\sqrt{2}} |1\rangle_N (|10\rangle_{KL} + |01\rangle_{KL}) \right] |000\rangle_{EFH} |111\rangle_{ABD} |1\rangle_J \end{aligned}$$

Fase 3: Parte c.

Esta parte se refiere a la medida en “K”, eliminar el registro y controlar la compuerta X.

$$\begin{aligned} |\psi_{3.c}\rangle = & |0\rangle_N |0\rangle_L |000\rangle_{EFH} |000\rangle_{ABD} |0\rangle_J + |1\rangle_N |1\rangle_L |000\rangle_{EFH} |111\rangle_{ABD} |1\rangle_J \\ & + |1\rangle_N |1\rangle_L |111\rangle_{EFH} |000\rangle_{ABD} |1\rangle_J + |0\rangle_N |0\rangle_L |111\rangle_{EFH} |111\rangle_{ABD} |0\rangle_J \end{aligned}$$

Fase 3: Resultado

Reescribiendo, al finalizar la Fase 3:

$$\begin{aligned} |\psi_3\rangle = & |000\rangle_{EFH} |000\rangle_{ABD} |000\rangle_{JNL} + |000\rangle_{EFH} |111\rangle_{ABD} |111\rangle_{JNL} \\ & + |111\rangle_{EFH} |000\rangle_{ABD} |111\rangle_{JNL} + |111\rangle_{EFH} |111\rangle_{ABD} |000\rangle_{JNL} \end{aligned}$$

Cálculos para una red mariposa N=1, M=2

Fase 4: Operaciones $CNOT_{L,B}$ y $CNOT_{N,F}$.

$$\begin{aligned} |\psi_4\rangle = & |000\rangle_{EFH} |000\rangle_{ABD} |000\rangle_{JNL} + |010\rangle_{EFH} |101\rangle_{ABD} |111\rangle_{JNL} \\ & + |101\rangle_{EFH} |010\rangle_{ABD} |111\rangle_{JNL} + |111\rangle_{EFH} |111\rangle_{ABD} |000\rangle_{JNL} \end{aligned}$$

Fase 5: Operaciones $Rem_{L \rightarrow J}$ y $Rem_{N \rightarrow J}$

$$\begin{aligned} |\psi_5\rangle = Rem_{L \rightarrow J} |\psi_4\rangle = Rem_{L \rightarrow J} [& |000\rangle_{JNL} (|000\rangle_{EFH} |000\rangle_{ABD} + |111\rangle_{EFH} |111\rangle_{ABD}) \\ & + |111\rangle_{JNL} (|010\rangle_{EFH} |101\rangle_{ABD} + |101\rangle_{EFH} |010\rangle_{ABD})] \end{aligned}$$

Hadamard en "L":

$$\begin{aligned} |\psi_{5.a}\rangle = & \frac{1}{\sqrt{2}} (|000\rangle_{JNL} + |001\rangle_{JNL}) (|000\rangle_{EFH} |000\rangle_{ABD} + |111\rangle_{EFH} |111\rangle_{ABD}) \\ & + \frac{1}{\sqrt{2}} (|110\rangle_{JNL} - |111\rangle_{JNL}) (|010\rangle_{EFH} |101\rangle_{ABD} + |101\rangle_{EFH} |010\rangle_{ABD}) \end{aligned}$$

Cálculos para una red mariposa N=1, M=2

Medir en “L” y controlar Z en “J” y descartar “L”:

$$\begin{aligned} |\psi_{5.b}\rangle = & |00\rangle_{JN} (|000\rangle_{EFH} |000\rangle_{ABD} + |111\rangle_{EFH} |111\rangle_{ABD}) \\ & + |11\rangle_{JN} (|010\rangle_{EFH} |101\rangle_{ABD} + |101\rangle_{EFH} |010\rangle_{ABD}) \end{aligned}$$

Ahora se realiza el segundo Removal. Hadamard en “N”:

$$\begin{aligned} |\psi_{5.c}\rangle = & \frac{1}{\sqrt{2}} (|00\rangle_{JN} + |01\rangle_{JN}) (|000\rangle_{EFH} |000\rangle_{ABD} + |111\rangle_{EFH} |111\rangle_{ABD}) \\ & + \frac{1}{\sqrt{2}} (|10\rangle_{JN} - |11\rangle_{JN}) (|010\rangle_{EFH} |101\rangle_{ABD} + |101\rangle_{EFH} |010\rangle_{ABD}) \end{aligned}$$

Medir en “N” y controlar compuerta Z, se descarta “N”.

$$\begin{aligned} |\psi_5\rangle = & |0\rangle_J (|000000\rangle_{EFHABD} + |111111\rangle_{EFHABD}) \\ & + |1\rangle_J (|010101\rangle_{EFHABD} + |101010\rangle_{EFHABD}) \end{aligned}$$

Cálculos para una red mariposa N=1, M=2

Fase 6: Operación $RemAdd_{J \rightarrow D, H}$, se realiza un Hadamard en “J” se mide y se controlan las compuertas Z en “D” y “H”, resulta en:

$$|\psi_6\rangle = |000000\rangle_{EFHABD} + |010101\rangle_{EFHABD} + |101010\rangle_{EFHABD} + |111111\rangle_{EFHABD}$$

