



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

CÓDIGOS DE SUPERFICIES

T E S I S

QUE PARA OBTENER EL TÍTULO DE:
MATEMÁTICO

PRESENTA:
DIEGO DOMENZAIN GONZÁLEZ

DIRECTOR DE TESIS:
Dr. OCTAVIO PÁEZ OSUNA



2012



Universidad Nacional
Autónoma de México

Dirección General de Bibliotecas de la UNAM

Biblioteca Central



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

1. Datos del alumno:

Domenzain
González
Diego
55 68 72 59
Universidad Nacional Autónoma de México
Facultad de Ciencias
Matemáticas
302518322

2. Datos del tutor:

Dr.
Octavio
Páez
Osuna

3. Datos del Sinodal 1:

Dr.
Pablo
Barberis
Blostein

4. Datos del Sinodal 2:

Dr.
Rodolfo
San Agustín
Chi

5. Datos del Sinodal 3:

Dr.
José de Jesús
Galaviz
Casas

6. Datos del Sinodal 4:

Dr.
Carlos
Velarde
Velázquez

7. Datos del trabajo escrito:

Códigos de Superficies
50 p
2012

Índice general

Índice general	II
Índice de figuras	III
1. Informando con Partículas	1
1.1. Partículas y su hábitat	1
1.2. El paso del tiempo	4
1.3. Códigos Intrínsecos	6
2. Espacio de Ciclos	10
2.1. Vías en Superficies	10
2.2. Cazando Ciclos	12
2.3. Ahorcando hoyos	13
2.4. Ciclos Duales	16
2.5. Espacios de ciclos	18
3. Incrustando Gráficas	21
3.1. Requisitos	21
3.2. Semillas	21
3.3. Diseño de semillas	27
3.3.1. Paso 1 :: \mathbf{Q} , Θ y \mathbf{G}	27
3.3.2. Paso 2 :: el Dual	30
3.3.3. Paso 3 :: Dimensiones Arbitrarias	32
4. Un Ejemplo	36
4.1. Introducción al Ejemplo	36
4.2. Paso 1 :: Semilla y Levantamiento	36
4.3. Paso 2 :: Ciclos de $\Theta^a \rightarrow \mathbb{T}_{23}$	38
4.3.1. Independencia Lineal en \mathbb{Z}_2^n	43
4.3.2. Independencia lineal en W_2^\perp/W_1	44
4.4. Paso 3 :: el código \mathcal{C}	46

Índice de figuras

2.1.	Oceanos, vías y planetas	10
2.2.	ciclos	11
2.3.	camino frontera de f	12
2.4.	nombrar a los vértices	13
2.5.	15
2.6.	La superficie \mathbb{T}_g vista como un polígono de $2g$ lados denotados por $a_i^{\pm 1}, b_i^{\pm 1}$ y una gráfica $\Xi \rightarrow \mathbb{T}_g$ indicada por las aristas de colores.	16
3.1.	Ejemplo de una gráfica de voltaje Θ y su levantamiento Θ^a	22
3.2.	regiones vecinas en Θ corresponden a regiones vecinas en Θ^a	23
3.3.	24
3.4.	Pegando regiones	25
3.5.	Diagrama de $\Theta^a \rightarrow \mathbf{Q}^a$	26
3.6.	ciclo de longitud 4 en Θ^a para un grupo G abeliano	27
3.7.	posibles e imposibles ciclos \hat{c} de longitud 3 con voltaje neto $v(\hat{c})$ en $\Theta^a \rightarrow \mathbb{T}_g$, donde $1 \leq i, j, k \leq 4$ y $i \neq j \neq k \neq i$	29
3.8.	posibles e imposibles ciclos \hat{c} de longitud 2 con voltaje neto $v(\hat{c})$ en $\Theta^a \rightarrow \mathbb{T}_g$, donde $1 \leq i, j \leq 4$ y $i \neq j$	30
3.9.	regiones y estrellas de $\Theta^a \rightarrow \mathbb{T}_g$ y su dual $[\Theta^a]^* \rightarrow \mathbb{T}_g$	31
3.10.	La gráfica $\Phi \rightarrow \mathbb{T}_2$ y su levantamiento $\Phi^b \rightarrow \mathbb{T}_g$	32
3.11.	$\Psi \rightarrow \mathbb{T}_h$	33
3.12.	deducción de $[\Psi^a]^* \rightarrow \mathbb{T}_H$ a partir de $\Psi^a \rightarrow \mathbb{T}_H$	34
3.13.	$\Phi \rightarrow \mathbb{T}_h$	34
4.1.	$\Theta \rightarrow \mathbb{T}_2$	37
4.2.	Pegado en banda	37
4.3.	$\Theta^a \rightarrow \mathbb{T}_{23}$	38
4.4.	Primer bloque de aristas enumeradas	39
4.5.	Segundo bloque de aristas enumeradas	40
4.6.	Tercer bloque de aristas enumeradas	41
4.7.	once ciclos con aristas verdes, amarillas y azules	42
4.8.	once ciclos con aristas amarillas, verdes y azules	42
4.9.	Ciclo con aristas azules y rojas	43

Capítulo 1

Informando con Partículas

1.1. Partículas y su hábitat

Entender el espacio donde vivimos es una actividad que intriga la curiosidad del ser Humano desde que su mente despierta del sueño original. Aunque algunos relajan el impulso de la intriga a lo largo de su vida, otros piensan, discuten y registran su esfuerzo para saciar su curiosidad. De todos los caminos que se han tomado por entender nuestro espacio vital, la Mecánica Cuántica es un esfuerzo por entender cómo funciona la materia que hay en nuestro espacio. El marco de referencia con el que se explica este particular camino, está basado en una estructura matemática derivada de ideas y observaciones que toda una comunidad de curiosos ha ido desarrollando desde principios del siglo XX, y cuyo punto de partida se enuncia en tres postulados.

Antes de enunciarlos aclaramos que para los fines de la computación cuántica basta trabajar con un subconjunto finito de la estructura infinita que describen originalmente los postulados de la mecánica cuántica. Con esto en mente definimos por \mathcal{H} a un espacio de Hilbert de dimensión finita n sobre los complejos, cuyo producto interno será definido más abajo. Los elementos de este espacio los vamos a denotar por $|\psi\rangle = (\psi_1, \dots, \psi_n)$ donde $\psi_i \in \mathbb{C}$.

Es necesario tomar en cuenta que esta notación para los elementos de \mathcal{H} otorga la libertad de escribir en $|\cdot\rangle$ el símbolo que uno desee porque sólo va a funcionar como una etiqueta que representa un elemento de \mathcal{H} .

Para ver un ejemplo pensemos en $\mathcal{H} = \mathbb{C}^2$. Sabemos que una base para \mathbb{C}^2 es

$$\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$$

si denotamos a los elementos de esta base como

$$|\circ\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |\bullet\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

entonces un elemento típico $|\psi\rangle \in \mathcal{H}$ es una combinación lineal de los elementos de su base:

$$|\psi\rangle = a|\circ\rangle + b|\bullet\rangle \quad a, b \in \mathbb{C}$$

Definimos un elemento en el espacio dual de \mathcal{H} por $\langle\varphi|$ donde $\langle\varphi|: \mathcal{H} \rightarrow \mathbb{C}$ es una función lineal, y denotamos $\langle\varphi|\psi\rangle := \langle\varphi|(|\psi\rangle)$.

Debido a que $\langle\varphi|$ es una función lineal, podemos pensar que $\langle\varphi|$ representa un vector

$$\langle\varphi| = (\varphi_1, \dots, \varphi_n) \quad \varphi_i \in \mathbb{C}$$

y de esta manera escribir

$$\langle\varphi|\psi\rangle = \sum_i \varphi_i \psi_i$$

Para definir el producto interno de \mathcal{H} , primero definimos un elemento $\langle\psi|$ a partir de $|\psi\rangle = (\psi_1, \dots, \psi_n)^t$ como $\langle\psi| = (\psi_1^*, \dots, \psi_n^*)$ donde el símbolo $*$ denota el conjugado complejo. Así el producto interno de $|\varphi\rangle, |\psi\rangle \in \mathcal{H}$ lo definimos como

$$\langle\varphi|\psi\rangle = \sum_i \varphi_i^* \psi_i$$

El siguiente paso será describir los operadores lineales que actúan sobre el espacio \mathcal{H} . Podemos pensar que un operador lineal $\mathbf{L}: \mathcal{H} \rightarrow \mathcal{H}$ está expresado por una matriz con entradas

$$\mathbf{L}_{ij} = \langle e_i | \mathbf{L} | e_j \rangle$$

donde $\{|e_k\rangle\}_k$ es una base ortonormal de \mathcal{H} .

Una matriz \mathbf{H} se dice que es **hermitiana** si $\mathbf{H}^\dagger = \mathbf{H}$ donde el símbolo \dagger significa transponer y conyugar. Notemos que los valores propios de \mathbf{H} son reales y que sus vectores propios forman una base ortonormal de \mathcal{H} .

Una matriz \mathbf{U} es **unitaria** si $\mathbf{U}^\dagger \mathbf{U} = \mathbf{I}_n$ donde \mathbf{I}_n es la matriz identidad. Observemos que una matriz unitaria cumple que $\det \mathbf{U} \cdot \det \mathbf{U}^\dagger = \det \mathbf{U} \cdot [\det \mathbf{U}]^* = |\det \mathbf{U}|^2 = 1$, lo cual motiva su nombre.

Decimos que un **operador** es hermitiano (unitario), si su matriz asociada bajo una base ortonormal es hermitiana (unitaria).

Con esta notación expresamos de la siguiente manera las características de una partícula, enunciando los tres postulados de la mecánica cuántica:

- Un **estado puro** es un vector normalizado $|\psi\rangle$ en un espacio de Hilbert \mathcal{H} . Si $\{|\psi_i\rangle\}_i$ es un conjunto de estados linealmente independientes en \mathcal{H} , entonces cualquier combinación lineal de ellos que esté en la esfera unitaria de \mathcal{H} , también es un estado del sistema, es decir

$$|\psi\rangle = \sum_i a_i |\psi_i\rangle \quad \sum_i |a_i|^2 = 1$$

es un estado general del sistema.

- Para cualquier observable m , existe un operador hermitiano \mathbf{M} que actúa sobre \mathcal{H} . Al medir m el estado $|\psi\rangle$ se proyecta bajo un operador \mathbf{P}_i en un vector propio del operador \mathbf{M} con una probabilidad $\langle \psi | \mathbf{P}_i | \psi \rangle$ e inmediatamente después de haberlo medido, el estado del sistema queda como

$$|\psi\rangle \xrightarrow{\text{medir}} \frac{\mathbf{P}_i |\psi\rangle}{\sqrt{\langle \psi | \mathbf{P}_i | \psi \rangle}}$$

- La evolución con respecto al tiempo, está regida por un operador unitario $\mathbf{U}(t)$ tal que si $|\psi(0)\rangle$ es el estado inicial del sistema, entonces al tiempo t el estado $|\psi(t)\rangle$ está definido por

$$|\psi(t)\rangle = \mathbf{U}(t) |\psi(0)\rangle$$

La restricción de que un estado $|\psi\rangle$ esté en la esfera unitaria de \mathcal{H} , se debe a que las normas de los coeficientes $a_i \in \mathbb{C}$ expresan la probabilidad de que una partícula esté en cada uno de los estados $|\psi_i\rangle$.

Como veremos más adelante, a diferencia de la probabilidad clásica, en este caso **no** quiere decir que un estado esté en alguno de todos los estados $|\psi_i\rangle$, y que como no sabemos en qué estado se encuentra la partícula, la expresemos como una combinación lineal de todos ellos. Lo que **sí** quiere decir es que la partícula se encuentra en todos los estados $|\psi_i\rangle$ al mismo tiempo, y que al medirla mediante una proyección \mathbf{P}_i asociada a un operador hermitiano \mathbf{M} , el estado de la partícula se colapsa.

La razón por la cual se restringen las mediciones observables a operadores hermitianos, es que las propiedades que le atribuimos a la partícula son cantidades reales, por lo que no tiene sentido que al observar una de estas características nos resulte una cantidad compleja.

Un estado general de una partícula con dos estados posibles expresado como una combinación lineal de estados puros será la **unidad de información** con la que va a funcionar la computadora cuántica, la cual vamos a llamar **qubit**.

Hasta ahora sólo hemos caracterizado cómo funciona un solo sistema descrito por dos estados, el cual lo pensamos como el sistema de una sola partícula con dos estados, por lo que sólo hemos caracterizado una unidad de información. Para tener más de una unidad de información, vamos a necesitar más de una partícula, y por lo tanto, describir el espacio donde n partículas quedan caracterizadas, cuyos estados llamaremos **n-qubits**.

Supongamos que tenemos n partículas cada una caracterizada en un espacio \mathcal{H}_i con $i = 1, \dots, n$, entonces definimos el espacio \mathcal{H} que las caracteriza a todas juntas como

$$\mathcal{H} = \mathcal{H}_1 \otimes \dots \otimes \mathcal{H}_n$$

donde una base para \mathcal{H} es

$$\{|e_{1,j}\rangle \otimes \dots \otimes |e_{n,j}\rangle\}_j \quad \text{donde cada } \{|e_{i,j}\rangle\}_j \text{ es una base para } \mathcal{H}_i$$

Para referirnos a un elemento $|\psi\rangle = |\psi_1\rangle \otimes \dots \otimes |\psi_n\rangle \in \mathcal{H}$ donde $|\psi_i\rangle \in \mathcal{H}_i$, definimos la notación

$$|\psi\rangle := |\psi_1\psi_2\dots\psi_n\rangle$$

Como ejemplo consideremos dos partículas, cada una caracterizada por los espacios $\mathcal{H}_1, \mathcal{H}_2$ con $\mathcal{H}_i = \mathbb{C}^2$. Entonces una base para $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ es $\{|\circ\circ\rangle, |\circ\bullet\rangle, |\bullet\circ\rangle, |\bullet\bullet\rangle\}$ y un estado general es

$$|\psi\rangle = a_{\circ\circ}|\circ\circ\rangle + a_{\circ\bullet}|\circ\bullet\rangle + a_{\bullet\circ}|\bullet\circ\rangle + a_{\bullet\bullet}|\bullet\bullet\rangle \quad \text{con} \quad |a_{\circ\circ}|^2 + |a_{\circ\bullet}|^2 + |a_{\bullet\circ}|^2 + |a_{\bullet\bullet}|^2 = 1$$

Además de utilizar los frutos físicos cosechados por la curiosidad científica para poder manipular información con ellos, la construcción de una computadora cuántica asoma una manera para empujar los horizontes cognitivos de la comunidad Humana. El empuje consiste en ofrecer una eficiencia mucho mayor a la actual para resolver problemas, la cual se logra con la capacidad de procesar mucha mayor información en menor tiempo. El procesamiento de esta información extra se lleva a cabo con estados de partículas que esconden este excedente a través de una correlación muy especial entre ellas, y la repetida creación de este tipo de estados.

Aunque este tipo de estados es posible con más de dos partículas, el ejemplo más pequeño posible es con sólo dos, por ejemplo el estado

$$|\varphi\rangle = \frac{|\circ\circ\rangle + |\bullet\bullet\rangle}{\sqrt{2}}$$

Suponemos que una persona llamada Jesús es capaz de generar dos partículas en este estado cada unidad de tiempo. Analicemos esta correlación pensando que por cada unidad de tiempo Jesús le da una partícula a Alicia y la otra a Bob. Tanto Alicia como Bob tienen la capacidad de saber dos propiedades distintas de sus partículas, llamemos m_1, m_2 a las de Alicia y m_3, m_4 a las de Bob. Suponemos que estas propiedades se miden por medio de los procesos $\mathbf{M}_1, \mathbf{M}_2, \mathbf{M}_3$ y \mathbf{M}_4 respectivamente, cuyos resultados sólo pueden ser 1 ó -1.

También pensamos que tanto Alicia como Bob sólo pueden hacer una medición por unidad de tiempo y que cuando la hacen, la hacen al mismo tiempo.

Ahora vamos a pensar de manera clásica y vamos a tomar dos consecuencias de haber pensado así:

1. Las propiedades m_1, m_2, m_3 y m_4 tienen valores definidos, independientemente si se observan o no.
2. Los resultados de los procesos de medición $\mathbf{M}_1, \mathbf{M}_2, \mathbf{M}_3$ y \mathbf{M}_4 son independientes de quién los hace.

Bajo estas dos maneras de interpretar las propiedades de las partículas, podemos decir que por (1) la probabilidad de que los valores de las propiedades m_i antes de medir sean $m_1 = \dot{\mathbf{1}}, m_2 = \dot{\mathbf{2}}, m_3 = \dot{\mathbf{3}}$ y $m_4 = \dot{\mathbf{4}}$, es $p(\dot{\mathbf{1}}, \dot{\mathbf{2}}, \dot{\mathbf{3}}, \dot{\mathbf{4}})$.

Por (2) podemos decir que después de que Jesús les haya dado muchos estados $|\varphi\rangle$, el valor medio E de que el evento $\mathbf{M}_1\mathbf{M}_3 + \mathbf{M}_2\mathbf{M}_3 + \mathbf{M}_2\mathbf{M}_4 - \mathbf{M}_1\mathbf{M}_4$ ocurra es

$$\begin{aligned} E(\mathbf{M}_1\mathbf{M}_3 + \mathbf{M}_2\mathbf{M}_3 + \mathbf{M}_2\mathbf{M}_4 - \mathbf{M}_1\mathbf{M}_4) &= \sum_{\mathbf{i} \cdot \dot{\mathbf{2}} \cdot \dot{\mathbf{3}} \cdot \dot{\mathbf{4}}} p(\dot{\mathbf{1}}, \dot{\mathbf{2}}, \dot{\mathbf{3}}, \dot{\mathbf{4}}) (\dot{\mathbf{1}} \cdot \dot{\mathbf{3}} + \dot{\mathbf{2}} \cdot \dot{\mathbf{3}} + \dot{\mathbf{2}} \cdot \dot{\mathbf{4}} - \dot{\mathbf{1}} \cdot \dot{\mathbf{4}}) \\ &= \sum_{\mathbf{i} \cdot \dot{\mathbf{2}} \cdot \dot{\mathbf{3}} \cdot \dot{\mathbf{4}}} p(\dot{\mathbf{1}}, \dot{\mathbf{2}}, \dot{\mathbf{3}}, \dot{\mathbf{4}}) \left(\underbrace{(\dot{\mathbf{1}} + \dot{\mathbf{2}}) \cdot \dot{\mathbf{3}} + (\dot{\mathbf{2}} - \dot{\mathbf{1}}) \cdot \dot{\mathbf{4}}}_{\pm 2} \right) \\ &\leq \sum_{\mathbf{i} \cdot \dot{\mathbf{2}} \cdot \dot{\mathbf{3}} \cdot \dot{\mathbf{4}}} p(\dot{\mathbf{1}}, \dot{\mathbf{2}}, \dot{\mathbf{3}}, \dot{\mathbf{4}}) \cdot 2 \\ &= 2 \end{aligned}$$

también sucede que si expandemos la primera igualdad resulta

$$E(\mathbf{M}_1\mathbf{M}_3 + \mathbf{M}_2\mathbf{M}_3 + \mathbf{M}_2\mathbf{M}_4 - \mathbf{M}_1\mathbf{M}_4) = E(\mathbf{M}_1\mathbf{M}_3) + E(\mathbf{M}_2\mathbf{M}_3) + E(\mathbf{M}_2\mathbf{M}_4) - E(\mathbf{M}_1\mathbf{M}_4) \leq 2 \quad (1.1)$$

ya que

$$\sum_{\mathbf{i} \cdot \mathbf{z} \cdot \mathbf{z} \cdot \mathbf{4}} p(\mathbf{i}, \mathbf{z}, \mathbf{z}, \mathbf{4})(\mathbf{i} \cdot \mathbf{j}) = E(\mathbf{M}_i\mathbf{M}_j)$$

Notemos que el evento que escogimos fue plenamente arbitrario.

Ahora vamos a interpretar el mismo evento usando los postulados de la mecánica cuántica, empezando por fijar lo que vamos a medir

$$\begin{aligned} \mathbf{M}_1|\circ\rangle &= |\circ\rangle & \mathbf{M}_2|\circ\rangle &= |\bullet\rangle & \mathbf{M}_3|\circ\rangle &= \frac{|\circ\rangle+|\bullet\rangle}{\sqrt{2}} & \mathbf{M}_4|\circ\rangle &= \frac{-|\circ\rangle-|\bullet\rangle}{\sqrt{2}} \\ \mathbf{M}_1|\bullet\rangle &= -|\bullet\rangle & \mathbf{M}_2|\bullet\rangle &= |\circ\rangle & \mathbf{M}_3|\bullet\rangle &= \frac{|\circ\rangle-|\bullet\rangle}{\sqrt{2}} & \mathbf{M}_4|\bullet\rangle &= \frac{|\bullet\rangle-|\circ\rangle}{\sqrt{2}} \end{aligned}$$

continuando por calcular el valor medio de los eventos donde Alicia mide \mathbf{M}_i y Bob mide \mathbf{M}_j , es decir el valor medio de los operadores $\mathbf{M}_i\mathbf{M}_j$ con respecto al estado $|\varphi\rangle$, el cual lo definimos como $\langle\varphi|\mathbf{M}_i\mathbf{M}_j|\varphi\rangle$ [1]. Así tenemos que

$$\begin{aligned} \mathbf{M}_1\mathbf{M}_3|\varphi\rangle &= \frac{|\circ\rangle}{\sqrt{2}} \otimes \left(\frac{|\circ\rangle+|\bullet\rangle}{\sqrt{2}} \right) - \frac{|\bullet\rangle}{\sqrt{2}} \otimes \left(\frac{|\circ\rangle-|\bullet\rangle}{\sqrt{2}} \right) & \mathbf{M}_2\mathbf{M}_3|\varphi\rangle &= \frac{|\bullet\rangle}{\sqrt{2}} \otimes \left(\frac{|\circ\rangle+|\bullet\rangle}{\sqrt{2}} \right) + \frac{|\circ\rangle}{\sqrt{2}} \otimes \left(\frac{|\circ\rangle-|\bullet\rangle}{\sqrt{2}} \right) \\ \mathbf{M}_2\mathbf{M}_4|\varphi\rangle &= \frac{|\bullet\rangle}{\sqrt{2}} \otimes \left(\frac{-|\circ\rangle-|\bullet\rangle}{\sqrt{2}} \right) + \frac{|\circ\rangle}{\sqrt{2}} \otimes \left(\frac{|\bullet\rangle-|\circ\rangle}{\sqrt{2}} \right) & \mathbf{M}_1\mathbf{M}_4|\varphi\rangle &= \frac{|\circ\rangle}{\sqrt{2}} \otimes \left(\frac{-|\circ\rangle-|\bullet\rangle}{\sqrt{2}} \right) - \frac{|\bullet\rangle}{\sqrt{2}} \otimes \left(\frac{|\bullet\rangle-|\circ\rangle}{\sqrt{2}} \right) \end{aligned}$$

por lo que el valor medio de cada evento es

$$\langle\varphi|\mathbf{M}_1\mathbf{M}_3|\varphi\rangle = \langle\varphi|\mathbf{M}_2\mathbf{M}_3|\varphi\rangle = \langle\varphi|\mathbf{M}_2\mathbf{M}_4|\varphi\rangle = -\langle\varphi|\mathbf{M}_1\mathbf{M}_4|\varphi\rangle = \frac{1}{\sqrt{2}}$$

de donde si interpretamos estos valores medios de manera clásica y sumamos como en 1.1 obtenemos

$$\langle\varphi|\mathbf{M}_1\mathbf{M}_3|\varphi\rangle + \langle\varphi|\mathbf{M}_2\mathbf{M}_3|\varphi\rangle + \langle\varphi|\mathbf{M}_2\mathbf{M}_4|\varphi\rangle - \langle\varphi|\mathbf{M}_1\mathbf{M}_4|\varphi\rangle = 2\sqrt{2}$$

aunque $2 < 2\sqrt{2}$, de donde hemos llegado a una contradicción por haber interpretado las características de la materia descritas por la mecánica cuántica de una manera clásica.

Rescatemos y nombremos dos estados que nos permitieron observar esta correlación y que serán útiles en lo que sigue

$$|+\rangle = \frac{|\circ\rangle + |\bullet\rangle}{\sqrt{2}} \quad |-\rangle = \frac{|\circ\rangle - |\bullet\rangle}{\sqrt{2}}$$

Nombramos al conjunto de estos dos estados como la **base de Bell**, mientras que al conjunto $\{|\circ\rangle, |\bullet\rangle\}$ lo llamamos **base computacional**.

1.2. El paso del tiempo

Utilizar partículas cuánticas como vehículos físicos cuyos pasajeros sean unidades de información, consiste en transformar los estados de las partículas con el paso del tiempo. Para poder realizar estas transformaciones, es necesario tomar en cuenta que el paso del tiempo transforma los estados de las partículas no sólo como nosotros las manipulemos para realizar operaciones, sino también bajo la correspondencia de un operador unitario \mathbf{U} y la interacción del sistema con su ambiente. Este hecho presenta dos dificultades para construir una computadora cuántica

1. ¿Cómo manipular estados de un sistema que interactúa con el ambiente?
2. ¿Cómo manipular estados de un sistema, si los estados interactúan entre ellos mientras los estamos manipulando?

La solución que plantean los **Códigos de Superficies** consiste en construir un sistema de partículas en el que sea posible despreocuparse de la interacción que tiene el sistema con el ambiente y en el que sepamos cómo evoluciona el sistema a través del paso del tiempo. Es decir, la primera pregunta la respondemos asumiendo que sabemos quién es \mathbf{U} y que

la interacción con el ambiente la podemos pensar como perturbaciones despreciables a este operador, mientras que la segunda pregunta la respondemos proponiendo un subconjunto de estados que resulten invariantes bajo el paso del tiempo, los cuales podamos manipular sin preocuparnos cómo cambian bajo \mathbf{U} .

En esta sección vamos a deducir una expresión para \mathbf{U} que nos permita construir un conjunto de estados invariantes para un sistema cualquiera, dejando para el final del próximo capítulo la tarea de construir un sistema de partículas especial que nos permita dar una expresión específica para \mathbf{U} .

Empecemos por fijar el espacio \mathcal{H} donde viven los estados de las partículas por $\mathcal{H} = \mathbb{C}^2$, y adoptar la base computacional para representar las matrices asociadas a los operadores lineales que actúan sobre \mathcal{H} .

Fijémonos en las matrices hermitianas:

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \sigma_y = \sigma_x \sigma_z = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

las cuales corresponden a los operadores lineales

$$\mathbf{I}|\psi\rangle = |\psi\rangle \quad \mathbf{X}|\psi\rangle = a|\bullet\rangle + b|\circ\rangle \quad \mathbf{Z}|\psi\rangle = a|\circ\rangle - b|\bullet\rangle \quad \mathbf{Y}|\psi\rangle = a|\bullet\rangle - b|\circ\rangle$$

donde $|\psi\rangle = a|\circ\rangle + b|\bullet\rangle$. Si pensamos que $|a|^2 + |b|^2 = 1$, decimos que el efecto que tienen los operadores \mathbf{X} , \mathbf{Z} y \mathbf{Y} sobre el estado $|\psi\rangle$, es un cambio *flip*, un cambio de *fase* y un cambio de *fase* y *flip* respectivamente.

Observemos también que estas matrices forman una base para todas las matrices $\mathbb{C}^2 \rightarrow \mathbb{C}^2$, ya que

$$\mathbf{E}_1 = \frac{1}{2}(\sigma_0 + \sigma_z) \quad \mathbf{E}_2 = \frac{1}{2}(\sigma_x - \sigma_y) \quad \mathbf{E}_3 = \frac{1}{2}(\sigma_x + \sigma_y) \quad \mathbf{E}_4 = \frac{1}{2}(\sigma_0 - \sigma_z)$$

de donde deducimos que el conjunto $\{\mathbf{I}, \mathbf{X}, \mathbf{Z}, \mathbf{Y}\}$ es una base para los operadores lineales de \mathcal{H} .

