UNIVERSITAT JAUME I

Grado en Matemática Computacional

Trabajo Final de Grado

Introducción a los códigos cuánticos

Autor:
Jesús Aguiló Salinas

Tutor académico:
Fernando Javier Hernando Carrillo

Fecha de lectura: __ de _____ de 20__
Curso académico 2022/2023

Resumen

El principal objetivo de este documento es ofrecer una explicación introductoria a los códigos correctores de errores utilizados en computación cuántica. Se comenzará con una revisión introductoria a códigos clásicos, específicamente códigos correctores de errores lineales, seguida de una revisión de los principales conceptos de la mecánica y la computación cuánticas. Para finalizar se reúnen estos conceptos en un estudio sobre códigos estabilizadores, sus principales cualidades y propiedades, y algunas relaciones que poseen con otros tipos de código corrector.

Palabras clave

Código cuántico, código corrector de errores, código estabilizador, código Reed-Solomon.

Keywords

Quantum code, error correcting code, stabilizer code, Reed-Solomon code.

Índice general

Capítulo 1

Introducción

1.1. Contexto y motivación del proyecto

Las nuevas tecnologías permitieron e incentivaron el intercambio de cantidades masivas de información a través de canales de muchos tipos diferentes. Este desarrollo fue acompañado de la creación de sistemas que pudiesen asegurar la integridad de la información transmitida, dichos sistemas toman la forma de códigos. De todas las familias de códigos una de las más importantes son los códigos correctores, que tratan de asegurar que la información recibida es igual a la que se deseaba enviar.

En los últimos años han aparecido nuevos sistemas de información, en especial la información cuántica que trabaja con sistemas muy diferentes a los de la información clásica conocida. Estas nuevas tecnologías requieren la creación de nuevas medidas de seguridad análogas a las ya conocidas que sean capaces de trabajar con las nuevas reglas que establece la mecánica cuántica.

El objetivo de este trabajo es ofrecer una visión introductoria a los códigos correctores cuánticos, estableciendo primero las características de los códigos correctores clásicos, seguido de una introducción a la mecánica cuántica y sus aspectos más relevantes a la hora de trabajar con información cuántica. Por último, se darán ejemplos de algunos de los códigos cuánticos que están siendo estudiados en la actualidad, en particular los códigos estabilizadores, y de cómo se pueden obtener.

Capítulo 2

Desarrollo del TFG

2.1. Introducción a códigos correctores de errores

En este apartado se introducirán los conceptos básicos de los códigos utilizados en computación clásica, así como las nociones de códigos correctores de errores presentadas en [5] y [8].

2.1.1. Códigos y codificación

Antes de comenzar a hablar de códigos correctores, es importante entender exactamente que es un código, para ello es necesario introducir algunos conceptos que saldrán repetidamente a lo largo de esta sección y las siguientes.

Los códigos se aplican a procesos de transmisión de la información. En este caso, y todos los sucesivos, se utilizará el término *información* para la *información digital* es decir información descrita mediante una sucesión de símbolos pertenecientes a un conjunto finito. Dicho conjunto recibirá el nombre de *alfabeto*.

Todo proceso de transmisión de la información sigue el esquema siguiente: un *emisor* envía un *mensaje* (la información) mediante un *canal* a un *receptor*. En el sentido más amplio del término, el canal puede transmitir la información espacial o temporalmente: cableado de diferentes tipos, almacenamiento de la información en discos duros, etc.

En numerosas ocasiones la manera en la que está escrita la información resulta inconveniente para su transmisión, esto puede ocurrir porque ocupe demasiado espacio o se encuentre abierta

a interferencias. Para solventar éstos errores la información se codifica, es decir, se reescribe de forma diferente, en ocasiones utilizando un alfabeto diferente, para adecuarla a nuestras necesidades y las del canal. En general, los objetivos que se buscan con la codificación son: *comprimir* la información, reduciendo su tamaño lo máximo posible, y *detectar y corregir*, en la medida de lo posible, errores que puedan suceder durante la transmisión.

Codificación

Ya se ha indicado que el *alfabeto fuente*, alfabeto en el que está escrita la información original, y el *alfabeto código*, en el que será codificada, no han de coincidir. Dado un alfabeto $\mathcal{A}$, se llamará *palabra* del alfabeto $\mathcal{A}$ a toda secuencia finita formada por elementos de $\mathcal{A}$. Se denota por $\mathcal{P}(\mathcal{A})$ al conjunto de todas las palabras escritas con $\mathcal{A}$.

Definición 2.1.1. *Codificar el alfabeto fuente* $\mathcal{A} = \{a_1, \cdots, a_{k_a}\}$ *en el alfabeto código* $\mathcal{B} = \{b_1, \cdots, b_{k_b}\}$ es crear una aplicación inyectiva $c : \mathbf{A} \subset \mathcal{P}(\mathcal{A}) \longrightarrow \mathcal{P}(\mathcal{B})$. Para cada $m_i \in \mathbf{A}$, $c(m_i)$ es la *codificación* de m_i, y el subconjunto $\mathcal{C} = Im(c)$ de $\mathcal{P}(\mathcal{B})$ es el *código* empleado. Se dice que $\mathcal{C}$ es un *código de* $\mathcal{A}$ *sobre* $\mathcal{B}$ y cada uno de sus elementos será llamado *palabra código*.

Se deben concretar algunas cosas sobre esta definición: la aplicación de codificación, c, debe ser inyectiva, ya que dos palabras diferentes no pueden tener la misma codificación; los términos código y codificación son usados en ocasiones como sinónimos, a pesar de no tener siempre el mismo significado; por último, los símbolos utilizados en la codificación son matemáticamente irrelevantes, la única cualidad relevante del alfabeto código es su tamaño, obteniendo así códigos binarios, ternarios, octales, etc. en función de la cantidad de elementos que posee el alfabeto $\mathcal{B}$, independientemente de la forma que tomen.

Otra de las características que se puede tener en cuenta al estudiar códigos es el tamaño de sus palabras, de aquí surgen dos definiciones:

Definición 2.1.2. La cantidad de símbolos que forman una palabra se denomina su *longitud*.

Definición 2.1.3. Dado un código, si todas sus palabras son de longitud n recibe el nombre de *código en bloque* de longitud n. En otro caso se dice que el código es de *longitud variable*.

La propia naturaleza de los códigos variables permite reducir en gran medida la longitud media de sus palabras respecto a la de un código en bloque que trate de codificar un mismo alfabeto, por tanto, son la clase de códigos utilizados en la compresión de información. Por otro lado, la fiabilidad de la longitud fija de los códigos en bloque permite que puedan ser usados para detectar y corregir errores causados durante la transmisión.

Como la codificación de palabras sueltas de $\mathcal{A}$ tiene una utilidad limitada, es necesaria una aplicación capaz de codificar *mensajes* escritos en el alfabeto $\mathcal{A}$. Esto se consigue concatenando

las palabras codificadas, extendiendo de la aplicación c una aplicación $c' : \mathcal{P}(\mathcal{A}) \longrightarrow \mathcal{P}(\mathcal{B})$ tal que $c'(m_{i_1} m_{i_2} \cdots m_{i_n}) = c(m_{i_1})c(m_{i_2}) \cdots c(m_{i_n})$.

2.1.2. Decodificación

Tras el proceso de transmisión de la información es necesario decodificar el mensaje, es decir, traducirlo al alfabeto fuente de nuevo. En el caso de mensajes formados por una sola letra siempre será posible, ya que c es inyectiva, sin embargo puede darse el caso de que un mensaje codificado pueda ser decodificado en varios mensajes diferentes.

Ejemplo 2.1.4. Sean $\mathcal{A} = \{0, 1, \cdots, 9\}$ y $\mathcal{B} = \{0, 1\}$, se define el código binario c tal que:

fuente	0	1	2	3	4	5	6	7	8	9
c	0	1	10	11	100	101	110	111	1000	1001

Utilizando el código c del ejemplo 2.1.4 se codificará el mensaje 012345 como 011011100101, sin embargo, existen varias decodificaciones aparentemente correctas, como pueden ser 011011100101, 02032021, 0670021, etc. Esta ambivalencia no puede permitirse a la hora de decodificar si se quiere que el mensaje se transmita correctamente por lo que los códigos han de tener decodificación única.

Definición 2.1.5. Un código tendrá *decodificación única* si la aplicación extendida c' es inyectiva.

Cabe indicar que todo código en bloque tiene decodificación única. Por otro lado los de longitud variable tienen que poder asegurarla, para ello algunos reservan un símbolo para la separación de letras, mientras que otros son creados de forma que tengan una decodificación única inherente.

2.1.3. Canales con ruido

En el apartado anterior se ha hablado de codificación y decodificación de mensajes sin prestar atención al canal, asumiendo que el mensaje llegaría a su destino sin sufrir ningún problema. En la práctica, sin embargo, los canales pueden sufrir perturbaciones o interferencias, lo que en teoría de la información se conoce como *ruido*, dando como resultado que el mensaje recibido difiera del mensaje enviado. Para solventar el problema del ruido existen los llamados *códigos correctores de errores* que tienen la finalidad de detectar e incluso deshacer los cambios ocurridos en la transmisión.

Errores y ruido

Existen diferentes tipos de errores que pueden ser causados por ruido. Según su carácter se puede distinguir entre *errores*, símbolos recibidos que son diferentes al enviado, y *borrones*, símbolos recibidos que el receptor es incapaz de interpretar; en general se suele referir a ambos como errores indistintamente. Por la naturaleza de los errores, es evidente que el receptor puede detectar sin mayor problema los borrones, pero los errores no pueden ser distinguidos con facilidad de los símbolos enviados correctamente. Por tanto, los borrones (que se representan mediante $\sqcup$) se pueden entender como errores de posición conocida.

Además, en función de la posición y periodicidad de los errores se puede distinguir entre errores/borrones *aleatorios*, que se producen de manera aislada y se reparten de forma aleatoria por todo el mensaje, y errores/borrones *a ráfagas*, si han ocurrido en varias posiciones consecutivas del mensaje.

Para razonar sobre el canal con ruido resulta de gran utilidad describirlo en términos matemáticos de la manera siguiente:

- el conjunto de símbolos de entrada, $\mathcal{A} = \{a_1, \cdots, a_k\}$
- el conjunto de símbolos de salida, $\mathcal{S} = \{s_1, \cdots, s_h\}$
- las relaciones entre las entradas y las salidas, en otras palabras, la probabilidad condicionada $\text{prob}(s_i|a_j)$ para todo $i = 1, \cdots, h$ y $j = 1, \cdots, k$

Cabe recordar que $\text{prob}(s_i|a_j)$ es la probabilidad de recibir s_i al enviar a_j. En lo que concierne a los símbolos del alfabeto de salida, existen dos tipos principales: si no ocurren borrones, entonces $\mathcal{S} = \mathcal{A}$ (y $s_i = a_i$ para $i = 1, \cdots, k$), por otro lado, si ocurren borrones se tiene que $\mathcal{S} = \mathcal{A} \cup \{\sqcup\}$ (y $s_i = a_i$ para $i = 1, \cdots, k$ y $s_{k+1} = \sqcup$).

Corrección de errores

Como norma general, los códigos utilizados para la corrección de errores son códigos en bloque. Se basan en el concepto de introducir información redundante que, tras la recepción del mensaje, pueda ser utilizada para detectar y recuperar la información alterada durante la transmisión.

Dado que la principal característica de los códigos en bloque es que todas sus palabras tienen la misma longitud (n), que recibe el nombre de *longitud de código*, se puede definir un código en bloque del alfabeto código $\mathcal{B}$ como un subconjunto de $\mathcal{B}^n$. Sus elementos se escribirán utilizando

al notación vectorial $\mathbf{x} = (b_1, \cdots, b_n), b_i \in \mathcal{B}$ o en casos en los que no pueda haber confusión se simplificará a $\mathbf{x} = b_1 b_2 \cdots b_n$.

La idea más básica que existe para la detección de errores es simplemente repetir la información n veces. Así, si los símbolos fuente son 0 y 1, se puede crear c tal que $c(0) = 000 \cdots 0$ (n veces) y $c(1) = 111 \cdots 1$ (n veces). Entonces c sería un código bloque binario de longitud n, llamado *de repetición*. Una vez recibido el mensaje codificado, basta con comprobar que símbolo es más común para decodificarlo. De esta manera, haciendo n lo suficientemente grande, se pueden reducir la posibilidad de que la decodificación falle tanto como sea necesario. El problema con esta codificación, evidentemente, es que la cantidad de información enviada también se reduce: cada n bits emitidos, solo se transmite un bit de información real.

