Computación cuántica

Procesamiento de datos a gran escala

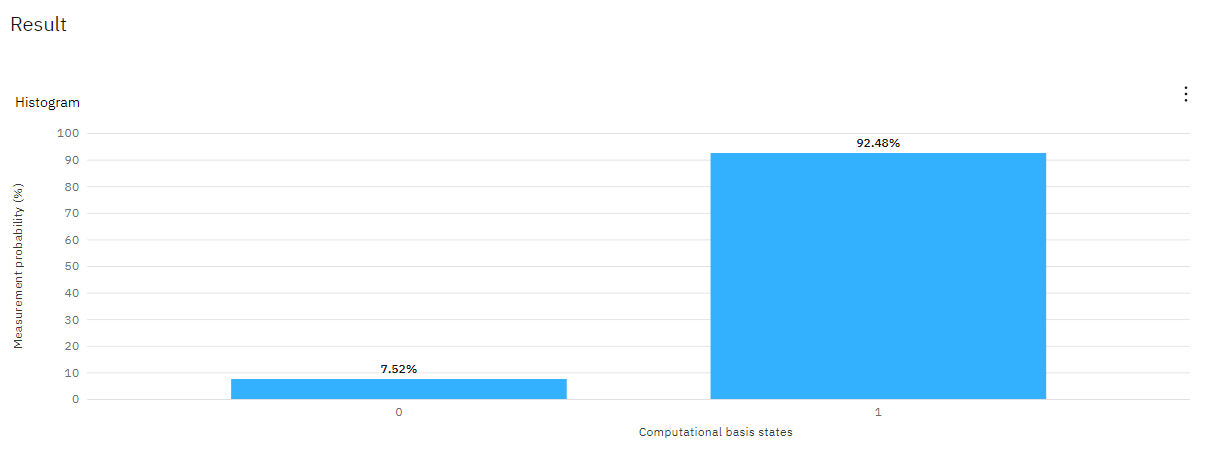
Alejandro Cabana Suárez y Óscar Gómez Borzdynski

MUCD20-21

# Puertas Cuánticas

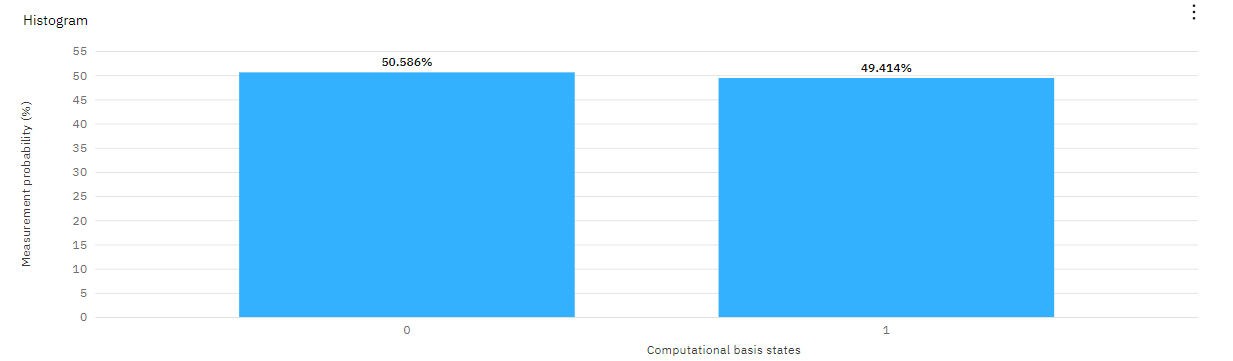
Como primeras puertas cuánticas a probar hemos elegido:

* **NOT:** Esta puerta intercambia las componentes |0〉 y |1〉. Hemos probado a aplicarla sobre un qubit inicializado en mínima energía (|0〉). Comprobamos que el resultado es el esperado con un pequeño margen de error.