Para caracterizar a los operadores lineales en un sistema con n partículas, consideremos

$$\mathcal{H}^{\otimes n} = \underbrace{\mathcal{H} \otimes \dots \otimes \mathcal{H}}_n \quad \text{y el conjunto} \quad P_n = \{\mathbf{I}, \mathbf{X}, \mathbf{Z}, \mathbf{Y}\}^{\otimes n}$$

Una manera agradable para trabajar con los elementos $\mathbf{M}_i \in P_n$, es hacer uso de la relación $\mathbf{XZ} = \mathbf{Y}$, e indicar en qué qubit están actuando los operadores \mathbf{X} y \mathbf{Z} dentro de \mathbf{M}_i . Para expresar esta idea definimos el vector $(\mathbf{v}|\mathbf{u}) \in \mathbb{Z}_2^{2n}$ y escribimos

$$\mathbf{M}_{(\mathbf{v}|\mathbf{u})} = \mathbf{X}_{\mathbf{v}} \mathbf{Z}_{\mathbf{u}} \quad \mathbf{X}_{\mathbf{v}} = \bigotimes_{\mathbf{v}} X^{\mathbf{v}_j} \quad ; \quad \mathbf{Z}_{\mathbf{u}} = \bigotimes_{\mathbf{u}} Z^{\mathbf{u}_j}$$

Esta expresión facilita ver cuántos elementos hay en P_n si nos fijamos en cuántas etiquetas $(\mathbf{v}|\mathbf{u})$ puede haber, concluyendo que P_n consta de 2^{2n} elementos. Veamos también que

$$\mathbf{M}_{(\mathbf{v}|\mathbf{u})}^\dagger = \mathbf{Z}_{\mathbf{u}}^\dagger \mathbf{X}_{\mathbf{v}}^\dagger = \mathbf{Z}_{\mathbf{u}} \mathbf{X}_{\mathbf{v}} \quad \mathbf{M}_{(\mathbf{v}|\mathbf{u})} \mathbf{M}_{(\mathbf{v}|\mathbf{u})}^\dagger = \mathbf{X}_{\mathbf{v}} \mathbf{Z}_{\mathbf{u}} \mathbf{Z}_{\mathbf{u}} \mathbf{X}_{\mathbf{v}} = \mathbf{I}^{\otimes n}$$

de donde la última igualdad se da porque $\sigma_x^2 = \sigma_z^2 = \sigma_y^2 = \sigma_0$, lo cual indica que todos los elementos de P_n son unitarios.

Observando que $\{\mathbf{I}, \mathbf{X}, \mathbf{Z}, \mathbf{Y}\}$ es una base para los operadores lineales de \mathcal{H} deducimos que P_n es una base para los operadores lineales de $\mathcal{H}^{\otimes n}$.

Esto nos permite expresar la evolución del sistema descrita por \mathbf{U} como una combinación lineal de elementos en P_n de la siguiente manera

$$|\psi\rangle \rightarrow \mathbf{U}|\psi\rangle = \sum_i^{2^{2n}} \mathbf{M}_i |\psi\rangle$$

donde la interacción con el ambiente quede expresada como perturbaciones al operador \mathbf{U} .

Recordando el objetivo de construir un sistema de partículas en el que sepamos cómo lo afecta el paso del tiempo, podríamos pensar que los estados que resulten invariantes en este sistema, quedan protegidos intrínsecamente bajo la naturaleza del sistema. En el siguiente capítulo vamos a motivar la construcción de dicho sistema a partir de las condiciones que los operadores \mathbf{M}_i deben de cumplir para poder construir un conjunto de estados invariantes.

1.3. Códigos Intrínsecos

Explicuemos primero qué significa que un estado sea invariante. Supongamos que un operador unitario \mathbf{M}_i es tal que $\mathbf{M}_i|\psi_j\rangle = |\psi_j\rangle$ para cierta colección de estados $\{|\psi_j\rangle\} \subset \mathcal{H}^{\otimes n}$. Debido a que \mathbf{M}_i no tiene ningún efecto sobre cada $|\psi_j\rangle$, la idea es coleccionar muchos operadores $\mathbf{M}_i \in P_n$ que cumplan la condición mencionada y con ellos definir un subconjunto $\mathcal{C} \subset \mathcal{H}^{\otimes n}$ que no sea afectado por todos los operadores coleccionados. El conjunto \mathcal{C} es el código que pretendemos construir, ya que va a funcionar como un subespacio privilegiado de $\mathcal{H}^{\otimes n}$ en donde ciertos estados de las partículas quedarán protegidos.

Para construir nuestra colección de operadores \mathbf{M}_i nos vamos a guiar por la caracterización $\mathbf{M}_{(\mathbf{v}|\mathbf{u})} = \mathbf{X}_{\mathbf{v}}\mathbf{Z}_{\mathbf{u}}$ de los elementos en P_n y la propiedad $\mathbf{XZ} = -\mathbf{ZX}$ para fijarnos qué condiciones caracterizan su conmutatividad, las cuales nos van a ayudar para elegir a los operadores que necesitamos.

Veamos primero que dos operadores $\mathbf{X}_{\mathbf{v}}, \mathbf{Z}_{\mathbf{u}}$ cumplen la propiedad $\mathbf{X}_{\mathbf{v}}\mathbf{Z}_{\mathbf{u}} = (-1)^{(\mathbf{v}\cdot\mathbf{u})}\mathbf{Z}_{\mathbf{u}}\mathbf{X}_{\mathbf{v}}$ debido que al conmutar, cada entrada del vector \mathbf{u} donde coincide con \mathbf{v} se tiene $\mathbf{XZ} = -\mathbf{ZX}$. Para conmutar el producto $\mathbf{X}_{\mathbf{v}}\mathbf{X}_{\mathbf{b}}$ ($\mathbf{Z}_{\mathbf{u}}\mathbf{Z}_{\mathbf{w}}$), no es necesario multiplicar por un factor de -1 puesto que en todas las entradas donde coinciden se tiene $\mathbf{XX} = \mathbf{I}$ ($\mathbf{ZZ} = \mathbf{I}$).

Supongamos que tenemos dos operadores $\mathbf{M}_{(\mathbf{v}|\mathbf{u})}, \mathbf{M}_{(\mathbf{b}|\mathbf{w})}$ de P_n . Entonces se cumple

$$\begin{aligned} \mathbf{M}_{(\mathbf{v}|\mathbf{u})}\mathbf{M}_{(\mathbf{b}|\mathbf{w})} &= (\mathbf{X}_{\mathbf{v}}\mathbf{Z}_{\mathbf{u}})(\mathbf{X}_{\mathbf{b}}\mathbf{Z}_{\mathbf{w}}) = (-1)^{(\mathbf{u}\cdot\mathbf{b})}\mathbf{X}_{\mathbf{v}}(\mathbf{X}_{\mathbf{b}}\mathbf{Z}_{\mathbf{u}})\mathbf{Z}_{\mathbf{w}} \\ &= (-1)^{(\mathbf{u}\cdot\mathbf{b})}\mathbf{X}_{\mathbf{b}}\mathbf{X}_{\mathbf{v}}\mathbf{Z}_{\mathbf{w}}\mathbf{Z}_{\mathbf{u}} \\ &= (-1)^{(\mathbf{u}\cdot\mathbf{b}+\mathbf{v}\cdot\mathbf{w})}\mathbf{X}_{\mathbf{b}}(\mathbf{Z}_{\mathbf{w}}\mathbf{X}_{\mathbf{v}})\mathbf{Z}_{\mathbf{u}} = (-1)^{(\mathbf{u}\cdot\mathbf{b}+\mathbf{v}\cdot\mathbf{w})}\mathbf{M}_{(\mathbf{b}|\mathbf{w})}\mathbf{M}_{(\mathbf{v}|\mathbf{u})} \end{aligned}$$

es decir, los dos operadores conmutan si y sólo si $(-1)^{(\mathbf{u}\cdot\mathbf{b}+\mathbf{v}\cdot\mathbf{w})} = 1$. Ahora vamos a ver bajo qué restricciones existen vectores $|\psi_i\rangle$ tales que los operadores $\mathbf{M}_{(\mathbf{v}|\mathbf{u})}, \mathbf{M}_{(\mathbf{b}|\mathbf{w})}$ los ignoren. Primero observemos que

$$\begin{aligned} \mathbf{M}_{(\mathbf{v}+\mathbf{b}|\mathbf{u}+\mathbf{w})} &= \mathbf{X}_{(\mathbf{v}+\mathbf{b})}\mathbf{Z}_{(\mathbf{u}+\mathbf{w})} \\ &= \mathbf{X}_{\mathbf{v}}\mathbf{X}_{\mathbf{b}}\mathbf{Z}_{\mathbf{u}}\mathbf{Z}_{\mathbf{w}} \\ &= (-1)^{(\mathbf{u}\cdot\mathbf{b})}\mathbf{X}_{\mathbf{v}}\mathbf{Z}_{\mathbf{u}}\mathbf{X}_{\mathbf{b}}\mathbf{Z}_{\mathbf{w}} = (-1)^{(\mathbf{u}\cdot\mathbf{b})}\mathbf{M}_{(\mathbf{v}|\mathbf{u})}\mathbf{M}_{(\mathbf{b}|\mathbf{w})} \end{aligned}$$

aunque también se tiene que $(\mathbf{v} + \mathbf{b}|\mathbf{u} + \mathbf{w}) = (\mathbf{b} + \mathbf{v}|\mathbf{w} + \mathbf{u})$, por lo que

$$(-1)^{(\mathbf{u}\cdot\mathbf{b})}\mathbf{M}_{(\mathbf{v}|\mathbf{u})}\mathbf{M}_{(\mathbf{b}|\mathbf{w})} = \mathbf{M}_{(\mathbf{v}+\mathbf{b}|\mathbf{u}+\mathbf{w})} = \mathbf{M}_{(\mathbf{b}+\mathbf{v}|\mathbf{w}+\mathbf{u})} = (-1)^{(\mathbf{v}\cdot\mathbf{w})}\mathbf{M}_{(\mathbf{b}|\mathbf{w})}\mathbf{M}_{(\mathbf{v}|\mathbf{u})}$$

Si existiera un vector $|\psi_i\rangle$ que ambos operadores dejen fijo y lo evaluamos en la igualdad anterior tenemos

$$(-1)^{(\mathbf{u}\cdot\mathbf{b})}|\psi_i\rangle = \mathbf{M}_{(\mathbf{v}+\mathbf{b}|\mathbf{u}+\mathbf{w})}|\psi_i\rangle = (-1)^{(\mathbf{v}\cdot\mathbf{w})}|\psi_i\rangle \quad (1.2)$$

lo cual sucede si

$$|\psi_i\rangle = (-1)^{(\mathbf{v}\cdot\mathbf{w}-\mathbf{u}\cdot\mathbf{b})}|\psi_i\rangle$$

es decir, para que $\mathbf{M}_{(\mathbf{v}|\mathbf{u})}$ y $\mathbf{M}_{(\mathbf{b}|\mathbf{w})}$ compartan los mismos vectores propios, es necesario que conmuten.

La ecuación (1.2) nos dice aún más porque motiva la construcción de subespacios vectoriales $W_1, W_2 \subset \mathbb{Z}_2^n$ tales que al elegir a los operadores $\mathbf{M}_{(\mathbf{v}|\mathbf{u})}$ y $\mathbf{M}_{(\mathbf{b}|\mathbf{w})}$ con $\mathbf{v}, \mathbf{b} \in W_1$ y $\mathbf{u}, \mathbf{w} \in W_2$, el operador que resulta de su composición también comparta los mismos vectores propios

$$\mathbf{M}_{(\mathbf{v}|\mathbf{u})}\mathbf{M}_{(\mathbf{b}|\mathbf{w})}|\psi_i\rangle = \mathbf{M}_{(\mathbf{v}+\mathbf{b}|\mathbf{u}+\mathbf{w})}|\psi_i\rangle = |\psi_i\rangle$$

siempre y cuando estos dos operadores conmuten.

Veamos qué otras características deben cumplir los subespacios W_1, W_2 . Primero evaluemos $\mathbf{M}_{(\mathbf{v}|\mathbf{u})}^2$ para $(\mathbf{v}|\mathbf{u}) \in \mathbb{Z}_2^{2n}$, entonces tenemos

$$(\mathbf{X}_{\mathbf{v}}\mathbf{Z}_{\mathbf{u}})(\mathbf{X}_{\mathbf{v}}\mathbf{Z}_{\mathbf{u}}) = (-1)^{(\mathbf{u}\cdot\mathbf{v})}(\mathbf{X}_{\mathbf{v}}\mathbf{X}_{\mathbf{v}})(\mathbf{Z}_{\mathbf{u}}\mathbf{Z}_{\mathbf{u}}) = (-1)^{(\mathbf{u}\cdot\mathbf{v})}\mathbf{I}^{\otimes n}$$

Si escogiéramos un operador $\mathbf{M}_{(\mathbf{v}|\mathbf{u})}$ para el cual $(\mathbf{u} \cdot \mathbf{v}) \neq 0$, un vector invariante $|\psi\rangle$ debería cumplir

$$|\psi\rangle = \mathbf{M}_{(\mathbf{v}|\mathbf{u})}|\psi\rangle = -|\psi\rangle \quad \Leftrightarrow \quad |\psi\rangle = \mathbf{0}$$

donde $\mathbf{0}$ denota el vector cero de $\mathcal{H}^{\otimes n}$. Como el conjunto de estados que nos van a interesar para construir el código va a ser el conjunto de todos los vectores que dejen invariantes una colección de operadores en P_n , escoger operadores

como el anterior reduciría el código a sólo el vector $\mathbf{0}$.

La manera más sencilla para resolver esta circunstancia, es tomando $\mathbf{u} = 0$ o $\mathbf{v} = 0$. Estas dos posibles soluciones motivan escoger operadores de la forma

$$\mathbf{M}_{(W_1|0)} \quad \mathbf{M}_{(0|W_2)}. \quad (1.3)$$

Veamos qué características debe cumplir un operador etiquetado con $(\mathbf{v}|\mathbf{u}) \in \mathbb{Z}_2^{2n}$ para que conmute con los operadores mencionados arriba

$$\begin{aligned} \mathbf{M}_{(W_1|0)}\mathbf{M}_{(\mathbf{v}|\mathbf{u})} &= (-1)^{0 \cdot \mathbf{v} - W_1 \cdot \mathbf{u}} \mathbf{M}_{(\mathbf{v}|\mathbf{u})} \mathbf{M}_{(W_1|0)} && \text{conmutan} \Leftrightarrow W_1 \cdot \mathbf{u} = 0 \\ \mathbf{M}_{(0|W_2)}\mathbf{M}_{(\mathbf{v}|\mathbf{u})} &= (-1)^{W_2 \cdot \mathbf{v} - 0 \cdot \mathbf{u}} \mathbf{M}_{(\mathbf{v}|\mathbf{u})} \mathbf{M}_{(0|W_2)} && \text{conmutan} \Leftrightarrow W_2 \cdot \mathbf{v} = 0 \end{aligned}$$

es decir, un operador con etiqueta $(\mathbf{v}|\mathbf{u})$ conmuta con los operadores etiquetados por $(W_1|0)$ y $(0|W_2)$ si y sólo si

$$\mathbf{u} \in W_1^\perp \quad \mathbf{v} \in W_2^\perp,$$

si queremos que los operadores con etiquetas $(W_1|0)$ y $(0|W_2)$ conmuten entre ellos, basta escoger

$$W_2 \subset W_1^\perp \quad W_1 \subset W_2^\perp$$

Notemos que esta última restricción sobre los subespacios W_1, W_2 permite la posibilidad que un operador con etiqueta $(\mathbf{v}|\mathbf{u})$ donde $\mathbf{v} \in W_1^\perp - W_2$ y $\mathbf{u} \in W_2^\perp - W_1$ conmute con los operadores descritos en (1.3). Esto significa que si escogemos el conjunto de todos los estados invariantes de los operadores en (1.3) como el código \mathcal{C} , van a existir operadores que bajo el criterio de conmutabilidad, *parezcan* que también dejan invariante al conjunto \mathcal{C} , aunque en realidad no lo hagan.

Dicho con otras palabras, para que un operador deje invariante al conjunto

$$\mathcal{C} = \{|\psi\rangle : \mathbf{M}_{(W_1|0)}|\psi\rangle = |\psi\rangle ; \mathbf{M}_{(0|W_2)}|\psi\rangle = |\psi\rangle\}$$

es necesario que conmute con los operadores $\mathbf{M}_{(W_1|0)}$ y $\mathbf{M}_{(0|W_2)}$, aunque no sea suficiente.

Esta ambigüedad en el criterio de conmutatividad, la vamos a utilizar para establecer la distancia mínima del código \mathcal{C} , en términos de qué operadores dejan invariantes al código y cuáles no.

Sabemos que un operador $\mathbf{M}_{(\mathbf{v}|\mathbf{u})}$ donde $(\mathbf{v}|\mathbf{u}) \in \mathbb{Z}_2^n$, que no conmuta con los operadores que escogimos, no deja invariante al código \mathcal{C} . Para este tipo de operadores podríamos determinar qué tanto corrompen los estados de \mathcal{C} y construir una transformación para detectar y tal vez corregir a los estados que cambió, pero para el propósito de los **Códigos de Superficies** esto no es necesario porque en el sistema de partículas que se propone, las perturbaciones que resulten de la interacción con el ambiente van a quedar caracterizadas por operadores que conmuten con los operadores que escogimos.

Bajo esta suposición tenemos que los únicos cambios en el sistema que pueden suceder incluyendo las perturbaciones con el ambiente, están representados por operadores $\mathbf{M}_{(W_2^\perp|W_1^\perp)}$. Consideremos un operador $\mathbf{M}_{(\mathbf{v}|\mathbf{u})}$ tal que

$$\mathbf{v} \in W_2^\perp - W_1 \quad \mathbf{u} \in W_1^\perp - W_2.$$

Tal operador representa un cambio permitido en el sistema porque conmuta con los operadores que escogimos, pero por la definición de \mathcal{C} vemos que no lo deja invariante, es decir, este tipo de operadores determinan los errores que pueden suceder en el código. Esto nos motiva etiquetar a todos los operadores que, aunque representan cambios que pueden suceder en nuestro sistema corrompen los estados que escogimos, por el subespacio de \mathbb{Z}_2^{2n}

$$\left(W_2^\perp/W_1 \mid W_1^\perp/W_2 \right),$$

y definir las distancias mínimas d_1, d_2 de los operadores $\mathbf{M}_{(W_1|0)}$ y $\mathbf{M}_{(0|W_2)}$ por

$$d_1 = \min\{|\mathbf{v}_i - \mathbf{v}_j| : \mathbf{v}_i, \mathbf{v}_j \in W_2^\perp/W_1\} \quad d_2 = \min\{|\mathbf{u}_i - \mathbf{u}_j| : \mathbf{u}_i, \mathbf{u}_j \in W_1^\perp/W_2\} \quad i \neq j$$

las cuales determinan qué tan diferentes son los operadores $\mathbf{M}_{(\mathbf{v}|0)}, \mathbf{M}_{(0|\mathbf{u})}$ de los que escogimos, es decir de $\mathbf{M}_{(W_1|0)}, \mathbf{M}_{(0|W_2)}$.

La **distancia mínima** d del código \mathcal{C} , la cual mide qué tan diferente es un operador $\mathbf{M}_{(\mathbf{v}|\mathbf{u})}$ de los operadores $\mathbf{M}_{(W_1|W_2)}$, la definimos como

$$d = \min\{d_1, d_2\}.$$

El siguiente paso en la descripción del código \mathcal{C} es determinar su dimensión. Antes de esto, veamos por separado cómo son los conjuntos que resultan invariantes bajo $\mathbf{M}_{(W_1|0)}$ y $\mathbf{M}_{(0|W_2)}$ para hacernos una idea de qué estados protege el código.

Para los operadores $\mathbf{M}_{(W_1|0)}$, recordamos que un operador $\mathbf{M}_{(\mathbf{v}|0)}$ es de la forma $\mathbf{X}_{\mathbf{v}}$ donde todas las entradas con 0 que hay en el vector $\mathbf{v} \in W_1$, indican un operador identidad en su expansión tensorial, y todas las entradas con 1 indican un operador X . Veamos con detalle qué pasa cuando evaluamos $\mathbf{X}_{\mathbf{v}}|\psi\rangle$

$$\begin{aligned}\mathbf{X}_{\mathbf{v}}|\psi\rangle &= X^{\mathbf{v}_1} \otimes \cdots \otimes X^{\mathbf{v}_n} (|\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle) \\ &= X^{\mathbf{v}_1}|\psi_1\rangle \otimes \cdots \otimes X^{\mathbf{v}_n}|\psi_n\rangle\end{aligned}$$

Motivados por el hecho de que $X|+\rangle = |+\rangle$ y $X|-\rangle = -|-\rangle$, tomamos al estado $|\psi\rangle$ como un estado puro expresado en la base de Bell, para representarlo con la etiqueta ψ vista como un vector en \mathbb{Z}_2^n bajo la asignación $\{+, -\} \rightarrow \{0, 1\}$ donde $+\mapsto 0$ y $-\mapsto 1$. De esta manera tenemos que

$$\mathbf{X}_{\mathbf{v}}|\psi\rangle = (-1)^{\mathbf{v}\cdot\psi}|\psi\rangle$$

para concluir que el estado puro $|\psi\rangle$ es un estado invariante de $\mathbf{M}_{(W_1|0)}$ si y sólo si $\psi \in W_1^\perp$.

Notemos que debido a que los operadores $\mathbf{M}_{(W_1|0)}$ son lineales, cualquier combinación lineal de estados puros expresados en la base de Bell cuyas etiquetas estén en W_1^\perp bajo la asignación indicada, también es un estado invariante de estos operadores.

Para los operadores $\mathbf{M}_{(0|W_2)}$ procedemos análogamente al caso anterior, sólo que en vez de tomar a estados puros expresados en la base de Bell, tomamos estados puros expresados en la base computacional bajo la asignación $\{\circ, \bullet\} \rightarrow \{0, 1\}$ donde $\circ \mapsto 0$ y $\bullet \mapsto 1$. Esto se debe a que $Z|\circ\rangle = |\circ\rangle$ y $Z|\bullet\rangle = -|\bullet\rangle$. De esta manera, un estado puro $|\varphi\rangle$ expresado en la base de computacional es invariante bajo $\mathbf{M}_{(0|W_2)}$ si y sólo si $\varphi \in W_2^\perp$.

Observemos que la asignación de los símbolos $\{+, -\} \rightarrow \{0, 1\}$ provoca que los operadores $\mathbf{M}_{(W_1|0)}$ ignoren errores de *fase* en la base $\{+, -\}$ de los estados $|\psi \in W_1^\perp\rangle$, lo que equivale a errores de *flip* en la base $\{\circ, \bullet\}$, mientras que la asignación de símbolos $\{\circ, \bullet\} \rightarrow \{0, 1\}$ provoca que los operadores $\mathbf{M}_{(0|W_2)}$ ignoren errores de *fase* en la base $\{\circ, \bullet\}$ de los estados $|\psi \in W_2^\perp\rangle$, lo que equivale a errores *flip* en la base $\{+, -\}$.

Para deducir la **dimensión** k del subespacio $\mathcal{C} \subset \mathcal{H}^{\otimes n}$, vamos a proponer una base con 2^k elementos para luego ver que los elementos generados por esta base, son los mismos elementos de \mathcal{C} . Esta base la definimos como el conjunto $\{|\zeta_i\rangle\}$ donde

$$|\zeta_i\rangle = \frac{1}{\sqrt{|W_1|}} \sum_{\mathbf{u} \in W_1} |\mathbf{u} + \bar{\mathbf{v}}_i\rangle \quad \bar{\mathbf{v}}_i \text{ representantes de } W_2^\perp/W_1 \quad (1.4)$$

Primero veamos que cualesquiera dos elementos $|\zeta_i\rangle$ y $|\zeta_j\rangle$ distintos de este conjunto son ortogonales, lo cual significa que el conjunto de estados que propusimos es linealmente independiente. Para esto observamos que cada etiqueta $\mathbf{u} + \bar{\mathbf{v}}_i$ de (1.4) es un elemento de la clase de equivalencia $\bar{\mathbf{v}}_i$ puesto que cada \mathbf{u} está en W_1 , luego recordamos que cualquier estado $|\psi \in W_2^\perp\rangle$ corresponde a un estado puro en la base computacional, por lo que al evaluar $\langle \zeta_j | \zeta_i \rangle$ todos los términos $\langle \mathbf{w} + \bar{\mathbf{v}}_j | \mathbf{u} + \bar{\mathbf{v}}_i \rangle$ son iguales a cero, y finalmente concluimos que $\langle \zeta_j | \zeta_i \rangle = 0$, ya que:

$$|\zeta_j\rangle = \frac{1}{\sqrt{|W_1|}} \sum_{\mathbf{w} \in W_1} |\mathbf{w} + \bar{\mathbf{v}}_j\rangle$$

Nuestro siguiente propósito es escribir un estado $|\zeta\rangle$ que sea una combinación lineal típica de $\{|\zeta_i\rangle\}$ para ver qué tipo de operadores $\mathbf{M}_{(\mathbf{b}|\mathbf{w})}$ lo dejan invariante. Empecemos por expresar $|\zeta\rangle$ de una manera conveniente y poder calcular fácilmente el cambio que le produce un operador,

$$|\zeta\rangle = \sum_i a_i |\zeta_i\rangle = \sum_i \hat{a}_i \sum_{\mathbf{u} \in W_1} |\mathbf{u} + \bar{\mathbf{v}}_i\rangle \stackrel{\diamond}{=} \sum_{\hat{\mathbf{u}} \in W_2^\perp} b_{\hat{\mathbf{u}}} |\hat{\mathbf{u}}\rangle$$

La segunda igualdad se debe a la definición de la base donde los coeficientes \hat{a}_i han absorbido la condición de normalización. Expliquemos la igualdad \diamond . Se escribe la etiqueta $\hat{\mathbf{u}} \in W_2^\perp$ para expresar el hecho de que la suma $\mathbf{u} + \bar{\mathbf{v}}_i$ para

cada elemento $\mathbf{u} \in W_1$, es un elemento de la clase de equivalencia de $\bar{\mathbf{v}}_i$ y por lo tanto, la podemos pensar como un elemento de W_2^\perp . Los coeficientes $b_{\hat{\mathbf{u}}}$ son los mismos coeficientes que \hat{a}_i sólo que reetiquetados y en algunos casos repetidos.

Ahora veamos qué efecto tiene un operador $\mathbf{M}_{(\mathbf{b}|\mathbf{w})}$ aplicado a un estado $|\zeta\rangle$

$$\mathbf{M}_{(\mathbf{b}|\mathbf{w})}|\zeta\rangle = \sum_{\hat{\mathbf{u}} \in W_2^\perp} b_{\hat{\mathbf{u}}} \mathbf{M}_{(\mathbf{b}|\mathbf{w})}|\hat{\mathbf{u}}\rangle \stackrel{\diamond}{=} \sum_{\hat{\mathbf{u}} \in W_2^\perp} b_{\hat{\mathbf{u}}} (-1)^{\hat{\mathbf{u}} \cdot \mathbf{w}} |\hat{\mathbf{u}} + \mathbf{b}\rangle$$

La primera igualdad se debe a la linealidad de $\mathbf{M}_{(\mathbf{b}|\mathbf{w})}$, para explicar \diamond primero vamos a fijarnos en el efecto que tienen los operadores $\mathbf{M}_{(\mathbf{b}|0)}$ y $\mathbf{M}_{(0|\mathbf{w})}$ sobre un estado $|\hat{\mathbf{u}} \in W_2^\perp\rangle$.

Con la asignación $\{\circ, \bullet\} \rightarrow \{0, 1\}$ que definimos para W_2^\perp , sabemos que

$$\mathbf{M}_{(0|\mathbf{w})}|\hat{\mathbf{u}}\rangle = \mathbf{Z}_{\mathbf{w}}|\hat{\mathbf{u}}\rangle = (-1)^{\hat{\mathbf{u}} \cdot \mathbf{w}} |\hat{\mathbf{u}}\rangle$$

Para los operadores $\mathbf{M}_{(\mathbf{b}|0)} = \mathbf{X}_{\mathbf{b}}$, recordamos que X intercambia los estados $|\circ\rangle$ y $|\bullet\rangle$, por lo que el operador $\mathbf{X}_{\mathbf{b}}$ tiene el mismo efecto sobre las entradas $\hat{\mathbf{u}}_i$ cuando se tiene $\mathbf{b}_i = 1$. Pensando que la etiqueta $\hat{\mathbf{u}}$ es un vector de \mathbb{Z}_2^n , podemos expresar este cambio como $\hat{\mathbf{u}}_i \rightarrow \hat{\mathbf{u}}_i + \mathbf{b}_i$ porque la suma está definida módulo 2. Así tenemos

$$\mathbf{M}_{(\mathbf{b}|0)}|\hat{\mathbf{u}}\rangle = \mathbf{X}_{\mathbf{b}}|\hat{\mathbf{u}}\rangle = |\hat{\mathbf{u}} + \mathbf{b}\rangle$$

De donde se sigue la igualdad \diamond por la linealidad de $\mathbf{M}_{(\mathbf{b}|\mathbf{w})}$. Para ver que esta base genera a \mathcal{C} y sólo a \mathcal{C} , observamos que $\hat{\mathbf{u}} \cdot \mathbf{w} = 0$ si y sólo si $\mathbf{w} \in W_2$, mientras que el vector $\hat{\mathbf{u}} + \mathbf{b}$ está en la misma clase de equivalencia que $\hat{\mathbf{u}}$ si y sólo si $\mathbf{b} \in W_1$.