Así surge el principal problema de los códigos correctores, permitir la corrección de la mayor cantidad de errores posibles mediante la menor cantidad de información redundante posible, manteniendo así la cantidad real de información transmitida en un nivel utilizable.

La principal cualidad que se utiliza en códigos de repetición es que sus palabras son muy diferentes entre ellas, de manera que es muy poco probable que una se transforme en otra por culpa del ruido. Esta es la idea que se encuentra en el centro de todos los códigos correctores.

Para medir esa diferencia entre palabras se utiliza la llamada *distancia de Hamming*, definida como sigue.

Definición 2.1.6. Si $\mathbf{x}, \mathbf{y} \in \mathcal{B}^n, \mathbf{x} = (x_1, \ldots, x_n), \mathbf{y} = (y_1, \ldots, y_n)$, se llama *distancia de Hamming* entre $\mathbf{x}$ e $\mathbf{y}$ a

$$d(\mathbf{x}, \mathbf{y}) = \#\{i | 1 \leq i \leq n, x_i \neq y_i\}.$$

La aplicación d definida de esta manera es una distancia en $\mathcal{B}^n$, o en otras palabras, verifica que:

- d es no negativa y $d(\mathbf{x}, \mathbf{y}) = 0$ si y solo si $\mathbf{x} = \mathbf{y}$;
- $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$;
- $d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z}) \geq d(\mathbf{x}, \mathbf{z})$

para todo $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathcal{B}^n$.

Definición 2.1.7. Dado un código $\mathcal{C}$, se llama *distancia mínima* de $\mathcal{C}$ a

$$d = d(\mathcal{C}) = min\{d(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}, \mathbf{y} \in \mathcal{C}, \mathbf{x} \neq \mathbf{y}\}$$

Aplicando estos conceptos para la corrección de errores, tras enviar una palabra $\mathbf{c} \in \mathcal{C}$, se recibirá en el otro lado una n-upla $\mathbf{y}$ (que puede incluir $\sqcup$ como componente), utilizando el *principio de distancia mínima* se decodificará $\mathbf{y}$ por la palabra de $\mathcal{C}$ que más se asemeje a $\mathbf{y}$ utilizando la distancia de Hamming, asumiendo que el error no ha sido lo suficientemente grande como para cambiar la palabra de manera significativa. Usando este método se obtiene un algoritmo a seguir:

Algoritmo 2.1.8. *Recibido* $\mathbf{y}$*,*

- *evalúa la distancia entre* $\mathbf{y}$ *y todas las palabras de* $\mathcal{C}$*;*
- *elegir la palabra más cercana a* $\mathbf{y}$ *como decodificación (si es única).*

De esta definición del algoritmo se puede deducir que fallará cuando la palabra más cercana no sea única. En cualquier otro caso proporcionara una decodificación para $\mathbf{y}$, aunque no tiene porque ser la correcta. Estudiando las propiedades más a fondo se puede demostrar la siguiente proposición.

Proposición 2.1.9. *Sea* $\mathcal{C}$ *un código de bloque de longitud* n *y distancia mínima* d*. El algoritmo 2.1.8 aplicado a una* n*-upla recibida,*

a) permite detectar cualquier configuración de t *errores siempre que* $t < d$*;*
b) permite corregir cualquier configuración de t *errores siempre que* $2t < d$*;*
c) permite corregir cualquier configuración de s *borrones siempre que* $s < d$*;*
d) permite corregir cualquier configuración de t *errores y* s *borrones siempre que* $2t + s < d$*;*

Demostración. Sea $\mathbf{c} \in \mathcal{C}$ la palabra enviada e $\mathbf{y}$ el mensaje recibido.

a) Si $\mathbf{y}$ contiene $t < d$ errores, con $t > 0$, entonces $\mathbf{y} \notin \mathcal{C}$ dado que toda palabra de $\mathcal{C}$ esta como mínimo a una distancia d de $\mathbf{c}$. Por tanto basta evaluar la condición $\mathbf{y} \in \mathcal{C}$ para comprobar si han habido errores.
b) Si $\mathbf{y}$ contiene t errores y $2t < d$, entonces $d(\mathbf{y}, \mathbf{c}) < d(\mathbf{y}, \mathbf{x})$ para todo $\mathbf{x} \in \mathcal{C}$. Por la propia definición de distancia mínima, las bolas de la métrica Hamming con centro en las palabras código y radio $(d-1)/2$ son disjuntas. Por tanto, si $2t < d$, $\mathbf{y}$ estará únicamente en una de dichas bolas, la cual tendrá como centro la palabra código más cercana. En caso contrario se tiene que existe un $\mathbf{x} \in \mathcal{C}, \mathbf{x} \neq \mathbf{c}$ tal que $d(\mathbf{y}, \mathbf{x}) \leq d(\mathbf{y}, \mathbf{c}) \leq (d-1)/d$, por lo que, al ser d una distancia, $d(\mathbf{c}, \mathbf{x}) \leq (d-1)/2$, contradiciendo la definición de d.
c) Si $\mathbf{y}$ contiene s borrones, $s < d$, se puede suponer (salvo reordenación) que todos los borrones están en las posiciones $y_1, \cdots, y_s$. Entonces $\mathbf{c}$ es la única palabra de $\mathcal{C}$ que coincide con $\mathbf{y}$ en las últimas $n - s$ posiciones. Asumiendo que existiese $\mathbf{x} \in \mathcal{C}$ que también coincida con $\mathbf{y}$ en las últimas $n - s$ posiciones, entonces $d(\mathbf{c}, \mathbf{x}) \leq s < d$, por tanto $\mathbf{c} = \mathbf{x}$.

d) Si † contiene t errores y s borrones, $2t+s<d$, se puede suponer, al igual que en el apartado anterior, que todos los borrones están en las posiciones $y_1,\cdots,y_s$. Sea $\pi:\mathcal{B}^n\longrightarrow\mathcal{B}^{n-s}$ la proyección de las últimas $n-s$ coordenadas. Entonces $d(\pi(\mathbf{y}),\pi(\mathbf{c}))<d(\pi(\mathbf{y}),\pi(\mathbf{x}))$ para todo $\mathbf{x}\in\mathcal{C}$. Si no fuese el caso existiría $\mathbf{x}\in\mathcal{C},\mathbf{x}\neq\mathbf{c}$ tal que $d(\pi(\mathbf{y}),\pi(\mathbf{x}))\leq d(\pi(\mathbf{y}),\pi(\mathbf{c}))\leq(d-s-1)/2$, y como d es una distancia, $d(\mathbf{c},\mathbf{x})\leq d-1$, contradiciendo la definición de d. Siguiendo el caso c), se demuestra que $\pi(c)$ determina unívocamente que $s<d$.

□

A partir de esta proposición anterior se obtiene la definición siguiente

Definición 2.1.10. Si d es la distancia mínima de $\mathcal{C}$, entones se dice que $\mathcal{C}$ *corrige* $\frac{d-1}{2}$ *errores*, o que $\mathcal{C}$ es un código $\frac{d-1}{2}$-*corrector*

Tasa de transmisión

Si $\mathcal{C}$ es un código de longitud n sobre un alfabeto $\mathcal{B}$ formado por q símbolos, como máximo puede estar formado por q^n palabras. Por lo tanto, todo código en bloque son m palabras tenga una longitud de al menos $\log_q(m)$. Es más, se puede considerar que de los n símbolos que forman una palabra de $\mathcal{C}$, solo $\log_q(m)$ contienen la información, mientras que todos los demás son bits de control. De aquí surge la definición

Definición 2.1.11. Si $\mathcal{C}$ es un código de longitud n con m palabras sobre un alfabeto de q elementos, recibe el nombre de *tasa de transmisión de información* $\mathcal{C}$ el cociente

$$R(\mathcal{C})=\frac{\log_q(m)}{n}.$$

Se dice que un código $\mathcal{C}$ de longitud n con m palabras y distancia mínima d es de tipo (m,n,d). Se llama *redundancia* de $\mathcal{C}$ a la diferencia $n-\log_q(m)$.

2.1.4. Códigos lineales

Tratar con la codificación y decodificación de códigos en bloque puede resultar computacionalmente costoso y requiere del almacenamiento de todas las palabras del código, lo que puede alcanzar un tamaño considerable. Es el intento de arreglar éstos problemas lo que llevo a incluir una estructura algebraica.

De esta manera, sea $\mathbf{F}_q$ el cuerpo finito de q elementos,

Definición 2.1.12. Un *código lineal de longitud n sobre* $\mathbf{F}_q$ es un subespacio vectorial de $\mathbf{F}_q^n$.

Todo código lineal $\mathcal{C}$ de longitud n cumple también que es un código en bloque de longitud n. Además, como $\mathcal{C}$ es un espacio vectorial, posee una *dimensión* k, por lo que su cardinal es siempre una potencia de q, q^k. Estos números, n, k y la distancia mínima d, forman los llamados *parámetros fundamentales de* $\mathcal{C}$. Para abreviar, se dice que un código de parámetros n, k, y d es de *tipo* $[n, k]$ o $[n, k, d]$. La *redundancia* de un código $[n, k]$ es $r = n - k$. Además, su tasa de transmisión de información será

$$R(\mathcal{C}) = \frac{k}{n}.$$

.

Se puede interpretar los subespacios de $\mathbf{F}_q^n$ de dimensión k como la imagen de una aplicación lineal inyectiva $f : \mathbf{F}_q^k \longrightarrow \mathbf{F}_q^n$. De esta manera, se puede entender $\mathbf{F}_q^k$ como la fuente de información y f como la aplicación de codificación, lo que nos lleva a la definición

Definición 2.1.13. Se llama *matriz generatriz* de $\mathcal{C}$ a la matriz de una aplicación lineal inyectiva $f : \mathbf{F}_q^k \longrightarrow \mathbf{F}_q^n$, es decir una matriz $k \times n$ cuyas filas son base de $\mathcal{C}$.

Como existen varias bases de $\mathcal{C}$, también existirán varias matrices generatrices. Por suerte todas las matrices generatrices de $\mathcal{C}$ serán semejantes, es decir, sean G_1, G_2 dos matrices generatrices existe una matriz invertible P tal que $G_1 = PG_2P^{-1}$.

Las matrices generatriz, además del código, también ofrecen una codificación. Dado que $\mathcal{C} = \{\mathbf{a}G \mid \mathbf{a} \in \mathbf{F}_q^k\}$, (en este apartado se describirán los vectores como filas) todo mensaje $\mathbf{a} \in \mathbf{F}_q^k$ se codifica por $\mathbf{a}G \in \mathbf{F}_q^n$. Por tanto, la codificación de códigos lineales es muy simple, y basta con almacenar en memoria la matriz G (es decir, de nk elementos de $\mathbf{F}_q$ en vez de los nq^k que habrían sido necesarios para un código no lineal).

Matriz de control y dualidad

Además de por un sistema de generadores, el subespacio vectorial $\mathbf{F}_q^n$ se puede describir mediante unas ecuaciones implícitas. De esta caracterización surge la definición siguiente.

Definición 2.1.14. Se dice que la matriz H es una *matriz de control* del código $\mathcal{C}$ si para todo vector $\mathbf{x} \in \mathbf{F}_q^n$ se verifica que $\mathbf{x} \in \mathcal{C}$ si y sólo si $H\mathbf{x}^t = 0$.

Si $\mathcal{C}$ está definido sobre $\mathbf{F}_q$ y es de tipo $[n, k]$, entonces H también estará definida sobre $\mathbf{F}_q$ y será de tamaño $(n - k) \times n$ y rango $n - k$.

Las matrices generatrices y de control tienen una relación, explicada en la proposición siguiente.

Proposición 2.1.15. *Si G y H son matrices generatriz y de control de C, entonces $GH^t = 0$.*

Dado que H tiene rango máximo, se puede interpretar como la matriz generatriz de otro código sobre $\mathbf{F}_q$. Dicho código recibe el nombre de *dual* de $\mathcal{C}$ y se denota por $\mathcal{C}^\perp$. Es evidente que si $\mathcal{C}$ tiene dimensión k, $\mathcal{C}^\perp$ tendrá dimensión $n-k$. Además, si G es la matriz generatriz de $\mathcal{C}$, se tiene que $GH^t = 0$ lo que implica que $HG^t = 0$ y por tanto G es una matriz de control para $\mathcal{C}^\perp$.