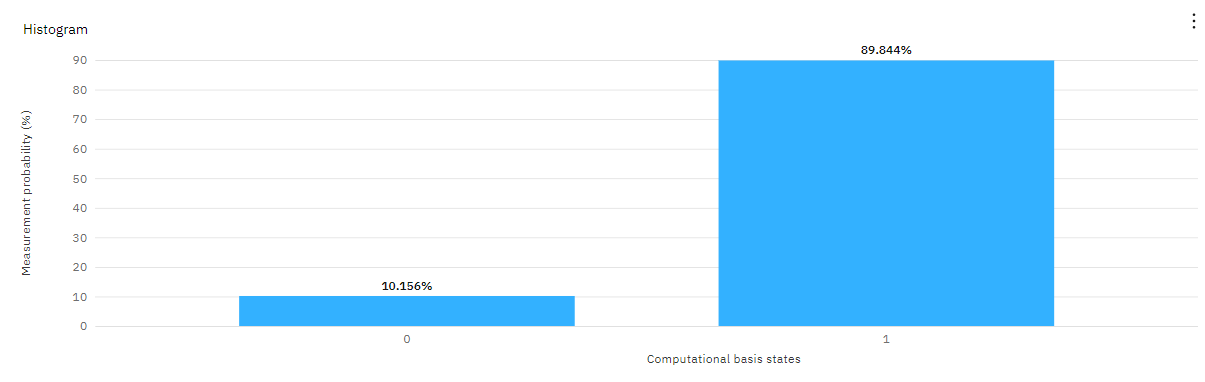
****

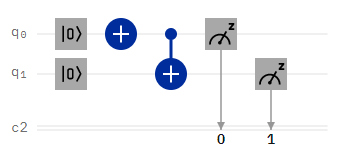
* **Hadamard:** Se usa para poner los qubits en estado de superposición. En caso de utilizarse sobre un qubit |0〉, devolverá el estado |+〉 = . En caso de aplicarse sobre un qubit |1〉, obtendremos el estado |〉 = .

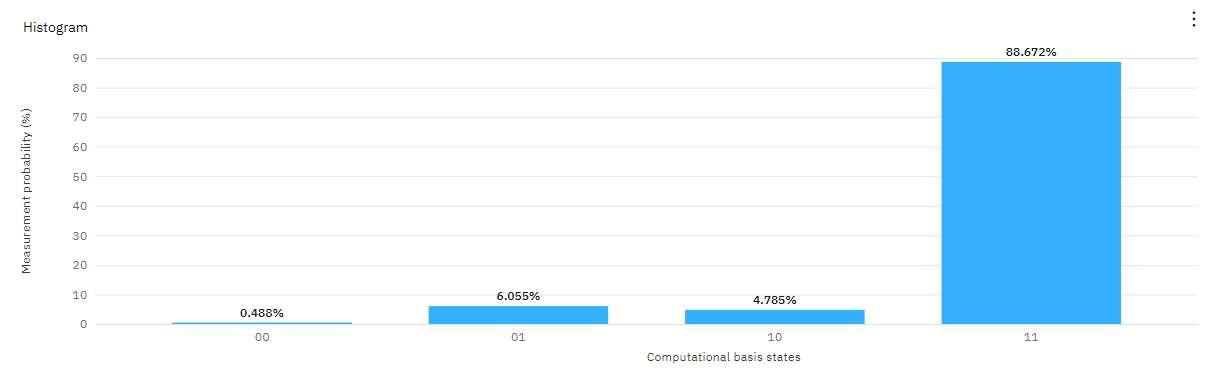
Al realizar mediciones en un computador cuántico, obtendremos equiprobabilidad entre el estado 0 y el 1.



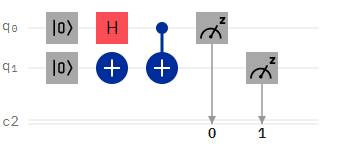
* **Z:** Esta puerta cambia el signo de la componente |1〉 del estado. Por tanto, al aplicarla sobre un |1〉 obtendremos -|1〉, que colapsa a 1 al ser observado.