Fase 7: Operación $Rem_{D \rightarrow A}$ y $Rem_{H \rightarrow E}$, esto queda en:

$$|\psi_7\rangle = |00\rangle_{EF} |00\rangle_{AB} + |01\rangle_{EF} |10\rangle_{AB} + |10\rangle_{EF} |01\rangle_{AB} + |11\rangle_{EF} |11\rangle_{AB}$$

Cálculos para una red mariposa N=1, M=2

Esta última fue la operación final, reescribiendo tenemos:

$$\begin{aligned} |\psi_f\rangle = & |0\rangle_A |0\rangle_F |0\rangle_B |0\rangle_E + |1\rangle_A |1\rangle_F |0\rangle_B |0\rangle_E \\ & + |0\rangle_A |0\rangle_F |1\rangle_B |1\rangle_E + |1\rangle_A |1\rangle_F |1\rangle_B |1\rangle_E \end{aligned}$$

Factorizando

$$|\psi_f\rangle = |00\rangle_{AF} (|00\rangle_{BE} + |11\rangle_{BE}) + |11\rangle_{AF} (|00\rangle_{BE} + |11\rangle_{BE})$$

Se obtiene como estado final:

$$|\psi_f\rangle = (|00\rangle_{AF} + |11\rangle_{AF})(|00\rangle_{BE} + |11\rangle_{BE})$$

Codificación de una red cuántica para una red troncal simétrica

Luego de las operaciones de codificación, se tiene el entrelazamiento requerido.

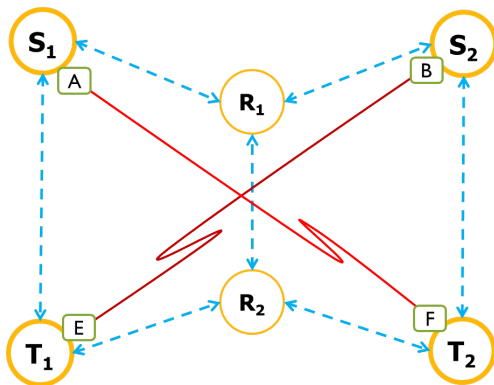


Figura 10: Red cuántica luego de la codificación

Codificación de una red cuántica para una red troncal simétrica

Existen otros tipos de redes mariposa de mayor tamaño, al aumentar la cantidad de saltos N entre repetidores es necesario añadir una Fase de codificación que enlace todo el troncal, al aumentar la cantidad de usuarios M aumentan las operaciones dentro de cada Fase.

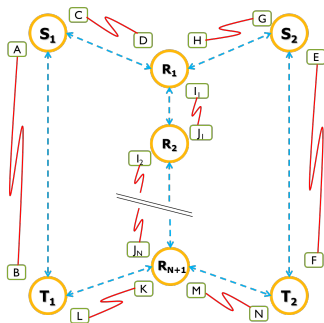
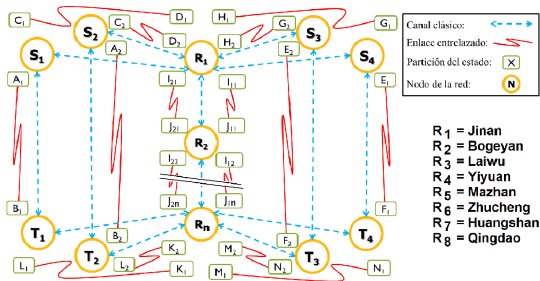
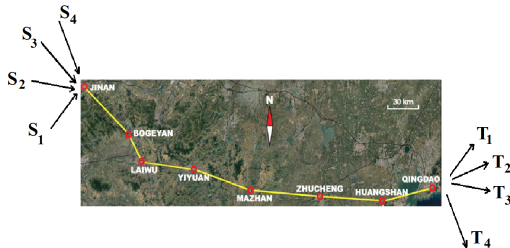


Figura 11: Red mariposa con N saltos arbitrarios y $M=2$ pares de usuarios

Codificación de una red cuántica para una red troncal simétrica



Distribución de entrelazamiento

Distribución o intercambio de entrelazamiento

Dado que se desea como objetivo realizar teleportación, y la teleportación requiere entrelazamiento a distancia, principalmente las redes cuánticas requieren distribuir entrelazamiento entre los nodos cercanos conectados por canales cuánticos.

La distribución de entrelazamiento se basa principalmente en la generación de entrelazamiento con fotones que son enviados por canales de fibra óptica o espacio libre hacia dos nodos adyacentes, estableciendo entrelazamiento a distancia.

Posterior a la distribución de entrelazamiento entre nodos cercanos, se necesita lograr un entrelazamiento a mayor escala, esto se puede lograr mediante la [codificación](#) de la red.