Sea el producto euclídeo $\cdot$ definido sobre $\mathbf{F}_q^n$ como:

$$\mathbf{u} \cdot \mathbf{v} = \sum_{i=1}^{n} u_i v_i \in \mathbf{F}_q \text{ para todo } \mathbf{u}, \mathbf{v} \in \mathbf{F}_q.$$

Dos vectores $\mathbf{u}, \mathbf{v} \in \mathbf{F}_q^n$ son *ortogonales* si $\mathbf{u} \cdot \mathbf{v} = 0$. Y, dado $S = \{\mathbf{v}_1, \cdots, \mathbf{v}_m\}$ un conjunto de vectores, se llama *ortogonal de S* al conjunto $S^\perp = \{\mathbf{u} \in \mathbf{F}_q^n \,|\, \mathbf{u} \cdot \mathbf{v}_i = 0 \text{ para todo } i = 1, \cdots, m\}$. El conjunto $S^\perp$ es un subespacio vectorial de $\mathbf{F}_q^n$, además, si S tiene dimensión k, $S^\perp$ tendrá dimensión $n-k$. De hecho, si $\mathbf{v}_1, \cdots, \mathbf{v}_k$ es una base de S, los elementos de $S^\perp$ son las soluciones $\mathbf{u}$ del sistema lineal homogéneo con k ecuaciones y n incógnitas

$$\mathbf{u} \cdot \mathbf{v} = 0 \ , \ i = 1, \cdots, k.$$

La intersección de los espacios S y $S^\perp$ puede ser no nula, es decir pueden existir vectores no nulos ortogonales a si mismos, como es el caso de $(1,1) \in \mathbf{F}_2^2$.

Proposición 2.1.16. *Si C es un código lineal, entonces su dual $C^\perp$ es el ortogonal de C.*

Demostración. Dadas G y H las matrices generatriz y de control de C. El resultado del enunciado surge de la igualdad $GH^t = 0$ y el hecho que $rango(G) + rango(H) = n$. □

2.1.5. Códigos cíclicos

Una de las familias de códigos lineales más conocidas y utilizadas son los códigos cíclicos, y su subgrupo más importante, los códigos cíclicos BCH [2].

Definición 2.1.17. Un código lineal $\mathcal{C}$ de longitud n sobre $\mathbf{F}_q$ será *cíclico* si se cumple la propiedad siguiente: si $(c_1, c_2, \cdots, c_n) \in \mathcal{C}$ entonces $(c_n, c_1, \cdots, c_{n-1}) \in \mathcal{C}$.

Para las propiedades que se ven a continuación resulta conveniente estudiar los isomorfismos siguientes. Sean $\mathbf{F}_{q,n-1}[X]$ el espacio vectorial de todos los polinomios sobre $\mathbf{F}_q$ con grado menor que n y A el anillo cociente $A = \mathbf{F}_q[X]/\langle X^n - 1\rangle$. Gracias a los isomorfismos de espacios vectoriales

$$\mathbf{F}_q^n \cong \mathbf{F}_{q,n-1}[X] \cong A$$

se puede identificar cada vector $(a_1, \cdots, a_n)$ con el polinomio $a_1 + a_2X + \cdots + a_nX^{n-1}$ y con la clase en A $a_1 + a_2X + \cdots + a_nX^{n-1} + \langle X^n - 1\rangle$.

Teorema 2.1.18. *Sea $\mathcal{C}$ un código lineal no nulo de longitud n sobre el cuerpo finito $\mathbf{F}_q$. $\mathcal{C}$ es cíclico si y solo si, considerando inmerso en A, es un ideal.*

Demostración. Si se asume que $\mathcal{C}$ es cíclico. Como $\mathcal{C}$ ya es un subgrupo abeliano de A, basta probar que si $a(X) \in A$ y $c(X) \in \mathcal{C}$, entonces $a(X)c(X) \in \mathcal{C}$, o, de manera equivalente y dado que $\mathcal{C}$ es cerrado para la suma y el producto por constantes, que $Xc(X) \in \mathcal{C}$. Entonces

$$X(c_1 + c_2X + \cdots + c_nX^{n-1}) = c_n + c_1X + \cdots + c_{n-1}X^{n-1}$$

Por la definición de código cíclico aplicada al lenguaje polinómico $Xc(X)$ pertenece al código. El recíproco se demuestra de la misma manera. □

Debido a las propiedades del anillo A, en particular que todo ideal de A es principal, es decir, consiste en un producto de múltiplos de un polinomio $g(X)$ divisor de $X^n - 1$, se obtiene el corolario siguiente.

Corolario 2.1.19. *Dado un código cíclico no nulo $\mathcal{C}$ de longitud n, existe un único polinomio mónico $g(X) \in \mathbf{F}_q[X]$ divisor de $X^n - 1$, tal que $\mathcal{C} = \langle g(X)\rangle$. Como consecuencia, los elementos de $\mathcal{C}$ pueden identificarse con los polinomios de grado menor que n múltiplos de $g(X)$.*

Ceros de un código cíclico

Sea $X^n - 1 = f_1(X)f_2(X)\cdots f_m(X)$ la descomposición de $X^n - 1$ en factores irreducibles y sea α_i una raíz de $f_i(X)$. Para el código cíclico $\mathcal{C}_i$ generado por $f_i(X)$, se tiene

$$\mathcal{C}_i = \langle f_i(X)\rangle = \{c(X) \in A \mid c(\alpha_i) = 0\}.$$

En general, para un código $\mathcal{C}$ engendrado por $g(X) = f_{i_1}f_{i_2}\cdots f_{i_r}$, se tendrá

$$\mathcal{C} = \langle g(X)\rangle = \{c(X) \mid c(\alpha_{i_1}) = c(\alpha_{i_2}) = \cdots = c(\alpha_{i_r}) = 0\},$$

por tanto, los códigos cíclicos pueden ser definidos como conjuntos de polinomios con ciertas raíces n-ésimas de 1 como ceros. Esta cualidad permite invertir el proceso, es decir, en lugar de

tomar un polinomio generador $g(X)$ y tomar los ceros adecuados, se puede elegir un conjunto de elementos $\{\alpha_1, \cdots \alpha_r\}$ en extensiones finitas $\mathbf{F}_{q^{t_1}}, \cdots, \mathbf{F}_{q^{t_r}}$ de $\mathbf{F}_q$ (todos los α_i estarán en la extensión finita $\mathbf{F}_{q^t}, t = \text{mcm}\{t_1, \cdots, t_r\}$) y definir

$$\mathcal{C} = \{c(X) \in A \mid c(\alpha_1) = \cdots = c(\alpha_r) = 0\}.$$

Este código es cíclico, ya que si $f_i(X)$ es el polinomio irreducible de α_i, se verifica que $\mathcal{C} = \langle g(X) \rangle = \text{mcm}(f_1, \cdots, f_r)$.

Esta definición de código cíclico se puede comprobar con facilidad si una palabra está o no en el código. Considerando la matriz

$$H' = \begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_r & \cdots & \alpha_r^{n-1} \end{pmatrix}$$

si, para un polinomio $f(X) = f_0 + f_1 X + \cdots + f_{(n-1)} X^{n-1}$ se considera, forzando las notaciones, que

$$H'f(X) = (f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_r))$$

entonces $f(X) \in \mathcal{C}$ si y sólo si $H'f(X) = 0$, esto da pie a considerar H' como una matriz de control del código. Cabe notar que H' no tiene coeficientes en $\mathbf{F}_q$, ni dimensiones $(n-k) \times n$, por lo que no es una matriz de control en sentido estricto. Además, la distancia mínima de $\mathcal{C}$ es $\geq d$ si cualesquiera $d-1$ columnas de H' son linealmente dependientes.

2.1.6. Códigos Reed-Solomon

Los códigos Reed-Solomon [10], o RS para abreviar, son una familia de códigos lineales definidos sobre cuerpos grandes tales que,

Definición 2.1.20. Para los enteros $1 \leq k < n$, un cuerpo $\mathbf{F}_q$ con $q \geq n$, y un conjunto $S = \{a_1, \cdots, a_n\} \subseteq \mathbf{F}_q$, se define a partir de la aplicación $ev : \mathbf{F}_q[X] \longrightarrow \mathbf{F}_q^n$, la cual se define como $ev(f) = (f(a_1), \cdots, f(a_n))$, el código Reed-Solomon

$$RS_{k,S} = \{ev(f) \in \mathbf{F}_q^n \mid f \in \mathbf{F}_q[X] \text{ tales que } \deg(f) < k\}$$

Proposición 2.1.21. *Los códigos RS son MDS.*

Demostración. Recuérdese que todo polinomio de grado d con coeficientes de un cuerpo $\mathbf{F}_q$ tiene como máximo d raíces en $\mathbf{F}_q$.

Al ser $RS_{k,S}$ lineal basta demostrar que toda palabra diferente de 0 tiene un peso de Hamming de al menos $n-k+1$.

Dado $(m_0, m_1, \cdots, m_{k-1}) \neq 0$, el polinomio $f(X) = m_0 + m_1 X + \cdots + m_{k-1}X^{k-1}$ es un polinomio distinto de 0 de grado igual o menor a $k-1$. Por la propiedad anterior f tiene como máximo $k-1$ raíces, por lo que $ev(f) = (f(a_1), \cdots, f(a_n))$ tendrá como máximo $k-1$ ceros.

Por el límite de Singleton la distancia no puede superar $n-k+1$, por tanto debe ser igual a $n-k+1$ y el código será por ello MDS. □

Lema 2.1.22. *Dado un código Reed-Solomon sobre* $\mathbf{F}_q$*,* $RS_{k,S}$*, si* $S = \mathbf{F}_q \setminus \{0\}$*, entonces* $RS_{k,S}$ *es cíclico.*

Demostración. Se puede ver que el código descrito es un código cíclico de longitud $n = q-1$ cuyo polinomio generador tiene por raíces los elementos de $\mathbf{F}_q \setminus \{0\} = \langle \alpha \rangle$, donde α es un elemento primitivo de $\mathbf{F}_q$. □

Otro conjunto S de mucho interés es $S = \mathbf{F}_q$, cuyos códigos se representarán por RS_k en secciones posteriores.

2.2. Introducción a la computación cuántica

En esta sección se van a introducir los fundamentos sobre los que se basa la computación cuántica siguiendo principalmente el contenido de [9].

2.2.1. Bits cuánticos

El *bit* es el concepto fundamental de la computación y la información clásicas. La computación y la información cuánticas se apoyan en un concepto análogo, el *bit cuántico*, o *cúbit*.

¿Qué es un cúbit? Al igual que los bits clásicos tienen un *estado* — 0 o 1 — un cúbit también tiene un estado. Los dos estados posibles de un cúbit son $|0\rangle$ y $|1\rangle$, que corresponden a los estados 0 y 1 de un bit clásico. La diferencia entre un bit y un cúbit es que el cúbit puede estar en un estado diferente a $|0\rangle$ o $|1\rangle$. Se pueden pueden hacer *combinaciones lineales* de estados, generalmente llamadas *superposiciones*:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,. \tag{2.1}$$

Los números α y β son números complejos, sin embargo para la mayoría de aplicaciones no se pierde mucho pensando en ellos como números reales. Puesto de otra manera, el estado de un cúbit es un vector de un espacio vectorial complejo bidimensional. Los estados especiales $|0\rangle$ y $|1\rangle$ se conocen como *estados básicos* y forman una base ortonormal de este espacio vectorial.

Se pueden examinar bits para determinar si está en el estado 1 o 0. Curiosamente, no es posible examinar cúbits para determinar su estado cuántico, es decir, los valores de α y β. La mecánica cuántica nos dice que solo es posible adquirir información mucho más limitada sobre el estado cuántico. Cuando se mide un cúbit se recibe el resultado 0, con probabilidad $|\alpha|^2$, o el resultado 1, con probabilidad $|\beta|^2$. Naturalmente $|\alpha|^2 + |\beta|^2 = 1$, dado que las probabilidades deben sumar 1. Geométricamente, se puede interpretar la condición como que el estado del cúbit debe estar normalizado a longitud 1. Por ello, en general, el estado de un cúbit es un vector unitario en un espacio vectorial complejo bidimensional.

La habilidad de los cúbits de estar en superposición desafía nuestro entendimiento del funcionamiento del mundo. Un bit clásico es como una moneda: o cara o cruz. Con monedas imperfectas puede haber estados intermedios, como que estuviese equilibrada en el canto, pero éstos se pueden ignorar en el caso ideal. En contraste, un cúbit puede existir en una continuidad de estados entre $|0\rangle$ y $|1\rangle$ — hasta que es observado. Cabe enfatizar que cuando se mide un cúbit el resultado solo será 0 o 1. Por ejemplo, un cúbit puede estar en el estado

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\,, \tag{2.2}$$

el cual, al medirlo, da el resultado 0 el cincuenta por ciento ($|1/\sqrt{2}|^2$) de las veces, y 1 el otro cincuenta por ciento. Éste estado se llama a veces $|+\rangle$.

