Ejercicios de criptografía cuántica

Adrián Enríquez Ballester

2 de abril de 2022

Ejercicio 1 - Corrección de errores clásica

Sea $C \subset \mathbb{Z}_2^6$ el código lineal $[6, 3]$ con matriz generadora

$$G = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

Calcular:

a) Todos los elementos de C.

b) Una matriz de check H para C.

c) La distancia mínima de C, el número de errores que permite detectar, y el número de errores que permite corregir.

Además, corregir los siguientes mensajes:

I) $\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$

II) $\begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$

III) $\begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$

Respuesta

Como C es la imagen de la aplicación lineal dada por la matriz $G^\top$, sea $(\lambda_1, \lambda_2, \lambda_3) \in \mathbb{Z}_2^3$:

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \end{pmatrix} = \lambda_1 \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}^\top$$

$$+ \lambda_2 \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}^\top$$

$$+ \lambda_3 \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}^\top$$

es decir, C es el subespacio lineal de $\mathbb{Z}_2^6$ generado por la base dada por los vectores fila de G, que tiene 2^3 elementos:

$$\begin{aligned} C = \{\ & \lambda_1 \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix} \\ & + \lambda_2 \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \\ & + \lambda_3 \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} \\ & : \forall (\lambda_1, \lambda_2, \lambda_3) \in \mathbb{Z}_2^3 \ \} \end{aligned}$$

Con tal de obtener una matriz de check H para C, podemos realizar las siguientes transformaciones elementales partiendo de C:

$$\begin{aligned} \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} &\rightsquigarrow \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} \\ &\rightsquigarrow \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \\ &\rightsquigarrow \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \end{aligned}$$

Al tener una diagonal en la mitad izquierda, sabemos que la matriz que resulta de transponer la mitad derecha seguida de una diagonal

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

determina una aplicación lineal en la que $C = \mathsf{Ker}(H)$ y, por tanto, H es una matriz de check para C.

En este caso, al tratarse de un código lineal, podemos obtener la distancia mínima de C como el número mínimo de columnas linealmente dependientes de H, que es $d = 3$. Esto quiere decir que el código puede detectar hasta $d - 1 = 2$ errores y corregir $\frac{d-1}{2} = 1$.

Vamos a aplicar los resultados anteriores a los mensajes propuestos. En cuanto al primero, obtenemos el siguiente síndrome:

$$H \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

Al no tratarse del vector nulo, esto quiere decir que se ha producido algún error, y como

$$H\begin{pmatrix}0\\0\\0\\0\\0\\1\end{pmatrix}=\begin{pmatrix}0\\0\\1\end{pmatrix}$$

el mensaje corregido sería $\begin{pmatrix}1 & 0 & 0 & 0 & 1 & 1\end{pmatrix}$.
En cuanto al segundo mensaje, su síndrome es

$$H\begin{pmatrix}0\\0\\1\\0\\1\\1\end{pmatrix}=\begin{pmatrix}1\\1\\0\end{pmatrix}$$

que de nuevo es no nulo. Como

$$H\begin{pmatrix}0\\1\\0\\0\\0\\0\end{pmatrix}=\begin{pmatrix}1\\1\\0\end{pmatrix}$$

el mensaje corregido sería $\begin{pmatrix}0 & 1 & 1 & 0 & 1 & 1\end{pmatrix}$.
En cuanto al último mensaje, su síndrome es

$$H\begin{pmatrix}1\\1\\1\\1\\0\\1\end{pmatrix}=\begin{pmatrix}1\\0\\1\end{pmatrix}$$

y como

$$H\begin{pmatrix}0\\0\\1\\0\\0\\0\end{pmatrix}=\begin{pmatrix}1\\0\\1\end{pmatrix}$$

el mensaje corregido sería $\begin{pmatrix}1 & 1 & 0 & 1 & 0 & 1\end{pmatrix}$.

Ejercicio 2 - Corrección de errores cuántica

El código de repetición *bitflip* está definido por

$$|0\rangle_L = |000\rangle$$
$$|1\rangle_L = |111\rangle$$

En vez de los operadores de medida del síndrome que hemos visto en clase, supongamos que al recibir un mensaje codificado, cada qubit se mide en la base canónica ($|0\rangle$ y $|1\rangle$).

a) Calcular los 8 operadores (proyecciones) que definen la medida.

b) Explicar cómo detectar la posición de un error a partir del síndrome.

c) Demostrar que la corrección del error solo funciona si el estado codificado era en la base canónica.

d) Asumiendo que el canal es perfecto y que no se producen errores, calcular la fidelidad mínima al usar este código de corrección de errores.