Intercambio de Entrelazamiento

Este protocolo de codificación de red busca establecer el entrelazamiento entre dos qubits lejanos, consiste en conectar dos pares entrelazados para obtener uno solo a una distancia mayor, esto se logra posterior a la distribución de entrelazamiento entre repetidoras cercanas. Este método es el más sencillo e intuitivo para conectar un par fuente-objetivo que se encuentra separados por una o más repetidoras cuánticas.

Se utilizan las operaciones siguientes en este orden

1. La operación *Connect*, $Con_{C \rightarrow D}^B$, que conecta $|B\rangle$ con $|C\rangle$, mide $|C\rangle$ y envía información clásica a $|D\rangle$, la partición $|C\rangle$ será descartada.
2. La operación *Removal*, $Rem_{B \rightarrow A}$, que mide en $|B\rangle$ y envía información clásica a $|A\rangle$, la partición $|B\rangle$ será descartada.

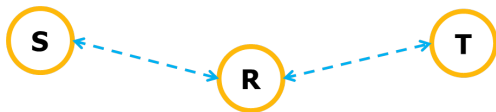


Figura 14: Esquema de tres nodos.

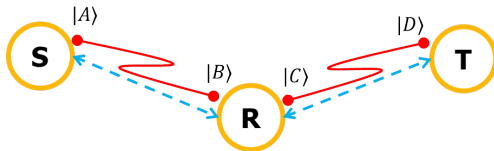


Figura 15: Esquema de tres nodos, luego de distribuir el entrelazamiento.

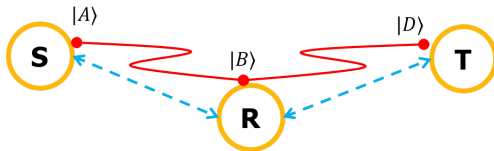


Figura 16: Esquema de tres nodos, luego de aplicar Connect en el repetidor.

Intercambio de Entrelazamiento

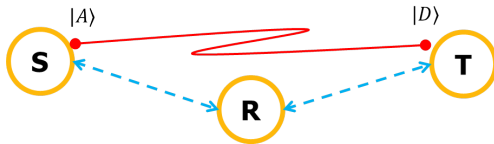


Figura 17: Esquema de tres nodos, luego de aplicar Removal en el repetidor. Se obtiene entonces el entrelazamiento requerido para aplicar la teleportación.

Esquema general de la red de comunicación cuántica

Esquema general de la red cuántica

Capa física clásica y cuántica

La red cuántica y sus capas requieren de un canal clásico auxiliar para comunicar información sobre las medidas y operaciones realizadas. Y la capa física cuántica se compone del medio o canal por el cual se transmiten los estados cuánticos como fotones, este canal puede ser espacio libre (aire), o bien fibras ópticas. Para este esquema, en esta capa los estados que se transmiten son estados entrelazados EPR.

Capa de entrelazamiento

Es necesario distribuir el entrelazamiento entre los nodos adyacentes de la red. La codificación de las redes requiere que los nodos compartan pares entrelazados inicialmente.

Esquema general de la red cuántica

Capa de codificación de red

Para lograr el entrelazamiento entre nodos distantes más allá de los nodos adyacentes, existen diversos métodos de codificación que varían dependiendo de la topología, el entrelazamiento a distancia es un recurso fundamental de la teleportación de la capa superior y es la contribución principal del paper de Nguyen.

Capa de teleportación

Luego de tener el entrelazamiento deseado se puede teleportar información cuántica, o bien utilizar el entrelazamiento para otro propósito.

Capa de seguridad

Sobre la teleportación pueden realizarse protocolos de criptografía cuántica, por ejemplo se pueden usar protocolos QKD que consisten en distribuir claves cuánticas.

Conclusiones

Conclusiones

Para resumir, el diseño de LQNC puede ser llevado a cabo usando los siguientes pasos.

1. Se requiere partir la red compleja dada en fragmentos. Entonces el más beneficioso entre los protocolos ES y LQNC puede ser usado para convertir la estructura arbitraria de los fragmentos a una extensión de la red mariposa.
2. Luego se interpretan los detalles de los requerimientos de diseño. Que puede abarcar los parámetros característicos de un sistema LQNC, incluyendo el número involucrado de pares M entrelazados y la fidelidad a la entrada y la salida, así como el número de repetidoras cuánticas disponibles definiendo el número de saltos N . Esto se puede notar que se debe a la conversión del paso 1, la fidelidad de un particular par entrelazado de qubits puede variar a través de la red, por lo tanto las distintas probabilidades de error se vuelven útiles.

3. Posteriormente Nguyen construye la arquitectura general del sistema y se determina su configuración basándose en las limitaciones y las especificaciones dadas. Luego, procede mediante la construcción del proceso específico de codificación y decodificación, lo cual conduce a patrones de error específico que pueden ser usados para predecir el desempeño del sistema.

Conclusión

El paper de Nguyen muestra los beneficios de la codificación De redes cuánticas en el contexto de redes cuánticas a gran escala, Los sistemas basados en LQNC son capaces de proveer 10 veces mejor rendimiento infidelidad a una alta tasa de codificación mayor que Los sistemas basados en ES cuando se considera una red a gran escala.

Muchas Gracias.

Preguntas.