A pesar de sus rarezas, los cúbits son definitivamente reales, su existencia y comportamiento han sido validados repetidamente por experimentos, y varios sistemas físicos pueden ser utilizados para describir cúbits. Para entender mejor como se puede describir un cúbit puede ser útil expresar diferentes maneras en la que dicha descripción puede ocurrir: como las dos diferentes polarizaciones de un fotón, la alineación del espín nuclear en un campo magnético uniforme, o dos estados de un electrón orbitando un solo átomo. En el modelo atómico, el electrón puede existir en los estados 'fundamental' o 'excitado', los cuales reciben el nombre de $|0\rangle$ y $|1\rangle$, respectivamente. Iluminando el átomo, con la energía y durante el tiempo apropiados,es posible mover el electrón del estado $|0\rangle$ al estado $|1\rangle$ y vice versa. Pero, lo que es más interesante, reduciendo el tiempo durante el que se ilumina el átomo, un electrón inicialmente en el estado $|0\rangle$ puede ser movido a un estado 'a medio camino' de $|0\rangle$ y $|1\rangle$, el estado $|+\rangle$.

Una manera muy útil de pensar en cúbits es la siguiente representación geométrica. Como $|\alpha|^2 + |\beta|^2 = 1$, se puede reescribir la Ecuación (2.1) como

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right), \tag{2.3}$$

donde θ, φ y γ son números reales. Dado que el factor $e^{i\gamma}$ no tiene efectos observables, puede ser ignorado, y se puede escribir

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\,. \tag{2.4}$$

Los números θ y φ definen un punto en la esfera tridimensional unitaria, como se muestra en la Figura 2.1. Esta esfera se suele llamar la esfera de Bloch; ofrece una forma muy útil de visualizar el estado de un único cúbit, y a menudo sirve como un excelente banco de pruebas para las ideas sobre computación e información cuánticas. Muchas de las operaciones con solo un cúbit se pueden describir con facilidad en el dibujo de una esfera de Bloch. Sin embargo, es necesario recordar que esta intuición es limitada, dado que no existe una generalización simple de la esfera de Bloch para múltiples cúbits.

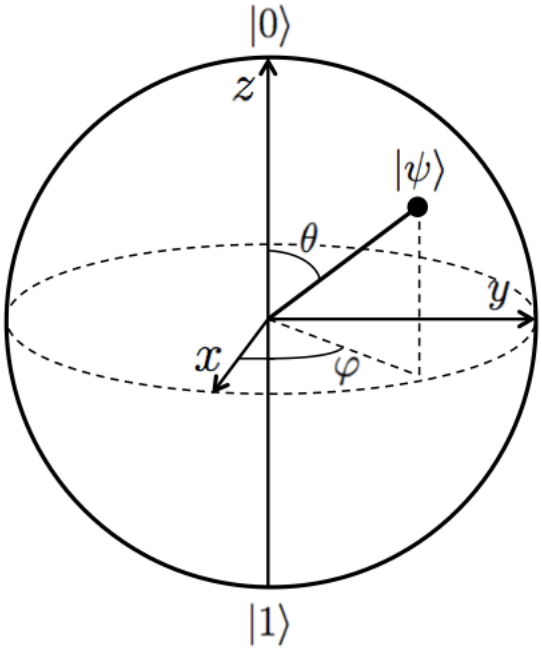

Figura 2.1: Representación de un cúbit usando la esfera de Bloch.

¿Cuánta información hay representada en un cúbit? paradójicamente, hay una cantidad infinita de puntos en la esfera unitaria, por lo que teóricamente se podría almacenar todo El Quijote en la infinita expansión binaria de θ. Sin embargo, esta conclusión resulta ser engañosa, debido al comportamiento de un cúbit al ser observado. Recuerde que la medición de un cúbit solo puede dar 0 o 1. Además, la medición cambia el estado del cúbit, colapsándolo desde su superposición de $|0\rangle$ y $|1\rangle$ al estado específico del resultado de la medición. Por ejemplo, si la medición de $|+\rangle$ da 0, entonces el estado posterior a la medición será $|0\rangle$. ¿Por qué ocurre este tipo de colapso? Nadie lo sabe, este comportamiento es simplemente uno de los *postulados fundamentales* de la mecánica cuántica. Lo que es relevante para nuestro propósito es que de

una sola medida se obtiene solo un bit de información sobre el estado del cúbit, resolviendo así la paradoja aparente, resulta que solo midiendo infinitos cúbits idénticamente preparados se pueden determinar el α y β de un cúbit en el estado dado en la Ecuación (2.1).

Múltiples cúbits

Dados dos bits clásicos, existen cuatro estados posibles, 00, 01, 10 y 11; de manera similar, un sistema de dos cúbits tiene cuatro estados básicos computacionales, denotados por $|00\rangle, |01\rangle, |10\rangle, |11\rangle$. Un par de cúbits también puede existir en superposición de estos cuatro estados, así que el estado cuántico de dos cúbits requiere asociar un coeficiente complejo —a veces llamado una *amplitud*— con cada estado básico, de tal forma que el vector de estado que describe dos cúbits es

$$|\psi\rangle = \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle\,. \tag{2.5}$$

De manera similar al caso de un solo cúbit, el resultado de la medición x (= 00, 01, 10, o 11) ocurre con probabilidad $|\alpha_x|^2$, con el estado de los cúbits después de la medición siendo $|x\rangle$. La condición de que las probabilidades sumen uno es expresada entonces por la condición de *normalización* que $\sum_{x\in\{0,1\}^2} |\alpha_x|^2 = 1$, donde la notación '$\{0,1\}^2$' significa 'el conjunto de secuencias de longitud 2 con cada elemento siendo o cero o uno'. Para un sistema de dos cúbits, es posible medir solo un subconjunto de éstos, por ejemplo el primer cúbit, lo que resulta en 0 con una probabilidad de $|\alpha_{00}|^2 + |\alpha_{01}|^2$, dejando el estado posterior a la medida

$$|\psi'\rangle = \frac{\alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}. \tag{2.6}$$

Cabe notar como el nuevo estado se halla *renormalizado* por el factor $\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}$ para que todavía satisfaga la condición de normalización, justo como se espera de un estado cuántico legítimo. Un estado de dos cúbits importante es el *estado de Bell* o *pareja EPR*,

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}. \tag{2.7}$$

Este estado es responsable de muchas de las cualidades de la computación e información cuánticas. Es el ingrediente clave de la teletransportación cuántica y la codificación superdensa, así como el origen de muchos otros estados interesantes. El estado de Bell tiene la propiedad de que al medir el primer cúbit se pueden obtener dos resultados: 0 con probabilidad 1/2, que deja el estado posterior a la medida $|\varphi'\rangle = |00\rangle$, y 1 con probabilidad 1/2, dejando $|\varphi'\rangle = |11\rangle$. Como resultado, medir el segundo cúbit siempre dará el mismo resultado que la medida del primero. Es decir, los resultados de la medida están relacionados. Esta relación entre las medidas del primer y segundo cúbits existe incluso tras aplicar diferentes operaciones a los cúbits, permitiendo una variedad de medidas diferentes.

2.2.2. Postulados de la mecánica cuántica

La mecánica cuántica es un marco matemático para el desarrollo de teorías físicas. La mecánica cuántica en sí misma no dice que leyes debe obedecer un sistema físico, pero si provee de un marco matemático y conceptual para el desarrollo de dichas leyes. En las siguientes secciones se ofrece una descripción de los postulados básicos de la mecánica cuántica. Estos postulados ofrecen una conexión entre el mundo físico y el formalismo matemático de la mecánica cuántica.

Espacio de estados

El primer postulado de la mecánica cuántica prepara el campo sobre el cual trabajar. Dicho campo es un conocido elemento del álgebra lineal, el espacio de Hilbert.

Postulado 1. *Todo sistema físico aislado tiene asociado un espacio vectorial complejo con producto interno (es decir, un espacio de Hilbert) conocido como el espacio de estados del sistema. El sistema se puede describir completamente por su vector de estado, que es un vector unitario en el espacio de estados del sistema.*

La mecánica cuántico no nos dice, dado un sistema físico, cual es el espacio de estados de dicho sistema, así como tampoco nos dice en que vector de estado se encuentra. Descubrir estos datos para un sistema específico es una tarea difícil para la que los físicos han desarrollado una serie de reglas.

El sistema de la mecánica cuántica más simple es el cúbit. Un cúbit tiene un espacio de estados bidimensional. Suponiendo que $|0\rangle$ y $|1\rangle$ forman una base ortonormal de dicho espacio. Entonces un vector de estado arbitrario en el espacio de estados se puede escribir como

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle\,, \tag{2.8}$$

donde a y b son números complejos. La condición de que $|\psi\rangle$ sea un vector unitario, $\langle\psi|\psi\rangle = 1$, es por tanto equivalente a $|a|^2 + |b|^2 = 1$. La condición $\langle\psi|\psi\rangle = 1$ se conoce normalmente como la *condición de normalización* para los vectores de estado.

Evolución

¿Cómo cambia el estado $|\psi\rangle$, de un sistema cuántico con el tiempo? Este postulado da una base para la descripción de dichos cambios.

Postulado 2. *La evolución de una sistema cuántico cerrado esta descrita por una transformación unitaria. Es decir, el estado $|\psi\rangle$ del sistema en el momento t_1 esta relacionado con*

el estado $|\psi'\rangle$ *en el momento* t_2 *por un operador unitario* U *que depende únicamente del los tiempos* t_1 *y* t_2*,*

$$\left|\psi'\right\rangle = U\left|\psi\right\rangle \tag{2.9}$$

Igual que la mecánica cuántica no nos dice el espacio de estados o el estado cuántico de un sistema cuántico particular, tampoco nos dice que operadores unitarios U describen la dinámica cuántica del mundo físico. La mecánica cuántica solo asegura que la evolución de cualquier sistema cuántico cerrado se puede describir de dicha manera.

Mediciones cuánticas

Se ha postulado que los sistemas cuánticos cerrados evolucionan siguiendo la evolución unitaria. La transformación de sistemas que no interactúan con el resto del mundo es interesante, pero en algún momento el científico y su equipo experimental — un sistema físico externo — debe observar el sistema para descubrir que está sucediendo en el interior de este, una interacción que hace que el sistema deje de ser cerrado, y por tanto no necesariamente sujeto a la evolución unitaria. Para explicar que ocurre cuando esta interacción tiene lugar, se introduce el Postulado 3, que provee una manera de describir el efecto de las mediciones en sistemas cuánticos.

Postulado 3. *Las mediciones cuánticas están descritas por una colección* $\{M_m\}$ *de operadores de medida. Éstos son operadores que actúan en el espacio de estados del sistema que esta siendo medido. El índice* m *se refiere a las diferentes salidas que pueden ocurrir en la medición del experimento. Si el estado del sistema cuántico es* $|\psi\rangle$ *inmediatamente antes de la medición entonces la probabilidad de que el resultado* m *ocurra viene dada por*

$$p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle\,, \tag{2.10}$$

y el estado del sistema tras la medida es

$$\frac{M_m\left|\psi\right\rangle}{\sqrt{\langle\psi| M_m^\dagger M_m \left|\psi\right\rangle}}. \tag{2.11}$$

Los operadores de medición satisfacen la ecuación de completitud,

$$\sum_m M_m^\dagger M_m = I. \tag{2.12}$$

La ecuación de completitud expresa el hecho de que las probabilidades suman uno:

$$1 = \sum_m p(m) = \sum_m \langle\psi| M_m^\dagger M_m |\psi\rangle\,. \tag{2.13}$$

Que esta ecuación se satisfaga para todo $|\psi\rangle$ es equivalente a la ecuación de completitud. Sin embargo, la ecuación de completitud es mucho mas fácil de comprobar directamente, y por ello aparece en el enunciado del postulado.

Un ejemplo simple pero importante de una medición es la *medición de un cúbit en la base computacional*. Ésta es una medición de un único cúbit con dos resultados definidos por los dos operadores de medición $M_0 = |0\rangle\langle 0|$, $M_1 = |1\rangle\langle 1|$. Se puede observar que cada operador es hermítico, y que $M_0^2 = M_0$, $M_1^2 = M_1$. Por tanto la relación de completitud se cumple, $I = M_0^\dagger M_0 + M_1^\dagger M_1 = M_0 + M_1$. Suponiendo que el estado a medir es $|\psi\rangle = a|0\rangle + b|1\rangle$. Entonces la probabilidad de obtener el resultado de la medición 0 es

$$p(0) = \langle\psi| M_0^\dagger M_0 |\psi\rangle = \langle\psi| M_0 |\psi\rangle = |a|^2. \tag{2.14}$$

Similarmente la probabilidad de que el resultado de la medición sea 1 es $p(1) = |b|^2$. El estado tras la medición en ambos casos es, por tanto

$$\frac{M_0|\psi\rangle}{|a|} = \frac{a}{|a|}|0\rangle \tag{2.15}$$

$$\frac{M_1|\psi\rangle}{|b|} = \frac{b}{|b|}|1\rangle. \tag{2.16}$$

Sistemas compuestos

Suponiendo un interés en un sistema cuántico complejo formado por dos (o más) sistemas físicos distintos. ¿Como se deberían describir los estados del sistema compuesto? El postulado siguiente describe como el espacio de estados de un sistema compuesto se construye a partir de los espacios de estados de las componentes del sistema.