Respuesta

Como cada qubit se mide en la base canónica, utilizamos los operadores de medida asociados a la proyección ortogonal de $(\mathbb{C}^2)^{\otimes 3}$:

$$\begin{aligned}
P_0 &= |000\rangle\langle 000| \qquad (\mathbb{1}\otimes\mathbb{1}\otimes\mathbb{1})\\
P_1 &= |001\rangle\langle 001| \qquad (\mathbb{1}\otimes\mathbb{1}\otimes X)\\
P_2 &= |010\rangle\langle 010| \qquad (\mathbb{1}\otimes X\otimes\mathbb{1})\\
P_3 &= |011\rangle\langle 011| \qquad (X\otimes\mathbb{1}\otimes\mathbb{1})\\
P_4 &= |100\rangle\langle 100| \qquad (X\otimes\mathbb{1}\otimes\mathbb{1})\\
P_5 &= |101\rangle\langle 101| \qquad (\mathbb{1}\otimes X\otimes\mathbb{1})\\
P_6 &= |110\rangle\langle 110| \qquad (\mathbb{1}\otimes\mathbb{1}\otimes X)\\
P_7 &= |111\rangle\langle 111| \qquad (\mathbb{1}\otimes\mathbb{1}\otimes\mathbb{1})
\end{aligned}$$

los cuales sabemos que definen una medida proyectiva válida.

Al lado de cada operador está indicado el error más probable que se habría producido en caso de que saliese su medida asociada y, por tanto, la corrección que se tendría que aplicar para corregirlo (e.g. $\mathbb{1}\otimes\mathbb{1}\otimes X$ quiere decir que se ha producido un *bitflip* en el tercer qubit).

Esta medida tiene un problema con respecto a la que hemos visto en clase y es que, al estar midiendo todos los qubits, el hecho de medir provoca un cambio en el estado que hace imposible corregir el error para ciertos mensajes.

Supongamos que se codifica un mensaje $|\varphi\rangle = a|0\rangle + b|1\rangle$ como $|\tilde{\varphi}\rangle = a|000\rangle + b|111\rangle$ y, tras ser enviado y posiblemente alterado, se recibe $|\tilde{\varphi}'\rangle$. En el caso de que no se hubiese producido ningún error, $|\varphi\rangle = |\tilde{\varphi}\rangle$ y las probabilidades de cada medida serían

$$p(0) = \langle\varphi|P_0|\varphi\rangle = |a|^2\langle 000|000\rangle\langle 000|000\rangle + |b|^2\langle 111|000\rangle\langle 000|111\rangle = |a|^2$$
$$p(7) = \langle\varphi|P_7|\varphi\rangle = |a|^2\langle 000|111\rangle\langle 111|000\rangle + |b|^2\langle 111|111\rangle\langle 111|111\rangle = |b|^2$$

y 0 para el resto, puesto que $|a|^2 + |b|^2 = 1$.

En caso de que saliese 0, el estado cambiaría a

$$\frac{P_0|\varphi\rangle}{\sqrt{|a|^2}} = \frac{a|000\rangle\langle 000|000\rangle + b|000\rangle\langle 000|111\rangle}{|a|} = \frac{a}{|a|}|000\rangle$$

y, en caso de que saliese 1, con un cálculo análogo se obtendría $\frac{b}{|b|}|111\rangle$.

Esto quiere decir que medir habría destruido la información y ya no admitiría la corrección que se pretende. Por otra parte, si $a = 0$ o $b = 0$, solo una de las medidas ocurriría con probabilidad 1 y el estado sería el mismo tras realizar la medida.

Con un razonamiento similar, los cálculos para un error en el primer qubit serían los siguientes:

$$|\tilde{\varphi}\rangle = (X \otimes \mathbb{1} \otimes \mathbb{1})|\varphi\rangle = a|100\rangle + b|011\rangle$$

$$p(3) = \langle\tilde{\varphi}|P_3|\tilde{\varphi}\rangle = |a|^2\langle 100|011\rangle\langle 011|100\rangle + |b|^2\langle 011|011\rangle\langle 011|011\rangle = |b|^2$$
$$p(4) = \langle\tilde{\varphi}|P_4|\tilde{\varphi}\rangle = |a|^2\langle 100|100\rangle\langle 100|100\rangle + |b|^2\langle 011|100\rangle\langle 100|011\rangle = |a|^2$$

$$\frac{P_3|\tilde{\varphi}\rangle}{\sqrt{|b|^2}} = \frac{a|011\rangle\langle 011|100\rangle + b|011\rangle\langle 011|011\rangle}{|b|} = \frac{b}{|b|}|011\rangle$$
$$\frac{P_4|\tilde{\varphi}\rangle}{\sqrt{|a|^2}} = \frac{a|100\rangle\langle 100|100\rangle + b|100\rangle\langle 100|011\rangle}{|a|} = \frac{a}{|a|}|100\rangle$$

En conclusión, los resultados serían similares para el resto de casos de error: para cada par de medidas que corresponden a un error en cierta posición, una

de ellas tiene probabilidad $|a|^2$, la otra $|b|^2$ y al medir se destruye la información salvo si $a = 0$ o $b = 0$.