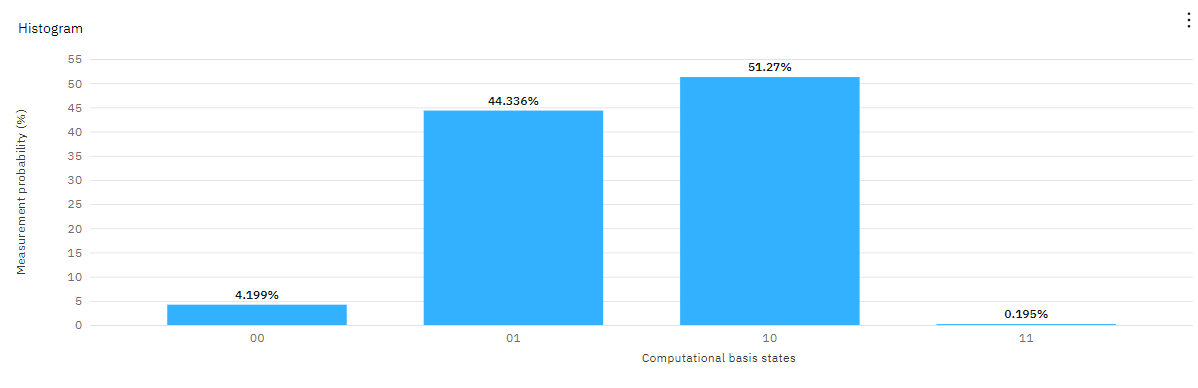


* **CNOT:** Controlled-NOT, se trata de una puerta de 2 qubits que aplica un NOT al qubit objetivo si el qubit de control toma valor |1〉.

****

Hemos probado a combinar algunas de las puertas anteriores en un mismo circuito:

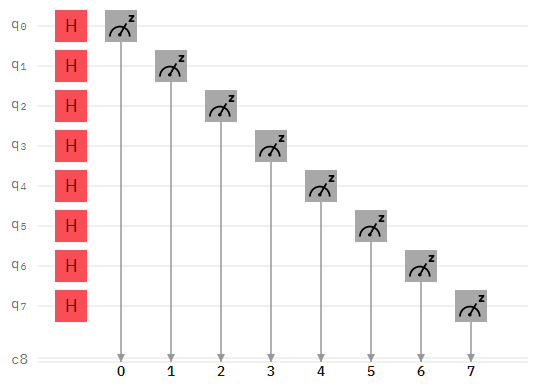


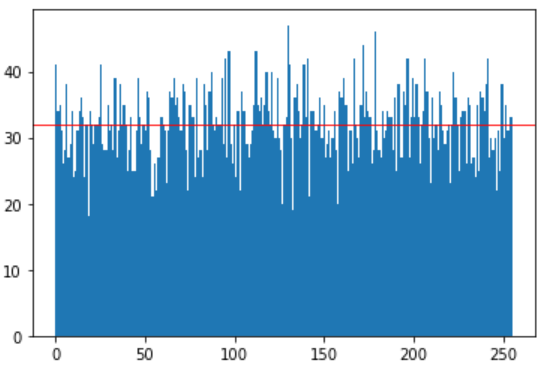


En este caso, el qubit de control está en superposición, pudiendo tomar los valores |0〉 y |1〉. Cuando al medir toma el valor 1, el qubit objetivo de la CNOT cambiará a |0〉. Al medir un 0, el objetivo de la CNOT no sufre ningún cambio, manteniéndose en |1〉.