Postulado 4. *El espacio de estado de un sistema físico compuesto es el producto tensorial de los espacios de estado de los sistemas físicos que lo componen. Además, si se tienen los sistemas numerados de 1 hasta n, y el sistema número i está preparado en el estado $|\psi_i\rangle$ entonces el estado conjunto del sistema total es $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$.*

2.3. Códigos correctores cuánticos

Este último apartado introduce y explica conceptos estudiados en [6] para posteriormente aplicarlos a la creación de códigos cuánticos.

2.3.1. Códigos estabilizadores

Sea q una potencia de un primo p, y sea $\mathbf{C}^q$ un espacio vectorial complejo q-dimensional que representa los estados de un sistema cuántico. Se denota por $|x\rangle$ a los vectores de una base ortonormal de $\mathbf{C}^q$, donde x toma los valores de un cuerpo finito $\mathbf{F}_q$ con q elementos. Un código corrector de errores cuántico $\mathcal{Q}$ es un subespacio K-dimensional de $\mathbf{C}^{q^n} = \mathbf{C}^q \otimes \cdots \otimes \mathbf{C}^q$.

Para poder medir el rendimiento de un código, es necesario un modelado de los errores apropiado. Se simplifica el problema eligiendo una base $\mathcal{E}_n$ del espacio vectorial de matrices complejas $q^n \times q^n$ para representar un conjunto discreto de errores. Un código estabilizador se define como el espacio propio común de un subconjunto de $\mathcal{E}_n$, por lo que los operadores de errores son muy importantes.

Bases de los errores

Sean a y b elementos del cuerpo finito $\mathbf{F}_q$. Se definen los operadores unitarios $X(a)$ y $Z(b)$ como

$$X(a)\,|x\rangle = |x+a\rangle\,, \quad Z(b)\,|x\rangle = \omega^{\mathrm{tr}(bx)}\,|x\rangle$$

Donde tr representa la operación traza de la extensión $\mathbf{F}_q$ al cuerpo primo $\mathbf{F}_p$, y $\omega = \exp(2\pi i/p)$ es una raíz p-ésima primitiva de la unidad.

Se forma el conjunto $\mathcal{E} = \{X(a)Z(b) \mid a, b \in \mathbf{F}_q\}$ de operadores de errores. Este conjunto tiene varias propiedades interesantes, a) contiene la matriz identidad, b) el producto de dos matrices en $\mathcal{E}$ es un múltiplo escalar de otro elemento de $\mathcal{E}$ y c) la traza $\mathrm{Tr}\big(A^\dagger B\big) = 0$ para dos elementos diferentes A, B de $\mathcal{E}$. Dado un conjunto finito de q^2 matrices unitarias que satisface las propiedades a), b) y c) se dice que es una buena base de errores [7].

El conjunto $\mathcal{E}$ de operadores de errores forma una base del conjunto de matrices complejas $q \times q$ debido a la propiedad c). Para comprobar que $\mathcal{E}$ es una buena base de errores son necesarias las demostraciones siguientes.

Lema 2.3.1. *El conjunto $\mathcal{E} = \{X(a)Z(b) \mid a, b \in \mathbf{F}_q\}$ es una buena base de errores en $\mathbf{C}^q$.*

Demostración. La matriz $X(0)Z(0)$ es la matriz identidad, por lo que la propiedad a) se cumple. Se tiene $\omega^{\mathrm{tr}(ba)}X(a)Z(b) = Z(b)X(a)$, lo que implica que el producto de dos operadores de errores viene dado por

$$X(a)Z(b)X(a')Z(b') = \omega^{\mathrm{tr}(ba')}X(a+a')Z(b+b'). \tag{2.17}$$

Dado que el resultado es un escalar de un operador de $\mathcal{E}$, se cumple la propiedad b).

Suponiendo que los operadores de errores son de la forma $A = X(a)Z(b)$ y $B = X(A)Z(b')$ para algunos $a, b, b' \in \mathbf{F}_q$, entonces

$$\mathrm{Tr}\Big(A^\dagger B\Big) = \mathrm{Tr}\big(Z(b'-b)\big) = \sum_{x \in \mathbf{F}_q} \omega^{\mathrm{tr}((b'-b)x)}$$

La aplicación $x \mapsto \omega^{\mathrm{tr}((b'-b)x)}$ es un carácter aditivo de $\mathbf{F}_q$. La suma de todos los valores del carácter es 0 a no ser que el carácter sea trivial; por tanto, $\mathrm{Tr}\big(A^\dagger B\big) = 0$ cuando $b' \neq b$.

Por otro lado, si $A = X(a)Z(b)$ y $B = X(a')Z(b')$ son dos operadores de errores con $a \neq a'$, entonces los elementos diagonales de la matriz $A^\dagger B = Z(-b)X(a'-a)Z(b')$ son 0, lo que implica que $\mathrm{Tr}\big(A^\dagger B\big) = 0$. Por tanto, cuando A y B son dos elementos diferentes de $\mathcal{E}$, entonces $\mathrm{Tr}\big(A^\dagger B\big) = 0$, demostrando c). □

Ejemplo 2.3.2. Para la construcción de una buena base de errores con $q = 4$ niveles, se toma el cuerpo finito $\mathbf{F}_4$, que consiste de los elementos $\mathbf{F}_4 = \{0, 1, \alpha, \bar{\alpha}\}$. Se denotan los 4 vectores de la base canónica del espacio vectorial complejo $\mathbf{C}^4$ por $|0\rangle, |1\rangle, |\alpha\rangle$ y $|\bar{\alpha}\rangle$.
Sea $\mathbf{1}_2$ la matriz identidad 2×2, $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, y $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Entonces

$$\begin{array}{ll} X(0) = \mathbf{1}_2 \otimes \mathbf{1}_2, & X(1) = \mathbf{1}_2 \otimes \sigma_x \\ X(\alpha) = \sigma_x \otimes \mathbf{1}_2, & X(\bar{\alpha}) = \sigma_x \otimes \sigma_x \\ Z(0) = \mathbf{1}_2 \otimes \mathbf{1}_2, & Z(1) = \sigma_z \otimes \mathbf{1}_2 \\ Z(\alpha) = \sigma_z \otimes \sigma_z, & Z(\bar{\alpha}) = \mathbf{1}_2 \otimes \sigma_z. \end{array}$$

Cabe notar que esta buena base de errores se obtiene mediante el producto tensorial de las matrices de Pauli, una buena base de errores en $\mathbf{C}^2$. El lema siguiente muestra que es un principio de diseño general para las buenas bases de errores.

Lema 2.3.3. *Si $\mathcal{E}_1$ y $\mathcal{E}_2$ son buenas bases de errores, entonces*

$$\mathcal{E} = \{E_1 \otimes E_2 \mid E_1 \in \mathcal{E}_1, E_2 \in \mathcal{E}_2\}$$

también es una buena base de errores.

La demostración de este lema surge directamente de las definiciones.

Sea $\mathbf{a} = (a_1, \cdots, a_n) \in \mathbf{F}_q^n$. Se indicará como $X(\mathbf{a}) = X(a_1) \otimes \cdots \otimes X(a_n)$ y $Z(\mathbf{a}) = Z(a_1) \otimes \cdots \otimes Z(a_n)$ el producto tensorial de n operadores de errores. El objetivo es proveer un modelo que represente los errores actuando localmente en un sistema cuántico. Con estas notaciones se puede formular dicho modelo.

Corolario 2.3.4. *El conjunto $\mathcal{E}_n = \{X(\mathbf{a})Z(\mathbf{b}) \mid \mathbf{a}, \mathbf{b} \in \mathbf{F}_q^n\}$ es una buena base de errores en el espacio vectorial complejo $\mathbf{C}^{q^n}$.*

Códigos estabilizadores

Sea G_n el grupo generado por las matrices de la buena base de errores $\mathcal{E}_n$. De (2.17) sale que

$$G_n = \{\omega^c X(\mathbf{a})Z(\mathbf{b}) \mid \mathbf{a}, \mathbf{b} \in \mathbf{F}_q^n, c \in \mathbf{F}_p\}.$$

Cabe notar que G_n es un grupo finito de orden pq^{2n}. G_n recibe el nombre de *grupo de errores* asociado con la buena base de errores $\mathcal{E}_n$.

Un *código estabilizador* Q es un subespacio no nulo de $\mathbf{C}^{q^n}$ que satisface

$$Q = \bigcap_{E \in S} \{v \in \mathbf{C}^{q^n} \mid Ev = v\} \tag{2.18}$$

para algún subgrupo S de G_n. En otras palabras, Q es el espacio propio común de valor propio 1 de un subgrupo S del grupo de errores G_n.

Cabe destacar que es crucial que el código estabilizador contenga a *todos* los vectores propios comunes de S con valor propio 1. Si el código es más pequeño y no los cubre todos, entonces no es un código estabilizador de S.

Distancia mínima

Las capacidades de corrección y detección de errores de un código corrector cuántico Q son los aspectos mas relevantes del código. Un código Q será capaz de detectar un error E en el grupo unitario $U(q^n)$ si y solo si la condición $\langle c_1| E |c_2\rangle = \lambda_E \langle c_1|c_2\rangle$ se cumple para todo $c_1, c_2 \in Q$.

Resulta que un código estabilizador Q con estabilizador S puede detectar todos los errores en G_n que son múltiplos escalares de los elementos de S o que no conmuten con algún elemento de S. En particular, un error de G_n que no puede ser detectado tiene que conmutar con todos los elementos del estabilizador. Los elementos conmutativos de G_n se caracterizan como sigue:

Lema 2.3.5. *Dos elementos $E = \omega^c X(\mathbf{a})Z(\mathbf{b})$ y $E' = \omega^{c'} X(\mathbf{a}')Z(\mathbf{b}')$ del grupo de errores G_n satisfacen la relación*

$$EE' = \omega^{\mathrm{tr}(\mathbf{b}\cdot\mathbf{a}' - \mathbf{b}'\cdot\mathbf{a})} E'E.$$

En particular, los elementos E y E' conmutan si y solo si la traza simpléctica de $tr(\mathbf{b}\cdot\mathbf{a}' - \mathbf{b}'\cdot\mathbf{a})$ desaparece.

Demostración. Se puede obtener de (2.17) que

$$EE' = \omega^{\mathrm{tr}(\mathbf{b}\cdot\mathbf{a}')} X(\mathbf{a}+\mathbf{a}')Z(\mathbf{b}+\mathbf{b}')$$

y

$$E'E = \omega^{\mathrm{tr}(\mathbf{b}'\cdot\mathbf{a})} X(\mathbf{a}+\mathbf{a}')Z(\mathbf{b}+\mathbf{b}').$$

Por tanto, multiplicar $E'E$ por el escalar $\omega^{tr(\mathbf{b}\cdot\mathbf{a}'-\mathbf{b}'\cdot\mathbf{a})}$ resulta en EE'. □

Se define el *peso simpléctico* swt de un vector $(\mathbf{a}|\mathbf{b})$ en $\mathbf{F}_q^{2n}$ como

$$\mathrm{swt}((\mathbf{a}|\mathbf{b})) = \#\{k \mid (a_k, b_k) \neq (0,0)\}.$$

El peso $\mathrm{wt}(E)$ de un elemento $E = \omega^c X(\mathbf{a})Z(\mathbf{b})$ del grupo de errores G_n se define como la cantidad de componentes tensoriales diferentes de la identidad, $\mathrm{w}(E) = \mathrm{swt}((\mathbf{a}|\mathbf{b}))$. En particular, el peso de un múltiplo escalar de la matriz identidad es por definición cero.

Un código cuántico Q tiene una *distancia mínima* d si y solo si puede detectar todos los errores de G_n con un peso menor que d, pero no puede detectar algún error de peso d. Se dirá que Q es un código $((n, K, d))_q$ si y solo si Q es un subespacio K-dimensional de $\mathbf{C}^{q^n}$ con una distancia mínima d. Un código $((n, q^k, d))_q$ también se puede llamar un código $[[n, k, d]]_q$.