Si fijamos $\dim W_i = k_i$, tenemos que $\dim W_2^\perp = n - k_2$ y $\dim(W_2^\perp/W_1) = n - k_2 - k_1$, por lo que $|W_2^\perp/W_1| = 2^{n-k_2-k_1}$. Decimos que la **dimensión** del código es $k = n - k_2 - k_1$.

Ahora que ya sabemos con cuántas partículas va a funcionar el código, cuál es su dimensión y cuál es su distancia mínima, podemos decir que el código \mathcal{C} tiene parámetros $[[n, k, d]]$.

Notemos que el único requisito para poder construir \mathcal{C} , fue definir subespacios de \mathbb{Z}_2^n con las propiedades

$$W_1 \subset W_2^\perp \quad W_2 \subset W_1^\perp$$

En el siguiente capítulo vamos a desarrollar una herramienta geométrica para construir este tipo de subespacios, la cual nos va a dar una idea de cómo va a ser el sistema de partículas con el que se va a construir la computadora cuántica que cumpla las necesidades de los códigos de superficies.

Capítulo 2

Espacio de Ciclos

2.1. Vías en Superficies

Una de las herramientas que se han desarrollado para construir espacios vectoriales que puedan funcionar como códigos cuánticos, es la de primero construir espacios topológicos y luego a partir de ellos construir espacios vectoriales que contengan información de su estructura. Más aún, emplear un espacio topológico como punto de partida para la construcción de códigos homológicos se motiva por la naturaleza física que ciertas partículas cuánticas tienen con respecto a su interacción con el espacio en donde se desenvuelven. Es decir, la información estructural de ciertos espacios topológicos, no sólo nos permite construir espacios vectoriales W_1, W_2 descritos en el capítulo anterior, sino que también nos permite describir un sistema de partículas cuyo hábitat material esté descrito geoméricamente por estos espacios topológicos.

Geoméricamente, los espacios topológicos que se van a utilizar pueden imaginarse como vías de tren que recorren planetas enteros con forma de una superficie cerrada y orientable (el caso no orientable también es posible aunque con algunas restricciones), donde cada que la vía se cruce con ella misma, hay una estación de tren. Para dibujar un mapa de una vía de tren Ξ en un planeta \mathbf{P} , vamos a convenir que las estaciones de tren son puntos negros y los tramos donde no hay estaciones de tren son líneas coloreadas, a las que llamaremos simplemente líneas.

A los habitantes de los \mathbf{P} planetas les gusta que las regiones bidimensionales de sus planetas por donde no pasa

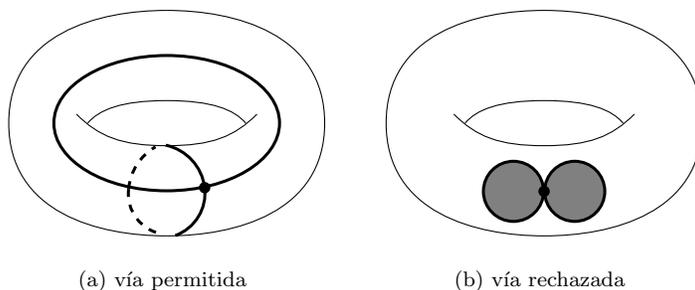


Figura 2.1: Oceanos, vías y planetas
(a) :: (b)

la vía, tengan la forma de un polígono deformable y que estén llenas de agua. Por ejemplo en la Figura 2.1(a), el océano del \mathbf{P} planeta tiene la forma de un cuadrado, mientras que en la Figura 2.1(b) hay un \mathbf{P} planeta que tiene un océano con la forma de un polígono con dos hoyos adentro (pintados de gris), lo cual no les gusta a sus habitantes por lo que tuvieron que quitar la Ξ vía.

Cuando se recorre una Ξ vía en un \mathbf{P} planeta, se puede llegar a la misma estación donde se empezó, o pasar muchas veces por la misma estación, o pasar muchas veces por muchas estaciones diferentes, es decir, se puede recorrer la vía formando ciclos. La información que se va a extraer de las Ξ vías en los \mathbf{P} planetas para construir buenos espacios vectoriales, va a estar relacionada con los ciclos que uno puede generar cuando las recorre. Más aún, esta información nos va a permitir diseñar un entorno físico donde vivan ciertas partículas cuánticas con las cuales vamos a construir

una computadora cuántica.

Describir las Ξ vías, los \mathbf{P} planetas y los ciclos que se generan al recorrerlas en lenguaje matemático para después describir un entorno físico donde habiten ciertas partículas cuánticas, es el propósito de este capítulo.

Una **gráfica** Ξ es un conjunto de vértices y aristas abreviados V y E respectivamente, tal que cada arista $e \in E$ es un segmento unidimensional con sólo un vértice $v \in V$ en cada extremo. Está permitido que los dos vértices en cada extremo, sea en realidad el mismo vértice.

Supongamos que existe una función continua e inyectiva $f: \Xi \rightarrow \mathbf{P}$ donde Ξ es una gráfica y \mathbf{P} es una superficie, entonces llamamos **regiones** a las componentes conexas de $P - f(\Xi)$ y al conjunto de todas las regiones lo abreviamos por F . Tenemos que la frontera de cada región es un subconjunto de $f(\Xi)$, si tomamos a f como la inclusión, entonces la frontera de cada región es una colección de elementos de V y E .

El gusto que tienen los habitantes del \mathbf{P} planeta para construir sus Ξ vías, se describe restringiendo la función f para que las regiones de $f: \Xi \rightarrow \mathbf{P}$ sean homeomorfas a un disco abierto. En este caso decimos que la gráfica Ξ está **inmersa** en \mathbf{P} y lo abreviamos como $\Xi \rightarrow \mathbf{P}$.

El siguiente paso es el de extraer la información que contienen los ciclos.

Un ciclo en las vías de tren es en realidad un recorrido de líneas que quién sabe cuál sea su recorrido, pero siempre acaban en la misma estación donde empezaron. Veamos a este recorrido como una sucesión de líneas, o de aristas, en la cual se escribe en orden las líneas, o aristas, que se van recorriendo. Por ejemplo en la Figura 2.2(a), el ciclo en rojo tiene una sucesión $[q_1, q_2, q_3, q_4]$ donde las $q_i \in E$. Si a cada arista en $\Xi \rightarrow \mathbf{P}$ le asignamos una dirección en la que

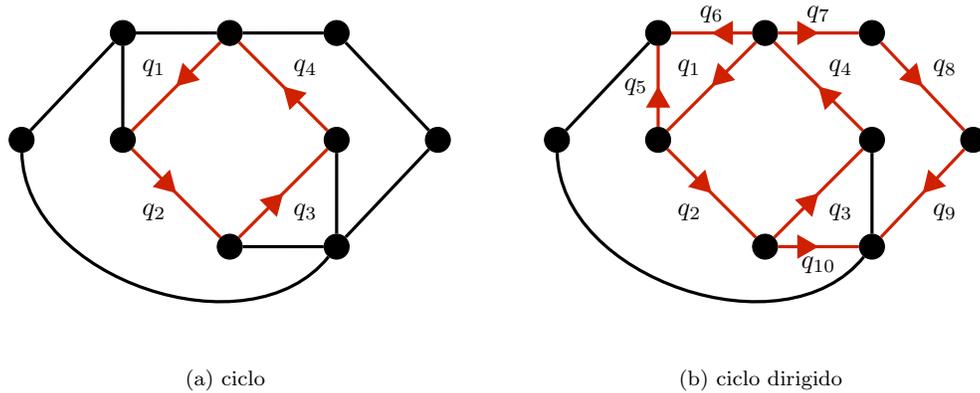


Figura 2.2: ciclos
(a) :: (b)

se recorre, podemos escribir cualquier recorrido de aristas como una suma formal de aristas $\sum_i d_i q_i$ donde las $d_i \in \mathbb{Z}$ describen las veces que el recorrido pasa por cada q_i , si d_i es positivo, entonces la arista se recorrió en el sentido que se le había asignado, si es negativo se recorrió en sentido contrario. Llamemos al conjunto de todas las **sumas formales** de aristas de $\Xi \rightarrow \mathbf{P}$ como $\Delta_1(\Xi)$.

Para expresar la información de las aristas que se repiten en un ciclo con la notación de sucesiones, vamos a escribir las aristas en la sucesión con en el orden en el que se van recorriendo sobre el ciclo, con la convención de que si una arista se recorre en sentido contrario al asignado, se le pone un exponente $\sigma = -1$, si no, se le pone $\sigma = 1$. Observemos que cada arista que se recorre en el ciclo, se escribe en la sucesión tantas veces como fue recorrida. Por ejemplo, el ciclo en rojo de la Figura 2.2(b) que tiene una sucesión $[q_1, q_2, q_3, q_4, q_1, q_5, q_6^{-1}, q_7, q_8, q_9, q_{10}^{-1}, q_3, q_4]$, tiene una suma formal $2 \cdot q_1 + q_2 + 2 \cdot q_3 + 2 \cdot q_4 + q_5 - q_6 + q_7 + q_8 + q_9 - q_{10}$.

Debido a que los vértices de $\Xi \rightarrow \mathbf{P}$ delimitan los elementos de E , podemos describir cada arista por los vértices que tenga en sus extremos. Denotando por $\Delta_0(\Xi)$ las sumas formales de los elementos de V , vamos a relacionar $\Delta_1(\Xi)$

con $\Delta_0(\Xi)$ a través de la función

$$\begin{aligned} \partial_1: \Delta_1(\Xi) &\longrightarrow \Delta_0(\Xi) \\ q &\longmapsto v_i - v_j \end{aligned}$$

donde el par $[v_i, v_j]$ denota los vértices extremos de la arista q con la dirección positiva de v_i a v_j .

Debido a que las regiones de $\Xi \rightarrow \mathbf{P}$ están delimitadas por elementos de V y E , podemos relacionar cada elemento $f \in F$ con la sucesión de aristas que describe su frontera. Diremos que una sucesión de aristas $[q_1^{\sigma_1}, \dots, q_m^{\sigma_m}]$ con $\sigma_i = 1$ ó -1 , describe la frontera de una región $f \in F$ si el recorrido de aristas que denota la sucesión es el camino de una curva simple cerrada dentro de la región f y lo más cercano posible su frontera. Este camino se llama el **camino frontera** de la región f . Por ejemplo en la Figura 2.3, el ciclo $[q_2, q_1^{-1}, q_2^{-1}, q_1]$ es el camino frontera de una región f con la curva roja.

Cabe destacar que la sucesión $[q_1^{\sigma_1}, \dots, q_m^{\sigma_m}]$ puede repetir aristas en más de un lugar, porque los elementos de la

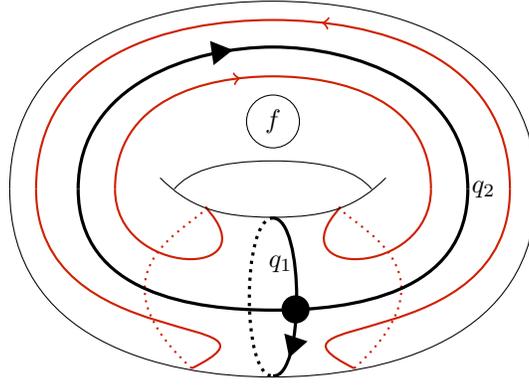


Figura 2.3: camino frontera de f

sucesión están tomados en el orden que aparecen sobre el camino-frontera.

Esta descripción de las regiones de $\Xi \rightarrow \mathbf{P}$ nos permite relacionar el conjunto de las sumas formales de F llamado $\Delta_2(\Xi)$, con $\Delta_1(\Xi)$ por medio de

$$\begin{aligned} \partial_2: \Delta_2(\Xi) &\longrightarrow \Delta_1(\Xi) \\ f &\longmapsto \sigma_1 q_1 + \dots + \sigma_m q_m \end{aligned}$$

Donde f está descrito por la sucesión $[q_1^{\sigma_1}, \dots, q_m^{\sigma_m}]$ con $\sigma_i = 1$ o -1 , y $(-1)q_i$ invierte la dirección de la arista q_i .

Los conjuntos $\Delta_2(\Xi)$, $\Delta_1(\Xi)$ y $\Delta_0(\Xi)$, son grupos finitos abelianos generados por F , E y V respectivamente, por lo tanto para establecer morfismos entre ellos, basta definirlos por medio de sus generadores. Así ∂_2 y ∂_1 son morfismos de grupos a los cuales vamos a llamar homomorfismos frontera.

2.2. Cazando Ciclos

Los espacios vectoriales que nos interesa construir para generar códigos cuánticos, como se mencionó en el capítulo anterior, serán construídos a partir de los ciclos que se generan en $\Xi \rightarrow \mathbf{P}$. Vistos como un subconjunto de $\Delta_1(\Xi)$, todos los ciclos que se pueden recorrer en $\Xi \rightarrow \mathbf{P}$ son muchos. Para discernir cuáles son los que en realidad nos interesan, vamos a clasificar a los ciclos en dos: los que delimitan una región y los que no.

Para este fin vamos a analizar la composición:

$$\Delta_2(\Xi) \xrightarrow{\partial_2} \Delta_1(\Xi) \xrightarrow{\partial_1} \Delta_0(\Xi)$$

Como los $\Delta_i(\Xi)$ son grupos libres abelianos finitamente generados, basta ver qué es lo que le sucede a los elementos de sus bases. Consideremos el diagrama de la Figura 2.4.

Debido a que las regiones de $\Xi \rightarrow \mathbf{P}$ son homeomorfas a un disco, podemos ver a una región $f_l \in F$ descrita por

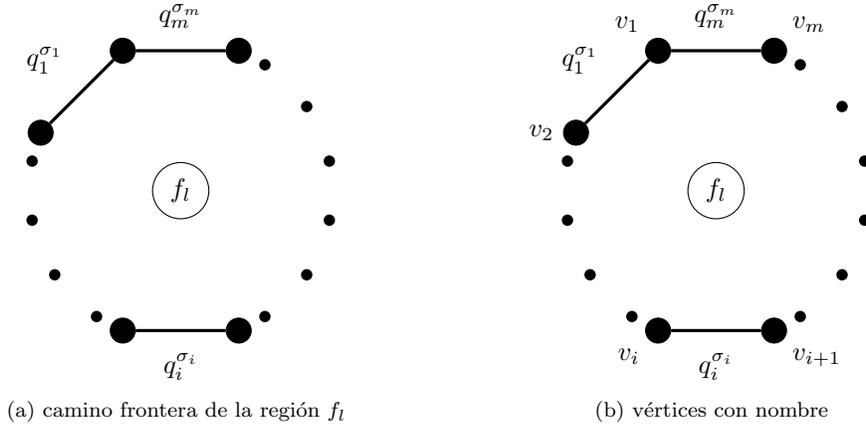


Figura 2.4: nombrar a los vértices
(a) :: (b)

una sucesión $[q_1^{\sigma_1}, \dots, q_m^{\sigma_m}]$ de aristas como un polígono cuyos lados son las aristas que recorre su camino frontera como en la Figura 2.4(a). En la Figura 2.4(b) se le asignan los nombres v_1, \dots, v_m a los vértices de las aristas en el camino frontera de f_l , para finalmente escribir:

$$f_l \xrightarrow{\partial_2} \sigma_1 q_1 + \dots + \sigma_m q_m \xrightarrow{\partial_1} (v_1 - v_2) + (v_2 - v_3) + \dots + (v_m - v_1)$$

Observando que $\partial_1 \partial_2(f)$ es una suma telescópica y que la elección de $f_l \in F$ fue arbitraria, concluimos que $\partial_1 \partial_2(f) = 0 \quad \forall f_l \in F$.

Así se tiene que $\text{Im}(\partial_2) \subset \text{Ker}(\partial_1)$, lo cual nos permite definir el grupo $\text{Ker}(\partial_1)/\text{Im}(\partial_2)$.

Para entender este nuevo grupo, falta conocer a $\text{Ker}(\partial_1)$. Un elemento $c \in \text{Ker}(\partial_1)$ es una suma formal $\sum_i d_i q_i$ de aristas q_i . El fin de la historia sobre la personalidad de $\text{Ker}(\partial_1)$ es que sus elementos son todos los ciclos de aristas que se pueden recorrer en $\Xi \rightarrow \mathbf{P}$, expresados como una suma formal de aristas.

Para demostrar esto, vamos a suponer que la suma $\sum_i d_i q_i$ corresponde a una colección conexa de aristas en $\Xi \rightarrow \mathbf{P}$. Si la colección conexa de aristas es un ciclo, entonces podemos escribir el recorrido del ciclo como una sucesión de aristas $[q_1^{\sigma_1}, \dots, q_m^{\sigma_m}]$ con el orden en el que se van recorriendo sobre el ciclo, indicando con $\sigma_i = 1$ o -1 , en qué dirección se recorrió la arista q_i , y por último ponerle nombres a los vértices como en la Figura 2.4(b) para convencerse que $\partial_1(\sum_i d_i q_i) = 0$. De esta manera vemos que todos los ciclos de $\Xi \rightarrow \mathbf{P}$ están contenidos en $\text{Ker}(\partial_1)$.

Para ver la otra contención, supongamos que una colección conexa de aristas q a la cual le asignamos la sucesión $[q_1^{\sigma_1}, \dots, q_m^{\sigma_m}]$ en el orden en el que se recorren las aristas sobre q , no es un ciclo. Entonces podemos nombrar a los vértices de manera similar a la Figura 2.4, con la diferencia que $v_1 \neq v_m$, por lo tanto al evaluarla con ∂_1 se eliminan todos los vértices excepto v_1 y v_m . Concluimos que si q no es un ciclo entonces $\partial_1(q) \neq 0$ por lo tanto $q \notin \text{Ker}(\partial_1)$.

Ahora podemos concluir que un elemento no trivial $c \in \text{Ker}(\partial_1)/\text{Im}(\partial_2)$ es la suma formal de ciclos, que no son el recorrido de ninguna región $f_l \in F$.

Este grupo cociente modificado ligeramente, es el espacio vectorial con el que vamos a poder construir códigos cuánticos. Antes de ver la construcción, vamos a conocer cómo se relaciona este grupo con la superficie \mathbf{P} en la que vive Ξ .

2.3. Ahorcando hoyos

Como la construcción de códigos va a estar definida a partir de la gráfica $\Xi \rightarrow \mathbf{P}$, es necesario poder deducir el rango de $\text{Ker}(\partial_1)/\text{Im}(\partial_2)$ a partir de los elementos de Ξ y la superficie \mathbf{P} .

Para esto, vamos a relacionar los conjuntos $\Delta_i(\Xi)$ con el rango de los grupos $\text{Ker}(\partial_i)/\text{Im}(\partial_{i+1})$ $i = 0, 1, 2, 3$ donde

$$0 \xrightarrow{\partial_3} \Delta_2(\Xi) \xrightarrow{\partial_2} \Delta_1(\Xi) \xrightarrow{\partial_1} \Delta_0(\Xi) \xrightarrow{\partial_0} 0$$

bajo la ecuación

$$\sum_i (-1)^i \text{rango}[\Delta_i(\Xi)] \stackrel{\diamond}{=} \sum_i (-1)^i \text{rango}[\text{Ker}(\partial_i)/\text{Im}(\partial_{i+1})] \quad (2.1)$$

Teniendo en cuenta que $\Delta_2(\Xi)$, $\Delta_1(\Xi)$ y $\Delta_0(\Xi)$ tienen como base a F , E y V respectivamente, se tiene que $\text{rango}[\Delta_2(\Xi)]$, $\text{rango}[\Delta_1(\Xi)]$ y $\text{rango}[\Delta_0(\Xi)]$ son iguales a $|F|$, $|E|$ y $|V|$ respectivamente.

Después vamos a ver que la suma $\sum_i (-1)^i \text{rango}[\Delta_i(\Xi)]$ es independiente de la elección de Ξ en una \mathbf{P} superficie dada.

Para demostrar la igualdad \diamond de la ecuación (1), consideremos las sucesiones cortas exactas de grupos finitos abelianos:

$$0 \rightarrow \text{Ker}(\partial_i) \xrightarrow{\iota} \Delta_i(\Xi) \xrightarrow{\partial_i} \text{Im}(\partial_i) \rightarrow 0 \quad 0 \rightarrow \text{Im}(\partial_{i+1}) \xrightarrow{\iota} \text{Ker}(\partial_i) \xrightarrow{\varsigma} \text{Ker}(\partial_i)/\text{Im}(\partial_{i+1}) \rightarrow 0$$

Donde ι denota la inclusión y ς denota la inclusión en su clase de equivalencia. Por ser sucesiones cortas exactas, se tiene que:

$$\text{rango}[\Delta_i(\Xi)] = \text{rango}[\text{Ker}(\partial_i)] + \text{rango}[\text{Im}(\partial_i)] \quad \text{rango}[\text{Ker}(\partial_i)] = \text{rango}[\text{Im}(\partial_{i+1})] + \text{rango}[\text{Ker}(\partial_i)/\text{Im}(\partial_{i+1})]$$

Sumando alternadamente $\text{rango}[\Delta_i(\Xi)]$ se sigue

$$\underbrace{\text{rango}[\Delta_0(\Xi)]}_{\text{rango}[\text{Ker}(\partial_0)] + \text{rango}[\text{Im}(\partial_0)]} - \underbrace{\text{rango}[\Delta_1(\Xi)]}_{\text{rango}[\text{Ker}(\partial_1)] + \text{rango}[\text{Im}(\partial_1)]} + \underbrace{\text{rango}[\Delta_2(\Xi)]}_{\text{rango}[\text{Ker}(\partial_2)] + \text{rango}[\text{Im}(\partial_2)]}$$

al sustituir $\text{rango}[\text{Ker}(\partial_i)] = \text{rango}[\text{Im}(\partial_{i+1})] + \text{rango}[\text{Ker}(\partial_i)/\text{Im}(\partial_{i+1})]$ se sigue

$$\text{rango}[\text{Ker}(\partial_0)/\text{Im}(\partial_1)] + \underbrace{\text{rango}[\text{Im}(\partial_0)]}_0 - \text{rango}[\text{Ker}(\partial_1)/\text{Im}(\partial_2)] + \underbrace{\text{rango}[\text{Im}(\partial_3)]}_0 + \text{rango}[\text{Ker}(\partial_2)/\text{Im}(\partial_3)]$$

observando que el rango de un grupo trivial es cero, concluimos

$$\begin{aligned} \sum_i (-1)^i \text{rango}[\Delta_i(\Xi)] &= \text{rango}[\text{Ker}(\partial_0)/\text{Im}(\partial_1)] - \text{rango}[\text{Ker}(\partial_1)/\text{Im}(\partial_2)] + \text{rango}[\text{Ker}(\partial_2)/\text{Im}(\partial_3)] \\ &= \sum_i (-1)^i \text{rango}[\text{Ker}(\partial_i)/\text{Im}(\partial_{i+1})] \quad \square \end{aligned}$$

Para ver que $\sum_i (-1)^i \text{rango}[\Delta_i(\Xi)]$ no depende de Ξ , sino de la superficie \mathbf{P} donde está inmersa, se va a demostrar que la suma $|V| - |E| + |F|$ para cualquier gráfica Ξ inmersa en una superficie \mathbf{P} dada, da el mismo valor.

Esto se va a hacer deduciendo recursivamente el valor de la suma $\chi(\Xi) := |V| - |E| + |F|$ sobre el género de la superficie cerrada \mathbf{P} , la cual se va a tomar orientable. Aunque este resultado también se aplica para superficies cerradas no orientables, la construcción geométrica de las inmersiones $\Xi \rightarrow \mathbf{P}$ no sólo nos ayudará para construir los subespacios W_i planteados en el capítulo anterior, sino también nos va a proporcionar un entorno físico para construir el sistema donde van a vivir las partículas cuánticas que vamos a utilizar.

El primer paso, es calcular $\chi(\Xi)$ para una gráfica Ξ inmersa en la superficie cerrada de género 0, la esfera $\mathbb{S}^2 = \mathbb{T}_0$.

Supongamos primero que $|F| = 1$, por el teorema de la curva de Jordan sabemos que Ξ no tiene ciclos porque si los tuviera, entonces dividirían a la esfera en más de una región. El hecho de que Ξ no tenga ciclos nos dice que se guarda la relación $|V| = |E| + 1$, por lo que $\chi(\Xi) = 2$. Ahora supongamos que $\chi(\Xi) = 2$ cuando $|F| = f > 1$. Tomemos Ξ tal que $|F| = f + 1$, entonces para dos regiones vecinas existe al menos una arista $e \in E$ que está sobre el camino frontera de ambas. Si quitamos esa arista de Ξ obtenemos una gráfica Ξ' conexa que también está inmersa y cumple $|F_{\Xi'}| = |F| - 1 = f$, de donde tenemos que $\chi(\Xi') = 2$. Aunque también tenemos que $|E_{\Xi'}| = |E| - 1$ y $|V_{\Xi'}| = |V|$, por lo que $\chi(\Xi) = \chi(\Xi')$. Ahora se va a calcular $\chi(\Xi)$ en la superficie cerrada de género g , el toro \mathbb{T}_g , el cual resulta

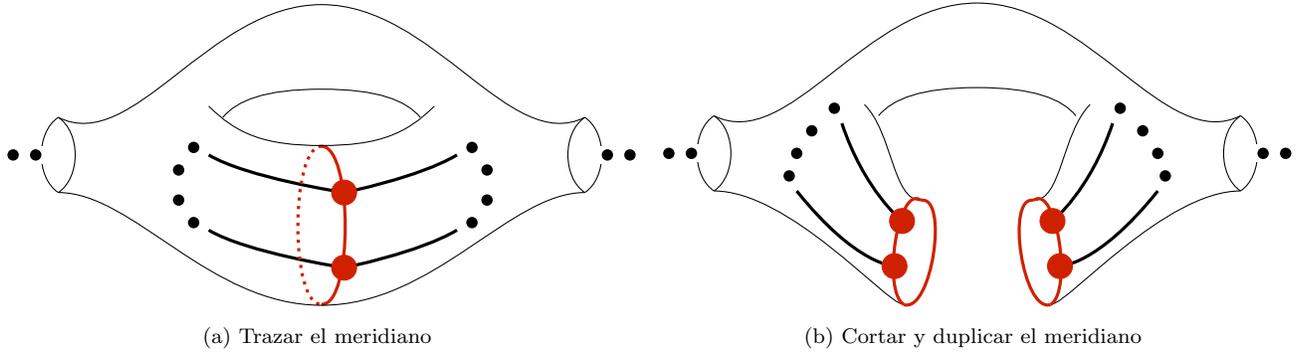


Figura 2.5
(a) :: (b)

de añadirle g asas a la esfera.

La idea de la demostración es transformar a cualquier inmersión $\Xi \rightarrow \mathbb{T}_g$ en una nueva inmersión $\Xi' \rightarrow \mathbb{T}_{g-1}$ cuyos vértices, regiones y aristas guarden cierta relación con $\Xi \rightarrow \mathbb{T}_g$. Esta transformación la vamos a realizar cortando $\Xi \rightarrow \mathbb{T}_g$ a lo largo de un meridiano ejemplificado en la Figura 2.5(a), el cual corta de manera transversal una cantidad finita de veces a las aristas de Ξ una vez por arista, y en cada corte por el que pasa ponemos un vértice. Procedemos por separar la superficie \mathbb{T}_g a lo largo del meridiano obteniendo dos copias de él, una por cada extremo, y por último tapamos los dos agujeros con dos discos como en la Figura 2.5(b).

Esta nueva superficie que resulta de la separación es homeomorfa a \mathbb{T}_{g-1} , puesto que al cortarla quitamos el asa que le habíamos puesto para construir \mathbb{T}_g . Supongamos que el meridiano cortó a Ξ en p aristas, entonces tenemos que el conjunto $E_{\Xi'}$ contiene todas las $|E| - p$ aristas de Ξ que no cortó el meridiano, más p aristas que constituyen cada copia del meridiano, más otras p aristas por cada copia del meridiano que resultan de las aristas de Ξ que son adyacentes a los p vértices. Debido a que sólo hay dos copias del meridiano, tenemos que $|E_{\Xi'}| = |E| - p + 2p + 2p$.