# Generación de números aleatorios con un Computador Cuántico

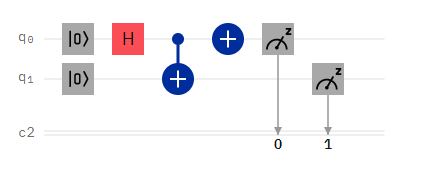
Para generar números aleatorios de 8 bits, lo más simple es utilizar 8 qubits en estado de superposición. Cada qubit individual colapsará a 0 o 1 con la misma probabilidad. Si los números de 8 bits obtenidos son realmente aleatorios, el histograma esperado después de 8192 ejecuciones tendrá valores parecidos para todas las opciones posibles de números de 8 bits. En este caso deberían estar en torno a 8192/256 = 32 apariciones de cada número.

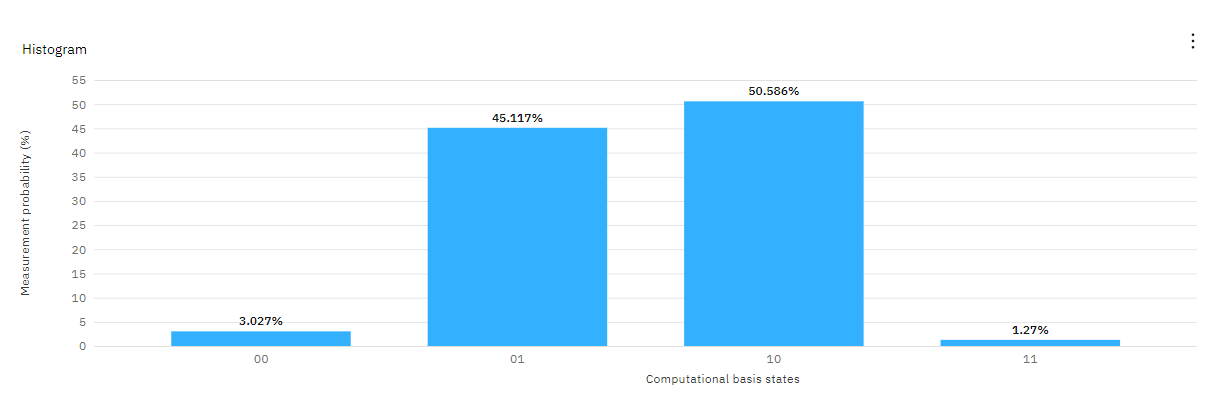




# Entrelazamiento

Dos qubits se encuentran entrelazados cuando el sistema toma valor . En mecánica cuántica dos partículas se encuentran entrelazadas cuando no pueden definirse como partículas individuales, sino que deben definirse como una única ecuación de onda para el sistema completo. Esto lleva a una relación en las mediciones realizadas en computación cuántica: si en uno de ellos medimos un 1 sabríamos con certeza que en el otro qubit mediríamos un 0 y viceversa.