En código cuántico Q se llamará *puro hasta* t si y solo si su grupo estabilizador S no contiene matrices no escalares de peso inferior a t. Un código cuántico se llamará *puro* si y solo si es puro hasta su distancia mínima. Se asume que un código $[[n, 0, d]]_q$ tiene que ser puro.

2.3.2. Conexión de Galois

En esta sección se busca clarificar la relación entre códigos estabilizadores y códigos cuánticos más generales. Sea $\mathcal{Q}$ el conjunto de todos los subespacios de $\mathbf{C}^{q^n}$. El conjunto $\mathcal{Q}$ se haya parcialmente ordenado por la relación de inclusión. Cualesquiera dos elementos de $\mathcal{Q}$ tienen al menos una cota superior mínima y una cota inferior máxima con respecto a la relación de inclusión,

$$\sup\{Q, Q'\} = Q + Q' \quad \text{y} \quad \text{ínf}\{Q, Q'\} = Q \cap Q'.$$

Por tanto, $\mathcal{Q}$ es un retículo completo. Un elemento de éste retículo es un código corrector cuántico o es igual al espacio vectorial $\{0\}$.

Sea $\mathcal{G}$ el retículo de los subgrupos del grupo de errores G_n. Se introducen dos aplicaciones entre $\mathcal{G}$ y $\mathcal{Q}$ que establecen una conexión de Galois. El objetivo es demostrar que los códigos estabilizadores son elementos específicos de $\mathcal{Q}$ que se mantienen invariantes al ser enviados al retículo $\mathcal{G}$ y devueltos al retículo $\mathcal{Q}$.

Se define la aplicación Fix del retículo $\mathcal{G}$ de subgrupos al retículo $\mathcal{Q}$ de subespacios que asocia al grupo S su espacio propio común de valor propio 1

$$\mathrm{Fix}(S) = \bigcap_{E \in S} \{v \in \mathbf{C}^{q^n} \mid Ev = v\}. \tag{2.19}$$

Se define en la dirección inversa una aplicación Stab del retículo $\mathcal{Q}$ al retículo $\mathcal{G}$ que asocia un código cuántico Q a su grupo estabilizador $\mathrm{Stab}(Q)$,

$$\mathrm{Stab}(Q) = \{E \in G_n \mid Ev = v \text{ para todo } v \in Q\}. \tag{2.20}$$

Se obtienen cuatro consecuencias directas de las definiciones 2.19 y 2.20:

G1) Si $Q_1 \subseteq Q_2$ son subespacios de $\mathbf{C}^{q^n}$, entonces $\mathrm{Stab}(Q_2) \leq \mathrm{Stab}(Q_1)$.

G2) Si $S_1 \leq S_2$ son subgrupos de G_n, entonces $\mathrm{Fix}(S_2) \subseteq \mathrm{Fix}(S_1)$.

G3) Un subespacio Q de $\mathbf{C}^{q^n}$ cumple que $Q \subseteq \mathrm{Fix}(\mathrm{Stab}(Q))$.

G4) Un subgrupo S de G_n cumple que $S \leq \mathrm{Stab}(\mathrm{Fix}(Q))$.

Las primeras dos propiedades establecen que Fix y Stab son aplicaciones que invierten el orden. Las propiedades extendidas G3 y G4 establecen que Fix y Stab forman una conexión de Galois [1, p. 56]. La teoría general de conexiones de Galois establece, entre otras cosas, que $\mathrm{Fix}(S) = \mathrm{Fix}(\mathrm{Stab}(\mathrm{Fix}(S)))$ y $\mathrm{Stab}(Q) = \mathrm{Stab}(\mathrm{Fix}(\mathrm{Stab}(Q)))$ se cumple para todo S en $\mathcal{G}$ y todo Q en $\mathcal{Q}$.

A un subespacio Q del espacio vectorial $\mathbf{C}^{q^n}$ que satisface G3 con la igualdad se le llama un *subespacio cerrado*, y a un subgrupo S del grupo de errores G_n que satisface G4 con la igualdad se le llama un *subgrupo cerrado*. Uno de los principales resultados de la teoría abstracta de Galois es

Proposición 2.3.6. *Los subespacios cerrados del espacio vectorial $\mathbf{C}^{q^n}$ forman un subretículo completo $\mathcal{Q}_c$ del retículo $\mathcal{Q}$. Los subgrupos cerrados de G_n forman un subretículo completo $\mathcal{G}_c$ del retículo $\mathcal{G}$ que es dual isomorfo al retículo $\mathcal{Q}_c$.*

Es necesario caracterizar los subespacios cerrados y los subgrupos cerrados para poder utilizar esta proposición.

Lema 2.3.7. *Un subespacio cerrado es un código estabilizador o tiene dimensión 0.*

Demostración. Por definición, un subespacio cerrado Q cumple que

$$Q = \mathrm{Fix}(\mathrm{Stab}(Q)) = \bigcap_{E \in \mathrm{Stab}(Q)} \{v \in \mathbf{C}^{q^n} \mid Ev = v\};$$

por tanto, es un código estabilizador o $\{0\}$. □

Lema 2.3.8. *Si Q es un subespacio no nulo de $\mathbf{C}^{q^n}$, entonces su estabilizador $S = Stab(Q)$ es un grupo abeliano que cumple $S \cap Z(G_n) = \{1\}$.*

Demostración. Suponiendo que E y E' son elementos no conmutativos de $S = \mathrm{Stab}(Q)$, por el lema 2.3.5 se tiene que $EE' = \omega^k E'E$ para algún $\omega^k \neq 1$. Un vector no nulo $v \in Q$ tendría que cumplir $v = EE'v = \omega^k E'Ev = \omega^k v$, contradicción. Por tanto, S es un grupo abeliano. El

estabilizador no puede contener ningún elemento $\omega^k \mathbf{1}$, a no ser que $k = 0$, lo que demuestra la segunda afirmación. □

Lema 2.3.9. *Suponiendo que S es el estabilizador de un espacio vectorial Q, un proyector ortogonal sobre el espacio propio común Fix(S) viene dado por*

$$P = \frac{1}{|S|} \sum_{E \in S} E.$$

Demostración. Un vector v en Fix(S) satisface $Pv = v$, por lo que Fix(S) está contenido en la imagen de P. A la inversa, notese que $EP = P$ se cumple para todo E en S, por tanto cualquier vector en la imagen de P es un vector propio con valor propio 1 de todos los operadores de errores E en S. Por ello, Fix(S) = image(P). El operador P es idempotente, ya que

$$P^2 = \frac{1}{|S|} \sum_{E \in S} EP = \frac{1}{|S|} \sum_{E \in S} P = P$$

se cumple. El inverso $E^\dagger$ de E esta contenido en el grupo S, por tanto $P^\dagger = P$. Por ello, P es un proyector ortogonal sobre Fix(S). □

Lema 2.3.10. *Un subgrupo S de G_n es cerrado si y solo si S es un subgrupo abeliano que satisface $S \cap Z(G_n) = \{1\}$ o si S es igual a G_n.*

Demostración. Suponiendo que S es un subgrupo cerrado de G_n, el espacio vectorial $Q = \text{Fix}(S)$ es, por definición, o un código estabilizador o un espacio vectorial de dimensión 0. Se sabe que $\text{Stab}(\{0\}) = G_n$, por tanto, si $Q \neq \{0\}$, entonces $\text{Stab}(Q) = S$ es un grupo abeliano que cumple $S \cap Z(G_n) = \{\mathbf{1}\}$ Por el lema 2.3.8.

A la inversa, suponiendo que S es un subgrupo abeliano de G_n tal que S trivialmente se intersecta con el centro $Z(G_n)$. Sea $S^* = \text{Stab}(\text{Fix}(S))$. Entonces $\text{Fix}(S^*) = \text{Fix}(\text{Stab}(\text{Fix}(S))) = \text{Fix}(S)$, ya que esto se cumple para todo par de aplicaciones que forman una conexión de Galois. Se obtiene del lema 2.3.9 que

$$q^n/|S^*| = \text{Tr}\left(\frac{1}{|S^*|} \sum_{E \in S^*} E\right) = \text{Tr}\left(\frac{1}{|S|} \sum_{E \in S} E\right) = q^n/|S|.$$

Como $S \leq S^*$, esto muestra que $S = S^* = \text{Stab}(\text{Fix}(S))$; por tanto S es un subgrupo cerrado de G_n. Notese que $\text{Fix}(G_n) = \{0\}$, por lo que $G_n = \text{Stab}(\text{Fix}(G_n))$ es cerrado. □

Dado que los códigos estabilizadores son mas fáciles de estudiar que un código cuántico arbitrario, se puede obtener en ocasiones una cota inferior de la distancia mínima de un código gracias a la siguiente observación:

Un código cuántico arbitrario Q esta contenido en el código estabilizador $Q^* = \mathrm{Fix}(\mathrm{Stab}(Q))$. Si un error E puede ser detectado por Q^*, entonces puede ser detectado por Q. Por tanto, si el código estabilizador Q^* tiene una distancia mínima d, el código cuántico Q tendrá al menos una distancia mínima d.

2.3.3. Códigos aditivos

Existe una relación entre los códigos estabilizadores y los códigos clásicos. Los códigos clásicos nos permiten caracterizar los errores de G_n que pueden ser detectados por un código estabilizador.

Para comenzare es necesario formalizar algunas de las propiedades de los errores detectables. Si S es un subgrupo de G_n, entonces $C_{G_n}(S)$ denota el centralizador de S en G_n

$$C_{G_n}(S) = \{E \in G_n \mid EF = FE \text{ para todo } F \in S\}$$

y $SZ(G_n)$ denota el grupo generado por S y el centro $Z(G_n)$.

Lema 2.3.11. *Suponiendo que $S \leq G_n$ es el grupo estabilizador de un código estabilizador Q de dimensión $\dim Q > 1$. Un error E en G_n es detectable por el código cuántico Q si y solo si o bien E es un elemento de $SZ(G_n)$ o bien E no pertenece al centralizador $C_{G_n}(S)$.*

Demostración. Un elemento E en $SZ(G_n)$ es un múltiplo escalar de un estabilizador; por tanto, actúa por multiplicación por un escalar λ_E en Q. De aquí surge que E es un error detectable.

Suponiendo ahora que E es un error en G_n que no conmuta con algún elemento F del estabilizador S; del lema 2.3.5 sale que $EF = \lambda FE$ para algún número complejo $\lambda \neq 1$.Todos los vectores u y v de Q satisfacen la condición

$$\langle v| E |v\rangle = \langle v| EF |v\rangle = \lambda \langle v| FE |v\rangle = \lambda \langle v| E |v\rangle ; \tag{2.21}$$

por lo que $\langle u| E |v\rangle = 0$. Se deduce el error es detectable.

Por último, se supone que E es un elemento de $C_{G_n}(S) \setminus SZ(G_n)$. Buscando una contradicción, se asume que E es detectable; esto implica que existe un escalar complejo λ_E al que $Ev = \lambda_E v$ para todo V en Q. El escalar λ_E no puede ser cero porque E conmuta con los elementos de S, por lo que $EP = PEP = \lambda_E P$ y claramente $EP \neq 0$. Sea S^* el grupo abeliano generado por λ_E^{-1} y los elementos de S. El espacio propio común de S^* con valor propio 1 tiene dimensión $q^n/|S^*| < \dim Q = q^n/|S|$. Esto implica que no todos los vectores de Q se mantienen invariantes al aplicarles $\lambda_E^{-1}E$, como contradicción a la capacidad de detección de E. □

Corolario 2.3.12. *Si un código estabilizador Q tiene distancia mínima d y es puro hasta t, entonces todos los errores $E \in G_n$ con $1 \leq w(E) < min\{t, d\}$ satisface que $\langle u| E |v\rangle = 0$ para todo u y v perteneciente a Q.*

Demostración. Por hipótesis, el peso de E es menor que la distancia mínima y por tanto es detectable. Sin embargo, E no es un elemento de $Z(G_n)S$, dado que el código es puro hasta $t > \mathrm{w}(E)$. Por tanto, E no pertenece a $C_{G_n}(S)$, y la afirmación sale de 2.21. □

Códigos sobre $\mathbf{F}_q$

El lema 2.3.6 caracteriza las capacidades de detección de errores de un código estabilizador con un grupo estabilizador S en términos de los grupos $SZ(G_n)$ y $C_{G_n}(S)$. La información de fase de un elemento en G_n no es relevante para lo que concierne a la detección, ya que un elemento E de G_n es detectable si y solo si ωE lo es. Por tanto, si se asocia a un elemento $\omega^c X(\mathbf{a})Z(\mathbf{b})$ de G_n un elemento $(\mathbf{a}|\mathbf{b})$ de $\mathbf{F}_q^{2n}$, entonces el grupo $SZ(G_n)$ se puede asignar al código aditivo

$$C = \{(\mathbf{a}|\mathbf{b}) \mid \omega^c X(\mathbf{a})Z(\mathbf{b}) \in SZ(G_n)\} = SZ(G_n)/Z(G_n).$$

Para describir la imagen del centralizador, es necesaria la noción de una forma traza-simpléctica de dos vectores $(\mathbf{a}|\mathbf{b})$ y $(\mathbf{a}'|\mathbf{b}')$ en $\mathbf{F}_q^{2n}$

$$\big\langle (\mathbf{a}|\mathbf{b}) \big| (\mathbf{a}'|\mathbf{b}') \big\rangle_s = \mathrm{tr}_{q/p}(\mathbf{b}\cdot\mathbf{a}' - \mathbf{b}'\cdot\mathbf{a}).$$

El centralizador $C_{G_n}(S)$ contiene todos los elementos de G_n que conmutan con todos los elementos de S; por tanto, por el lema 2.3.5, $C_{G_n}(S)$ se puede mapear al código dual traza-simpléctico $C^{\perp_s}$ del código C,

$$C^{\perp_s} = \{(\mathbf{a}|\mathbf{b}) \mid \omega^c X(\mathbf{a})Z(\mathbf{b}) \in C_{G_n}(S)\}.$$

La conexión entre los códigos clásicos y el código estabilizador se precisa en el teorema siguente.