Por último, en cuanto a la fidelidad mímima al utilizar el código asumiendo que no se producen errores por el canal, el resultado tras enviar un mensaje $|\varphi\rangle = a|0\rangle + b|1\rangle$ es

$$\begin{cases} \frac{a}{|a|}|0\rangle & \text{con probabilidad } |a|^2 \\ \frac{b}{|b|}|1\rangle & \text{con probabilidad } |b|^2 \end{cases}$$

por lo que la fidelidad para un mensaje genérico sería

$$\begin{aligned} F_c(a|0\rangle + b|1\rangle) &= |a|^2 \left| (\overline{a}\langle 0| + \overline{b}\langle 1|)\frac{a}{|a|}|0\rangle \right|^2 + |b|^2 \left| (\overline{a}\langle 0| + \overline{b}\langle 1|)\frac{b}{|b|}|1\rangle \right|^2 \\ &= |a|^2 \left| \frac{|a|^2}{|a|} \right|^2 + |b|^2 \left| \frac{|b|^2}{|b|} \right|^2 = |a|^2|a|^2 + |b|^2|b|^2 = |a|^4 + |b|^4 \end{aligned}$$

Para minimizar la expresión anterior, como $|a|^2 + |b|^2 = 1$, podemos describir $|b|^2$ en función de $|a|^2$ y reescribirla como:

$$(|a|^2)^2 + |b|^4 = (1 - |b|^2)^2 + |b|^4 = 2|b|^4 - 2|b|^2 + 1$$

Si derivamos con respecto a $|b|^2$ e igualamos a 0 obtenemos

$$\begin{aligned} 4|b|^2 - 2 &= 0 \\ |b|^2 &= \frac{1}{2} \end{aligned}$$

por lo que la fidelidad mímima del canal es, teniendo en cuenta que si $|b|^2 = \frac{1}{2}$ entonces $|a|^2 = \frac{1}{2}$:

$$F_c^{min} = \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$$

Ejercicio 3 - Protocolo BB84

Durante la realización del protocolo BB84, Alice ha elegido como cadenas de bits iniciales

$$\begin{aligned} \vec{a} &= (01100100) \\ \vec{s} &= (ZZXXXZXZ) \end{aligned}$$

mientras que Bob ha elegido

$$\vec{v} = (ZXXZXXXX)$$

Asumiendo que no haya errores ni ataques durante el protocolo, calcular:

a) Una posible cadena de bits $\vec{b}$ de los resultados de las medidas de Bob.

b) La clave compartida entre Alice y Bob al terminar el protocolo.

Respuesta

Vamos a seguir el protocolo para hallar una posible cadena de bits que sea el resultado de las medidas de Bob.

En primer lugar, Alice codifica cada bit a_i de $\vec{a}$ en la base $|0\rangle, |1\rangle$ si s_i es Z, y en la base $|+\rangle, |-\rangle$ si s_i es X, siendo s_i el elemento en la posición i de $\vec{s}$. Esto significa que, tras ser enviados, Bob recibe la siguiente secuencia de qubits:

$$|0\rangle,\ |1\rangle,\ |-\rangle,\ |+\rangle,\ |+\rangle,\ |1\rangle,\ |+\rangle,\ |0\rangle$$

A continuación, Bob mide cada uno de esos qubits según la base asociada a su cadena $\vec{v}$. Medir $|0\rangle$ o $|1\rangle$ en la base $|0\rangle, |1\rangle$ provoca que el resultado sea respectivamente 0 o 1 con probabilidad 1. Lo mismo sucede al medir $|+\rangle$ o $|-\rangle$ en la base $|+\rangle, |-\rangle$:

$$\vec{b} = (0?1?0?0?)$$

Por otra parte, medir $|+\rangle$ o $|-\rangle$ en la base $|0\rangle, |1\rangle$ provoca que el resultado sea 0 o 1 con probabilidad 0,5. Lo mismo sucede al medir $|0\rangle$ o $|1\rangle$ en la base $|+\rangle, |-\rangle$. Un posible resultado final podría ser el siguiente:

$$\vec{b} = (00110101)$$

Para finalizar el protocolo, Alice y Bob revelan $\vec{s}$ y $\vec{v}$, y descartan las posiciones de sus cadenas de bits en las que $s_i \neq v_i$. En este caso, la clave compartida resultante sería

$$(0100)$$