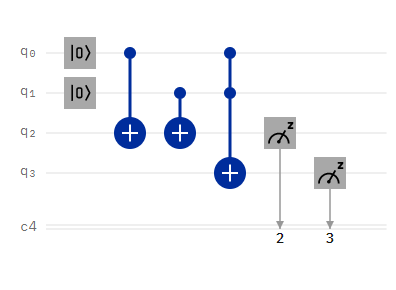




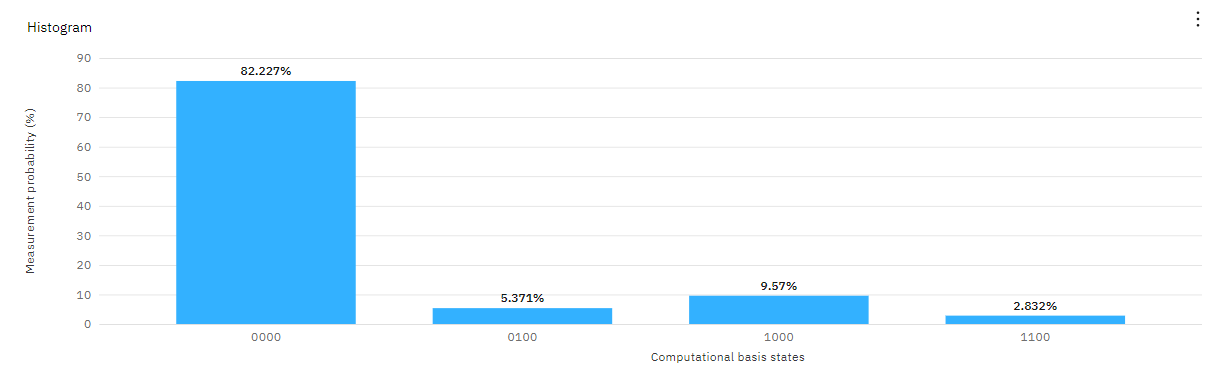
En el histograma podemos ver que, para valor 0 en el primero qubit, obtenemos un 1 en la medición del segundo y un 1 en el primer qubit implica un 0 en el segundo.

# Sumador de dos qubits

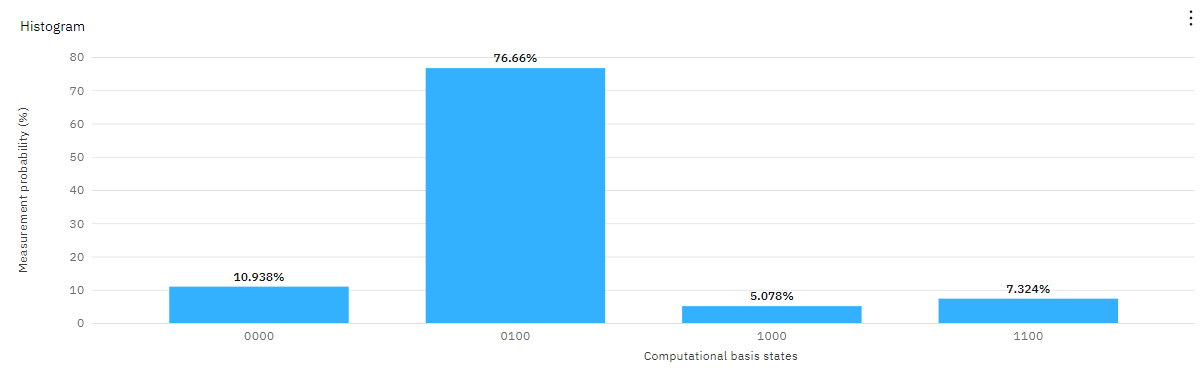
La operación suma entre dos qubits se define con el siguiente circuito:



En la imagen del circuito se colocan los qubits 0 y 1 a 0 y serán las entradas del sumador.



Podemos comprobar que la suma 0 + 0 es 0. Probando con otros valores de entrada obtenemos los resultados esperados en los qubits de salida. Por ejemplo, para 1 + 0 obtenemos el siguiente resultado:



La manera en que funciona el circuito que hemos usado es la siguiente:

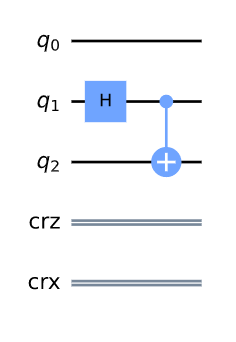
1. La primera CNOT esencialmente copia q0 en q2 para no sobrescribir las entradas (si q0 es 0, se queda a 0 y si es 1, realiza un NOT y escribe 1).
2. El segundo CNOT hace las veces de la puerta XOR de un sumador tradicional, devolviéndonos el qubit menos significativo de nuestra suma.
3. La tercera puerta que utilizamos se llama puerta de Toffoli. Podemos pensar en ella como un CNOT con dos qubits de control: sólo aplica el NOT si los dos son 1. En este sentido, si se la aplicamos a un qubit inicializado a 0, se comporta como la puerta AND tradicional. Con esto conseguimos el bit de acarreo de nuestra suma (que sólo es 1 cuando sumamos dos 1).