Teorema 2.3.13. *Un código estabilizador $((n, K, d))_q$ existe si y solo si existe un código aditivo $C \leq \mathbf{F}_q^{2n}$ de tamaño $|C| = q^n/K$ tal que $C \leq C^{\perp_s}$ y $swt(C^{\perp_s} \setminus C) = d$ si $K > 1$ (y $swt(C^{\perp_s}) = d$ si $K = 1$).*

Demostración. Suponiendo que un código estabilizador $((n, K, d))_q$, Q, existe, implica que existe un subgrupo cerrado S de G_n de orden $|S| = q^n/K$ tal que $Q = \mathrm{Fix}(S)$. El grupo S es abeliano y satisface $S \cap Z(G_n) = 1$, por el lema 2.3.10. El cociente $C \cong SZ(G_n)/Z(G_n)$ es un subgrupo aditivo de $\mathbf{F}_q^{2n}$ tal que $|C| = |S| = q^n/K$. Se tiene, por el lema 2.3.5, $C^{\perp_s} = C_{G_n}(S)/Z(G_n)$. Como S es un grupo abeliano, $SZ(G_n) \leq C_{G_n}(S)$, por lo que $C \leq C^{\perp_S}$. Recordando que el peso de un elemento $\omega^c X(\mathbf{a})\mathbf{Z}(\mathbf{b})$ en G_n es igual a $\mathrm{swt}(\mathbf{a}|\mathbf{b})$. Si $K = 1$, entonces Q es un código cuántico puro, por lo que $\mathrm{wt}(C_{G_n}(S)) = \mathrm{swt}(C^{\perp_s}) = d$ Si $K > 1$, entonces los elementos de $C_{G_n}(S) \setminus SZ(G_n)$ tienen al menos peso d por el lema 2.3.11, por lo que $\mathrm{swt}(C^{\perp_s} \setminus C) = d$.

Por otro lado, se supone que C es un subcódigo aditivo de $\mathbf{F_q^{2n}}$ tal que $|C| = q^n/K$, $C \leq C^{\perp_s}$ y $\mathrm{swt}(C^{\perp_s} \setminus C) = d$ si $K > 1$ (y $\mathrm{swt}(C^{\perp_s}) = d$ si $K = 1$). Sea

$$N = \{\omega^c X(\mathbf{a}) Z(\mathbf{b}) \mid c \in \mathbf{F}_p \text{ y } (\mathbf{a}|\mathbf{b}) \in C\}.$$

Nótese que N es un subgrupo normal abeliano de G_n, ya que es la antiimagen de $C = N/Z(G_n)$. Tomando un carácter χ de N tal que $\chi(\omega^c \mathbf{1}) = \omega^c$. Entonces

$$P_N = \frac{1}{|N|} \sum_{E \in N} \chi(E^{-1}) E$$

es un proyector ortogonal sobre un espacio vectorial Q, porque P_N es idempotente en el anillo $\mathbf{C}[C_n]$. Se tiene

$$\dim Q = \mathrm{Tr}\, P_N = |Z(G_n)| q^n / |N| = q^n/|C| = K.$$

Cada clase de N módulo $Z(G_n)$ contiene exactamente una matriz E tal que $Ev = v$ para todo $v \in Q$. Entonces S es un subgrupo abeliano de G_n de orden $|S| = |C| = q^n/K$. Se tiene $Q = \mathrm{Fix}(S)$, ya que Q es claramente un subespacio de $\mathrm{Fix}(S)$, pero $\dim Q = q^n/|S| = K$. Un elemento $\omega^c X(\mathbf{a}) Z(\mathbf{b})$ en $C_{G_n}(S) \setminus SZ(G_n)$ no puede tener peso inferior a d, ya que esto implicaría que $(\mathbf{a}|\mathbf{b}) \in C^{\perp_s} \setminus C$ tiene un peso inferior a d, lo que es imposible. Por la misma razón, si $K = 1$, entonces todas los elementos diferentes de la identidad del centralizador $C_{G_n}(S)$ deben tener un peso de d o superior. Por tanto, Q es un código estabilizador $((n, K, d))_q$. □

Códigos sobre $\mathbf{F}_{q^2}$

El principal inconveniente de utilizar los códigos anteriores es la poca familiaridad que se tiene con los pesos simplécticos explicados. Por tanto, sería beneficioso si se pudiese crear una relación para utilizar el peso de Hamming en su lugar.

Sea (β, β^q) una base normal de $\mathbf{F}_{q^2}$ sobre $\mathbf{F}_q$. Se define una forma traza-alternante de dos vectores v y w en $\mathbf{F}_{q^2}^n$ como

$$\langle v|w\rangle_a = \mathrm{tr}_{q/p}\left(\frac{v \cdot w^q - v^q \cdot w}{\beta^{2q} - \beta^q}\right). \tag{2.22}$$

Cabe notar que el argumento de la traza es invariante bajo el automorfismo de Galois $x \mapsto x^q$, por lo que es un elemento de $\mathbf{F}_q$, demostrando que (2.22) está bien definida.

La forma traza-alternante es bi-aditiva, es decir, $\langle u + v|w\rangle_a = \langle u|w\rangle_a + \langle v|w\rangle_a$ y $\langle u|v + w\rangle_a = \langle u|v\rangle_a + \langle u|w\rangle_a$ se cumple para todo $u, v, w \in \mathbf{F}_{q^2}^n$. Es $\mathbf{F}_p$-lineal, pero no $\mathbf{F}_q$-lineal, a no ser que $q = p$ y es alternante en el sentido de que $\langle u|u\rangle_a = 0$ para todo $u \in \mathbf{F}_{q^2}^n$. Se dirá $u \perp_a w$ si y solo si $\langle u|w\rangle_a = 0$.

Se define una aplicación biyectiva ϕ que toma un elemento $(\mathbf{a}|\mathbf{b})$ del espacio vectorial $\mathbf{F}_q^{2n}$ a un vector en $\mathbf{F}_{q^2}$ mediante $\phi((\mathbf{a}|\mathbf{b})) = \beta\mathbf{a} + \beta^q\mathbf{b}$. La aplicación ϕ es isométrica en el sentido de que el peso simpléctico de $(\mathbf{a}|\mathbf{b})$ es igual al peso de Hamming de $\phi((\mathbf{a}|\mathbf{b}))$.

Lema 2.3.14. *Dados c y d dos vectores de $\mathbf{F}_q^{2n}$. Entonces*

$$\langle c|d\rangle_s = \langle \phi(c)|\phi(d)\rangle_a .$$

En particular, c y d son ortogonales con respecto a la forma traza-simpléctica si y solo si $\phi(c)$ y $\phi(d)$ son ortogonales con respecto a la forma traza-alternante.

Demostración. Sea $c = (\mathbf{a}|\mathbf{b})$ y $d = (\mathbf{a}'|\mathbf{b}')$. Se puede calcular

$$\phi(c) \cdot \phi(d)^q = \beta^{q+1}\mathbf{a}\cdot\mathbf{a}' + \beta^2\mathbf{a}\cdot\mathbf{b}' + \beta^{2q}\mathbf{b}\cdot\mathbf{a}' + \beta^{q+1}\mathbf{b}\cdot\mathbf{b}'$$

$$\phi(c)^q \cdot \phi(d) = \beta^{q+1}\mathbf{a}\cdot\mathbf{a}' + \beta^{2q}\mathbf{a}\cdot\mathbf{b}' + \beta^2\mathbf{b}\cdot\mathbf{a}' + \beta^{q+1}\mathbf{b}\cdot\mathbf{b}'$$

Por tanto, la forma traza-alternante de $\phi(c)$ y $\phi(d)$ viene dada por

$$\langle \phi(c)|\phi(d)\rangle_a = \mathrm{tr}_{q/p}\left(\frac{\phi(c)\cdot\phi(d)^q - \phi(c)^q\cdot\phi(d)}{\beta^{2q}-\beta^2}\right) = \mathrm{tr}_{q/p}(\mathbf{b}\cdot\mathbf{a}' - \mathbf{a}'\cdot\mathbf{b}),$$

que es precisamente la forma traza-simpléctica $\langle c|d\rangle_s$. □

Teorema 2.3.15. *Un código estabilizador $((n, K, d))_q$ existe si y solo si existe un subcódigo aditivo D de $\mathbf{F}_{q^2}^n$ de cardinalidad $|D| = q^n/K$ tal que $D \leq D^{\perp_a}$ y $wt(D^{\perp_a} \setminus D) = d$ si $K > 1$ (y $wt(D^{\perp_a}) = d$ si $K = 1$).*

Demostración. El teorema 2.3.13 muestra que existe un código estabilizador $((n, K, d))_q$ si y solo si existe un código $C \leq \mathbf{F}_q^{2n}$ con $|C| = q^n/K$, $C \leq C^{\perp_s}$ y $\mathrm{swt}(C^{\perp_s} \setminus C) = d$ si $K = 1$ (y $\mathrm{swt}(C^{\perp_s}) = d$ si $K = 1$). Se obtine el resultado del teorema aplicando la isometría ϕ. □

Como consecuencia directa del teorema anterior se obtiene la posterior condición de existencia de un código estabilizador.

Corolario 2.3.16. *Si existe un código aditivo clásico $[n, k]_{q^2}$ $D \leq \mathbf{F}_{q^2}$ tal que $D \leq D^{\perp_a}$ y $d^{\perp_a} = wt(D^{\perp_a})$. entonces existe un código estabilizador $[[n, n-2k, \geq d^{\perp_a}]]_q$ que es puro hasta $d^{\perp_a}$.*

Códigos clásicos

Los códigos auto ortogonales respecto a la forma traza-alternante no suelen ser estudiados en la teoría de códigos clásica; son mucho más comunes los códigos auto ortogonales con respecto a los productos escalares euclidiano o hermítico. Se relacionan estos conceptos de ortogonalidad como sigue. Sea el producto hermítico $\mathbf{x} \cdot \mathbf{y}^q$ de dos vectores $\mathbf{x}$ e $\mathbf{y}$ en $\mathbf{F}_{q^2}^n$; se escribe $\mathbf{x} \perp_h \mathbf{y}$ si y solo si $\mathbf{x} \cdot \mathbf{y}^q = 0$.

Lema 2.3.17. *Si dos vectores* $\mathbf{x}$ *e* $\mathbf{y}$ *en* $\mathbf{F}_{q^2}^n$ *satisfacen* $\mathbf{x} \perp_h \mathbf{y}$*, entonces satisfacen* $\mathbf{x} \perp_a \mathbf{y}$*. En particular, si* $D \leq \mathbf{F}_{q^2}^n$*, entonces* $D^{\perp_h} \leq D^{\perp_a}$*.*

Demostración. De $\mathbf{x} \cdot \mathbf{y}^q = 0$ se tiene que $\mathbf{x}^q \cdot \mathbf{y} = 0$, por tanto

$$\langle \mathbf{x} | \mathbf{y} \rangle_a = \mathrm{tr}_{q/p} \left(\frac{\mathbf{x} \cdot \mathbf{y}^q - \mathbf{x}^q \cdot \mathbf{y}}{\beta^{2q} - \beta^2} \right) = 0$$

como se indicaba. □

Por tanto, todo código auto ortogonal con respecto al producto hermítico es auto ortogonal respecto a la forma traza-alternante. En general, los dos espacios duales $D^{\perp_h}$ y $D^{\perp_a}$ no son el mismo. Sin embargo, si D es $\mathbf{F}_{q^2}$-lineal, entonces los dos espacios duales coinciden.