Más aún, sabemos que $V_{\Xi'}$ contiene a todos los $|V|$ vértices de Ξ , más los p vértices de cada copia del meridiano. También tenemos que $F_{\Xi'}$ contiene a todas las $|F|$ regiones de Ξ más dos nuevas regiones que resultan de los dos discos que añadimos, más p nuevas regiones que resultan de haber partido en dos a las p regiones por las que pasó el meridiano. De esta manera deducimos que $|V_{\Xi'}| = |V| + 2p$ y $|F_{\Xi'}| = |F| + 2 + p$, por lo que

$$\begin{aligned} \chi(\Xi) &= |V| - |E| + |F| \\ &= (|V_{\Xi'}| - 2p) - (|E_{\Xi'}| - 3p) + (|F_{\Xi'}| - 2 - p) \\ &= \chi(\Xi') - 2 \end{aligned}$$

Recursivamente aplicamos el argumento anterior a la inmersión $\Xi' \rightarrow \mathbb{T}_{g-1}$ hasta llegar a una inmersión $\Xi^g \rightarrow \mathbb{T}_0$ con $\chi(\Xi^g) = 2$ y deducir que

$$\begin{aligned} \chi(\Xi) &= \chi(\Xi') - 2 = (\chi(\Xi'') - 2) - 2 = \dots = (\dots (\chi(\Xi^g) \overbrace{-2}^{g \text{ veces}}) \dots) - 2 \\ &= \chi(\Xi^g) - 2g = 2 - 2g \end{aligned}$$

para cualquier inmersión $\Xi \rightarrow \mathbb{T}_g$. Uniendo la ecuación 2.1 y la anterior se tiene que para una gráfica $\Xi \rightarrow \mathbf{P}$, donde \mathbf{P} es una superficie orientable \mathbb{T}_g ,

$$\begin{aligned} 2 - 2g &= \chi(\Xi) \\ &= |V| - |E| + |F| \\ &= \sum_i (-1)^i \text{rango}[\Delta_i(\Xi)] \\ &= \sum_i (-1)^i \text{rango}[\text{Ker}(\partial_i) / \text{Im}(\partial_{i+1})] \end{aligned} \tag{2.2}$$

es decir, la suma $\sum_i (-1)^i \text{rango}[\text{Ker}(\partial_i)/\text{Im}(\partial_{i+1})]$ no depende de la gráfica Ξ sino del género g .

Para poder calcular el rango del grupo de ciclos con el que queremos trabajar, es decir $\text{Ker}(\partial_1)/\text{Im}(\partial_2)$, basta tomar una inmersión agradable en \mathbb{T}_g donde sea fácil calcular $\text{rango}[\text{Ker}(\partial_i)/\text{Im}(\partial_{i+1})]$ con $i = 0, 2$, y despejar el rango que nos interesa de la ecuación anterior.

Tomemos la gráfica como en la Figura 2.6. Veamos que si recorremos la superficie empezando por v sobre el lado

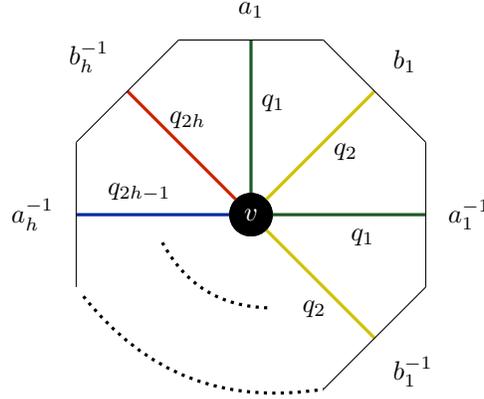


Figura 2.6: La superficie \mathbb{T}_g vista como un polígono de $2g$ lados denotados por $a_i^{\pm 1}, b_i^{\pm 1}$ y una gráfica $\Xi \rightarrow \mathbb{T}_g$ indicada por las aristas de colores.

izquierdo de la arista q_1 y asignamos las orientaciones a las aristas q_i conforme las vamos recorriendo, obtenemos una sucesión

$$\mathbf{f} = q_1, q_2, q_1^{-1}, q_2^{-1}, \dots, q_{2h-1}, q_{2h}, q_{2h-1}^{-1}, q_{2h}^{-1}$$

la cual pasó por todos los lados a_i, b_i del polígono con el que representamos la superficie \mathbb{T}_g . Esto nos dice que \mathbf{f} es el camino frontera de la única frontera f que tiene $\Xi \rightarrow \mathbb{T}_g$, es decir $\Delta_2(\Xi)$ está generado por el elemento f . Calculando $\partial_2(f)$ tenemos que

$$\partial_2(f) = q_1 + q_2 - q_1 - q_2 + \dots + q_{2h-1} + q_{2h} - q_{2h-1} - q_{2h} = 0$$

de donde concluimos que $\text{Ker} \partial_2 = \Delta_2(\Xi)$. Ahora observemos que todas las aristas q_i tienen a v como su vértice inicial y final, por lo que para cada q_i tenemos que

$$\partial_1(q_i) = v - v = 0$$

de donde concluimos que $\text{Im} \partial_1 = 0$, ya que $\{q_i\}$ es una base para $\Delta_1(\Xi)$. Estas conclusiones nos dicen que

$$\begin{aligned} \text{Ker}(\partial_2) &= \Delta_2(\Xi) \\ \text{Im}(\partial_3) &= 0 \end{aligned} \quad \Rightarrow \quad \text{Ker}(\partial_2)/\text{Im}(\partial_3) = \Delta_2(\Xi)$$

$$\begin{aligned} \text{Ker}(\partial_0) &= \Delta_0(\Xi) \\ \text{Im}(\partial_1) &= 0 \end{aligned} \quad \Rightarrow \quad \text{Ker}(\partial_0)/\text{Im}(\partial_1) = \Delta_0(\Xi)$$

Observando que $\text{rango}[\Delta_i(\Xi)] = 1$ para $i = 0, 2$, despejamos $\text{Ker}(\partial_1)/\text{Im}(\partial_2)$ de la ecuación 2.2 para deducir que

$$\text{rango}[\text{Ker}(\partial_1)/\text{Im}(\partial_2)] = 2 - \chi(\Xi) = 2g$$

2.4. Ciclos Duales

Los espacios vectoriales con los que vamos a construir al código cuántico están casi listos, nos faltan dos pasos para terminar de construirlos. Un paso, es convertir a $\text{Im} \partial_2$ en un espacio vectorial W_2 , porque hasta ahora sólo ha sido definido como grupo. El otro paso es encontrar un espacio vectorial W_1 tal que $W_2 \subset W_1^\perp$.

En esta sección se va a construir el grupo que después de una ligera modificación, se convertirá en W_1 , dejando para la siguiente sección la conversión de grupos a espacios vectoriales.

Para construir este grupo, primero se van a construir los duales de $\Delta_i(\Xi)$ para $\Xi \rightarrow \mathbf{P}$ donde \mathbf{P} es una superficie

cerrada.

Definimos al **dual** de $\Delta_i(\Xi)$ para $i = 0, 1, 2$ como el espacio de todos los homomorfismos $\varphi: \Delta_i(\Xi) \rightarrow G$ donde G es un grupo abeliano, denotado por $\Delta^i(\Xi, G)$. Es decir, $\Delta^i(\Xi, G) := \text{hom}(\Delta_i(\Xi), G)$.

Igual que en la sección anterior, la intención es relacionar los grupos $\Delta^i(\Xi, G)$ bajo homomorfismos δ_i para construir grupos cocientes, y que además estén relacionados con los grupos $\Delta_i(\Xi)$.

Con esto en mente se define δ_1, δ_2 de la siguiente manera:

$$\begin{array}{ccccc} \Delta^0(\Xi, G) & \xrightarrow{\delta_1} & \Delta^1(\Xi, G) & \xrightarrow{\delta_2} & \Delta^2(\Xi, G) \\ \varphi \mapsto & & \delta_1\varphi & & \\ & & \psi \mapsto & & \delta_2\psi \\ & & \delta_1\varphi = \varphi\partial_1 & & \\ & & \delta_2\psi = \psi\partial_2 & & \end{array}$$

Por ejemplo, para $q_l \in E \subset \Delta_1(\Xi)$ con orientación positiva de v_{l+1} a v_l , y $f_l \in F \subset \Delta_2(\Xi)$ como en la Figura 2.4, se tiene

$$\begin{aligned} \delta_1\varphi(q_l) &= \varphi(v_{l+1} - v_l) = \varphi(v_{l+1}) - \varphi(v_l) \\ \delta_2\psi(f_l) &= \psi(\sigma_1q_1 + \cdots + \sigma_mq_m) = \psi(\sigma_1q_1) + \cdots + \psi(\sigma_mq_m) \end{aligned}$$

Para analizar la composición $\delta_1\delta_2\varphi$ tomemos cualquier $f_l \in F \subset \Delta_2(\Xi)$ como en la Figura 2.4. Calculando $\delta_2\delta_1\varphi(f_l)$ se tiene

$$\begin{array}{c} \delta_2\delta_1\varphi(f_l) \\ \parallel \\ \overbrace{\delta_1\varphi(\sigma_1q_1) + \cdots + \delta_1\varphi(\sigma_mq_m)} \\ \parallel \qquad \qquad \qquad \parallel \\ \underbrace{(\varphi(v_1) - \varphi(v_2)) + \cdots + (\varphi(v_m) - \varphi(v_1))} \\ \parallel \\ 0 \end{array}$$

De esto queda claro que $\text{Im}(\delta_1) \subset \text{Ker}(\delta_2)$ lo cual nos permite construir el grupo $\text{Ker}(\delta_2)/\text{Im}(\delta_1)$, que después de modificarlo un poco, será el espacio vectorial W_2 .

Debido a que los grupos $\Delta^i(\Xi, G)$ se definieron a partir de homomorfismos, puede resultar complicado visualizarlos, y decepcionante el apartarse de la naturaleza visual que hasta ahora han tenido las Ξ vías, para entrar en un campo de estudio completamente abstracto definido por funciones. Para que esta decepción no ocurra, veremos que los grupos $\Delta^i(\Xi, G)$ se pueden pensar como los grupos $\Delta_j(\Xi^*)$ de una gráfica $\Xi^* \rightarrow \mathbf{P}$ construida a partir de $\Xi \rightarrow \mathbf{P}$, a la cual llamamos la **gráfica dual** de $\Xi \rightarrow \mathbf{P}$.

Primero definimos la **estrella** de un vértice v , $v[\star]$, como el conjunto de aristas que son adyacentes a él. Decimos que la estrella es orientada si le asignamos la orientación positiva a cada arista q adyacente a v cuyo vértice final sea v , mientras que le asignamos la orientación negativa si v es su vértice inicial. En caso de que exista una arista q en donde v sea su vértice final y su vértice inicial, lo consideramos dos veces en $v[\star]$, una vez con orientación positiva, y otra negativa.

Definimos los vértices de $\Xi^* \rightarrow \mathbf{P}$ como las regiones de $\Xi \rightarrow \mathbf{P}$, y sus regiones F^* como los vértices de $\Xi \rightarrow \mathbf{P}$, con el cuidado de que las adyacencias de vértices en $\Xi^* \rightarrow \mathbf{P}$ sean iguales a las adyacencias de regiones en $\Xi \rightarrow \mathbf{P}$. Para orientar los caminos frontera de cada $f^* \in F^*$, tomamos la orientación de $v[\star]$ donde a v le corresponde la región f^* . Observemos que al orientar los caminos frontera de f^* también orientamos las aristas q^* . A la construcción $\Xi^* \rightarrow \mathbf{P}$ se le conoce como el dual de $\Xi \rightarrow \mathbf{P}$.

Aunque esta definición de $\Xi^* \rightarrow \mathbf{P}$ está bien, cabe la duda si en realidad Ξ^* está inmersa en \mathbf{P} como les gusta a los habitantes de los \mathbf{P} planetas. Es decir, si cada región en F^* es homeomorfa a un disco.

Para demostrar esto, observemos que las regiones de Ξ^* quedan determinadas por las estrellas de Ξ como polígonos homeomorfos a un disco, y que cada arista en Ξ^* es adyacente a dos y sólo dos regiones, de donde se sigue que el pegado de sus caras es una superficie orientable. Para ver que es la misma, vemos que $|V^*| = |F|$, $|F^*| = |V|$ y $|E^*| = |E|$ por lo que $\chi(\Xi^*) = \chi(\Xi)$, de donde deducimos que el género es el mismo.

Ahora necesitamos una relación biyectiva entre los grupos $\Delta^i(\Xi, G)$ y $\Delta_j(\Xi^*)$ que nos permita afirmar que los grupos $\text{Ker}(\delta_2), \text{Im}(\delta_1)$ corresponden a ciclos de aristas y regiones en $\Xi^* \rightarrow \mathbf{P}$. Con este fin construimos una base para $\Delta^i(\Xi, G)$ $i = 0, 1, 2$ de la siguiente manera, para cada $v_l \in V$, $q_l \in E$ y $f_l \in F$ se definen las funciones:

$$\varphi_{v_l}(v_j) = \begin{cases} 0 & \text{si } v_l \neq v_j \\ 1 & \text{si } v_l = v_j \end{cases} \quad \varphi_{q_l}(q_j) = \begin{cases} 0 & \text{si } q_l \neq q_j \\ 1 & \text{si } q_l = q_j \end{cases} \quad \varphi_{f_l}(f_j) = \begin{cases} 0 & \text{si } f_l \neq f_j \\ 1 & \text{si } f_l = f_j \end{cases}$$

Así los conjuntos $\{\varphi_{v_l}\}_{v_l \in V}$, $\{\varphi_{q_l}\}_{q_l \in E}$ y $\{\varphi_{f_l}\}_{f_l \in F}$ forman una base para $\Delta^i(\Xi, G)$ $i = 0, 1, 2$ respectivamente.

Haber definido estas bases nos permite plantear la relación biyectiva que necesitamos como

$$\delta_1 \varphi_v \stackrel{\circ}{\simeq} \partial_1 f^* \quad \delta_2 \varphi_q \stackrel{\circ}{\simeq} \partial_2 q^*$$

para todo vértice $v \in V$ y para toda arista $q \in E$, donde f^* es la región que le corresponde al vértice v y q^* la arista que le corresponde a q .

Antes de definir el isomorfismo que necesitamos, escribamos de una manera más clara quiénes son $\delta_1 \varphi_v$ y $\delta_2 \varphi_q$. Tenemos que $\delta_1 \varphi_v$ es un elemento de $\Delta^1(\Xi, G)$, por lo que lo podemos pensar como una combinación lineal de elementos φ_{q_l} . Más aún observemos que $\delta_1 \varphi_v$ evalúa como cero a cada elemento de $\Delta_1(\Xi)$ cuyas aristas no contengan al vértice v como extremo, de donde se sigue que la combinación lineal en elementos φ_{q_l} sólo toma las funciones cuyas aristas q_l son adyacentes a v . Los coeficientes de esta combinación lineal son los exponentes de las aristas en la estrella orientada de v porque en ellos recae la información de si v es un extremo final o inicial de cada arista.

Para $\delta_2 \varphi_q$ observamos que lo podemos escribir como una combinación lineal de elementos φ_{f_l} , donde sólo se toman las funciones cuya región f_l contiene a la arista q , puesto que todas las demás regiones son evaluadas como cero bajo $\delta_2 \varphi_q$. Sabemos que a lo más sólo hay dos de tales regiones f_l , una a la izquierda de q y otra a la derecha. Notemos que los coeficientes de estos dos sumandos es arbitrario ya que no sea ha definido cuál es la izquierda y cuál la derecha. Resumiendo estos dos últimos párrafos escribimos

$$\delta_1 \varphi_v = \sum_{q \in v[\star]} \sigma_q \varphi_q \quad \delta_2 \varphi_q = \varphi_{f_2} - \varphi_{f_1}$$

Ahora sólo hace falta escribir $\partial_1 f^*$ y $\partial_2 q^*$ de una manera más clara para poder definir el isomorfismo \diamond . Notemos que $\partial_1 f^*$ es la combinación lineal de los elementos del camino frontera de f^* , cuyos coeficientes son los exponentes de cada arista q^* en este camino frontera. Por la definición de $\Xi^* \rightarrow \mathbf{P}$ sabemos que el camino frontera de f^* corresponde a la estrella orientada $v[\star]$. También sabemos que $\partial_2 q^*$ es la suma de su vértice final v_2^* menos su vértice inicial v_1^* , los cuales corresponden a las regiones f_2 y f_1 adyacentes a q . Resumiendo el párrafo tenemos

$$\partial_1 f^* \stackrel{\mathbf{d}}{\simeq} \sum_{q \in v[\star]} \sigma_q q \quad \partial_2 q^* \stackrel{\mathbf{d}}{\simeq} f_2 - f_1$$

donde \mathbf{d} denota la correspondencia dual entre $\Xi \rightarrow \mathbf{P}$ y $\Xi^* \rightarrow \mathbf{P}$. De esta manera, construimos el isomorfismo \diamond como $\varphi_q \mapsto q$ y $\varphi_f \mapsto f$ seguido por \mathbf{d} .

Esto nos permite representar elementos del grupo $\text{Ker } \delta_2 / \text{Im } \delta_1 \subset \Delta^1(\Xi, G)$ como elementos del grupo $\text{Ker } \partial_1 / \text{Im } \partial_2$ evaluados en $\Delta_1(\Xi^*)$, los cuales corresponden a ciclos de aristas en la gráfica $\Xi^* \rightarrow \mathbf{P}$.

2.5. Espacios de ciclos

Como fue mencionado en el capítulo anterior, la idea de los códigos de superficies consiste en construir un sistema de partículas para el cual podamos aproximar su comportamiento con el paso del tiempo y construir en él un conjunto de estados \mathcal{C} que evolucione invariante con respecto a la aproximación que se propone. También vimos que la construcción abstracta de \mathcal{C} se basa en el diseño de subespacios $W_1 \subset W_2^\perp, W_2 \subset W_1^\perp$.

Antes de definir los subespacios W_1, W_2 veamos dos propiedades entre los grupos $\text{Im } \delta_1, \text{Ker } \partial_1$ y $\text{Im } \partial_2, \text{Ker } \delta_2$ que nos van a ayudar a plantear la noción de ortogonalidad.

La primera propiedad es que para todo elemento $v \in V$ tenemos

$$\delta_1 \varphi_v(\mathbf{c}) = 0 \quad \Leftrightarrow \quad \mathbf{c} \in \text{Ker } \partial_1$$

Para explicar la relación \diamond escribimos $\delta_1 \varphi_v(\mathbf{c}) = \varphi_v \partial_1(\mathbf{c})$. Si $\mathbf{c} \notin \text{Ker } \partial_1$, es decir si \mathbf{c} corresponde a una colección de aristas que no es un ciclo en $\Xi \rightarrow \mathbf{P}$, entonces existe una arista $q \in \mathbf{c}$ tal que tiene un vértice v extremo, el cual no se cancela al evaluar $\partial_1(\mathbf{c})$. Cuando evaluamos $\varphi_v \partial_1(\mathbf{c})$ para este mismo vértice v , tenemos que φ_v tampoco cancela lo que no canceló $\partial_1(\mathbf{c})$, por lo que $\delta_1 \varphi_v(\mathbf{c}) \neq 0$.

Si $\mathbf{c} \in \text{Ker } \partial_1$, entonces $\partial_1(\mathbf{c}) = 0$ y como φ_v es un homomorfismo tenemos que $\delta_1 \varphi_v(\mathbf{c}) = 0$.

La segunda propiedad que nos interesa es que para todo elemento $f \in F$ tenemos

$$\psi \partial_2(f) = 0 \quad \Leftrightarrow \quad \psi \in \text{Ker } \delta_2$$

en donde \diamond se sigue de la definición de $\text{Ker } \delta_2$ cuando escribimos $\psi \partial_2(f) = \delta_2 \psi(f)$ y recordamos que $\{f \in F\}$ es una base para $\Delta_2(\Xi)$.

La idea de definir los subespacios vectoriales que nos interesan, consiste en traducir las dos propiedades previamente mencionadas junto con las otras dos propiedades $\text{Im } \delta_1 \subset \text{Ker } \delta_2$ y $\text{Im } \partial_2 \subset \text{Ker } \partial_1$, en un lenguaje que represente los estados de las partículas bajo las asignaciones de símbolos definidos en el capítulo anterior. Con este fin en mente, tomamos G como $G = \mathbb{Z}_2$ y definimos

$$\mathbb{T}_1: \Delta^1(\Xi, G) \longrightarrow \mathbb{Z}_2^{|E|} \qquad \mathbb{T}_2: \Delta_1(\Xi) \longrightarrow \mathbb{Z}_2^{|E|}$$

$$\mathbb{T}_1\left(\sum_{q \in E} \mathbf{v}_q \varphi_q\right) = \underbrace{(\mathbf{v}_1, \dots, \mathbf{v}_{|E|})}_{\mathbf{v}} \qquad \mathbb{T}_2\left(\sum_{q \in E} \mathbf{u}_q q\right) = \underbrace{(\mathbf{u}_1, \dots, \mathbf{u}_{|E|})}_{\mathbf{u}}$$

$$W_2 := \mathbb{T}_1(\text{Im } \delta_1)$$

$$W_1 := \mathbb{T}_2(\text{Im } \partial_2)$$

Observemos que para cada $q \in E$ debido a que $\varphi_q(q) = 1$ y $\varphi_q(q_l) = 0$ si $q_l \neq q$, tenemos

$$\mathbf{v}_q \varphi_q(\mathbf{u}_q q) = \mathbf{v}_q \mathbf{u}_q \varphi_q(q) = \mathbf{v}_q \mathbf{u}_q$$

de donde se obtiene que

$$\varphi(\mathbf{c}) = \mathbf{v} \cdot \mathbf{u} \qquad \text{donde} \qquad \varphi = \sum_{q \in E} \mathbf{v}_q \varphi_q \qquad \mathbf{c} = \sum_{q \in E} \mathbf{u}_q q$$

Esto nos permite deducir el espacio W_2^\perp :

$$\mathbf{u} \in W_2^\perp \quad \Leftrightarrow \quad \mathbf{v} \cdot \mathbf{u} = 0 \quad \forall \mathbf{v} \in W_2$$

Observando que $\{\mathbb{T}_1(\delta_1 \varphi_v)\}_{v \in V}$ es una base para W_2 , tenemos que lo anterior sucede si y sólo si

$$\mathbb{T}_1(\delta_1 \varphi_v) \cdot \mathbf{u} = 0 \quad \forall v \in V$$

Escribiendo $\mathbb{T}_2(\mathbf{c}) = \mathbf{u}$ para algún $\mathbf{c} \in \Delta_1(\Xi)$, lo anterior sucede si y sólo si

$$\delta_1 \varphi_v(\mathbf{c}) = 0 \quad \forall v \in V$$

de donde deducimos que $\mathbf{c} \in \text{Ker } \partial_1$ y por lo tanto $W_2^\perp = \mathbb{T}_2(\text{Ker } \partial_1)$.

Para ver quién es W_1^\perp , observamos que $\{\mathbb{T}_2(\partial_2 f)\}_{f \in F}$ es una base para W_1 . De manera muy parecida al caso anterior, obtenemos que $W_1^\perp = \mathbb{T}_1(\text{Ker } \delta_2)$.

Ahora sólo falta verificar que $W_1 \subset W_2^\perp$ y $W_2 \subset W_1^\perp$ para que nuestra elección de subespacios esté bien definida. Recordemos que

$$\text{Im } \partial_2 \subset \text{Ker } \partial_1 \quad \text{Im } \delta_1 \subset \text{Ker } \delta_2$$

y que T_i son homomorfismos, por lo que las contenciones se conservan al aplicarlos, de donde se sigue el resultado que queríamos.

Notemos que la dimensión del código $k = \dim(W_2^\perp/W_1)$ la podemos calcular como

$$k = \text{rango}[\text{Ker } \partial_1 / \text{Im } \partial_2] = 2g$$

Observemos que $\text{rango}[\text{Ker } \partial_1 / \text{Im } \partial_2]$, visto como subgrupo de $\Delta_1(\Xi)$, no depende de Ξ sino del género g de la superficie \mathbf{P} donde esté inmersa, la cual es la misma superficie donde está inmersa Ξ^* , por lo que la relación que construimos entre los grupos $\Delta^i(\Xi, G)$ y $\Delta_j(\Xi^*)$ nos dice que

$$\text{rango}[\text{Ker } \delta_2 / \text{Im } \delta_1] = \text{rango}[\text{Ker } \partial_1 / \text{Im } \partial_2]$$

lo cual indica que podemos intercambiar los índices i de los subespacios W_i . Este intercambio equivale a trabajar con Ξ^* en vez de Ξ .

Notemos también que la distancia mínima d , la podemos interpretar como la mínima longitud de un elemento no trivial en

$$\text{Ker } \partial_1 / \text{Im } \partial_2 \quad \text{y} \quad \text{Ker } \delta_2 / \text{Im } \delta_1$$

los cuales corresponden geoméricamente al ciclo más pequeño que no sea un camino frontera de $\Xi \rightarrow \mathbf{P}$ y al ciclo más pequeño que no sea un camino frontera de $\Xi^* \rightarrow \mathbf{P}$ respectivamente.

Estas dos interpretaciones geométricas de los parámetros k y d , nos dicen que para construir un buen código \mathcal{C} necesitamos construir una inmersión $\Xi \rightarrow \mathbf{P}$ tal que \mathbf{P} tenga un género grande (para aumentar la dimensión k), mientras que $\Xi \rightarrow \mathbf{P}$ y $\Xi^* \rightarrow \mathbf{P}$ tengan ciclos que no sean caminos frontera lo más grande posible (para aumentar la distancia mínima d), y conservando el número de aristas de Ξ lo más cercano posible a $2g$ (para que la longitud $n = |E|$ del código sea lo más cercana a k).

Notemos que estos tres propósitos para construir a \mathcal{C} están en discordancia mutua, porque para obtener una gráfica inmersa en una superficie de género grande al mismo tiempo que sus ciclos que no sean caminos frontera sean muy largos, se necesitan muchas aristas.

Sin entrar en detalles ni apartarnos del propósito matemático de este trabajo, mencionamos que el sistema de partículas que se construye para poder utilizar los **Códigos de Superficies** consiste en asignar una partícula a cada arista. Para una descripción más detallada el lector puede referirse a [12, 8, 3].

Capítulo 3

Incrustando Gráficas

3.1. Requisitos

Siguiendo los pasos del capítulo anterior, la construcción de espacios vectoriales W_1, W_2 que funcionen para determinar un **código cuántico** \mathcal{C} es equivalente a construir gráficas $\Xi \rightarrow \mathbb{T}_g$, teniendo en cuenta que $|E|$ es la **longitud** del código, $2g$ es la **dimensión**, y la **distancia mínima** está determinada por el ciclo más pequeño que no sea el camino frontera de una región tanto en $\Xi \rightarrow \mathbb{T}_g$ como en $\Xi^* \rightarrow \mathbb{T}_g$.

Visto de esta manera, el objetivo es construir gráficas $\Xi \rightarrow \mathbb{T}_g$ tales que $|E|$ sea lo más cercano posible a $2g$, mientras que los ciclos que no son el camino frontera de una región tanto en $\Xi \rightarrow \mathbb{T}_g$ como en $\Xi^* \rightarrow \mathbb{T}_g$ sean lo más grande posible. El reto es que la realización de estos dos objetivos es opuesta, ya que para tener ciclos grandes se necesitan muchas aristas, y para mantener a $|E|$ lo más cercano posible a $2g$ se necesitan pocas aristas.

Pensemos en el ejemplo de la Figura 2.6, donde hay exactamente $2g$ aristas pero el ciclo más pequeño que no es un camino frontera tanto en $\Xi \rightarrow \mathbb{T}_g$ como en su dual, es el recorrido sobre cualquier arista y tiene longitud 1.

Debido a que los parámetros del código \mathcal{C} no sólo dependen de Ξ sino también del género de la superficie donde está inmersa, el método que se desarrollará para la construcción de una gráfica $\Xi \rightarrow \mathbf{P}$ será el de hacer 'crecer' a una gráfica $\Theta \rightarrow \mathbf{Q}$ donde Θ tiene menos vértices y aristas que Ξ , y el género de \mathbf{Q} es menor al de \mathbf{P} .

3.2. Semillas

Para hacer 'crecer' a una gráfica $\Theta \rightarrow \mathbf{P}$ vamos a utilizar un grupo finito G que por ahora y hasta el final de esta sección se va a considerar abeliano. La idea es asignarle valores del grupo G a las aristas de Θ para que las adyacencias en Ξ conserven la información de las adyacencias en Θ al igual que las relaciones entre los elementos del grupo G , y que las regiones de \mathbf{P} correspondan a regiones en \mathbf{Q} .

Teniendo en cuenta que $\Xi \rightarrow \mathbf{P}$ se va a obtener de $\Theta \rightarrow \mathbf{Q}$ mediante una asignación de elementos del grupo G a las aristas de Θ , vamos a escribir a Ξ como Θ^a donde a es la asignación de elementos en G a las aristas de Θ , y a \mathbf{P} como \mathbf{Q}^a .