# Algoritmos cuánticos

## Teleportación cuántica

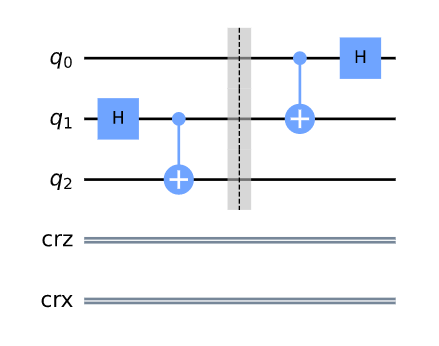
La teleportación cuántica es un algoritmo que permite transmitir el estado de un qubit a otro por canales de comunicación clásicos, valiéndonos del fenómeno de entrelazamiento.

En la versión más simple de este algoritmo se consideran tres qubits. Dos de ellos comienzan en estado entrelazado, y uno lo posee el emisor y otro el receptor. Además, el emisor tiene también el qubit cuyo estado quiere transmitir. La manera de entrelazar dos qubits, como ya hemos mencionado, es hacer pasar uno de ellos por una puerta de Hadamard y usarlo como control de una CNOT sobre el otro.



Esta operación deja el par de qubits en el estado .

El primer paso del algoritmo consiste en que el emisor usa el qubit que quiere enviar (en este ejemplo q0) como control de una CNOT sobre su qubit del par entrelazado. A continuación, le aplica una puerta de Hadamard al qubit que se quiere enviar.



Con esto se consigue dejar el qubit que tiene el receptor en un estado que depende enteramente del estado al que colapsen los qubits del emisor. Si el qubit que queremos transmitir es , podemos escribir el sistema completo como uno de 3 qubits. Después de aplicarle las puertas de este paso obtendríamos un estado que podríamos factorizar de la siguiente manera:

Aquí podemos ver claramente que si los dos primeros qubits colapsan a , el estado del tercero será exactamente el que queremos transmitir. Si colapsan a , serán el mismo, pero con los coeficientes intercambiados, etc.

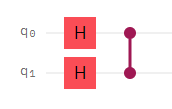
El segundo paso, por tanto, será que el emisor mida sus dos qubits y envíe los dos bits que obtenga a través de canales convencionales. En principio, obtendrá uno de los cuatro estados posibles con la misma probabilidad. De esta manera, si el emisor recibe ‘00’, sabrá que su qubit está en el estado que le querían enviar. Si recibe ‘01’, entonces podrá aplicar una puerta NOT (intercambiar los coeficientes) a su qubit para recuperar el estado deseado. Si recibe ‘10’, tendrá que aplicar una puerta Z (cambiar el signo del segundo coeficiente) y si recibe ‘11’, tendrá que aplicar primero una NOT y luego una Z.

De esta manera, utilizando ciertas operaciones que dependen de las mediciones del emisor, el receptor puede conseguir un qubit con el estado deseado.

## Algoritmo de Grover

El algoritmo de Grover es un algoritmo de búsqueda que supera en gran medida el rendimiento de los algoritmos clásicos. Para implementar este algoritmo vamos a separarlo en dos partes: el oráculo y la amplificación de amplitud.

El oráculo es un conjunto de puertas cuánticas que invierte la fase del estado que estamos buscando. Por ejemplo, para dos qubits, supongamos que estamos buscando el estado |11〉. Necesitaríamos una puerta que invierta la fase de dicho estado. Casualmente la puerta CZ hace exactamente eso, por ello comenzaremos con un estado |s〉 (mediante el uso de puertas Hadamard) y aplicaremos dicha puerta sobre ambos qubits.



La puerta CZ se expresa mediante la matriz .

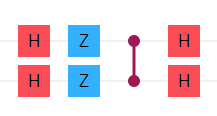
La regla para crear un oráculo es que solo modifique la fase del estado buscado, dejando invariables todos los demás. En caso de disponer de 3 qubits tendremos una matriz de tamaño 8x8 diagonal con todo 1s excepto para el estado buscado, donde aparecerá un -1.