Lema 2.3.18. *Si* $D \leq \mathbf{F}_{q^2}^n$ *es* $\mathbf{F}_{q^2}$*-lineal, entonces* $D^{\perp_h} = D^{\perp_a}$*.*

Demostración. Sea $q = p^m$, p primo. Si D es un subespacio k-dimensional de $\mathbf{F}_{q^2}^n$, entonces $D^{\perp_h}$ es un subespacio $(n-k)$-dimensional de $\mathbf{F}_{q^2}^n$. También es posible ver D como un subespacio $2mk$-dimensional de $\mathbf{F}_p^{2mn}$, y $D^{\perp_a}$ como un subespacio $2m(n-k)$-dimensional de $\mathbf{F}_p^{2mn}$. Dado que $D^{\perp_h} \subseteq D^{\perp_a}$ y las cardinalidades de $D^{\perp_a}$ y $D^{\perp_h}$ son las mismas, se puede concluir que $D^{\perp_a} = D^{\perp_h}$. □

Corolario 2.3.19. *Si existe un código* $[n, k, d]_{q^2}$ $\mathbf{F}_{q^2}$*-lineal* B *tal que* $B \leq B^{\perp_h}$*, entonces existe un código cuántico* $[[n, n-2k, \geq d^{\perp_h}]]_q$ *que es puro hasta* d*.*

Demostración. El producto hermítico es no degenerado, por lo que el dual hermítico del código $D := B^{\perp_h}$ es B. El código $[n, n-k]_{q^2}$ D es $\mathbf{F}_{q^2}$-lineal, por lo que $D^{\perp_h} = D^{\perp_a}$ por el lema 2.3.18, y el enunciado sale a partir del corolario 2.3.16. □

Así que es suficiente considerar formas hermíticas en el caso de códigos $\mathbf{F}_{q^2}$-lineales. Serán necesarias las formas traza-alternantes para códigos aditivos que no sean lineales sobre $\mathbf{F}_{q^2}$.

Sin embargo el enlace más directo a la teoría de códigos clásica es la construcción de códigos CSS descritos en 1996 por Calderbank y Shor [3] y por Steane [11], de quienes heredan su nombre.

Lema 2.3.20. *Sea C_1 y C_2 dos códigos lineales clásicos con parámetros $[n, k_1, d_1]_q$ y $[n, k_2, d_2]_q$ tales que $C_2^{\perp} \leq C_1$. Entonces existe un código estabilizador $[[n, k_1 + k_2 - n, d]]_q$ con distancia mínima $d = \min\{wt(c) \mid c \in (C_1 \setminus C_2^{\perp}) \cup (C_2 \setminus C_1^{\perp})\}$ que es puro hasta $\min\{d_1, d_2\}$.*

Demostración. Sea $C = C_1^{\perp} \times C_2^{\perp} \leq \mathbf{F}_q^{2n}$. Si $(c_1 \,|\, c_2)$ y $(c_1' \,|\, c_2')$ son dos elementos de C, entonces se observa que

$$\operatorname{tr}\big(c_2 \cdot c_1' - c_2' \cdot c_1\big) = \operatorname{tr}(0 - 0) = 0$$

Por tanto, $C \leq C^{\perp_s}$. Además, el dual traza-simpléctico de C contiene $C_2 \times C_1$, y un argumento de dimensionalidad muestra que $C^{\perp_s} = C_2 \times C_1$. Dado que el producto cartesiano $C_1^{\perp} \times C_2^{\perp}$ tiene $q^{2n-(k_1+k_2)}$ elementos, el código estabilizador tiene dimensión $q^{k_1+k_2-n}$por el teorema 2.3.13. La afirmación sobre la distancia mínima y la pureza es obvia de la construcción. □

Corolario 2.3.21. *Si C es un código lineal clásico $[n, k, d]_q$ contenido en su dual, $C \leq C^{\perp_e}$, entonces existe un código estabilizador $[[n, n - 2k, \geq d^{\perp_e}]]_q$ que es puro hasta d.*

2.4. Códigos Reed-Solomon cuánticos

2.4.1. Construcción de códigos estabilizadores a partir de códigos Reed-Solomon clásicos

Dualidad euclídea

Sea un código Reed-Solomon de parámetros $[q, k, q - k + 1]$, $RS_k^q = \{ev(f) \mid f \in \mathbf{F}_q[X]$ tales que $\deg(f) < k\}$, se añade el superíndice q para distinguirlo del código del apartado siguiente, que se marcará con q^2.

Proposición 2.4.1. *Dados X^i y X^j se cumple que $ev(X^i) \cdot ev(X^j) = 0$ si y solo si $i + j \neq q - 1$.*

Demostración. Se tiene que

$$ev(X^i) = (a_1^i, \cdots, a_q^i) \text{ y } ev(X^j) = (a_1^j, \cdots, a_q^j)$$

por tanto, se obtiene

$$ev(X^i) \cdot ev(X^j) = \sum_{l=1}^{q} a_l^{i+j}.$$

Sea α un elemento primitivo del cuerpo $\mathbf{F}_q$, se tiene el grupo cíclico $\langle\alpha\rangle = \{\alpha^0, \cdots, \alpha^{q-2}\} = \{a_1, \cdots a_n\} \setminus \{0\}$, por tanto se puede reescribir la suma anterior como

$$0^{i+j} + \sum_{l=0}^{q-2} (\alpha^l)^{i+j} = \sum_{l=0}^{q-2} (\alpha^l)^{i+j}$$

Tomando $i + j = q - 1$ se tiene que

$$\sum_{l=0}^{q-2} (\alpha^l)^{q-1} = \sum_{l=0}^{q-2} (\alpha^l)^0 = q - 1 \neq 0 \text{ (en } \mathbf{F}_q)$$

Por otro lado, para $i + j = c \not\equiv 0 \mod (q-1)$ se puede afirmar

$$\sum_{l=0}^{q-2} (\alpha^l)^c = \sum_{l=0}^{q-2} (\alpha^c)^l = \frac{1 - (\alpha^c)^{q-1}}{1 - \alpha^c} = 0$$

Por tanto, $ev(X^i) \perp_e ev(X^j)$ si y solo si $i + j \neq q - 1$. □

Proposición 2.4.2. *RS_k^q está contenido en su dual euclídeo, $RS_k^{q\perp_e}$, si y solo si $k \leq \frac{q}{2}$*

Demostración. Sea $\{1, X, \cdots, X^{k-1}\}$ una base del espacio de polinomios de grado menor que k, es suficiente demostrar que sus evaluaciones son ortogonales entre ellas para comprobar que RS_k^q está incluido en su dual. Por la proposición anterior se sabe que $ev(X^i) \perp_e ev(X^j)$ si $i + j \neq q - 1$, por tanto para que todos los elementos de la base sean ortogonales entre ellos debe darse que $(k-1) + (k-1) < q - 1$ es decir $k < \frac{q+1}{2}$ dado que k y q son números naturales, se tiene $k \leq \frac{q}{2}$. □

Proposición 2.4.3. *Existe un código estabilizador $[[q, q - 2k, k + 1]]_q$ para $k \leq \frac{q}{2}$.*

Demostración. Aplicando las proposiciones 2.3.19 y 2.4.2 se obtiene el código indicado. □

Dualidad hermítica

De manera similar al apartado anterior, sea $\mathbf{F}_{q^2}$ un cuerpo finito y $a_1, \cdots, a_{q^2} \in \mathbf{F}_{q^2}$ sus elementos. Tomando la aplicación $ev : \mathbf{F}_{q^2}[X] \longrightarrow \mathbf{F}_{q^2}^{q^2}$ se obtiene el código $RS_k^{q^2} = \{ev(f) \mid f \in \mathbf{F}_{q^2}[X] \text{ tales que } \deg(f) < k\}$ de parámetros $[q^2, k, q^2 - k + 1]$.

Proposición 2.4.4. *Dados X^i y X^j se cumple que $\langle ev(X^i) | ev(X^j) \rangle_h = 0$ si y solo si $i + qj \neq q^2 - 1$.*

Demostración. Se tiene que, por la linealidad de la aplicación $ev(f)$,

$$\left\langle ev(X^i) \middle| ev(X^j) \right\rangle_q = ev(X^i) \cdot ev(X^j)^q = ev(X^i) \cdot ev(X^{qj})$$

Aplicando la proposición 2.4.5 se tiene que $ev(X^i) \perp_h ev(X^j)$ si y solo si $i + qj \neq q^2 - 1$. □

Proposición 2.4.5. *RS_k^q está contenido en su dual hermítico, $RS_k^{q\perp_h}$, si y solo si $k < q$.*

Demostración. Sea $\{1, X, \cdots, X^{k-1}\}$ una base del espacio de polinomios de grado menor que k, es suficiente demostrar que sus evaluaciones son ortogonales hermíticas entre ellas para comprobar que $RS_k^{q^2}$ está incluido en su dual. Por la proposición anterior se sabe que $ev(X^i) \perp_h ev(X^j)$ si $i + qj \neq q^2 - 1$, por tanto para que todos los elementos de la base sean h-ortogonales entre ellos debe darse que $(k-1) + q(k-1) < q^2 - 1$ es decir $k - 1 < \frac{q^2-1}{q+1}$ aplicando la propiedad de suma por diferencia en $q^2 - 1$ se obtiene $k - 1 < q - 1$ es decir $k < q$. □

Proposición 2.4.6. *Existe un código estabilizador $[[q^2, q^2 - 2k, k + 1]]_q$ para $k < q$.*

Demostración. Aplicando las proposiciones 2.3.21 y 2.4.5 se obtiene el código indicado. □

Se han encontrado dos códigos estabilizadores a partir de los códigos clásicos Reed-Solomon, se pueden encontrar demostraciones para situaciones más generales en el artículo [4].

Capítulo 3

Conclusiones

En el primer apartado hemos introducido el uso de códigos cuando se transmite información, así como las razones para utilizarlos. Por ello, hemos visto el concepto de ruido y el uso de códigos correctores para minimizar sus efectos sobre los mensajes, junto con algunas de sus clases más importantes.

Posteriormente hemos introducido los conceptos del bit cuántico y su comportamiento, así como los postulados que gobiernan la mecánica cuántica y por tanto todos los sistemas necesarios para la construcción de un computador cuántico.

Por último, introducimos los códigos estabilizadores, primero estudiando la forma que toman los errores en la computación cuántica y luego los códigos utilizados para combatirlos mirando principalmente a los códigos estabilizadores y como se relacionan con otros tipos de códigos tanto cuánticos como clásicos. Para completar el apartado hemos visto los códigos Reed-Solomon y como se pueden utilizar para definir códigos estabilizadores.

Bibliografía

[1] G. Birkhoff. *Lattice Theory*. American Mathematical Society. American Mathematical Society, 1961.

[2] R.C. Bose and D.K. Ray-Chaudhuri. On a class of error correcting binary group codes. *Information and Control*, 3(1):68–79, 1960.

[3] A. R. Calderbank and Peter W. Shor. Good quantum error-correcting codes exist. *Physical Review A*, 54(2):1098–1105, aug 1996.

[4] Carlos Galindo, Fernando Hernando, and Diego Ruano. Stabilizer quantum codes from j-affine variety codes and a new steane-like enlargement, 2015.

[5] Juan Munuera Gómez and Juan Tena Ayuso. *Codificación de la Información*. Secretariado de Publicaciones e Intercambio Científico. Universidad de Valladolid, 1997.

[6] Avanti Ketkar, Andreas Klappenecker, Santosh Kumar, and Pradeep Kiran Sarvepalli. Nonbinary stabilizer codes over finite fields. *IEEE transactions on information theory*, 52(11):4892–4914, 2006.

[7] E. Knill. Non-binary unitary error bases and quantum codes, 1996.

[8] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*. North-holland Publishing Company, 2nd edition, 1978.

[9] Michael A Nielsen and Isaac Chuang. Quantum computation and quantum information, 2002.

[10] I. S. Reed and G. Solomon. Polynomial codes over certain finite fields. *Journal of the Society for Industrial and Applied Mathematics*, 8(2):300–304, 1960.

[11] A. M. Steane. Simple quantum error-correcting codes. *Physical Review A*, 54(6):4741–4751, dec 1996.