Intuitivamente se puede pensar que la gráfica $\Theta \rightarrow \mathbf{Q}$ es una semilla Θ dentro de una maceta \mathbf{Q} que se riega con el agua de un grupo G para que crezca una planta Θ^a en una maceta \mathbf{Q}^a . Otra manera de pensarlo es que la gráfica $\Theta \rightarrow \mathbf{Q}$ es una representación de voltajes de elementos de G en el diagrama de un circuito Θ inmerso en una superficie \mathbf{Q} . Esta metáfora de voltajes se debe a quien originalmente desarrolló esta construcción [9] y por eso a la gráfica $\Theta \rightarrow \mathbf{Q}$ se le llama **gráfica de voltaje** Θ inmersa en \mathbf{Q} y a Θ^a se le dice el **levantamiento** de la gráfica de voltaje.

Antes de especificar la construcción de $\Theta^a \rightarrow \mathbf{Q}^a$, se va explicar sólo la construcción de Θ^a sin explicar los detalles de la inmersión en \mathbf{Q}^a . Para que la información de las relaciones de G quede descrita en Θ^a , el conjunto de aristas E^a de Θ^a se define como el conjunto $E \times G$ y el conjunto de vértices V^a como $V \times G$. Además de asignarle a cada arista q de Θ un elemento $a(q) = g \in G$, también se le asigna una dirección $+$ o $-$ para que si la arista $q^+ \in E$ tiene la dirección positiva del vértice v al vértice u , entonces la arista \hat{q}_l^+ de Θ^a , tenga la dirección positiva de sus vértices \hat{v}_l a \hat{u}_{lg} con $l \in G$.

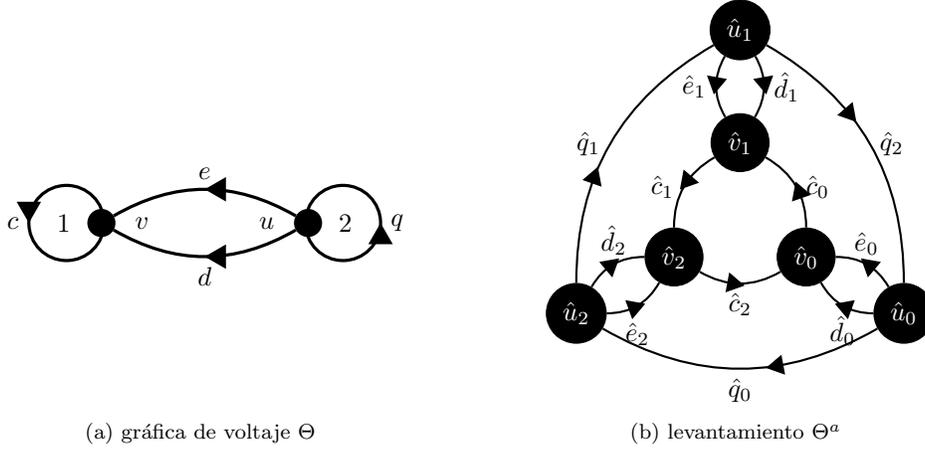


Figure 3.1: Ejemplo de una gráfica de voltaje Θ y su levantamiento Θ^a
(a) :: (b)

Veamos un ejemplo para $G = (\mathbb{Z}_3, +)$ con voltajes $a(q) = 2$, $a(c) = 1$ y $a(e) = a(d) = 0$ como en la Figura 3.1(a). Decimos que para cada vértice $v \in \Theta$ el conjunto de vértices $\hat{v}_g \in V^a$ para cada $g \in G$ es la fibra sobre v , y que para cada arista $q \in \Theta$ el conjunto de aristas $\hat{q}_g \in E^a$ para cada $g \in G$ es la fibra sobre q .

Una propiedad que nos interesa en la construcción de Θ^a , es que los ciclos en Θ correspondan a ciclos en Θ^a conservando sus orientaciones. Esto se puede expresar en el ejemplo observando que si se recorre la figura 3.1(a) por el camino $[c, d^-, q^-]$, los posibles caminos que le correspondan sean $[\hat{c}_1, \hat{d}_2^-, \hat{q}_0^-]$, $[\hat{c}_2, \hat{d}_0^-, \hat{q}_2^-]$ o $[\hat{c}_0, \hat{d}_1^-, \hat{q}_1^-]$.

Para expresar este hecho en general, definimos que a un camino $\mathbf{c} = [q_1^{\sigma_1}, \dots, q_m^{\sigma_m}]$ en Θ le corresponde un camino $\hat{\mathbf{c}} = [\hat{q}_1^{\sigma_1}, \dots, \hat{q}_m^{\sigma_m}]$ en Θ^a , donde cada \hat{q}_i está en la fibra de q_i y observamos que si el camino \mathbf{c} empezó en el vértice v , entonces para cada vértice \hat{v}_g en la fibra de v hay un único camino $\hat{\mathbf{c}}$ que empieza en \hat{v}_g .

De esta manera nos podemos referir a un camino $\hat{\mathbf{c}}$ en Θ^a indicando el vértice \hat{v}_g donde empieza porque sabemos que este camino es único. Decimos que el camino $\hat{\mathbf{c}}_g$ es el camino que le corresponde a \mathbf{c} empezando por el vértice \hat{v}_g .

También podemos saber en qué vértice termina el camino $\hat{\mathbf{c}}_g$ si sabemos que \mathbf{c} termina en el vértice u . Para esto se multiplican todos los valores $a(q_i) \in G$ asignados a las m aristas del camino \mathbf{c} con la convención de que $a(q^{-1}) = [a(q)]^{-1}$ y la multiplicación es la operación del grupo G . Ahora supongamos que $l_i = a(q_i^{\sigma_i})$ para cada $q_i^{\sigma_i}$ en el camino \mathbf{c} y que el **voltaje neto** \mathbf{v} es el producto de todas las l_i , entonces el camino $\hat{\mathbf{c}}_g$ tiene sus vértices etiquetados sucesivamente por $g, g \cdot l_1, \dots, g \cdot l_1 \cdot \dots \cdot l_m = g \cdot \mathbf{v}$, por lo tanto su último vértice es $\hat{u}_{g\mathbf{v}}$ y su longitud es m .

Estas propiedades de los caminos nos permiten estudiar los ciclos de Θ^a para poder definir la inmersión del levantamiento de $\Theta \rightarrow \mathbf{Q}$ a partir de sus caminos frontera.

Con este fin en mente, vamos a ver qué ciclos le corresponden a Θ^a partiendo de un ciclo en Θ . Supongamos que \mathbf{k} es un ciclo cuyo vértice de partida es v , que tiene longitud m y que la multiplicación de todos los valores asignados a sus aristas da un valor $l \in G$ de orden t . Para ver qué caminos le corresponden a $\hat{\mathbf{k}}_g$ en Θ^a fijemos un vértice v_g sobre la fibra de v , entonces al recorrer una vez el ciclo \mathbf{k} en Θ se recorre el camino $\hat{\mathbf{c}}_g$ en Θ^a de longitud m cuyo vértice final es v_{gl} . Como $l^t = 1$, el ciclo \mathbf{k} se tiene que recorrer un total de t veces formando los caminos sucesivos $\hat{\mathbf{c}}_g, \hat{\mathbf{c}}_{gl}, \dots, \hat{\mathbf{c}}_{gl^{t-1}}$ para que el último camino tenga un vértice final con subíndice $gl^{t-1} \cdot l = gl^t = g$. El ciclo $\hat{\mathbf{k}}_g$ formado por los caminos $\hat{\mathbf{c}}_{gl^i}$ es el levantamiento del ciclo \mathbf{k} . Debido a que cada uno de los caminos $\hat{\mathbf{c}}_{gl^i}$ tienen longitud m , y se recorrieron t caminos, el ciclo $\hat{\mathbf{k}}_g$ tiene longitud mt .

Para saber cuántos ciclos distintos $\hat{\mathbf{k}}_g$ hay en Θ^a , basta escoger un elemento g por cada una de las distintas clases de equivalencia de G/l , de las cuales hay $|G|/t$.

Estas propiedades de los ciclos entre la gráfica de voltaje y su levantamiento, motivan la inmersión de Θ^a en una

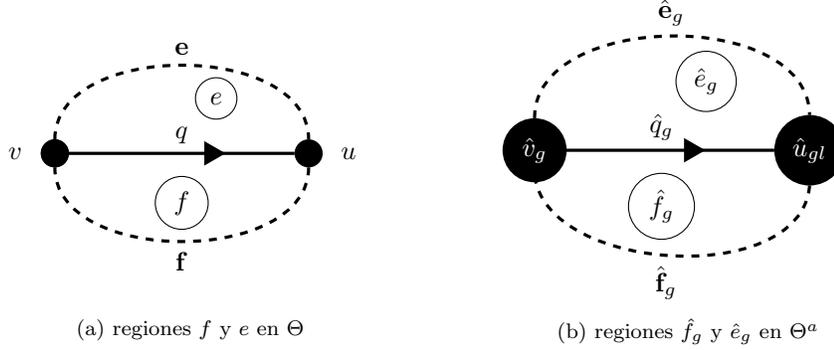


Figure 3.2: regiones vecinas en Θ corresponden a regiones vecinas en Θ^a
(a) :: (b)

superficie \mathbf{Q}^a definida por los caminos frontera de $\Theta \rightarrow \mathbf{Q}$.

Decimos que un camino frontera \mathbf{c} de $\Theta \rightarrow \mathbf{Q}$ con una sucesión de aristas $[q_1^{\sigma_1}, \dots, q_m^{\sigma_m}]$ cuyo vértice inicial es v , se levanta en un camino frontera $\hat{\mathbf{c}}_g = [\hat{q}_1^{\sigma_1}, \dots, \hat{q}_m^{\sigma_m}]$ cuyo vértice inicial es v_g y cada \hat{q}_i está en la fibra de q_i . Sabemos que si la multiplicación de todos los valores asignados a las aristas de \mathbf{c} es l , y l tiene orden t en el grupo G , entonces hay $|G|/t$ caminos frontera $\hat{\mathbf{c}}_{\bar{g}}$, uno para cada clase de equivalencia $\bar{g} \in Gl$.

Si todos los caminos frontera de $\Theta \rightarrow \mathbf{Q}$ se levantan por separado, se obtienen regiones poligonales \hat{f}_i cuyas aristas están repetidas sólo una vez en algún \hat{f}_j para $i \neq j$. Esto se deduce observando que una arista q con voltaje l en $\Theta \rightarrow \mathbf{Q}$ tiene sólo dos regiones vecinas f y e con caminos frontera \mathbf{f} y \mathbf{e} , digamos que con voltaje neto l_f y l_e como se muestra en la figura 3.2(a). Entonces los levantamientos $\hat{\mathbf{f}}_g$ y $\hat{\mathbf{e}}_g$ para un elemento $g \in G$ comparten la arista \hat{q}_g como en la figura 3.2(b). Como sabemos que los caminos frontera $\hat{\mathbf{f}}_g$ y $\hat{\mathbf{e}}_g$ son únicos para cada clase de equivalencia en Gl_f y Gl_e respectivamente, cualquier otro camino $\hat{\mathbf{e}}_r$ con $r \in G$ que tenga a la arista \hat{q}_g , es el camino frontera $\hat{\mathbf{e}}_g$. Razonando de manera similar para $\hat{\mathbf{f}}_g$ se tiene que la arista q_g sólo se repite una vez en las regiones \hat{f}_i . Construimos a la superficie cerrada \mathbf{Q}^a pegando a todas las regiones \hat{f}_i sobre las aristas que tengan en común. Este pegado de caras es en realidad una superficie cerrada porque todas las regiones se pegan entre ellas y ninguna se pega en más de dos caras, más aun el pegado contiene a todos los vértices y aristas de Θ^a porque cada vértice y arista de $\Theta \rightarrow \mathbf{Q}$ está en algún camino frontera \mathbf{c}_f de una región f .

Este pegado es una inmersión $\Theta^a \rightarrow \mathbf{Q}^a$.

Como ya fue mencionado en el capítulo anterior, las superficies que nos interesan son superficies orientables \mathbb{T}_g . Por este motivo nos interesan las superficies $\mathbf{Q}^a = \mathbb{T}_g$, que son el levantamiento de $\mathbf{Q} = \mathbb{T}_h$ para una $h < g$.

Partiendo de la definición de las regiones \hat{f}_i como levantamientos de caminos frontera en Θ , vemos que cada región \hat{f}_i con $i \in G$, recibe una orientación inducida por la región f cuyo levantamiento de su camino frontera define la región \hat{f}_i . De aquí deducimos que el pegado de las regiones \hat{f}_i conservan esta orientación y la superficie \mathbf{Q}^a es orientable.

De ahora en adelante vamos a tomar a G como un grupo cuya operación es la suma, su elemento neutro es 0 y $|G| = \Omega$.

Para saber el género g de $\mathbf{Q}^a = \mathbb{T}_g$ vamos a forzar que los voltajes netos de todas las regiones en $\Theta \rightarrow \mathbb{T}_h$ tengan orden 1, para que cada región se levante en $|G|/1 = \Omega$ regiones y de esta manera concluir que

$$2 - 2g = |V^a| - |E^a| + |F^a| = |V \times G| - |E \times G| + \Omega|F| = \Omega|V| - \Omega|E| + \Omega|F| = \Omega(2 - 2h)$$

$$g = \Omega(h - 1) + 1$$

Para ver un ejemplo, consideremos la gráfica $\Theta \rightarrow \mathbb{T}_2$ como en la figura 3.3(a) con voltajes $l_i \in G$, donde las aristas están distinguidas por colores en vez de letras y los vértices en Θ^a están indicados por sus subíndices.

La única región de Θ se levanta como el polígono en la figura 3.3(b), donde las flechas indican la dirección en la

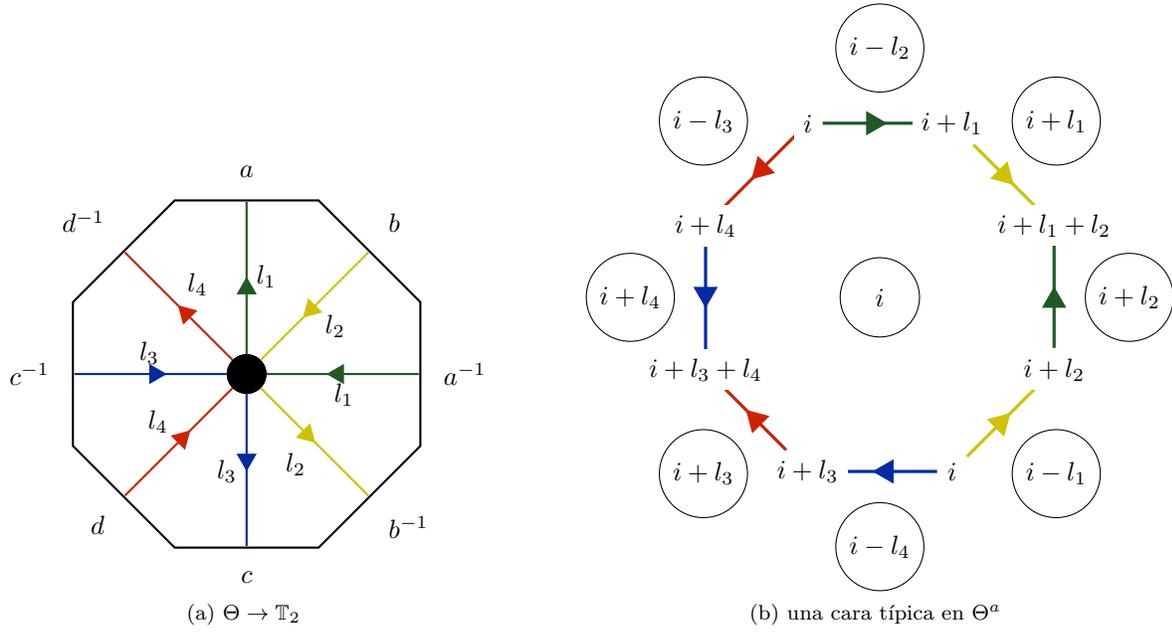


Figure 3.3
(a) :: (b)

que se recorrió la arista sobre el camino frontera de Θ y las regiones vecinas están representadas por círculos etiquetados por dentro. También podemos apreciar como no importa qué voltajes l_i le asignemos a cada arista porque la suma de ellos sobre el camino frontera siempre da 0. En nuestro ejemplo vamos a fijar $G = (\mathbb{Z}_{12}, +)$ con los voltajes $l_1 = 1$, $l_2 = 2$, $l_3 = 4$ y $l_4 = 3$. Para pegar las $\Omega = 12$ regiones de Θ^a procedemos como en la Figura 3.4, pegando primero las regiones 10, 7, 4 y 1, indicando por un punto gris dentro de un punto negro la parte del diagrama que no corresponde a ninguna región. Luego en cada región 10, 7, 4, 1 se une el vértice 1, 10, 7, 4 respectivamente, los cuales están repetidos, dejando un hueco dentro de cada región de este diagrama bidimensional. A continuación se le pegan las regiones 9, 6, 3 y 0 a las regiones 10, 7, 4 y 1 respectivamente, habiendo antes unido los vértices 9, 6, 3, 0 en las regiones 9, 6, 3 y 0 respectivamente.

Finalmente se pegan las regiones 11, 5, 8 y 2 a las regiones 9, 6, 3 y 0 respectivamente como lo muestra la figura 3.5, donde previamente se unieron los vértices i en las regiones $i = 11, 5, 8, 2$. Como el diagrama de la figura 5 es una representación bidimensional de un objeto tridimensional, todavía falta pegar varias aristas, aunque representar esto en un diagrama bidimensional resultaría en varios cruces de aristas. Aún así podemos ver que la fórmula para calcular el género de $\mathbf{Q}^a = \mathbb{T}_g$ nos dice que

$$g = \Omega(h - 1) + 1 = 12 \cdot (2 - 1) + 1 = 13$$

lo que en nuestro diagrama corresponde a los 13 huecos que en la superficie completamente pegada $\mathbf{Q}^a = \mathbb{T}_{13}$, corresponden a 13 generadores de los 26 que hay.

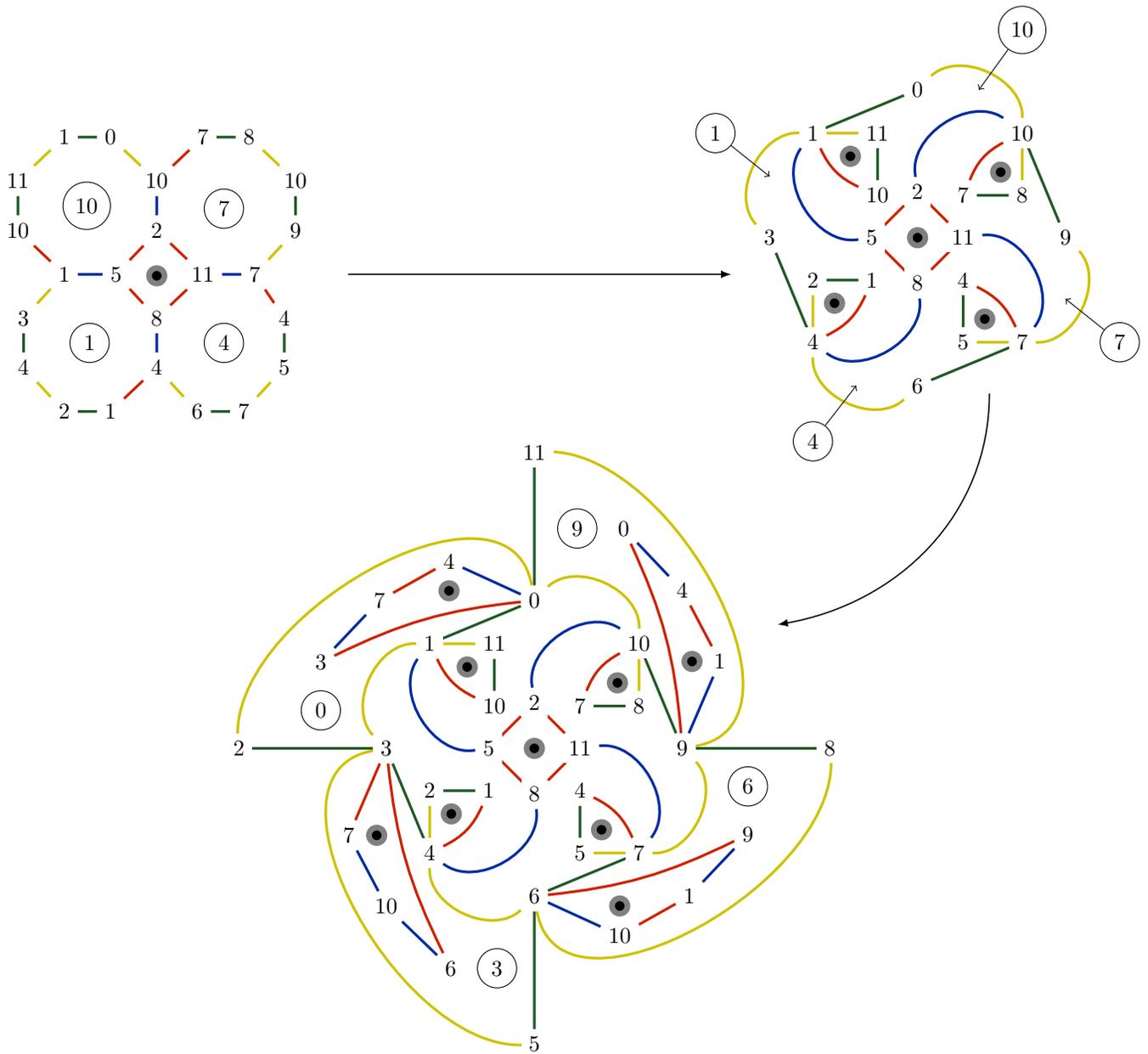


Figure 3.4: Pegando regiones

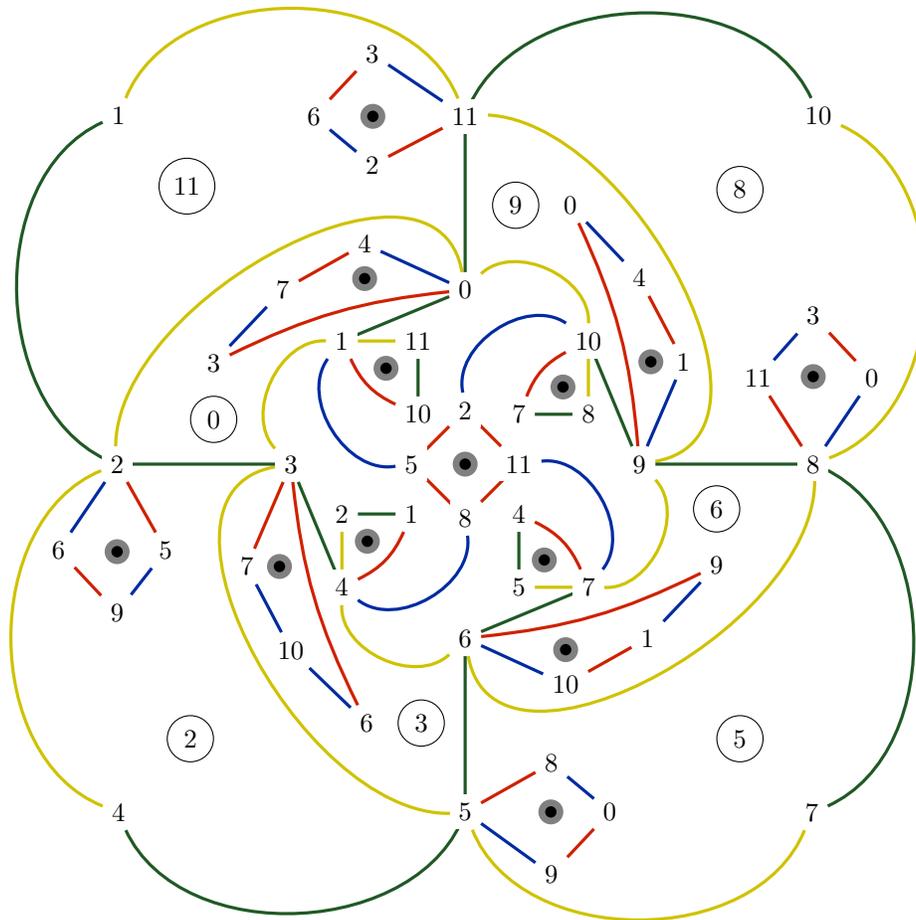


Figure 3.5: Diagrama de $\Theta^a \rightarrow \mathbf{Q}^a$

3.3. Diseño de semillas

Motivados por la propiedad de que las gráficas de voltaje 'crecen' cual semillas con todo y maceta, el objetivo de esta sección es diseñar toda una familia de códigos cuánticos como los construidos en el capítulo anterior, con dimensión arbitraria y la mejor distancia mínima posible.

Esto se llevará a cabo en tres pasos. El primer paso será construir el levantamiento de una gráfica $\Theta \rightarrow \mathbf{Q}$ justificando la elección de \mathbf{Q} , Θ y G para que el código W_1 generado por la gráfica $\Theta^a \rightarrow \mathbf{Q}^a$ tenga la mayor dimensión y distancia mínima posible manteniendo la longitud del código lo más cercano a su dimensión. El segundo paso será verificar que el código W_2 generado por el dual de $\Theta^a \rightarrow \mathbf{Q}^a$ denotado por $[\Theta^a]^* \rightarrow \mathbf{Q}^a$, tiene la misma distancia mínima. Por último se generalizará la construcción para dimensiones arbitrarias del código W .

3.3.1. Paso 1 :: \mathbf{Q} , Θ y G

Para elegir la superficie orientable \mathbf{Q} vamos a observar que si tomamos $\mathbf{Q} = \mathbb{S}^2, \mathbb{T}_1$ entonces para cualquier gráfica $\Theta \rightarrow \mathbf{Q}$ cuyos voltajes netos sobre cada camino frontera tengan orden 1 para cualquier grupo G , el género g de la superficie \mathbf{Q}^a es igual que el género de \mathbf{Q} . Con la ayuda de la fórmula para calcular g a partir del género de \mathbf{Q} tenemos

$$g = \Omega(0 - 1) + 1 = 1 - \Omega \quad \text{para } \mathbf{Q} = \mathbb{S}^2$$

$$g = \Omega(1 - 1) + 1 = 1 \quad \text{para } \mathbf{Q} = \mathbb{T}_1$$

Observando que el género siempre es positivo, el primer caso no tiene sentido mas que para un grupo trivial, regresando a \mathbb{S}^2 como la superficie \mathbf{Q}^a . En el segundo caso observamos que no importa el orden del grupo, la superficie \mathbf{Q}^a siempre es \mathbb{T}_1 .

Aunque el género de \mathbf{Q}^a no crece con respecto al género de \mathbf{Q} para estas dos superficies, veamos que para $\mathbf{Q} = \mathbb{T}_h$ con $h \geq 2$ se tiene

$$g = \Omega(h - 1) + 1 \geq \Omega(2 - 1) + 1 = \Omega + 1 > h \quad \text{si } \Omega > h - 1$$

por lo tanto, para diseñar un primer código basta con tomar $h = 2$ y $\Omega > 1$, es decir tomar $\mathbf{Q} = \mathbb{T}_2$ y G un grupo que no sea trivial.

Con el objetivo de mantener la longitud del código lo más apegado a su dimensión, es necesario que $\Theta \rightarrow \mathbf{Q}$ tenga la menor cantidad de aristas posible. Esto se debe a que si tenemos dos gráficas Θ_1 y Θ_2 inmersas en una misma superficie \mathbf{Q} tales que $|E_1| < |E_2|$, entonces sus respectivos $\Theta_i^a \rightarrow \mathbf{Q}^a$ levantamientos con el mismo grupo G dan códigos con longitudes n_i conservando la relación

$$n_1 = \Omega|E_1| < \Omega|E_2| = n_2$$

Mientras que el género g de \mathbf{Q} determina las dimensiones del código como $2g$ para ambas gráficas.

Esto sugiere usar la gráfica $\Theta \rightarrow \mathbb{T}_2$ como en la figura 3.3(a) donde la orientación de cada arista fue arbitraria.

La elección del grupo G va a estar sujeta a la propiedad de que no importa qué grupo abeliano G se utilice para asignar voltajes a las aristas de Θ , en la gráfica Θ^a siempre hay ciclos de longitud 4 como se muestra en la Figura 3.6 para los voltajes asignados $a(q) = l_1, a(s) = l_2$ donde q y s son cualesquiera dos aristas distintas en Θ . Esta propiedad

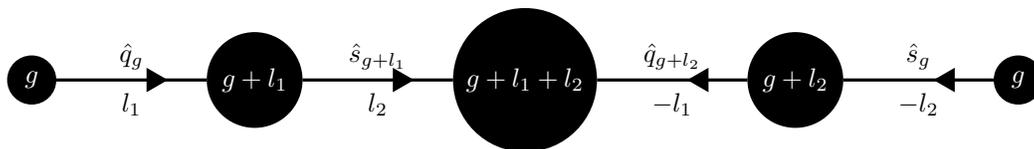


Figure 3.6: ciclo de longitud 4 en Θ^a para un grupo G abeliano

de los ciclos en $\Theta^a \rightarrow \mathbb{T}_g$ para cualquier grupo G abeliano, afecta directamente la distancia mínima del código W , ya que a lo más la distancia mínima es 4.

Una posible manera para que la distancia mínima no sea 4, es que todos los ciclos de longitud 4 sean caminos frontera de la gráfica $\Theta^a \rightarrow \mathbf{Q}^a$, resultando en una cuadrícula de la superficie $\mathbf{Q}^a = \mathbb{T}_g$ como los códigos originales de Kitaev [12].

Más allá de construir gráficas motivados por la ociosidad, las gráficas que cuadrícula a las superficies \mathbb{T}_g tienen muchas más aristas que las gráficas obtenidas por el levantamiento de la gráfica que se escogió para levantar. Esto se puede ver calculando los parámetros $[[n, k, d]]$ de los códigos obtenidos por el levantamiento $\Theta^a \rightarrow \mathbb{T}_g$ de la gráfica que escogimos y el de una gráfica cuadrícula de \mathbb{T}_g . Para el código obtenido de la gráfica $\Theta^a \rightarrow \mathbb{T}_g$, tomando en cuenta que la distancia mínima a lo más es 4, se tiene:

$$\begin{aligned} n &= |E^a| = \Omega|E| = \Omega \cdot 4 \\ g &= \Omega(2 - 1) + 1 = \Omega + 1 \Rightarrow k = 2(\Omega + 1) \\ d &= 4 \end{aligned}$$

Mientras que para el código obtenido de una cuadrícula para \mathbb{T}_g , donde $g = \Omega + 1$ y d es su distancia mínima, se tiene:

$$\begin{aligned} n &= 2(\Omega + 1) \cdot d^2 \\ k &= 2(\Omega + 1) \end{aligned}$$

Si fijamos su distancia mínima como $d = 4$, al comparar la longitud de los dos códigos se tiene

$$2(\Omega + 1) \cdot 4^2 > \Omega \cdot 4$$

aunque para esto se pague el precio reducir la distancia mínima a una distancia mínima constante $d = 4$.

Otra solución para que la distancia mínima de $\Theta^a \rightarrow \mathbb{T}_g$ no siempre sea 4, es escoger al grupo G con el que se levantó de manera que no sea abeliano para que no se generen los ciclos como los de la figura 3.6.

Por esta propiedad, el objetivo para diseñar al grupo G es que el ciclo más pequeño en $\Theta^a \rightarrow \mathbb{T}_g$ sea de longitud 4 y que el orden Ω no sea más grande de lo que deba ser para que se cumpla este propósito y así optimizar la dimensión del código W con respecto a su longitud.

Con este fin en mente, primero vamos a enlistar en la figura 3.7 todos los ciclos \hat{c} de longitud 3 que podría haber salvo permutaciones, teniendo en cuenta que cada vértice en la gráfica $\Theta^a \rightarrow \mathbb{T}_g$ es adyacente a sólo dos aristas \hat{q}^+ y \hat{q}^- en la fibra de una arista q de Θ .

Para asegurar que no se puedan formar estos ciclos, basta comprobar que el voltaje neto $v(\hat{c})$ de cada uno de los ciclos en la figura 3.7 no sea 0. Debido a que nos interesa construir un grupo abeliano y finito, podemos suponer que $G = (\mathbb{Z}_\Omega, +)$, de esta manera pensemos que todos los voltajes l_i están etiquetados de forma que $0 < l_i < l_{i+1} < \Omega$, y llamemos L al voltaje más grande.

Para que $v(\hat{c}) \neq 0$ en el inciso (a) de la figura 3.7, podemos forzar la restricción $3L < \Omega$ para tener

$$0 < \underbrace{3l_i}_{v(\hat{c})} \leq 3L < \Omega$$

y asegurar que $v(\hat{c})$ no sea cero.

Para el inciso (b) observemos que para toda $1 \leq i, j \leq 4$, imponiendo la condición $3L < \Omega$ se tiene

$$0 < \underbrace{2l_i + l_j}_{v(\hat{c})} < 3L < \Omega$$

por lo que deducimos que $v(\hat{c}) \neq 0$ para este ciclo también.

Para ver que el inciso (c) tampoco existe, basta con notar que por haber tomado $i \neq j \neq k \neq i$ se cumple que el valor neto de los voltajes es menor a $3L$ y de esta manera escribir

$$0 < \underbrace{l_i + l_j + l_k}_{v(\hat{c})} < 3L < \Omega$$

concluyendo que su voltaje neto no puede ser 0.

Para el inciso (d) observamos que debido a que $0 < 2l_i < 3L < \Omega$ y a que $0 < l_j < \Omega$, la condición

$$2l_i - l_j \equiv 0 \pmod{\Omega} \Leftrightarrow 2l_i \equiv l_j \pmod{\Omega} \Leftrightarrow 2l_i = l_j \text{ en } \mathbb{Z}$$

impone una nueva condición para los voltajes l_i , es decir, no se quiere que $2l_i = l_j$ para cuales quiera voltajes l_i y l_j .

Para el último ciclo en la figura 3.7 pensemos que debido a que $0 < l_i + l_j < 3L < \Omega$ y a que $0 < l_k < \Omega$ la condición

$$l_i + l_j - l_k \equiv 0 \Leftrightarrow l_i + l_j \equiv l_k \Leftrightarrow l_i + l_j = l_k \text{ en } \mathbb{Z}$$

impone una última restricción sobre los voltajes l_i, l_j, l_k ; que ningún voltaje l_k sea la suma de otros dos voltajes l_i, l_j .

Para ver que tampoco hay ciclos de longitud 2, veamos los posibles ciclos que se podrían formar, salvo permutaciones, en la figura 3.8.

Para los incisos (a) y (b) de la figura 3.8, observemos respectivamente que

$$0 < \underbrace{2l_i}_{v(\hat{c})} < \Omega \quad 0 < \underbrace{l_i + l_j}_{v(\hat{c})} < 2L < \Omega$$

de donde se deduce que estos ciclos no existen ya que el voltaje neto de ambos ciclos no es 0.

Para el inciso (c) observemos que como $0 < l_i, l_j < \Omega$ para $1 \leq i, j \leq 4$ entonces se tiene

$$l_i - l_j \equiv 0 \Leftrightarrow l_i \equiv l_j \Leftrightarrow l_i = l_j \text{ en } \mathbb{Z}$$

de donde la última igualdad no es posible por haber escogido $i \neq j$.

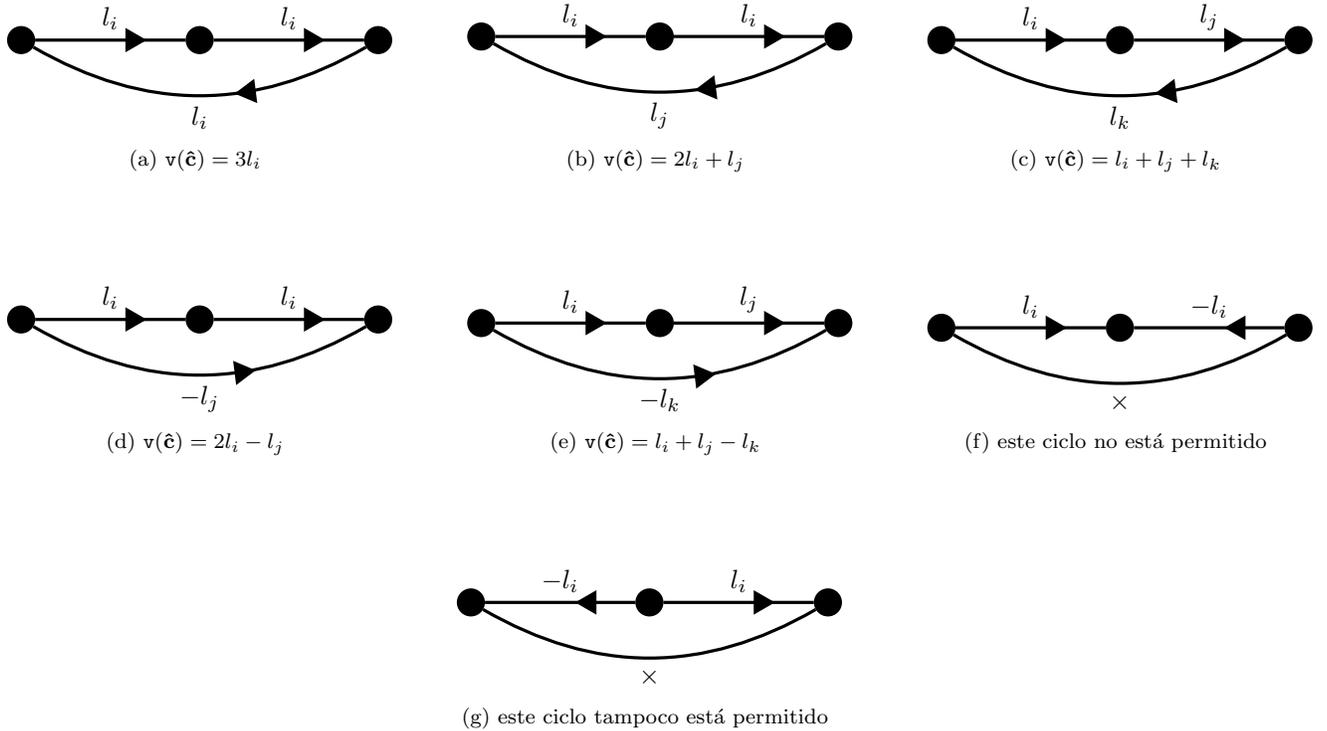


Figure 3.7: posibles e imposibles ciclos \hat{c} de longitud 3 con voltaje neto $v(\hat{c})$ en $\Theta^a \rightarrow \mathbb{T}_g$, donde $1 \leq i, j, k \leq 4$ y $i \neq j \neq k \neq i$

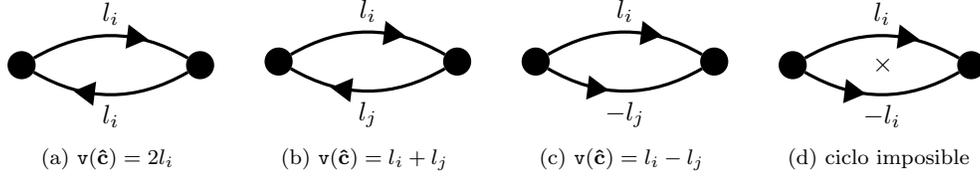


Figure 3.8: posibles e imposibles ciclos \hat{c} de longitud 2 con voltaje neto $v(\hat{c})$ en $\Theta^a \rightarrow \mathbb{T}_g$, donde $1 \leq i, j \leq 4$ y $i \neq j$

Ahora que ya hemos descartado los ciclos de longitud 3 y 2, sólo falta notar que no puede haber ciclos de longitud 1 en $\Theta^a \rightarrow \mathbb{T}_g$ porque no hay voltajes 0 en $\Theta \rightarrow \mathbb{T}_2$, y de este modo concluir que los ciclos más pequeños que hay en $\Theta^a \rightarrow \mathbb{T}_g$ son de longitud 4.

Por último resumimos que la gráfica $\Theta \rightarrow \mathbb{T}_2$ como en la figura 3.3(a) con los voltajes l_i que cumplan las restricciones

$$\begin{aligned} 3l_i &< \Omega \\ 2l_i &\neq l_j \\ l_k &\neq l_i + l_j \end{aligned} \quad (3.1)$$

en el grupo \mathbb{Z}_Ω donde $\Omega > 3L$, se levanta en una gráfica $\Theta^a \rightarrow \mathbb{T}_g$, donde debido a que el único camino frontera de $\Theta \rightarrow \mathbb{T}_2$ tiene voltaje neto 0, se da que $|F^a| = |E^a| = |V^a| = \Omega \cdot 4$ y así el género de \mathbb{T}_g cumple $g = \Omega(2 - 1) + 1 = \Omega + 1$.

3.3.2. Paso 2 :: el Dual

Para el segundo paso, vamos a construir el dual $[\Theta^a]^* \rightarrow \mathbb{T}_g$ de $\Theta^a \rightarrow \mathbb{T}_g$ recordando que las regiones del dual corresponden a los vértices de $\Theta^a \rightarrow \mathbb{T}_g$ donde las adyacencias entre ellos corresponden a las adyacencias entre las regiones de $[\Theta^a]^* \rightarrow \mathbb{T}_g$, es decir, cada región del dual se construye a partir de las estrellas de $\Theta^a \rightarrow \mathbb{T}_g$ y cada estrella del dual se construye a partir de las regiones de $\Theta^a \rightarrow \mathbb{T}_g$ como en la figura 3.9.

Es importante notar que las aristas del dual están representadas sin direcciones en la figura 3.9 porque aún no se ha visto que $[\Theta^a]^* \rightarrow \mathbb{T}_g$ sea el levantamiento de alguna gráfica.

Si observamos las adyacencias de las estrellas del dual, podemos ver que las dos aristas por cada color que tiene, tienen vértices extremos $i \pm l_j$, por ejemplo las dos aristas rojas tienen extremos $i + l_2$ y $i - l_2$. Si prestamos atención a las regiones del dual, vemos que la sucesión de vértices que tiene son muy parecidas a las regiones de la gráfica $\Theta^a \rightarrow \mathbb{T}_g$ y que la sucesión de aristas es igual respecto a los colores.

Aunque esto no demuestra nada, motiva construir una gráfica Φ inmersa en alguna superficie \mathbf{I} tal que con los voltajes adecuados en algún grupo G' tenga un levantamiento isomorfo a $[\Theta^a]^* \rightarrow \mathbb{T}_g$ para poder calcular la distancia mínima de sus ciclos apoyándose en la estructura del grupo G' como lo hicimos para $\Theta^a \rightarrow \mathbb{T}_g$.

La construcción en realidad va a ser una adivinanza y luego vamos a ver que esta adivinanza y $[\Theta^a]^* \rightarrow \mathbb{T}_g$ son la misma inmersión.

Tomemos $\Phi \rightarrow \mathbf{I}$ igual a $\Theta \rightarrow \mathbb{T}_2$ y $G' = \mathbb{Z}_\Omega$ con los voltajes l_i como en la figura 3.10(a). Entonces sabemos que la superficie \mathbf{I}^b del levantamiento de $\Phi \rightarrow \mathbf{I}$ es una superficie orientable $\mathbb{T}_{g'}$, que debido a que el camino frontera de la única región que hay en $\Phi \rightarrow \mathbb{T}_2$ tiene voltaje neto 0, hay exactamente Ω regiones en $\mathbb{T}_{g'}$ y podemos calcular el género g' por medio de

$$g' = \Omega(2 - 1) + 1 = \Omega + 1 = g$$

Más aun, podemos ver que una región i en $\Phi^b \rightarrow \mathbb{T}_g$ correspondiente a un camino frontera $\hat{\mathbf{k}}_i$, tiene una sucesión de aristas y vértices como en la figura 3.10(b), donde los vértices están representados por círculos etiquetados por dentro y las regiones adyacentes a la región i están representadas por su subíndice justo al lado de la arista que comparten con la región.

Ahora observamos que las regiones de $[\Theta^a]^* \rightarrow \mathbb{T}_g$ son iguales a las regiones de $\Phi^b \rightarrow \mathbb{T}_g$ sin considerar las direcciones del levantamiento, es decir, tienen la misma sucesión de vértices, aristas y adyacencias.

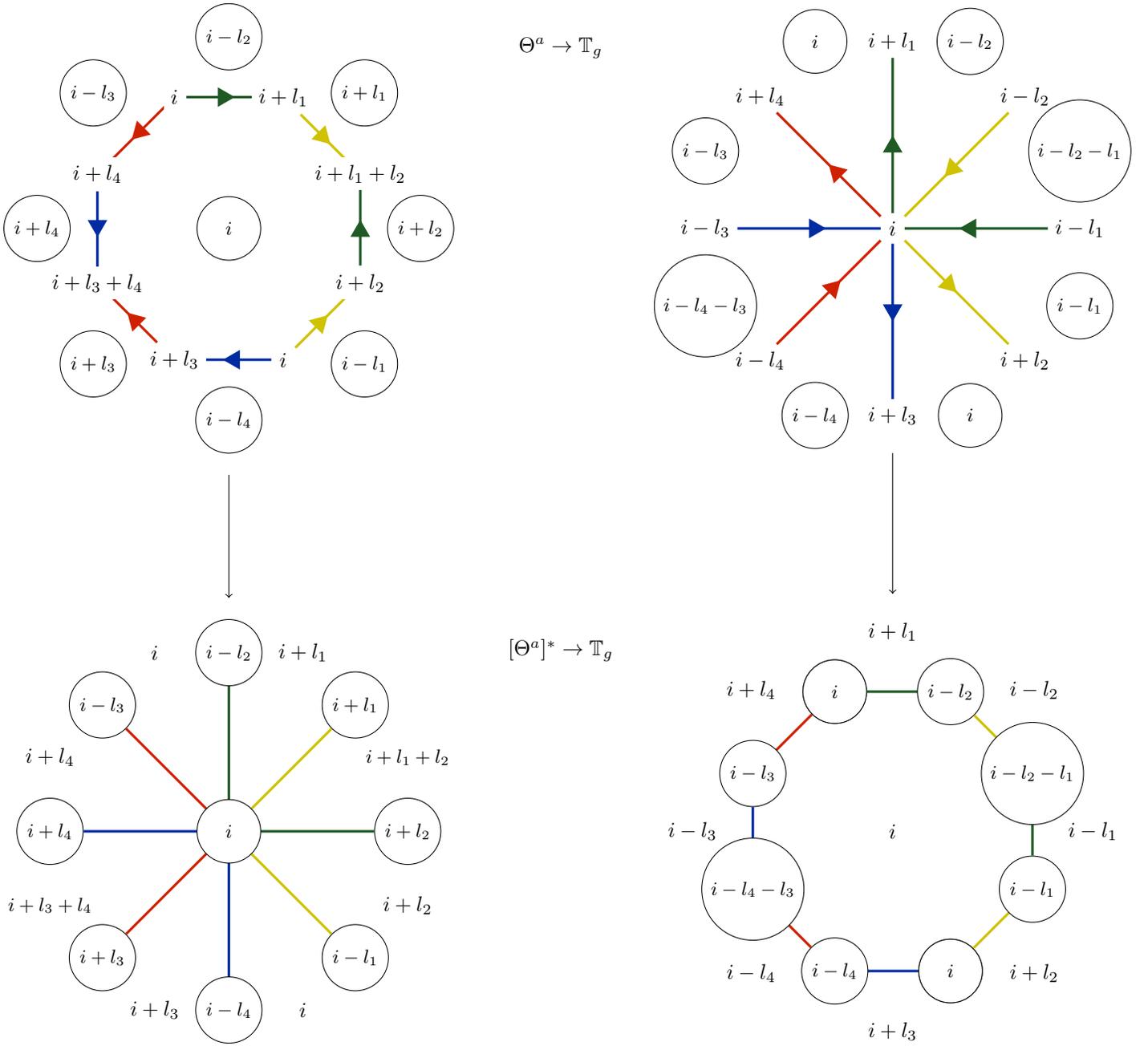
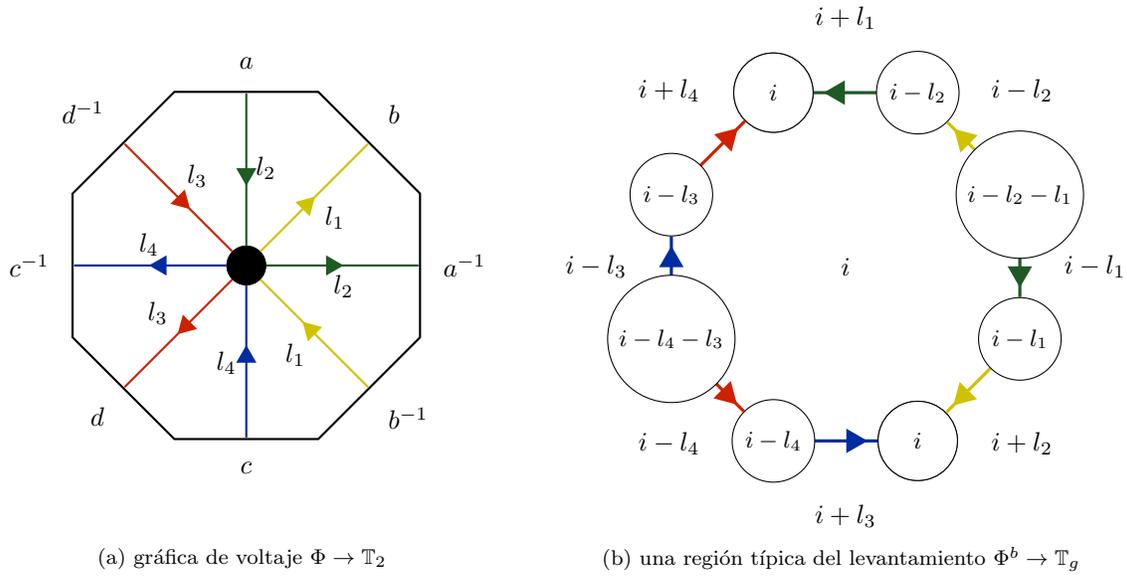


Figure 3.9: regiones y estrellas de $\Theta^a \rightarrow \mathbb{T}_g$ y su dual $[\Theta^a]^* \rightarrow \mathbb{T}_g$

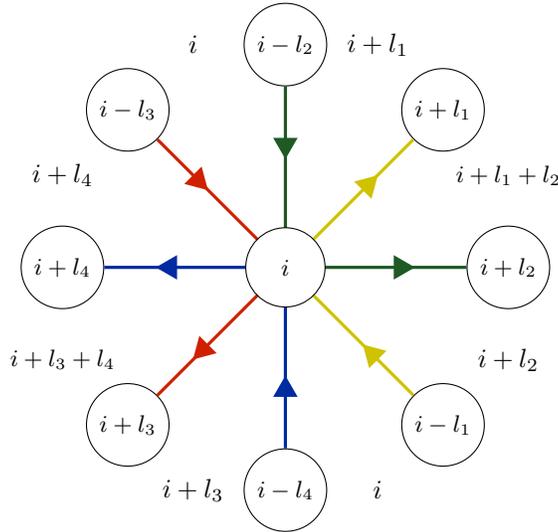
Teniendo en cuenta que la inmersión de una gráfica está determinada salvo isomorfismo por el pegado de sus regiones, concluimos que $[\Theta^a]^* \rightarrow \mathbb{T}_g$ y $\Phi^b \rightarrow \mathbb{T}_g$ son iguales salvo isomorfismo.

Para deducir la distancia mínima que puede tener un ciclo \hat{c}^* en $[\Theta^a]^* \rightarrow \mathbb{T}_g$, o equivalentemente en $\Phi^b \rightarrow \mathbb{T}_g$, vemos que las restricciones de aristas para cada vértice en $\Phi^b \rightarrow \mathbb{T}_g$ son las mismas que en $\Theta^a \rightarrow \mathbb{T}_g$, es decir, un vértice en $\Phi^b \rightarrow \mathbb{T}_g$ sólo puede tener 2 aristas \hat{q}^+ y \hat{q}^- en la fibra de una arista q de $\Phi \rightarrow \mathbb{T}_2$, por lo tanto los argumentos para calcular la distancia mínima de los ciclos en $\Theta^a \rightarrow \mathbb{T}_g$ se aplican de la misma manera para $\Phi^b \rightarrow \mathbb{T}_g$, o equivalentemente en $[\Theta^a]^* \rightarrow \mathbb{T}_g$, concluyendo que la distancia mínima para \hat{c}^* es 4.



(a) gráfica de voltaje $\Phi \rightarrow \mathbb{T}_2$

(b) una región típica del levantamiento $\Phi^b \rightarrow \mathbb{T}_g$



(c) una estrella típica del levantamiento $\Phi^b \rightarrow \mathbb{T}_g$

Figure 3.10: La gráfica $\Phi \rightarrow \mathbb{T}_2$ y su levantamiento $\Phi^b \rightarrow \mathbb{T}_g$

3.3.3. Paso 3 :: Dimensiones Arbitrarias

Resumiendo los últimos dos pasos para la construcción de códigos W , vemos que para la gráfica $\Theta^a \rightarrow \mathbb{T}_g$ obtenida de levantar a la gráfica $\Theta \rightarrow \mathbb{T}_2$ con el grupo \mathbb{Z}_Ω , se obtienen códigos W con parámetros $[[n, k, d]]$ donde

$$\begin{aligned} n &= |E^a| = \Omega \cdot 4 \\ k &= 2g = 2(\Omega + 1) \\ d &= 4 \end{aligned} \quad \text{para } \Omega > 3L$$

Para aumentar la dimensión del código hay dos caminos basándose en el que ya construimos. El primero consiste en incrementar el valor de L para aumentar el orden del grupo \mathbb{Z}_Ω . El segundo consiste en levantar gráficas similares a $\Theta \rightarrow \mathbb{T}_2$ pero inmersas en superficies \mathbb{T}_h y aumentar no sólo el orden del grupo \mathbb{Z}_Ω , sino también aumentar el género h .

Para explicar el segundo camino supongamos que tenemos una gráfica $\Psi \rightarrow \mathbb{T}_h$ con una región, un vértice y $2h$ aristas a las cuales les asignamos los voltajes necesarios para que el voltaje neto del único camino frontera sea de orden

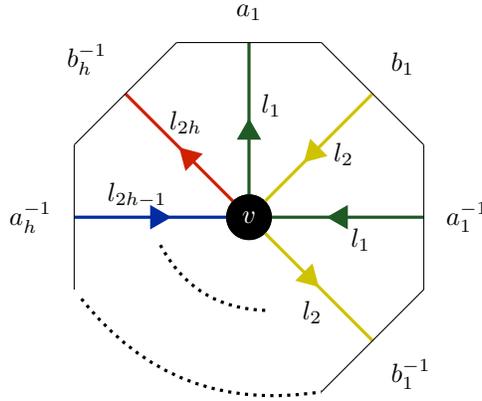


Figure 3.11: $\Psi \rightarrow \mathbb{T}_h$

1 en un grupo $\mathbb{Z}_{\Omega'}$ y para que la distancia mínima de los ciclos en su levantamiento sea 4 tanto para ella como para su dual, entonces obtendríamos un código con parámetros

$$\begin{aligned} n' &= \Omega' \cdot 2h \\ k' &= 2g = 2(\Omega'(h-1) + 1) \\ d' &= 4 \end{aligned}$$

Para saber qué camino elegir, comparemos n' con n fijando el género $h > 2$ y el grupo $\mathbb{Z}_{\Omega'}$ de la siguiente manera:

$$\begin{aligned} k' &= k \\ 2(\Omega'(h-1) + 1) &= 2(\Omega + 1) \\ \Omega'(h-1) &= \Omega \\ &\text{teniendo en cuenta que } 2 < h \\ 4\Omega' &< 2\Omega'h \\ 2\Omega'h &< 4\Omega'h - 4\Omega' \\ 2\Omega'h &< 4\Omega'(h-1) \\ n' = 2\Omega'h &< 4\Omega = n \end{aligned}$$

Por lo tanto, si pudiéramos construir dicha gráfica $\Psi \rightarrow \mathbb{T}_h$ con voltajes en un grupo $\mathbb{Z}_{\Omega'}$, el código generado por su gráfica de levantamiento, sería un mejor código que el construido por el primer camino con la misma dimensión.

Para construir $\Psi \rightarrow \mathbb{T}_h$ vamos a asignar los voltajes $a(q_i) = l_i$ donde las aristas q_i están etiquetadas en el sentido de las manecillas del reloj y los voltajes l_i cumplen las restricciones deducidas en el **Paso 2** en un grupo $\mathbb{Z}_{\Omega'}$. En la figura 3.11 se muestra dicha gráfica donde la arista verde es q_1 y \mathbb{T}_h está representado por un polígono de $2h$ lados.

El único camino frontera \hat{c}_f que hay en $\Psi \rightarrow \mathbb{T}_h$ tiene una sucesión de aristas $[\hat{q}_1^+, \hat{q}_2^+, \dots, \hat{q}_{2h-1}^-, \hat{q}_{2h}^-]$ con voltaje neto

$$v(\hat{c}_f) = l_1 + l_2 - l_1 - l_2 + \dots + l_{2h-1} + l_{2h} - l_{2h-1} - l_{2h} = 0$$

de donde el levantamiento $\Psi^a \rightarrow \mathbb{T}_H$ es tal que $H = \Omega'(h-1) + 1$ y una región \hat{f}_i en el levantamiento tiene una sucesión de aristas

$$[\hat{q}_1^+, \hat{q}_2^+, \hat{q}_1^-, \hat{q}_2^-, \dots, \hat{q}_{2h-1}^-, \hat{q}_{2h}^-]$$

donde sus vértices siguen la sucesión

$$[\hat{v}_i, \hat{v}_{i+l_1}, \hat{v}_{i+l_1+l_2}, \hat{v}_{i+l_2}, \hat{v}_i, \dots, \hat{v}_{i+l_{2h}}]$$

Para construir el dual $[\Psi^a]^* \rightarrow \mathbb{T}_H$ veamos que la estrella de un vértice \hat{v}_i en $\Psi^a \rightarrow \mathbb{T}_H$ está descrita por la sucesión de vértices $[\hat{v}_{i+l_1}, \hat{v}_{i-l_2}, \dots, \hat{v}_{i+l_{2h}}]$ con las regiones

$$[\hat{f}_{i-l_2}, \hat{f}_{i-l_2-l_1}, \hat{f}_{i-l_1}, \hat{f}_i, \dots, \hat{f}_{i-l_{2h-1}}, \hat{f}_i]$$

entre cada dos aristas de la estrella.

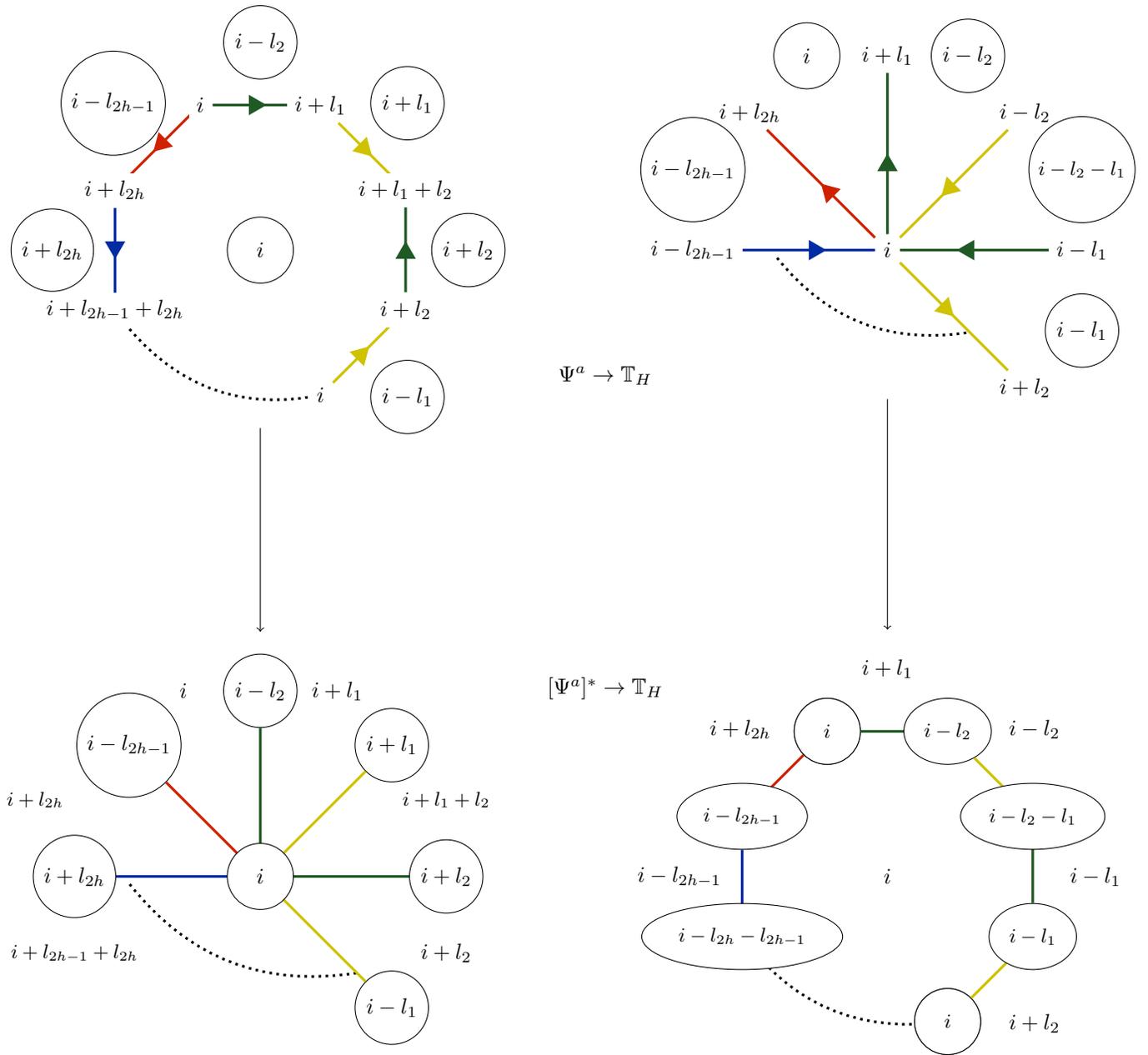


Figure 3.12: deducción de $[\Psi^a]^* \rightarrow \mathbb{T}_H$ a partir de $\Psi^a \rightarrow \mathbb{T}_H$

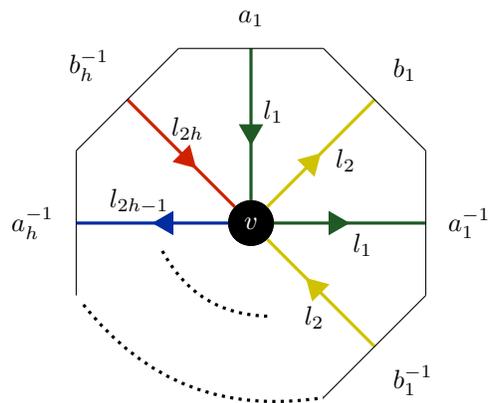


Figure 3.13: $\Phi \rightarrow \mathbb{T}_h$

Ahora que ya sabemos cómo son las estrellas de un vértice \hat{v}_i , deducimos el dual como en el **Paso 2** para describirlo a partir de sus regiones \hat{f}_i^* , las cuales resultan de unir las regiones vecinas de la estrella de \hat{v}_i con aristas como en la figura 3.12.

Por último definimos la gráfica $\Phi \rightarrow \mathbb{T}_h$ como en la figura 3.13, cuyo levantamiento $\Phi^b \rightarrow \mathbb{T}_H$ es isomorfo al dual $[\Psi^a]^* \rightarrow \mathbb{T}_H$ ya que sus regiones tienen la misma sucesión de vértices, aristas y adyacencias.

Para concluir que la distancia mínima de los ciclos tanto en $\Psi^a \rightarrow \mathbb{T}_H$ como en $\Phi^b \rightarrow \mathbb{T}_H$ es 4, notamos que las mismas restricciones que se dedujeron en el **Paso 2** aplican para estas gráficas y que por haber tomado los voltajes con estas restricciones, hemos asegurado que todos los ciclos tengan distancia mínima 4.

Capítulo 4

Un Ejemplo

4.1. Introducción al Ejemplo

Pongamos en pausa el hambre de conocimiento para hacer un resumen de lo aprendido en los últimos tres capítulos. Bajo la motivación de poder utilizar partículas cuánticas para realizar cálculos con ellas, en el **Capítulo 1** se dedujeron ciertas propiedades algebraicas que deben cumplir sus estados para que el paso del tiempo no los afecte y les podamos asignar valores de información. En el **Capítulo 2** vimos que estas propiedades pueden ser construidas a partir de una estructura geométrica, la cual también proporciona el esquema de una estructura física en donde ciertas partículas cuánticas puedan vivir, y utilizar a este sistema como una computadora. En el **Capítulo 3** vimos una herramienta para construir espacios geométricos a partir de otros más pequeños, especificando ciertas propiedades para que los parámetros del código que inducen estos espacios geométricos, sean lo mejor posible con respecto a esta herramienta.

En este capítulo vamos a construir un ejemplo de un **Código de Superficie** en tres pasos. El primer paso será construir una gráfica inmersa en una superficie bajo las condiciones especificadas en el **Capítulo 3**, el segundo paso será dotar explícitamente a los ciclos de aristas de esta gráfica una estructura algebraica como en el **Capítulo 2**, para finalmente proporcionar una base para el código como la que se proporcionó en el **Capítulo 1**.

4.2. Paso 1 :: Semilla y Levantamiento

Para poder construir la semilla necesitamos tres ingredientes, una superficie, una gráfica inmersa en ella y una asignación de voltajes. La superficie la vamos a tomar como \mathbb{T}_2 y la gráfica como en la Figura 3.3(a). Para la elección de los voltajes recordemos que los tomaremos en un grupo $(\mathbb{Z}_\Omega, +)$ donde las condiciones que necesitamos para garantizar que la distancia mínima de los ciclos que no son un camino frontera sea 4, son

$$3l_i < \Omega \tag{4.1}$$

$$2l_i \neq l_j \tag{4.2}$$

$$l_k \neq l_i + l_j \tag{4.3}$$

Notemos que si tomamos a cada l_i como un número impar, las dos últimas condiciones se cumplen. Motivados por esta observación, vamos a tomar

$$l_1 = 1$$

$$l_2 = 3$$

$$l_3 = 5$$

$$l_4 = 7$$

Para que la tercera propiedad se cumpla, basta tomar $\Omega = 22$, puesto que

$$3 \cdot 7 = 21 < 22 = \Omega$$

Resumimos estos resultados en la Figura 4.1.

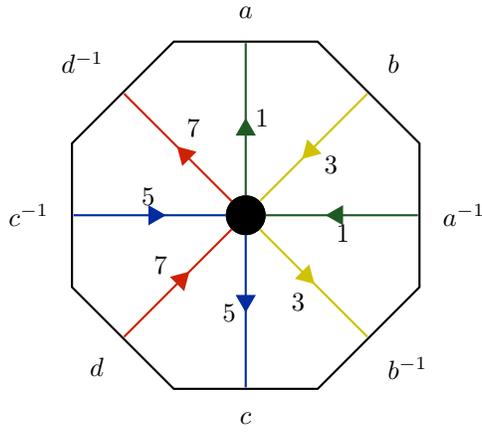


Figura 4.1: $\Theta \rightarrow \mathbb{T}_2$

Antes de levantar explícitamente a la semilla de la Figura 4.1, veamos algunas de sus propiedades. Empecemos por expresar cuántos vértices, aristas y regiones tiene.

$\Theta \rightarrow \mathbb{T}_2$	\Rightarrow	$\Theta^a \rightarrow \mathbb{T}_g$
$ V = 1$		$ V^a = \Omega$
$ E = 4$		$ E^a = 4 \cdot \Omega$
$ F = 1$		$ F^a = \Omega$

de donde podemos deducir su género g

$$2g = 2 - \chi(\Theta^a) = 2 - \Omega \cdot \chi(\Theta) = 2 + \Omega \cdot 2 = 46$$

$$g = 23$$

Para construir su levantamiento, primero vamos a pegar los dos vértices repetidos de cada una de las 22 regiones que tiene $\Theta^a \rightarrow \mathbb{T}_{23}$, formando un agujero rodeado por aristas rojas y azules en cada una. Luego pegamos las regiones formando una banda como en la Figura 4.2, procediendo por pegar la arista \blacktriangle deslizando bidimensionalmente las regiones para formar un polígono con las aristas verdes y amarillas que ya están pegadas, y finalmente obtener la Figura 4.3.

Notemos que la construcción dual de $\Theta^a \rightarrow \mathbb{T}_{23}$ la podemos ver como el levantamiento de la gráfica en la Figura 3.10(a), la cual conserva las propiedades 4.1 necesarias para que el ciclo más pequeño que no sea un camino frontera sea 4.

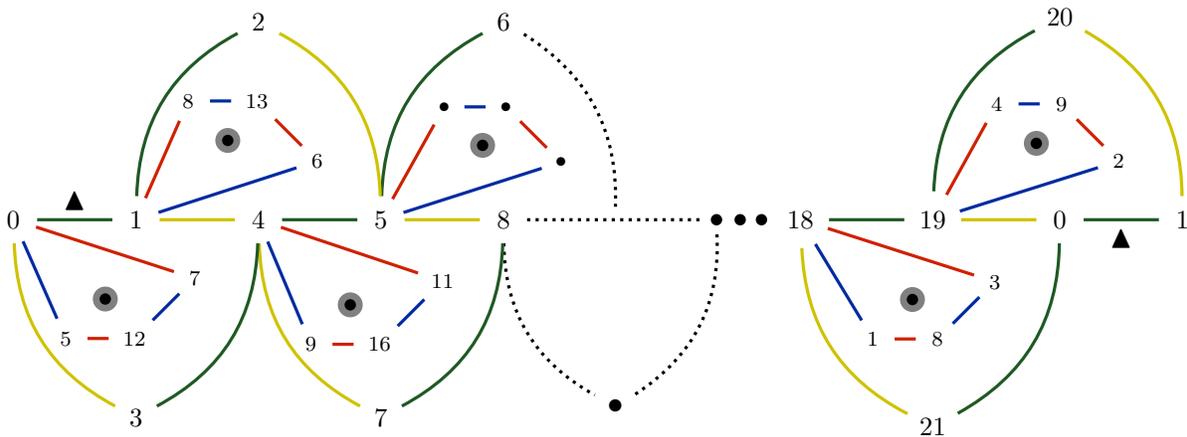


Figura 4.2: Pegado en banda

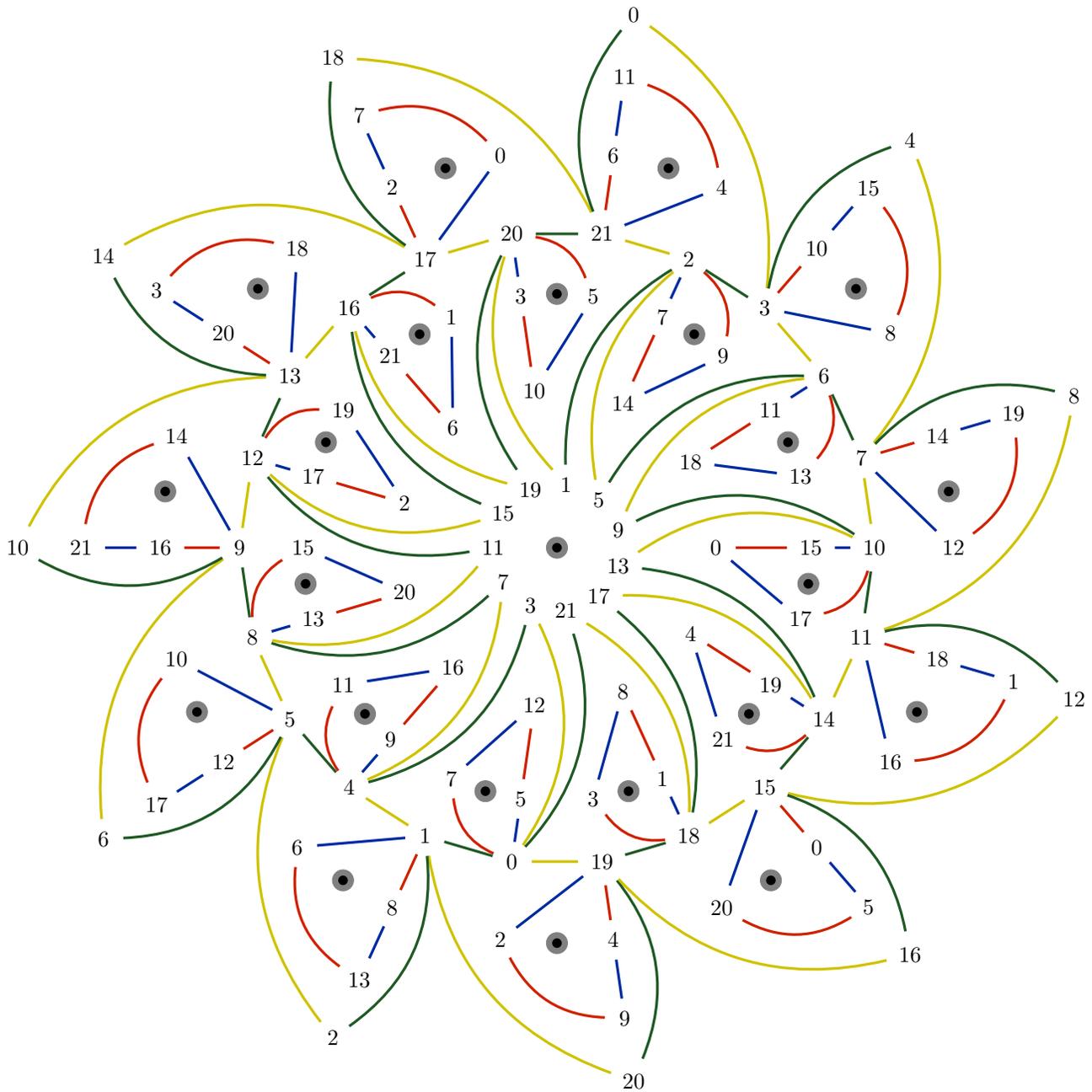


Figura 4.3: $\Theta^a \rightarrow \mathbb{T}_{23}$

En el siguiente paso veremos cómo aunque al diagrama de la Figura 4.3 le falta pegar muchas aristas para completar la superficie \mathbb{T}_{23} , este diagrama basta para encontrar la estructura algebraica de sus ciclos.

4.3. Paso 2 :: Ciclos de $\Theta^a \rightarrow \mathbb{T}_{23}$

Para poder utilizar la estructura algebraica desarrollada en el **Capítulo 2**, necesitamos darle un nombre a cada arista, para clarificar qué ciclos corresponden a una combinación de caminos frontera y qué ciclos no.

Empezamos por etiquetar con números consecutivos en sentido de las manecillas del reloj al polígono formado por 22 aristas amarillas y verdes, por el cual comenzamos a pegar en la Figura 4.2. La primera arista que se etiqueta es la arista amarilla correspondiente a la región 1 como en la Figura 4.4.

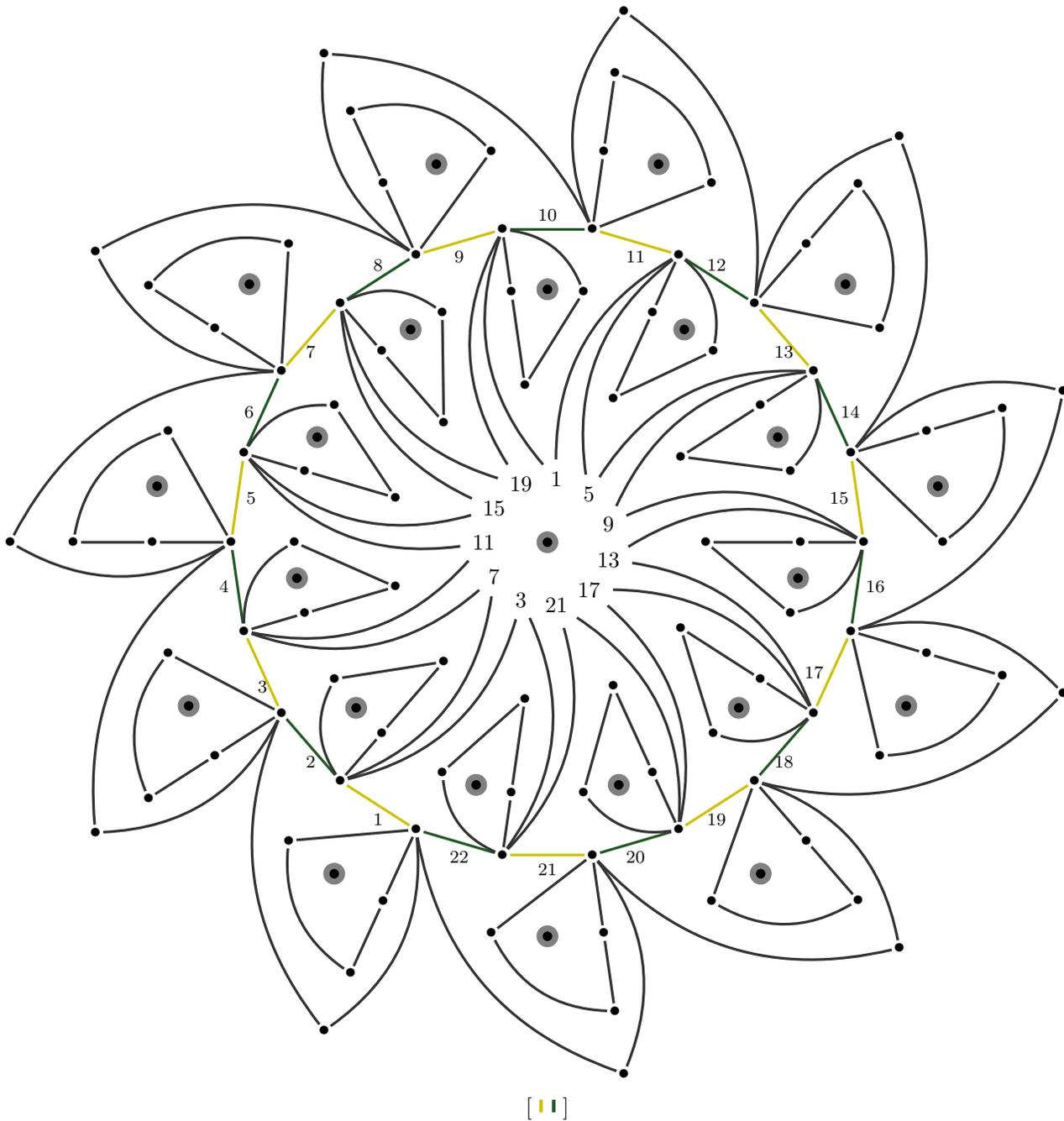


Figura 4.4: Primer bloque de aristas enumeradas

Seguimos por etiquetar todos los 11 ciclos de longitud 4 formados por aristas azules y rojas que se encuentran dentro de las regiones exteriores en la Figura 4.3. La primera arista que etiquetamos es la arista con extremos 1, 6 de color azul dentro de la región 1, continuando en sentido contrario a las manecillas del reloj por este ciclo. Los siguientes ciclos se etiquetan de manera análoga al caso anterior, tomándolos consecutivamente en orden de las manecillas del reloj sobre la Figura 4.3 como se muestra en la Figura 4.5.

Por último etiquetamos las 22 aristas verdes y amarillas que se encuentran en las regiones exteriores y que no hemos enumerado, empezando por la arista verde con extremos 1, 2 y siguiendo el orden de las manecillas del reloj como en la Figura 4.6. Las aristas de la región interior no se ponen porque a cada una le corresponde la misma etiqueta con la que aparece en la región exterior.

Ahora que ya tenemos nombradas a las aristas podemos definir las funciones T_1, T_2 como en 2.5, las cuales nos

permiten representar los caminos frontera y los ciclos de aristas en $\Theta^a \rightarrow \mathbb{T}_{23}$ recorridos bajo la acción del grupo \mathbb{Z}_2 como los subespacios $W_1, W_2^\perp \subset \mathbb{Z}_2^{|E^a|}$ con los que vamos a construir la estructura algebraica del código \mathcal{C}

$$\mathbb{T}_1: \Delta^1(\Theta^a, G) \longrightarrow \mathbb{Z}_2^{|E^a|}$$

$$\mathbb{T}_2: \Delta_1(\Theta^a) \longrightarrow \mathbb{Z}_2^{|E^a|}$$

$$W_2 := \mathbb{T}_1(\text{Im } \delta_1)$$

$$W_1 := \mathbb{T}_2(\text{Im } \partial_2)$$

$$\mathbb{T}_2(\text{Im } \partial_2) = W_1 \subset W_2^\perp = \mathbb{T}_2(\text{Ker } \partial_1)$$

Observemos que esta enumeración nos permite representar cualquier sucesión de aristas en un vector con 88 entradas, en donde las primeras 22 denotan las aristas amarillas y verdes del polígono por el cual empezamos a pegar la inmersión, las siguientes 44 corresponden a todas las aristas azules y rojas, y las últimas 22 corresponden a las aristas verdes y amarillas al exterior de la Figura 4.3. De esta manera un vector típico en \mathbb{Z}_2^n , tras haber abreviado $n = |E^a|$, lo vemos

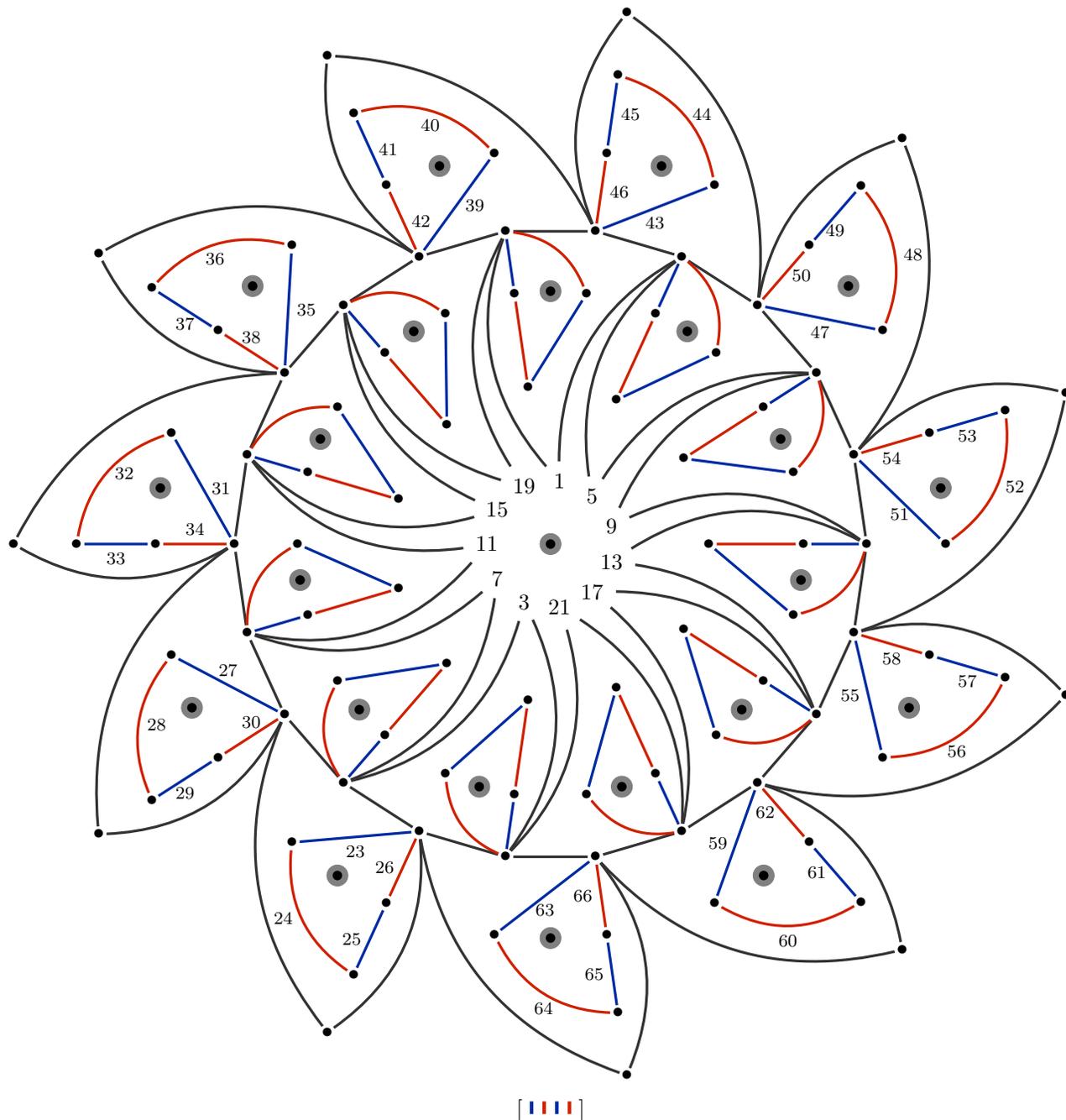


Figura 4.5: Segundo bloque de aristas enumeradas

como

$$\left(\overbrace{[\begin{smallmatrix} 22 \\ \color{red}{\rule{0.5em}{0.4pt}} \color{green}{\rule{0.5em}{0.4pt}} \color{blue}{\rule{0.5em}{0.4pt}} \end{smallmatrix}]}^{22} \mid \overbrace{[\begin{smallmatrix} 44 \\ \color{red}{\rule{0.5em}{0.4pt}} \color{blue}{\rule{0.5em}{0.4pt}} \color{red}{\rule{0.5em}{0.4pt}} \color{blue}{\rule{0.5em}{0.4pt}} \end{smallmatrix}]}^{44} \mid \overbrace{[\begin{smallmatrix} 22 \\ \color{red}{\rule{0.5em}{0.4pt}} \color{green}{\rule{0.5em}{0.4pt}} \color{blue}{\rule{0.5em}{0.4pt}} \end{smallmatrix}]}^{22} \right) \quad (4.4)$$

Sabemos que los representantes de la clase de equivalencia del espacio cociente W_2^\perp/W_1 equivalen a ciclos de aristas en $\Theta^a \rightarrow \mathbb{T}_{23}$ los cuales no pueden ser expresados como una suma de caminos frontera, de los cuales sabemos que hay exactamente $2g$. Por lo tanto, para decir quiénes son estos representantes tenemos que encontrar $2g = 46$ ciclos en $\Theta^a \rightarrow \mathbb{T}_{23}$ cuya expresión en \mathbb{Z}_2^n sea linealmente independiente, y también sean linealmente independientes en W_2^\perp/W_1 .

Para esto, primero vamos a definir 46 ciclos, luego vamos a ver que son linealmente independientes con respecto a su representación en \mathbb{Z}_2^n , y luego vamos a ver su independencia lineal en W_2^\perp/W_1 .

Guiándonos por el diagrama que construimos de $\Theta^a \rightarrow \mathbb{T}_{23}$ como en la Figura 4.3, el primer ciclo que vamos a

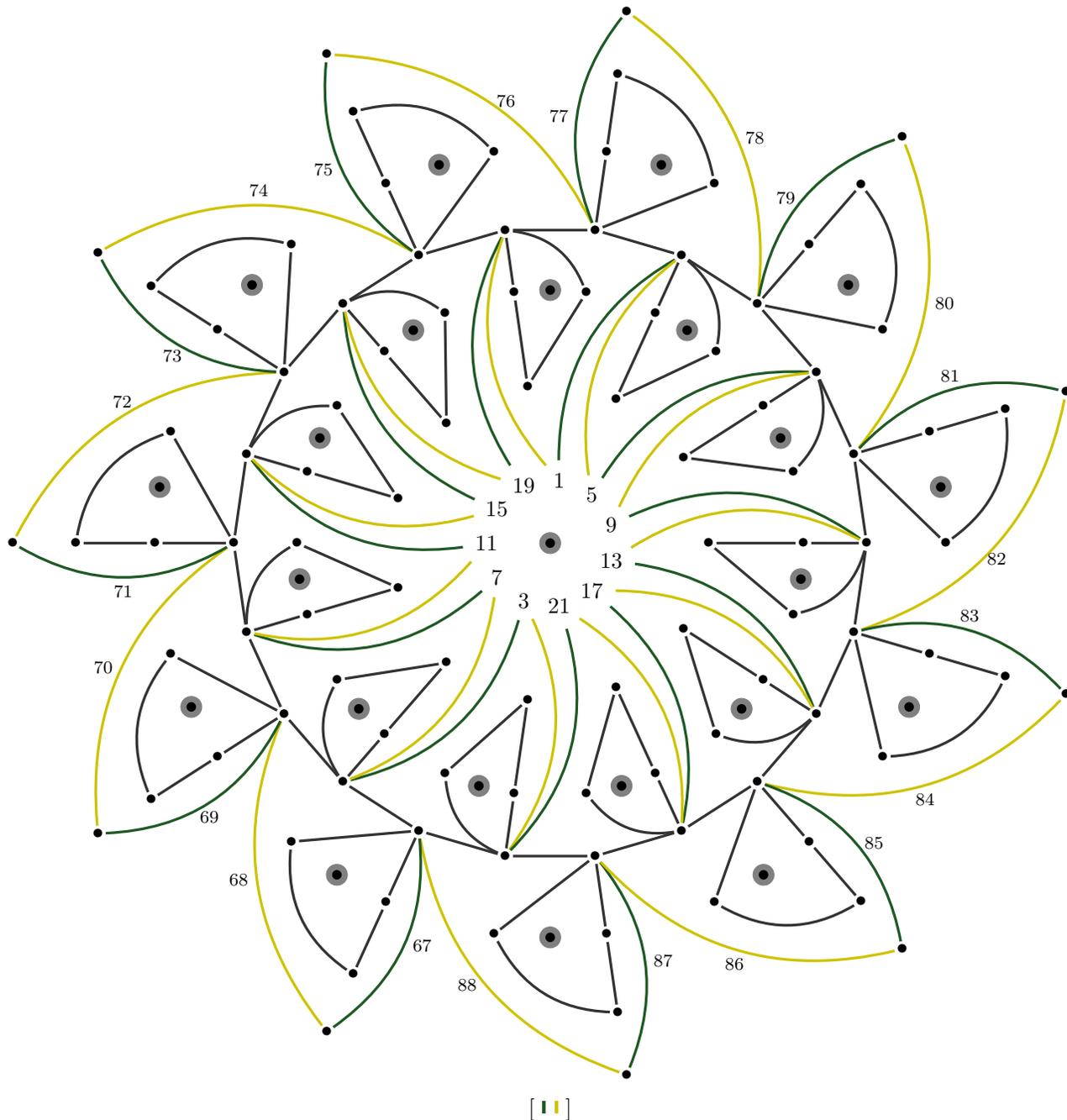


Figura 4.6: Tercer bloque de aristas enumeradas

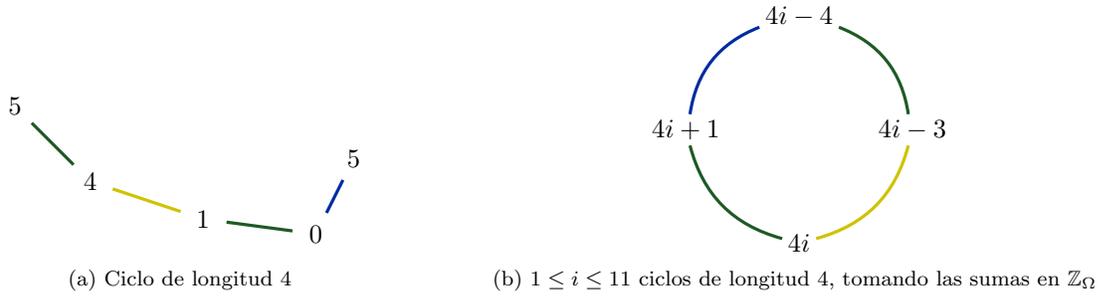


Figura 4.7: once ciclos con aristas verdes, amarillas y azules
(a) :: (b)

escoger va a ser el polígono con aristas amarillas y verdes por el cual empezamos a pegar, a este ciclo lo vamos a llamar $\hat{c}[\text{■} \text{■}]$.

El segundo ciclo será el formado por el resto de las aristas verdes y amarillas. A este ciclo lo llamamos $\hat{c}[\text{■} \text{■}]$.

Ahora vamos a tomar los 11 ciclos de aristas azules y rojas dentro de las regiones exteriores de la Figura 4.3 empezando por el ciclo de la región 1 y continuando en sentido de las manecillas del reloj. A continuación tomamos los 10 ciclos de aristas rojas y azules dentro de las regiones interiores comenzando por el ciclo en la región 0 y continuando en sentido de las manecillas del reloj. El onceavo ciclo, correspondiente a la región 18 se excluye por razones que veremos más adelante. Llamamos a estas dos clases de ciclos por $\hat{c}[\text{■} \text{■}]_i$ y $\hat{c}[\text{■} \text{■}]_l$ respectivamente, con $1 \leq i \leq 11$ y $1 \leq l \leq 10$.

Hasta ahora tenemos $1 + 1 + 11 + 10 = 23$ ciclos, faltan 23 más. Veamos la Figura 4.3 y tomemos el ciclo como en la Figura 4.7(a), generalizando como en la Figura 4.7(b) tomándolos en sentido de las manecillas del reloj. A estos ciclos los denotamos por $\hat{c}[\text{■} \text{■}]_i$ con $1 \leq i \leq 11$.

A continuación tomamos los ciclos como en la Figura 4.8, y los denotamos por $\hat{c}[\text{■} \text{■} \text{■}]_i$ con $1 \leq i \leq 11$.

Para el último ciclo que nos falta, tomamos el ciclo como en la Figura 4.9 y lo denotamos por $\hat{c}[\text{■} \text{■} \text{■}]$.

Observemos que las etiquetas que les asignamos a las aristas nos permite trabajar en cada uno de los tres bloques del vector 4.4 por separado tomando mod 22, mod 44 y mod 22 respectivamente, si después de haberlo hecho sumamos 22 al segundo bloque y 66 al tercero. Con esto en mente escribiremos suscitivamente los ciclos anteriormente

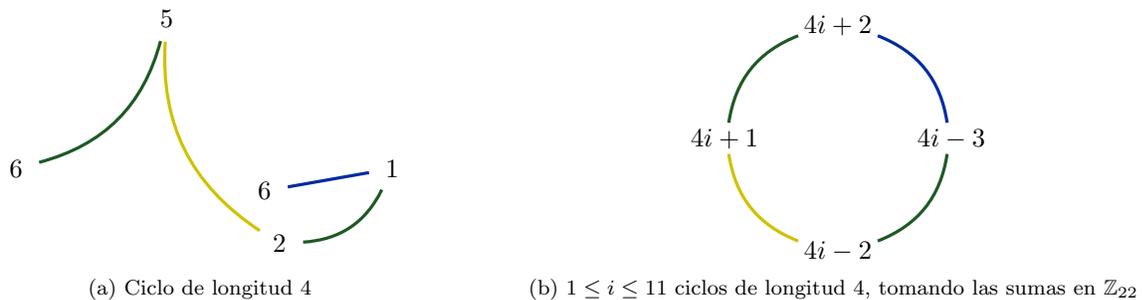


Figura 4.8: once ciclos con aristas amarillas, verdes y azules
(a) :: (b)

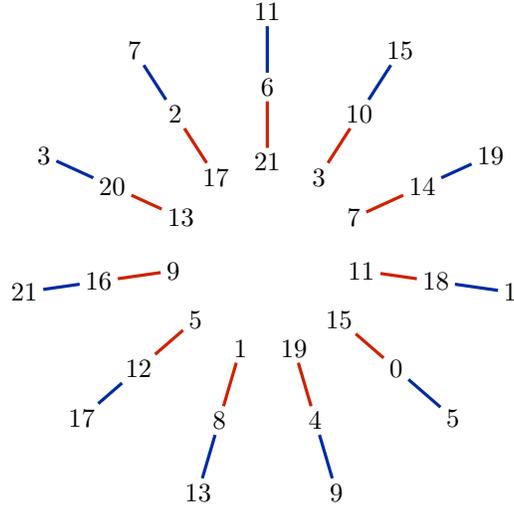


Figura 4.9: Ciclo con aristas azules y rojas

descritos como

$$\begin{aligned}
 & \left(\begin{array}{c|c|c} [\text{■ ■}] & [\text{■ ■ ■}] & [\text{■ ■}] \end{array} \right) & (4.5) \\
 \hat{c}[\text{■ ■}] &= \left(\begin{array}{c|c|c} 1 & \cdots & 1 \end{array} \mid \begin{array}{c} \mathbf{0} \\ \mathbf{0} \end{array} \mid \begin{array}{c} \mathbf{0} \\ \mathbf{0} \end{array} \right) \\
 \hat{c}[\text{■ ■}] &= \left(\begin{array}{c|c|c} \mathbf{0} & & \mathbf{0} \end{array} \mid \begin{array}{c} \mathbf{0} \\ \mathbf{0} \end{array} \mid \begin{array}{c} 1 & \cdots & 1 \end{array} \right) \\
 \hat{c}[\text{■ ■}]_i &= \left(\begin{array}{c|c|c} \mathbf{0} & & \mathbf{0} \end{array} \mid [\text{■ ■}]_i \mid \begin{array}{c} \mathbf{0} \\ \mathbf{0} \end{array} \right) \\
 \hat{c}[\text{■ ■}]_l &= \left(\begin{array}{c|c|c} \mathbf{0} & & \mathbf{0} \end{array} \mid [\text{■ ■}]_l \mid \begin{array}{c} \mathbf{0} \\ \mathbf{0} \end{array} \right) \\
 \hat{c}[\text{■ ■ ■}]_i &= \left(\begin{array}{c|c|c} [\text{■ ■ ■}]_i & & \mathbf{0} \end{array} \mid [\text{■}]_i \mid \begin{array}{c} \mathbf{0} \\ \mathbf{0} \end{array} \right) \\
 \hat{c}[\text{■ ■ ■}]_i &= \left(\begin{array}{c|c|c} \mathbf{0} & & \mathbf{0} \end{array} \mid [\text{■ ■}]_i \mid [\text{■ ■ ■}]_i \right) \\
 \hat{c}[\text{○}] &= \left(\begin{array}{c|c|c} \mathbf{0} & & \mathbf{0} \end{array} \mid [\text{○}]_i \mid \begin{array}{c} \mathbf{0} \\ \mathbf{0} \end{array} \right)
 \end{aligned}$$

donde

$$\begin{aligned}
 [\text{■ ■}]_i &= [4i - 3, 4i - 2, 4i - 1, 4i]_{\text{mod } 44} \\
 [\text{■ ■}]_l &= [4l + 4, 4l + 14, 4l + 25, 4l + 35]_{\text{mod } 44} \\
 [\text{■ ■ ■}]_i &= [2i - 2, 2i - 1, 2i]_{\text{mod } 22} & [\text{■}]_i &= [i + 3(i - 3)]_{\text{mod } 44} \\
 [\text{■ ■ ■}]_i &= [2i - 1, 2i, 2i + 1]_{\text{mod } 22} & [\text{■ ■}]_i &= [i + 3(i - 1)]_{\text{mod } 44} \\
 [\text{○}]_i &= [4i - 1, 4i]_{\text{mod } 44}
 \end{aligned}$$

representan las entradas que no son cero en cada ciclo.

4.3.1. Independencia Lineal en \mathbb{Z}_2^n

Para ver que esta colección de ciclos es linealmente independiente, vamos a ver que ningún ciclo se puede expresar como combinación lineal de los demás. Con éste propósito en mente, primero vamos a ver que los ciclos $\hat{c}[\text{■ ■}]_i$ y $\hat{c}[\text{■ ■}]_l$ son linealmente independientes, para $1 \leq i \leq 11$ y $1 \leq l \leq 10$.

Observemos que para dos ciclos distintos $\hat{c}[\text{■ ■}]_{i,j}$, las entradas $[\text{■ ■}]_{i,j}$ donde no son cero, son distintas para toda $1 \leq i, j \leq 11$. Esto se debe a que estos ciclos no comparten ninguna arista entre ellos como se puede ver en la Figura 4.3. De esta observación deducimos que los ciclos $\hat{c}[\text{■ ■}]_i$ son linealmente independientes. También veamos que esta

familia de ciclos contiene a todas las aristas azules y rojas de la gráfica.

De manera similar tenemos que los ciclos $\hat{c}[\blacksquare]_l$ tampoco comparten entradas con 1 entre ellos, y que también son linealmente independientes entre ellos. Veamos también que esta familia de ciclos no contiene a todas las aristas rojas y azules de la gráfica, puesto que sólo estamos tomando 10 ciclos.

Para ver que estas dos familias de ciclos distintas son linealmente independientes entre ellas, notamos que debido a las dos observaciones anteriores no es posible hacer una combinación lineal no trivial entre ellos que dé el vector $\mathbf{0}$, puesto que los ciclos $\hat{c}[\blacksquare]_l$ sólo son 10 de los 11 ciclos interiores.

Ahora veamos que el ciclo $\hat{c}[\circlearrowleft]$ es linealmente independiente con los ciclos $\hat{c}[\blacksquare]_i$ y $\hat{c}[\blacksquare]_l$ observando que no es posible hacer una combinación lineal entre ellos que dé $\hat{c}[\circlearrowleft]$.

Esto lo vemos de la siguiente manera. Supongamos que queremos escribir la entrada etiquetada por

$$[\circlearrowleft]_1 = [3, \underline{4}]$$

Debido a que sólo escogimos 10 ciclos de la forma $\hat{c}[\blacksquare]_{i-1}$, tenemos que la única manera de escribir la entrada subrayada $\underline{4}$, es sumando el ciclo etiquetado por

$$[\blacksquare]_1 = [1, \underline{2}, 3, 4]$$

donde la entrada $\underline{2}$ no está en el ciclo $\hat{c}[\circlearrowleft]$, y la única manera de eliminarla es sumando el ciclo etiquetado por

$$[\blacksquare]_8 = [2, \underline{13}, 23, 36]$$

aunque ahora la entrada $\underline{13}$ tampoco está en el ciclo $\hat{c}[\circlearrowleft]$ y la única manera de hacerla cero es sumando el ciclo etiquetado por

$$[\blacksquare]_4 = [13, \underline{14}, 15, 16]$$

Nos encontramos con la entrada $\underline{14}$ la cual no está sobre el ciclo que queremos generar y sólo se puede eliminar sumando el ciclo

$$\hat{c}[\blacksquare]_{11}$$

ya que éste ciclo está etiquetado por $[4, \underline{14}, 25, 35]$. Sólo que éste ciclo no está en nuestra lista de ciclos por haber escogido $\hat{c}[\blacksquare]_l$ con $1 \leq l \leq 10$. De donde obtenemos el resultado buscado.

Ahora veamos que el ciclo $\hat{c}[\blacksquare\blacksquare]$ no puede ser expresado como una combinación lineal de los ciclos $\hat{c}[\blacksquare\blacksquare]_i$. Esto lo hacemos observando que cualesquiera dos ciclos consecutivos etiquetados por

$$[\blacksquare\blacksquare]_i \quad [\blacksquare\blacksquare]_{i+1}$$

comparten la primera y última etiqueta. Esta observación nos dice que la suma de cualesquiera dos ciclos que no son consecutivos dejan una hilera de ceros entre las entradas que tienen 1, la cual no se puede llenar de 1's sumando ciclos $\hat{c}[\blacksquare\blacksquare]_i$. De donde obtenemos el resultado buscado.

De manera similar obtenemos que el ciclo $\hat{c}[\blacksquare\blacksquare]$ no puede ser el resultado de una combinación lineal de los ciclos $\hat{c}[\blacksquare\blacksquare]_i$.

Para ver el resto de las independencias lineales que nos faltan, observamos que las que ya hemos clarificado las explican trivialmente.

4.3.2. Independencia lineal en W_2^\perp/W_1

Ahora que hemos visto que nuestra elección de 46 ciclos corresponde a un conjunto linealmente independiente en \mathbb{Z}_2^n , para ver que también forman un conjunto linealmente independiente en W_2^\perp/W_1 tenemos que checar que todos corresponden a clases de equivalencia distintas y que ninguno corresponde a la clase de equivalencia trivial.

Para poder justificar estas dos propiedades, expresamos los elementos de W_1 de la siguiente manera

$$\begin{aligned} & (\quad [\text{III}] \quad | \quad [\text{IIII}] \quad | \quad [\text{IIII}] \quad) \\ \hat{c} [\text{△}]_i &= (\quad [\text{IIII}]_i \quad | \quad [\text{IIII}]_i \quad | \quad [\text{IIII}]_i \quad) \\ \hat{c} [\text{▽}]_i &= (\quad [\text{IIII}]_i \quad | \quad [\text{IIII}]_i \quad | \quad [\text{IIII}]_i \quad) \end{aligned}$$

donde los símbolos Δ y ∇ representan las regiones al exterior y al interior de la Figura 4.3 respectivamente, habiendo enumerado las regiones en sentido de las manecillas del reloj y

$$\begin{aligned} [\text{IIII}]_i &= [2i - 1, 2i]_{\text{mod } 22} \\ [\text{IIII}]_i &= [2i - 2, 2i - 1]_{\text{mod } 22} \\ [\text{IIII}]_i &= [2i, 2i + 1]_{\text{mod } 22} \end{aligned}$$

• Clases distintas

Para ver que los ciclos que escogimos corresponden a clases de equivalencia distintas, tenemos que checar que para cualesquiera dos ciclos distintos \hat{c}, \hat{k} de los que escogimos se tiene

$$\hat{c} + \hat{k} \notin W_1$$

Observemos que las etiquetas $[\text{IIII}]_i$ no comparten entradas distintas de cero entre ellas, y que esto también sucede con las etiquetas $[\text{IIII}]_i$ y con $[\text{IIII}]_i$. Aunque estas familias de etiquetas no comparten entradas con 1's entre ellas por separado, una etiqueta $[\text{IIII}]_j$ para una j fija, comparte sólo una entrada 1 con las etiquetas $[\text{IIII}]_{j,j+1}$ y con $[\text{IIII}]_{j,j-1}$.

Esto nos indica que si queremos hacer una combinación lineal con elementos de W_1 , que tenga las primeras 22 o las últimas 22 entradas con 0, sólo la podemos hacer si sumamos

$$\sum_{i=1}^{11} \hat{c} [\text{△}]_i + \hat{c} [\text{▽}]_i = \mathbf{0} \in \mathbb{Z}_2^n.$$

Observemos también que la mínima cantidad de 1's que podemos formar con una combinación lineal de las etiquetas $[\text{IIII}]_i$ y $[\text{IIII}]_l$ es cuatro.

La primera observación esclarece el hecho de que las siguientes sumas

$$\begin{aligned} \hat{c} [\text{IIII}] + \begin{cases} \hat{c} [\text{IIII}]_i \\ \hat{c} [\text{IIII}]_l \\ \hat{c} [\text{IIII}]_i \\ \hat{c} [\text{○}] \end{cases} & \quad \hat{c} [\text{IIII}] + \begin{cases} \hat{c} [\text{IIII}]_i \\ \hat{c} [\text{IIII}]_l \\ \hat{c} [\text{IIII}]_i \\ \hat{c} [\text{○}] \end{cases} & \quad \hat{c} [\text{IIII}]_i + \begin{cases} \hat{c} [\text{IIII}]_j \\ \hat{c} [\text{IIII}]_l \\ \hat{c} [\text{IIII}]_t \\ \hat{c} [\text{IIII}]_t \\ \hat{c} [\text{○}] \end{cases} & \quad \hat{c} [\text{IIII}]_l + \begin{cases} \hat{c} [\text{IIII}]_s \\ \hat{c} [\text{IIII}]_t \\ \hat{c} [\text{IIII}]_t \\ \hat{c} [\text{○}] \end{cases} \\ \hat{c} [\text{IIII}]_i + \begin{cases} \hat{c} [\text{IIII}]_j \\ \hat{c} [\text{○}] \end{cases} & \quad \hat{c} [\text{IIII}]_i + \begin{cases} \hat{c} [\text{IIII}]_j \\ \hat{c} [\text{○}] \end{cases} \end{aligned}$$

no pueden ser combinación lineal de los elementos de W_1 donde

$$1 \leq i, j, t \leq 11 \quad i \neq j \quad 1 \leq l, s \leq 10 \quad l \neq s$$

Mientras que la segunda observación se encarga de esclarecer que las sumas

$$\hat{c} [\text{IIII}] + \hat{c} [\text{IIII}]_i \quad \hat{c} [\text{IIII}] + \hat{c} [\text{IIII}]_i \quad \hat{c} [\text{IIII}]_i + \hat{c} [\text{IIII}]_t$$

tampoco pueden ser expresadas como una combinación lineal de elementos de W_1 .

- **Clases no triviales**

La primera observación que hicimos también nos sirve para ver que los ciclos que escogimos no pueden ser una combinación lineal de los elementos de W_1 , puesto que todos los ciclos que escogimos tienen 0's en las primeras o en las últimas 22 entradas, o en las dos.

Esto concluye el segundo paso del ejemplo, tras haber proporcionado una colección de ciclos linealmente independientes que funcionan como representantes de las 46 clases de equivalencia que tiene el espacio cociente W_2^\perp/W_1 .

4.4. Paso 3 :: el código \mathcal{C}

Ahora que ya sabemos quiénes son los ciclos de $\Theta^a \rightarrow \mathbb{T}_{23}$ que no pueden ser expresados como un camino frontera, recordamos la base $\{|\varsigma_i\rangle\}$ del código \mathcal{C} construida en el **Capítulo 1** 1.4

$$|\varsigma_i\rangle = \frac{1}{\sqrt{|W_1|}} \sum_{\mathbf{u} \in W_1} |\mathbf{u} + \bar{\mathbf{v}}_i\rangle \quad \bar{\mathbf{v}}_i \text{ representantes de } W_2^\perp/W_1$$

donde cada $\bar{\mathbf{v}}_i$ es uno de los ciclos que escogimos en 4.5. Notemos que una base para el subespacio $W_1 \subset \mathbb{Z}_2^n$ tiene 21 elementos, de donde $|W_1| = 2^{21}$ por lo que cada elemento $|\varsigma_i\rangle$ se expresa como una suma de 2^{21} elementos.

Por último recopilamos los parámetros $[[n, k, d]]$ del código \mathcal{C} recordando qué significan.

n denota la cantidad de partículas con la que vamos a trabajar, cada una modelada en $\mathcal{H} = \mathbb{C}^2$ y todas juntas en $\mathcal{H}^{\otimes n}$. Como en los códigos de superficies tenemos una partícula por cada arista de $\Theta^a \rightarrow \mathbb{T}_{23}$, tenemos que

$$n = |E^a| = 4 \cdot \Omega = 88$$

k denota la dimensión del subespacio $\mathcal{C} \subset \mathcal{H}^{\otimes n}$, la cual corresponde a la dimensión de W_2^\perp/W_1 . En la construcción que hicimos, la dimensión de este espacio cociente corresponde a los representantes de los ciclos que no son caminos frontera en $\Theta^a \rightarrow \mathbb{T}_{23}$, por eso

$$k = 46$$

d denota qué tanto se pueden parecer los operadores que no dejan invariante a \mathcal{C} pero parece que sí lo hacen, es decir qué tan distintos son los elementos de W_2^\perp comparados con los de W_1 y qué tan diferentes son los elementos de W_1^\perp comparados con los de W_2 . Para los códigos de superficie se traduce en encontrar el ciclo más pequeño que no sea un camino frontera tanto de la gráfica construida como de su dual, lo que para la construcción que hicimos se traduce en sólo encontrar el ciclo más pequeño que no sea un camino frontera de $\Theta^a \rightarrow \mathbb{T}_{23}$, así tenemos que

$$d = 4$$

FIN

Bibliografía

- [1] Mikio Nakahara, Tetsuo Ohmi. *Quantum Computing, from linear algebra to physical realizations*. CRC Press, 2008.
- [2] Phillip Kaye, Raymond Laflamme, Michelle Mosca. *An introduction to Quantum Computing*. Oxford University Press, 2007.
- [3] John Preskill. *Lecture Notes for Physics 229: Quantum Information and Computation*. California Institute of Technology, <http://www.theory.caltech.edu/~preskill/ph229> 1998.
- [4] Michael A. Nielsen, Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
- [5] Goong Chen, Rane K. Brylinsky. *Mathematics of Quantum Computation*. Chapman & Hall, 2002.
- [6] A. R. Calderbank, Peter W. Shor. *Good quantum error-correcting codes exist*. arXiv:quant-ph/9512032v2. 16 Apr 1996.
- [7] A. R. Calderbank, Peter W. Shor, N. J. A. Sloane. *Quantum Error Correction and Orthogonal Geometry*. arXiv:quant-ph/9605005v3. 2 Jul 1996.
- [8] Román Orús, Tzu-Chieh Wei. *Topological Geometric Entanglement of Blocks*. arXiv:1108.1537v1[cond-mat.strl-el], 7 Aug 2011.
- [9] Jonathan L. Gross, Thomas W. Tucker. *Topological Graph Theory*. Wiley-Interscience publication, 1987.
- [10] Allen Hatcher. *Algebraic Topology*. Cambridge University Press, 2002.
- [11] S. K. Lando, A. K. Zvonkin. *Graphs on Surfaces and their Applications*. Springer-Verlag, 2004.
- [12] A. Yu. Kitaev. *Fault-tolerant quantum computation by anyons*. arXiv:quant-ph/9707021v1. 9 Jul 1997.
- [13] H. Bombín, M. A. Martín-Delgado. *Homological error correction: Classical and quantum codes*. <http://dx.doi.org/10.1063/1.2731356>, 21 Mayo 2007.
- [14] Gilles Zémor. *On Cayley graphs, surface codes, and the limits of homological coding for quantum error correction*. <http://www.math.u-bordeaux.fr/~zemor>, 30 Diciembre 2008.