La siguiente fase sería la amplificación de la amplitud. Lo que haremos es amplificar la amplitud del elemento objetivo (el que hemos marcado con un -1 en el oráculo). Al aumentar su amplitud, disminuiremos en igual medida la amplitud de los demás estados, incrementando la probabilidad del estado buscado.

Para realizar este proceso se comienza con el estado obtenido del oráculo y realizaremos las siguientes operaciones:

1. Transformar |s〉 en un estado de todo 0.
2. Invertir los elementos que no sean 0.
3. Transformar de nuevo a |s〉.

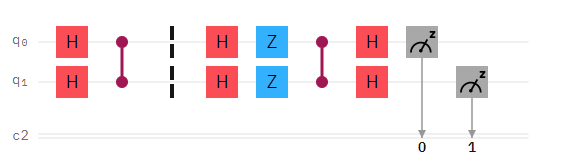
Para ello, en dos qubits realizamos el siguiente circuito:



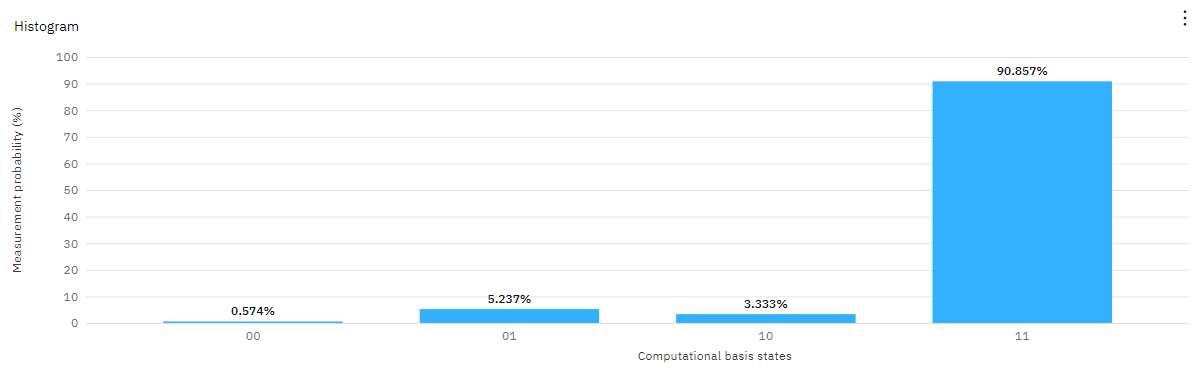
En primer lugar, pasamos de |s〉 a ceros mediante el uso de puertas Hadamard, realizamos la inversión mediante puertas Z y CZ y, finalmente, recuperamos el estado |s〉 mediante el uso de puertas H. Como la entrada será |s〉 salvo por la componente que estamos buscando, tras este circuito la amplitud del estado modificado será máxima.

El circuito intermedio realiza la siguiente operación:

Por tanto, el circuito completo sería el siguiente.

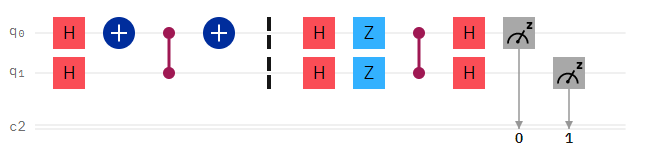


Al ejecutarlo en un computador cuántico obtenemos las siguientes probabilidades:



Pudemos ver que el estado |11〉, que era el objetivo, ha sido encontrado.

En caso de buscar el estado |10〉 deberemos modificar el oráculo, introduciendo dos puertas NOT:



En este caso el oráculo invertirá el estado |10> y por tanto la amplificación de amplitud lo hará el resultado más probable, como podemos comprobar al ejecutar en un ordenador cuántico:

