



**CONSTANTE DE CUANTIZACIÓN PARA
RETÍCULOS EUCLIDEANOS DE TIPO I EN
DIMENSIÓN 5**

DANIEL STIVEN TOVAR PASTRANA

**UNIVERSIDAD DEL VALLE
FACULTAD DE CIENCIAS NATURALES Y EXACTAS
DEPARTAMENTO DE MATEMÁTICAS
SANTIAGO DE CALI
2024**

CONSTANTE DE CUANTIZACIÓN PARA RETÍCULOS EUCLIDEANOS DE TIPO I EN DIMENSIÓN 5

Daniel Stiven Tovar Pastrana

Trabajo de investigación presentado como requisito parcial para optar al título de
Magíster en Ciencias Matemáticas 7179

Director:
Juan Miguel Velásquez Soto, Dr

Universidad del Valle Sede Cali
Facultad de Ciencias Naturales y Exactas
Departamento de Matemáticas
Santiago de Cali, Colombia
2024

*Para mis padres, mi hermano, Daniela y Chester,
quienes me brindan todo su apoyo y cariño.*

Agradecimientos

En este trabajo agradezco principalmente a mis padres, a mi hermano y Mayi, por todo su amor, esfuerzo y dedicación en todos estos años, para que pudiera culminar mi carrera universitaria.

A todos mis profesores, por todos los conocimientos que me brindaron, en especial a mi director de trabajo de grado, Juan Miguel, por confiarme parte de su trabajo académico e ideas para que pudiéramos trabajar como equipo.

A Daniela, por otorgarme su tiempo, amor y ayuda incondicional; gracias por aportarme tanto conocimiento y apoyo emocional en el tiempo que hemos compartido.

A mis amigos, que tenerlos es una de las alegrías más grandes que me han dejado estos años, gracias por hacer mucho más satisfactoria mi vida universitaria.

Contenido

Agradecimientos.	II
Resumen.	v
Introducción.	vii
1. Preliminares	1
1.1. Lattices	1
1.2. Celdas y Vectores de Voronoi	5
1.3. Parámetros de Selling y Lattices Tipo I	8
1.4. Tipos de coordenadas para $\mathbb{R}^n$	11
1.5. Cuantización con Lattices	15
1.6. Constante de cuantización para lattices en dimensiones bajas	17
1.6.1. Descripción de la celda de Voronoi en dimensión 3	17
1.6.2. Cálculo de la constante de cuantización en dimensión 3	21
1.6.3. Constante de cuantización para lattice en dimensión 4	24
2. Descripción de la celda de Voronoi	26
2.1. La celda de Voronoi para Lattices de primer tipo y el permutaedro	26
2.2. Caracterización combinatoria de la celda de Voronoi para lattices de tipo I en dimensión 5	33
2.2.1. Caras 0-dimensionales de la celda	34
2.2.2. Caras 1-dimensionales de la celda	34
2.2.3. Caras 2-dimensionales de la celda	34

2.2.4. Caras 3-dimensionales de la celda	35
2.3. Caracterización vectorial del la celda de Voronoi	38
2.3.1. Vértices de la Celda	39
2.4. Aristas de la celda	41
2.5. Caras de dimensión 2 de la celda	47
2.6. Caras k -dimensionales de la celda	51
3. Cálculo de la constante de cuantización	55
3.1. Motivación	56
3.2. Partición de la celda de Voronoi	62
3.3. Árboles de búsqueda binarios	71
3.4. Volumen de un simplex	75
3.5. Segundo momento de un simplex	81
4. Conclusiones y propuestas futuras	86
4.1. Problemas asociados a lattices y una posible aplicación en Criptografía . . .	87
4.2. Lattices de primer tipo como cuantizadores	90
Bibliografía	108

Resumen

Un *retículo euclideo* o *lattice euclideo* es un subconjunto Λ de $\mathbb{R}^n$ que consiste de todas las combinaciones lineales enteras de n vectores linealmente independientes. Los lattices de primer tipo son especiales porque poseen la propiedad de tener superbase obtusa. Esta característica se traduce en que debe existir un conjunto de $n + 1$ vectores del lattice donde la suma de todos estos vectores sea cero, donde cualquier subconjunto de n vectores es una base del mismo, y el producto interno de cualquiera dos de estos vectores es negativo. La región de puntos que están más cerca de $\mathbf{v} \in \Lambda$ que de cualquier otro punto de Λ se conoce como la celda de Voronoi en $\mathbf{v}$.

El contexto de esta investigación surge al enfrentar el desafío de encontrar el mejor lattice cuantizador para lattices de primer tipo, eficiencia que se mide con la constante de cuantización G_n de cada lattice

$$G_n(\Lambda) = \frac{1}{n} \frac{\int_{V(\mathbf{0})} \mathbf{x} \cdot \mathbf{x} d\mathbf{x}}{\text{vol}(V(\mathbf{0}))^{1+\frac{2}{n}}},$$

donde $V(0)$ es la celda de Voronoi centrada en el origen. En este sentido, a lo largo del documento, exploraremos resultados que no solo tienen un impacto en la teoría de lattices, sino que también establecen puentes entre geometría, combinatoria y grafos. Se muestra que las celdas de Voronoi en estos lattices son permutahedros. Esta conexión entre geometría y combinatoria abre nuevas perspectivas y posibilidades para abordar problemas relacionados con lattices. Lo anterior se obtuvo con una generalización de la técnica usada por Barnes en [4] y [8]. .

Entre los resultados destacados se encuentra la determinación del volumen y el segundo momento de la celda de Voronoi, desde una perspectiva combinatoria, además se demuestra una fórmula combinatoria sintética para la constante de cuantización para lattices de primer tipo en dimensión 5, lo que proporciona información esencial para resolver el problema del mejor lattice cuantizador y se plantean posibles aplicaciones en Criptografía y Teoría de la Información.

Palabras Clave: Lattices Euclideos, Permutohedro, Celda de Voronoi, Segundo Momento,

problema del vector más cercano, Criptografía basada en lattices.

Introducción

Un *retículo* o *lattice euclidean* es un subconjunto Λ de $\mathbb{R}^n$ que consiste de todas las combinaciones lineales enteras de n vectores linealmente independientes de $\mathbb{R}^n$, es decir, $\Lambda = \{\sum_{i=1}^n k_i \mathbf{v}_i : k_i \in \mathbb{Z}\}$ donde el conjunto $B = \{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ es una base de $\mathbb{R}^n$.

Un ejemplo muy sencillo de lattice es $\mathbb{Z}^n$, es decir, todos los puntos del espacio $\mathbb{R}^n$ cuyas coordenadas son todas enteras; y es llamado, el *lattice cúbico* o el *lattice canónico* (*standard*).

De otro lado, un *cuantizador* o *quantizer* puede ser pensado como un conversor analógico-digital, son extensamente usados en el mundo real. Intuitivamente un cuantizador es un dispositivo que aproxima una señal analógica continua mediante una señal digital discreta, o como dice Conway en [8] (Capítulo 2 pág 56), enfocándonos en cuantizadores en $\mathbb{R}$: un cuantizador es un aparato que transforma números “feos” en “bonitos”.

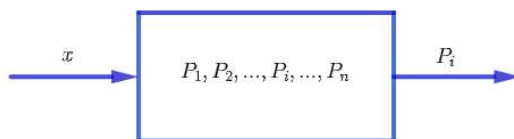


Figura 1: Representación de un cuantizador.

En la figura, $\mathbf{x}$ es una señal que pasa por el dispositivo, cuantizador, el cual lo transforma en uno de sus puntos $\mathbf{P}_i$. Un ejemplo muy sencillo de un cuantizador, es redondear números reales a números enteros.

En el proceso de cuantización, se agrupan señales analógicas en colecciones que se asocian a

un elemento de un conjunto discreto de señales digitales, es decir, cada señal de esa colección se cambia por el valor digital asociado.

Los cuantizadores son útiles en la codificación de señales, por ejemplo, de audio y video, y en la transmisión de información digital. Su uso permite comprimir datos y reducir la cantidad de información necesaria para representar una señal, logrando una mejor eficiencia en la transmisión y el almacenamiento de información digital.

Desde un punto de vista más formal, se puede construir un cuantizador utilizando un subconjunto discreto H de $\mathbb{R}^n$. Para ello, se asigna a cada punto $\mathbf{x} \in \mathbb{R}^n$ un punto $\mathbf{P}_i \in H$ que cumpla la condición de ser el más cercano a $\mathbf{x}$ con respecto a la métrica euclidiana. En otras palabras, un cuantizador sobre H es una relación que asigna a cada punto $\mathbf{x} \in \mathbb{R}^n$ un punto $\mathbf{P}_i \in H$, de manera que la distancia euclidiana entre $\mathbf{x}$ y H sea igual a la distancia entre $\mathbf{x}$ y $\mathbf{P}_i$. La región de puntos que están más cerca de $\mathbf{P}_i$ que de cualquier otro punto de H se conoce como la *celda de Voronoi en $\mathbf{P}_i$* , note el lector que dichas celdas generan una partición del espacio.

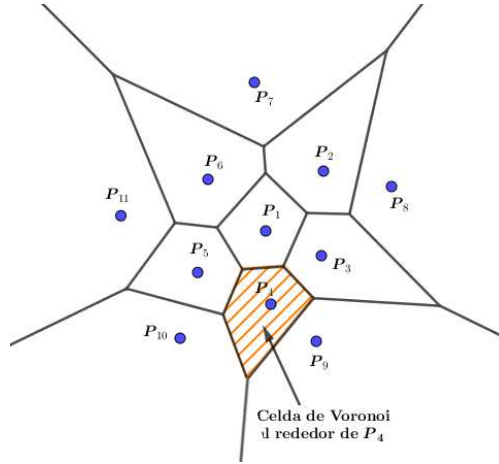


Figura 2: Ejemplo de un cuantizador finito y de la partición generada en el plano.

También se puede observar que en algunos casos la asignación realizada en el proceso no es única, esto pasa en aquellos puntos que se encuentran en las fronteras de las celdas de Voronoi. Para estos casos, se realiza la asignación de manera aleatoria, al ser la frontera delgada, esos puntos no interfieren en el proceso de cuantización.

Como es evidente, el proceso de identificación que lleva a cabo un cuantizador, es decir, asignar puntos de H a los puntos de $\mathbb{R}^n$, introduce errores ya que el punto que entra al cuantizador generalmente no es el mismo punto que se le asigna. Estos errores se miden usualmente con el *error cuadrático medio*. Se pueden consultar los detalles técnicos en [8] (Capítulo 2, página 56).

El problema del cuantizador óptimo consiste en encontrar una forma de elegir los puntos $\mathbf{P}_i$ de manera que se minimice este error cuadrático medio, es decir, se busca minimizar

$$E = \frac{1}{n} \int_{\mathbb{R}^n} N(\mathbf{x} - \mathbf{P}_i) p(\mathbf{x}) d\mathbf{x}, \quad (1)$$

donde $\mathbf{P}_i$ es el punto de H más cercano a $\mathbf{x}$, $N(\mathbf{x}) = \mathbf{x} \cdot \mathbf{x}$ y $p(\mathbf{x})$ es la distribución de densidad de $\mathbf{x}$, que además de decir como se comportan las señales o puntos $\mathbf{x}$, dan un grado de controlabilidad de la integral, ya que esta función, por definición, en puntos muy dispersos tiende a cero. El valor de $p(\mathbf{x})$ en los puntos de la fronteras de las celdas de Voronoi se toma despreciable.

Un lattice es una estructura matemática que puede ser usada como cuantizador. Una de las principales ventajas de utilizar un lattice como cuantizador es que los puntos de cuantización están ubicados regularmente sobre el espacio y las celdas de Voronoi son todas congruentes entre sí, lo que hace el cálculo de E , más sencillo. En la sección (1.5) se muestra una generalidad del proceso que se usa para llegar a definir la constante de cuantización, G_n , de un lattice en $\mathbb{R}^n$, que mide la eficiencia de un lattice como cuantizador, y dicha constante es la que se debe minimizar evaluándola sobre todos los lattices en una dimensión específica n . La constante de cuantización G_n para un lattice Λ en $\mathbb{R}^n$ viene dada por:

$$G_n(\Lambda) = \frac{1}{n} \frac{\int_{V(\mathbf{0})} \mathbf{x} \cdot \mathbf{x} d\mathbf{x}}{\text{vol}(V(\mathbf{0}))^{1+\frac{2}{n}}} \quad (2)$$

donde $V(0)$ es la celda de Voronoi centrada en el origen. La solución del problema de cuantización en dimensión 1, se logra al colocar los puntos P_i de manera uniforme a lo largo de la recta real. Esto resulta, sin pérdida de generalidad, en la formación del lattice entero

$\mathbb{Z}$. De esta manera, las celdas de Voronoi son intervalos de longitud 1.

El cálculo del error cuadrático promedio en la cuantización unidimensional uniforme se puede realizar utilizando la integral

$$G_1 = \frac{\int_{-1/2}^{1/2} x^2 dx}{\int_{-1/2}^{1/2} dx} = \frac{1}{12} = 0.083333 \dots,$$

donde $[-\frac{1}{2}, \frac{1}{2}]$ es el intervalo de cuantización y 0 es el valor digital asociado a los puntos dentro del intervalo.

G. Fejes Tóth resolvió el problema para dimensión 2 [15], donde como era de esperarse el retículo hexagonal es el mejor cuantizador. En dimensión 3 el problema fue resuelto por Barnes y Sloane [4]. Conway y Sloane realizaron una serie de cálculos de constantes de cuantización para algunos lattices y reunieron resultados en capítulo 21 [8]. Estos resultados se calcularon explícitamente utilizando la técnica empleada por Barnes y Sloane en [4] y que servirá como paso inicial para el desarrollo de este documento.

La siguiente es una gráfica de resultados generales sobre el problema de cuantización, la cual ha sido tomada de [1].¹

¹El dual de un retículo es otro retículo obtenido a partir del original por medio de un proceso llamado *dualización*. El proceso consiste en tomar el conjunto de todos los vectores de $\mathbb{R}^n$ que son perpendiculares a cada vector del retículo original y formar un nuevo retículo con ellos. Es decir, el dual de un retículo en $\mathbb{R}^n$ está compuesto por todos los vectores de la forma $(y_1, y_2, \dots, y_n)$, donde cada y_i es un número entero, tal que su producto escalar con cualquier vector del retículo original es un número entero, el dual de Λ se denota por Λ^* .

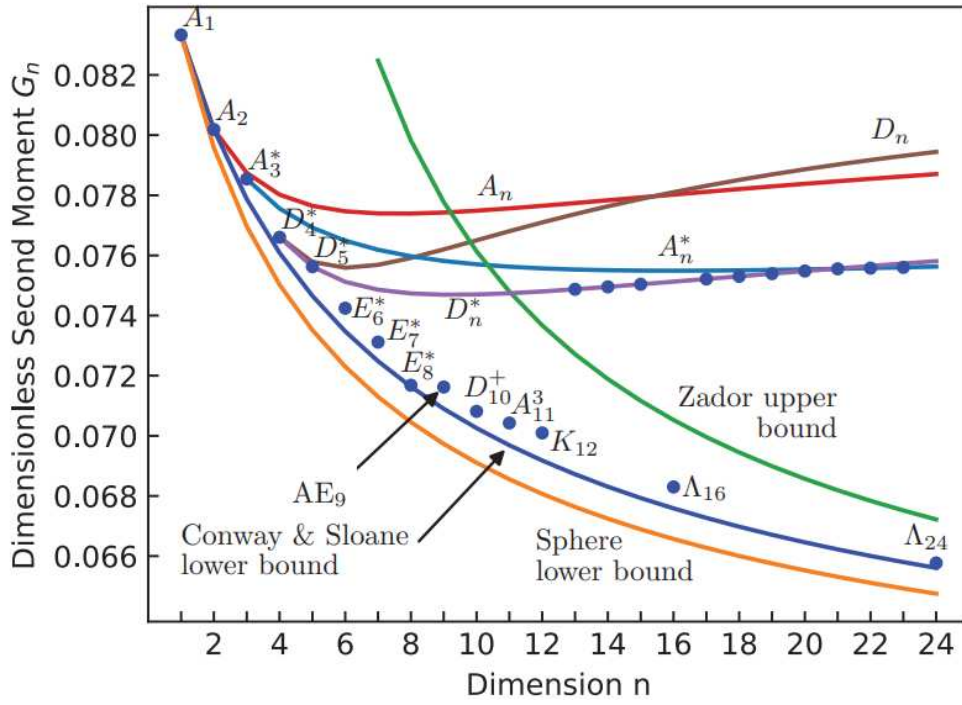


Figura 3: Problema de cuantización en dimensiones menores a 24.

En la gráfica presentada, la curva aproximada, dada por la familia de retículos A_n , se representa mediante una línea roja. Este tipo de retículo se define en $\mathbb{R}^{n+1}$ como el conjunto de vectores $(x_1, x_2, \dots, x_{n+1}) \in \mathbb{Z}^{n+1}$ cuya suma es igual a cero, es decir, $\sum_{i=1}^{n+1} x_i = 0$. La línea naranja representa la cota inferior obtenida al calcular el segundo momento normalizado de la esfera, mientras que la línea verde representa la cota superior dada por Zador. La línea azul, por su parte, representa la cota inferior dada por Conway. Además, se menciona que existen otros retículos especiales como E_n y K_{12} , pero no serán objeto de estudio en este proyecto. Si el lector desea profundizar sobre alguno de los tópicos tratados en este párrafo puede consultar [8] Capítulo 2 sección 3, Capítulo 4 donde se hace la construcción y el estudio de los retículos mencionados y Capítulo 21 donde encontrará una serie de resultados sobre la constante de cuantización en diferentes familias de retículos.

n	Name of quantizer	Mean squared error G
0	Λ_0	0
1	Z	0.083333
2	$A_2^* \cong A_2$	0.080188
3	$A_3^* \cong D_3^*$	0.078543
	$A_3 \cong D_3$	0.078745
4	$D_4^* \cong D_4$	0.076603
	A_4^*	0.077559
	A_4	0.078020
5	D_5^*	0.075625
	D_5	0.075786
	A_5^*	0.076922
	A_5	0.077647
6	E_6^*	0.074244
	E_6	0.074347
7	E_7^*	0.073116
	E_7	0.073231
8	$E_8^* \cong E_8$	0.071682
	D_8^*	0.074735
	D_8	0.075914
	A_8^*	0.075972
	A_8	0.077391
9	AE_9	0.071622
12	$K_{12}^* \cong K_{12}$	0.070100 ± 0.000024
16	$\Lambda_{16}^* \cong \Lambda_{16}$	0.068299 ± 0.000027
24	$\Lambda_{24}^* \cong \Lambda_{24}$	0.065771 ± 0.000074

Tabla 1: Mejores retículos cuantizadores conocidos en dimensiones menores a 24.

La Tabla 1.1 y la Figura (3) muestran los mejores reticulos cuantizadores encontrados hasta dimensión $n \leq 24$. Para algunos de estos retículos $G(\Lambda)$ se determinó exactamente, (ver [8] Capítulo. 21).

Es importante destacar que cualquier avance que se logre en esta dirección será significativo, ya que representaría nuevos logros en la comprensión del problema general en donde se enmarca esta investigación, dicho sea de paso los últimos resultados completos son los que corresponden a dimensión 3, hay otros resultados parciales en dimensión 4 obtenidos por el asesor de este proyecto, y los que recientemente, y de manera computacional, usando

métodos de estimación han obtenido Agrell et al [1]. Además, dado que la cuantización es un problema de optimización, cualquier contribución que permita calcular la constante de cuantización para diferentes lattices (como en este caso la familia de lattices Tipo I) sería un avance significativo en la comprensión del comportamiento del problema. Esto ayudaría a determinar el camino apropiado a seguir para encontrar la solución óptima, así como también evitaría seguir por caminos que no conducen a la solución.

Como es de esperarse, la esfera tiene el menor segundo momento normalizado debido a su simetría esférica perfecta y su distribución uniforme de puntos. El segundo momento normalizado se puede entender como una medida de la dispersión de los puntos en una figura, por lo que la esfera sería un candidato ideal para la cuantización, desafortunadamente, los cuantizadores no pueden ser contruidos con esferas como celdas de Voronoi a excepción de dimensión 1, ya que estos objetos no llenan el espacio. Aún así la esfera puede ayudar a determinar qué politopo es mejor para la cuantización, ya que se puede comparar su segundo momento normalizado con el de la esfera y evaluar cuánto distan los resultados, sabiendo que el segundo momento normalizado de la esfera

$$G(S_n) \rightarrow \frac{1}{2\pi e} = 0.0585498 \dots \text{ cuando } n \rightarrow \infty$$

genera una cota inferior a la constante de cuantización la cual es conocida como la cota de Zador, estos cálculos se pueden ver en [8] y [27].

En este trabajo de investigación, se estudiará el ***problema del retículo cuantizador óptimo*** o ***lattice quantizer problem*** en dimensión 5. En particular aportamos una manera de expresar la constante de cuantización de un lattice de primer Tipo en dimensión 5 mediante una fórmula combinatoria sintética de fácil recordación.

El trabajo se organiza de la siguiente manera: en el Capítulo 1 se presenta una breve introducción a los lattices euclidianos, se incluyen definiciones y propiedades fundamentales para el desarrollo del estudio que hemos realizado. En particular se presentan tres sistemas de coordenadas para puntos en $\mathbb{R}^n$, los cuales serán útiles para manipular los cálculos que se harán. Además, se ofrece un breve estado del arte sobre cómo se han calculado las fórmulas

para la constante de cuantización en lattices de primer tipo en dimensión 2, 3 y 4.

En el Capítulo 2, ofrecemos una descripción detallada, tanto combinatoria como vectorial, de la celda de Voronoi para lattices de primer tipo en cualquier dimensión. Exploramos el comportamiento de los vértices y aristas de la celda en dimensiones arbitrarias, lo que proporciona una comprensión más completa de su estructura y características. Además, presentamos ejemplos concretos en dimensión 5, que es el enfoque principal de este trabajo. Al final de este capítulo, presentamos una fórmula que conjetura la constante de cuantización para lattices de primer tipo en cualquier dimensión, lo cual abre la puerta al Capítulo 3.

En el Capítulo 3, validamos la conjetura en dimensión 5 para lattices de primer tipo. Para hacerlo nos apoyamos fuertemente en la descripción detallada de la celda de Voronoi presentada en el capítulo anterior y nos inspiramos en el trabajo realizado por Barnes y Sloane en [4]. Además, realizamos un análisis exhaustivo de las simetrías de la celda y descubrimos que, utilizando nociones de otras áreas de las matemáticas, como árboles binarios y grafos, los algoritmos para calcular esta constante pueden optimizarse considerablemente, lo cual hizo posible el cálculo. Estos algoritmos optimizados se detallarán en el apéndice al final del trabajo.

En el Capítulo 4, concluimos nuestro trabajo destacando las contribuciones realizadas y explorando las posibles direcciones futuras que se derivan de nuestra investigación. Presentando algunas generalidades sobre posibles aplicaciones de lattices a la criptografía moderna. Además, identificamos áreas de investigación más teóricas, como la exploración de nuevas dimensiones y familias de lattices, que podrían ampliar aún más nuestra comprensión de estos objetos matemáticos. Por último, hacemos referencia a dos artículos específicos [22] y [24] que tienen alta sinergia con nuestro trabajo, ya que presentan algoritmos para resolver el problema del vector más cercano para lattices de primer tipo en tiempo polinomial. Además, destacamos que estos artículos abren la posibilidad de aplicar estas ideas en el mundo real, especialmente en áreas como la transmisión de información y la criptografía pos-cuántica [18].

Capítulo 1

Preliminares

En esta primera sección de los preliminares, exploramos algunos aspectos algebraicos de los lattices, los cuales serán el soporte para las cuentas que realizaremos. Es así como, se explorarán conceptos y definiciones fundamentales, entre estas la noción de base y superbase, la norma de un vector de un lattice y la norma de un vector de Voronoi. Estos conceptos son esenciales en nuestro acercamiento al problema del retículo cuantizador. Algunos resultados se presentan únicamente en calidad de información complementaria y por tal razón se omiten sus pruebas.

1.1. Lattices

Definición 1.1. Un subconjunto Λ de $\mathbb{R}^n$ es un *lattice* (o retículo) n -dimensional o de rango n si existe un subconjunto $B = \{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\}$ de n vectores linealmente independientes en $\mathbb{R}^n$ tales que

$$\Lambda = \left\{ \sum_{i=1}^n x_i \mathbf{v}_i : x_i \in \mathbb{Z} \right\}.$$

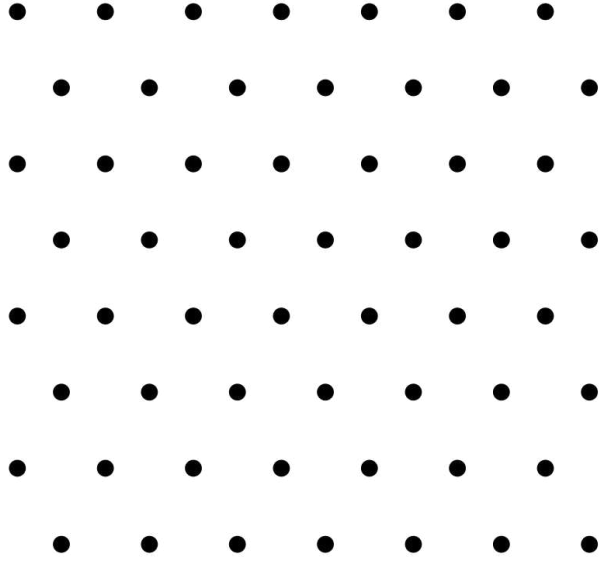


Figura 1.1: Puntos de un lattice en dimensión 2.

Es bien sabido que cualquier combinación lineal de vectores puede representarse como el producto de un vector por una matriz. Por lo tanto, se define la *matriz generadora* M del lattice como aquella que tiene como columnas los vectores de la base del lattice, es decir, considerando las coordenadas de los vectores de B en la base canónica de $\mathbb{R}^n$,

$$\begin{aligned} \mathbf{v}_1 &= (\mathbf{v}_{11}, \mathbf{v}_{21}, \dots, \mathbf{v}_{n1})^T \\ \mathbf{v}_2 &= (\mathbf{v}_{12}, \mathbf{v}_{22}, \dots, \mathbf{v}_{n2})^T \\ &\vdots \\ \mathbf{v}_n &= (\mathbf{v}_{1n}, \mathbf{v}_{2n}, \dots, \mathbf{v}_{nn})^T. \end{aligned}$$

Se tiene que la matriz generadora es de la forma

$$M = \begin{pmatrix} \mathbf{v}_{11} & \mathbf{v}_{12} & \cdots & \mathbf{v}_{1n} \\ \mathbf{v}_{21} & \mathbf{v}_{22} & \cdots & \mathbf{v}_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{v}_{n1} & \mathbf{v}_{n2} & \cdots & \mathbf{v}_{nn} \end{pmatrix}.$$

En consecuencia, para cualquier elemento $\mathbf{t} \in \Lambda$, existe $\mathbf{x} = (x_1, x_2, \dots, x_n)^T \in \mathbb{Z}^n$ tal que $\mathbf{t} = M\mathbf{x}$. De esta manera, el lattice también se puede representar como $\Lambda = \{M\mathbf{x} : \mathbf{x} \in \mathbb{Z}^n\}$.

La matriz de Gram A del lattice se define como $A = M^T M$. La matriz de Gram es muy importante en el desarrollo de este trabajo, entre otras cosas debido a que sus entradas se utilizarán como parámetros del lattice y a través de ellos se puede obtener una descripción detallada no sólo del lattice sino también de su celda de Voronoi.

Definición 1.2. Sea Λ un lattice n -dimensional y $B = \{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\}$ una base para Λ . Al conjunto

$$P := \left\{ \sum_{i=1}^n t_i \mathbf{v}_i : 0 \leq t_i < 1 \right\}$$

se le llama *Paralelotopo fundamental* para Λ .

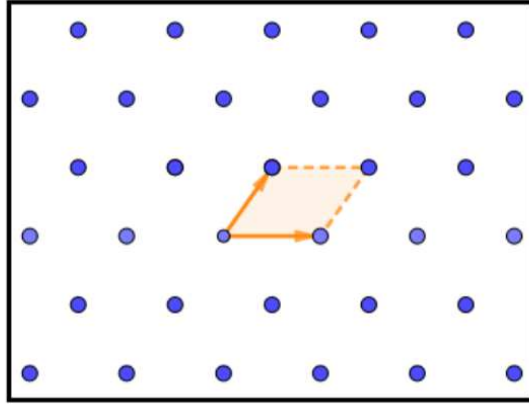


Figura 1.2: Paralelotopo fundamental en dimensión 2.

Es importante destacar que el paralelotopo fundamental cubre el espacio $\mathbb{R}^n$ por traslación sobre los vectores del lattice.

En general, el paralelotopo fundamental proporciona una comprensión intuitiva de cómo se organiza un lattice en el espacio. A partir del paralelotopo se pueden inferir propiedades importantes del lattice, y cómo se asemeja a otros lattices.

En ese sentido, una pregunta importante que resulta es ¿cuándo dos lattices son equivalen-

tes o semejantes?, es decir, ¿cuándo tienen la misma estructura geométrica y pueden ser transformados uno en el otro mediante una transformación rígida del espacio o incluso una homotecia?

Esta cuestión es interesante ya que muchos problemas en lattices se reducen a encontrar una base de un lattice equivalente a otro con ciertas propiedades deseables.

Proposición 1.3. Dos bases distintas generan el mismo lattice, si y solo si, existe una matriz invertible (con determinante ± 1) que relaciona las coordenadas de una base con las de la otra. Es decir, si B_1 y B_2 son dos bases para $\mathbb{R}^n$, entonces B_1 y B_2 generan el mismo lattice si, y solo si existe una matriz U invertible con determinante ± 1 y entradas enteras tal que $M_2 = M_1 U$, siendo M_1 y M_2 las respectivas matrices generadoras asociadas a B_1 y B_2 .

De esta manera, se pueden encontrar bases que sean más convenientes para ciertos cálculos o para la resolución de problemas específicos. La matriz U pertenece al grupo lineal simétrico $GL_n(\mathbb{Z})$, que es el conjunto de todas las matrices invertibles de $n \times n$ con coeficientes enteros y determinante ± 1 .

Decimos que el *volumen de un lattice* es el volumen de su paralelotopo fundamental. Ahora, si las bases B_1 y B_2 se representan mediante las matrices generadoras M_1 y M_2 , respectivamente, es evidente que el volumen del lattice generado por B_1 es igual al volumen del lattice generado por B_2 , ya que el volumen del paralelotopo fundamental es el mismo para ambas bases, por esto se puede decir que el volumen del paralelotopo fundamental es una característica propia del lattice independiente de la base.

Así que, cada lattice tiene asociado un volumen, que se le conoce como el volumen del lattice y se denota por $\text{vol}(\Lambda)$. Más aún, el volumen del lattice y el determinante de la matriz de Gram, A , asociada al lattice se relacionan de la siguiente forma:

$$\text{vol}(\Lambda)^2 = \det(A).$$

1.2. Celdas y Vectores de Voronoi

En esta sección trataremos el concepto de celdas de Voronoi de un lattice, las cuales son regiones que particionan el espacio y su forma muestra parte del comportamiento del lattice. Las celdas fueron introducidas por el matemático ruso Georgy Voronoi en 1907 en un estudio sobre las formas cuadráticas. [25].

Definición 1.4. Sea Λ un lattice n -dimensional, y $\mathbf{u} \in \Lambda$. La celda de Voronoi al rededor de $\mathbf{u}$, que se denota por $V(\mathbf{u})$, es el conjunto de puntos de $\mathbb{R}^n$ que están al menos tan cerca de $\mathbf{u}$ como de cualquier otro punto del lattice, esto es:

$$V(\mathbf{u}) = \{\mathbf{x} \in \mathbb{R}^n : d(\mathbf{x}, \mathbf{u}) \leq d(\mathbf{x}, \mathbf{v}) \text{ para todo } \mathbf{v} \in \Lambda\}$$

donde $d(\cdot, \cdot)$ es la distancia euclídea en $\mathbb{R}^n$

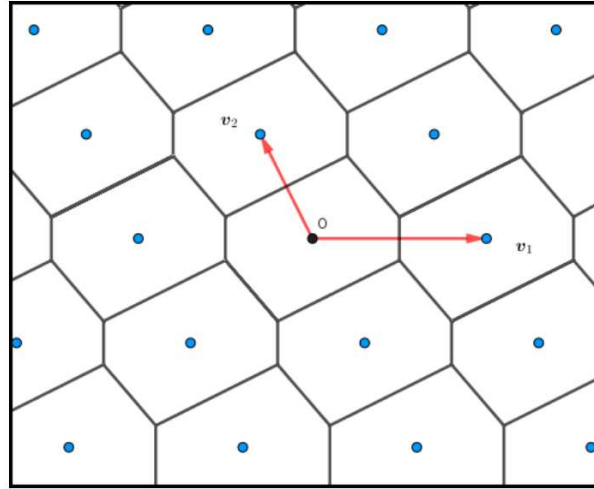


Figura 1.3: Ejemplo de celda de Voronoi para un lattice en dimensión 2.

Estas celdas son una herramienta importante en el estudio de los lattices, ya que permiten construir un teselado o embaldosamiento del espacio, y su forma es una característica propia del lattice. Considerando la celda de Voronoi asociada al origen, $V(\mathbf{0})$, mediante traslaciones de dicha celda por vectores del lattice, se puede cubrir todo el espacio,

$$V(\mathbf{u}) = \mathbf{u} + V(\mathbf{0}) \text{ para todo } \mathbf{u} \in \Lambda.$$

Por otro lado, si P es el paralelotopo fundamental de un lattice Λ , y $V(\mathbf{0})$ es la celda de Voronoi centrada en el origen, y además

$$A_v = P \cap (\mathbf{v} + V(\mathbf{0})) \text{ y } B_v = V(\mathbf{0}) \cap (\mathbf{v} + \mathbf{P}), \text{ para } \mathbf{v} \in \Lambda.$$

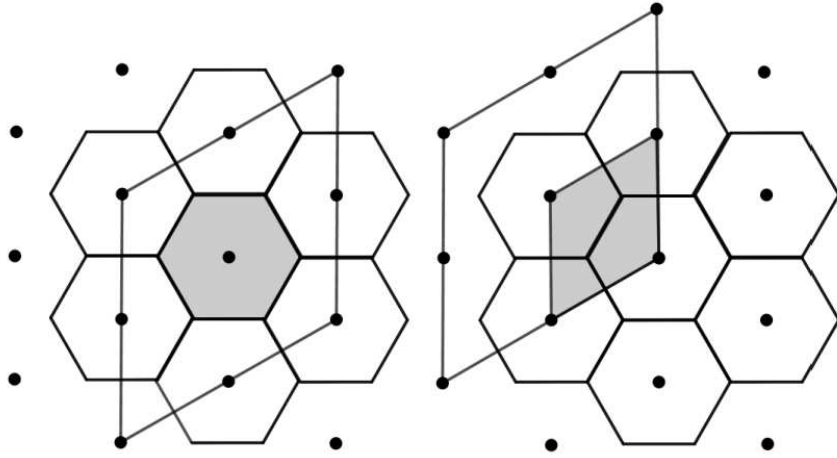


Figura 1.4: Relación entre el paralelotopo fundamental y la celda de Voronoi.

Se puede probar, sin mucha dificultad, que

$$B_v = [(-\mathbf{v} + V(\mathbf{0})) \cap \mathbf{P}] + \mathbf{v} = \mathbf{A}_{-\mathbf{v}} + \mathbf{v}.$$

Debido a la construcción del paralelotopo fundamental y las celdas de Voronoi, los conjuntos A_v son disjuntos, de igual manera pasa con los elementos de B_v . Así que

$$\text{Vol}(V(\mathbf{0})) = \text{Vol}(\dot{\cup}_{\mathbf{v} \in \Lambda} B_v) = \text{Vol}(\dot{\cup}_{\mathbf{v} \in \Lambda} A_{-\mathbf{v}}) = \text{Vol}(P).$$

Lo que se recoge en el siguiente resultado.

Proposición 1.5. [26] La celda de Voronoi $V(\mathbf{0})$ y el paralelotopo fundamental P de un lattice Λ tienen el mismo volumen. Aún más, si A es la matriz de Gram asociada al lattice,

$$\text{Vol}(\Lambda) = \text{Vol}(V(\mathbf{0})) = \text{Vol}(P) = \sqrt{\det A}.$$

Definición 1.6. Sea Λ un lattice n -dimensional, un vector $\mathbf{v} \in \Lambda$ se dice que es *un vector de Voronoi* si el hiperplano

$$H'_{\mathbf{v}} := \left\{ \mathbf{x} \in \mathbb{R}^n : \mathbf{x} \cdot \mathbf{v} = \frac{1}{2} \mathbf{v} \cdot \mathbf{v} \right\} \quad (1.1)$$

tiene intersección no vacía con $V(\mathbf{0})$ (la celda de Voronoi centrada en el origen).

Además, se dice que un vector de Voronoi es *estricto o relevante*, si la intersección anterior es una facet o cara $(n - 1)$ -dimensional de $V(\mathbf{0})$, en caso contrario se dice que es laxo o irrelevante.

Se puede observar que para cada $\mathbf{v} \neq \mathbf{0}$ en el lattice, los semiespacios de la forma

$$H_{\mathbf{v}} := \left\{ \mathbf{x} \in \mathbb{R}^n : \mathbf{x} \cdot \mathbf{v} \leq \frac{1}{2} \mathbf{v} \cdot \mathbf{v} \right\} \quad (1.2)$$

definen un semiespacio que contiene a la celda de Voronoi $V(\mathbf{0})$. En otras palabras, para cualquier punto $\mathbf{x}$ en la celda de Voronoi, se cumple que $\mathbf{x} \cdot \mathbf{v} \leq \frac{1}{2} \mathbf{v} \cdot \mathbf{v}$ para todo $\mathbf{v} \in \Lambda \setminus \mathbf{0}$. Por lo tanto, la celda de Voronoi $V(\mathbf{0})$ se puede expresar como la intersección de todos los semiespacios $H_{\mathbf{v}}$ para $\mathbf{v} \in \Lambda \setminus \mathbf{0}$.

A continuación, se presenta un resultado dado por Conway y Sloane, que ofrece una caracterización de los vectores de Voronoi.

Teorema 1.7 ([10], pág 56). Sea Λ un lattice en $\mathbb{R}^n$ y $\mathbf{v}$ un vector no cero de Λ . Entonces

- $\mathbf{v}$ es un vector de Voronoi, si y solo si, $\mathbf{v}$ es uno de los vectores más cortos de la clase

$$\mathbf{v} + 2\Lambda.$$

- $\mathbf{v}$ es un vector de Voronoi estricto si y sólo si $\mathbf{v}$ y $-\mathbf{v}$ son los únicos vectores más cortos en $\mathbf{v} + 2\Lambda$.

Dado que hay $2^n - 1$ clases no nulas en $\Lambda/2\Lambda$, según el primer ítem del teorema, hay a lo sumo $2(2^n - 1)$ vectores de Voronoi.

1.3. Parámetros de Selling y Lattices Tipo I

Definición 1.8. Sea Λ un lattice en $\mathbb{R}^n$, se dice que:

- $B = \{\mathbf{v}_0, \mathbf{v}_1, \dots, \mathbf{v}_n\}$, un conjunto de $n + 1$ vectores de Λ , es una *superbase* de Λ si $\{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\}$ es una base de Λ y $\sum_{i=0}^n \mathbf{v}_i = \mathbf{0}$.
- Si el producto interno de cualquier par de vectores de una superbase B , es menor o igual que cero, a B se le llama una *superbase obtusa* de Λ . En caso de que Λ admita una superbase obtusa se dirá que es un lattice de Tipo I, si el producto de cada par de vectores de la superbase es estrictamente menor que cero, decimos que B es una *superbase obtusa estricta*.

En la definición de superbase obtusa estricta, uno de los requisitos es que el producto interno entre cualesquiera dos elementos de la superbase sea negativo. Esto se debe a que el producto interno está relacionado con el coseno del ángulo entre los vectores, y si los ángulos son obtusos, garantiza que las sumas de vectores sean vectores más cortos que restas de ellos. Por ejemplo, si se tienen dos vectores con un ángulo agudo entre ellos, la suma de los vectores será un vector más grande que la resta de ellos. Al tener ángulos obtusos en la superbase, se evita esta situación y se asegura que todas las sumas de vectores sean cortos, estos vectores cortos finalmente serán los vectores de Voronoi del lattice, resultado que se presenta en el Teorema (1.11).

En dimensión 2 y 3, todos los lattices son de tipo I, es decir admiten una superbase obtusa, pero de dimensión 4 en adelante, hay lattices que no admiten dicho tipo de superbases, en dimensión 4 hay 3 posibles tipos de lattices, en dimensión 5 hay 222 tipos de lattices, este número crece considerablemente a medida que la dimensión del lattice crece.

Definición 1.9. Si $B = \{\mathbf{v}_0, \mathbf{v}_1, \dots, \mathbf{v}_n\}$ es una superbase de un lattice Λ , a los $\binom{n+1}{2}$ valores

$$p_{ij} = -\mathbf{v}_i \cdot \mathbf{v}_j, \quad \text{con } 0 \leq i < j \leq n$$

se les llama *parámetros de Selling* de Λ relativos a la superbase B . Adicionalmente, si se denota por $p_{i|jk\dots l} = p_{ij} + p_{ik} + \dots + p_{il}$, siendo p_{ij} a los parámetros de Selling, entonces *la matriz de Gram aumentada* para la superbase es

$$A' = \begin{pmatrix} p_{0|12\dots n} & -p_{01} & \cdots & -p_{0n} \\ -p_{01} & p_{1|02\dots n} & \cdots & -p_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ -p_{0n} & -p_{1n} & \cdots & p_{n|01\dots n-1} \end{pmatrix}. \quad (1.3)$$

Teorema 1.10. Sea Λ un lattice n -dimensional y $B = \{\mathbf{v}_0, \mathbf{v}_1, \dots, \mathbf{v}_n\}$ una superbase de Λ con parámetros de Selling asociados $p_{ij} = -\mathbf{v}_i \cdot \mathbf{v}_j$ para $0 \leq i < j \leq n$, y sea $\mathbf{x} = \sum_{i=0}^n x_i \mathbf{v}_i$, con $x_i \in \mathbb{R}$. Entonces, la norma de $\mathbf{x}$, es decir, $N(\mathbf{x}) = \mathbf{x} \cdot \mathbf{x}$ se expresa de la siguiente forma:

$$N(\mathbf{x}) = \sum_{i < j} p_{ij} (x_i - x_j)^2.$$

Demostración. Consideremos $\mathbf{x} = \sum_{i=0}^n x_i \mathbf{v}_i$, de ahí que

$$\begin{aligned}
N(\mathbf{x}) &= \left(\sum_{i=0}^n x_i \mathbf{v}_i \right) \cdot \left(\sum_{i=0}^n x_i \mathbf{v}_i \right) \\
&= \sum_{i=0}^n x_i^2 \mathbf{v}_i \cdot \mathbf{v}_i + 2 \sum_{i < k} x_i x_k \mathbf{v}_i \cdot \mathbf{v}_k \\
&= \sum_{i=0}^n x_i^2 \mathbf{v}_i \cdot \left(- \sum_{j \neq i} \mathbf{v}_j \right) - 2 \sum_{i < k} p_{ik} x_i x_k \\
&= \sum_{i=0}^n x_i^2 \sum_{j \neq i} p_{ij} - 2 \sum_{i < k} p_{ik} x_i x_k \\
&= \sum_{i < j} p_{ij} (x_i^2 + x_j^2) - 2 \sum_{i < k} p_{ik} x_i x_k \\
&= \sum_{i < j} p_{ij} (x_i^2 + x_j^2 - 2x_i x_j) \\
&= \sum_{i < j} p_{ij} (x_i - x_j)^2.
\end{aligned}$$

□

Nota. Los x_i dependen de $\mathbf{x}$ mientras que los p_{ij} dependen de la superbase.

Teorema 1.11 ([10], pág 57). Sea Λ un lattice n -dimensional de Tipo I y $B = \{\mathbf{v}_0, \mathbf{v}_1, \dots, \mathbf{v}_n\}$ una superbase obtusa para Λ . Sean S un subconjunto propio de $I_n = \{0, 1, 2, \dots, n\}$ y $\bar{S}$ su complemento respecto a I_n , entonces

- La suma $\mathbf{v}_S = \sum_{i \in S} \mathbf{v}_i$ es un vector de Voronoi de Λ . Además, $\mathbf{v}_S$ y $\mathbf{v}_{\bar{S}} = -\mathbf{v}_S$.
- Los vectores $\mathbf{v}_S$ son todos estrictos si y sólo si la superbase es estricta.

Proposición 1.12. Si Λ es un lattice de Tipo I y $B = \{\mathbf{v}_0, \mathbf{v}_1, \dots, \mathbf{v}_n\}$ es una superbase obtusa de Λ con parámetros de Selling $p_{ij} = -\mathbf{v}_i \cdot \mathbf{v}_j$, y $0 \leq i < j \leq n$, entonces las normas de los vectores de Voronoi de Λ vienen dadas por:

$$N(\mathbf{v}_S) = \sum_{i \in S, j \in \bar{S}} p_{ij}.$$

La prueba de esta proposición se sigue directamente de los dos teoremas anteriores.

1.4. Tipos de coordenadas para $\mathbb{R}^n$

Existen ciertos tipos de coordenadas para representar un elemento de $\mathbf{t} \in \mathbb{R}^n$ que son muy útiles para describir la celda de Voronoi en función de los parámetros de Selling del Lattice. En particular, si se considera una base $B = \{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\}$ de un lattice n -dimensional Λ , se puede representar cada vector $\mathbf{t}$ de tres formas:

- En coordenadas euclídeas. En este caso, al punto $\mathbf{t} \in \mathbb{R}^n$ lo puedo escribir en términos de la base canónica $e_1, e_2, \dots, e_n$, es decir, $\mathbf{t} = (t_1, t_2, \dots, t_n)^T = t_1 e_1 + t_2 e_2 + \dots + t_n e_n$.
- Las x -coordenadas de $\mathbf{t}$ asociadas a la base B . Si $\mathbf{x} = (x_1, x_2, \dots, x_n)^T$, entonces $\mathbf{t} = x_1 \mathbf{v}_1 + x_2 \mathbf{v}_2 + \dots + x_n \mathbf{v}_n$. Además, si M es la matriz generadora del lattice Λ asociada a la base B , se tiene que $\mathbf{t} = M\mathbf{x}$.
- Si A es la matriz de Gram asociada a la base B , se definen las y -coordenadas de $\mathbf{t}$ como $\mathbf{y} = A\mathbf{x}$.

Se puede deducir que $\mathbf{y} = M^T M \mathbf{x} = M^T \mathbf{t}$. De esta forma, las y -coordenadas de $\mathbf{t} \in \mathbb{R}^n$ respecto a la base B son los productos internos del vector $\mathbf{t}$ con los elementos de B , lo que se expresa como $\mathbf{y} = (\mathbf{v}_1 \cdot \mathbf{t}, \mathbf{v}_2 \cdot \mathbf{t}, \dots, \mathbf{v}_n \cdot \mathbf{t})^T$.

Si se considera una superbase en lugar de una base para el lattice, se pueden utilizar las llamadas “coordenadas aumentadas”. En este caso, para un punto $\mathbf{t} \in \mathbb{R}^n$, las coordenadas aumentadas no son únicas, pero capturan la simetría de la celda en mejor manera, este sistema de coordenadas corrige un defecto del usado por Barnes y Sloane en [4], en el que no se captura totalmente la simetría de la celda al ser descrita con los parámetros de Selling.

Ahora, si $\mathbf{t} \in \Lambda$, la norma de $\mathbf{t}$, que denotada $N(\mathbf{t})$, se puede escribir en términos de sus

$\mathbf{x}$ -coordenadas, esto es

$$\begin{aligned} N(\mathbf{t}) &= \mathbf{t}^T \mathbf{t} \\ &= (M\mathbf{x})^T M\mathbf{x} \\ &= \mathbf{x}^T A\mathbf{x}. \end{aligned}$$

Adicionalmente, $N(\mathbf{t})$ se puede expresar con respecto a las $\mathbf{y}$ -coordenadas de $\mathbf{t}$, utilizando el hecho de que $\mathbf{y} = A\mathbf{x}$, concluimos que

$$N(\mathbf{t}) = \mathbf{y}^T A^{-1} \mathbf{y}.$$

Ahora bien, dado que $A^{-1} = \frac{1}{\det(A)} \text{adj}(A)$, siendo $\text{adj}(A)$ la matriz adjunta de A . Al calcular $\text{adj}(A)$, expandir y reordenar se logra establecer la siguiente proposición:

Proposición 1.13. Sea $B = \{\mathbf{v}_0, \mathbf{v}_1, \dots, \mathbf{v}_n\}$ una superbase de un lattice n -dimensional Λ en $\mathbb{R}^n$, con matriz de productos internos $A = (\mathbf{v}_i \cdot \mathbf{v}_j)$, con $0 \leq i \leq j \leq n$, $\Delta = \det(\Lambda)$ y $\Delta_{ij} = \frac{\partial \Delta}{\partial p_{ij}}$. Sea $\mathbf{t} \in \Lambda$, si $\mathbf{x} = (x_0, x_1, \dots, x_n)^T$ son las $\mathbf{x}$ -coordenadas de $\mathbf{t}$, e $\mathbf{y} = A\mathbf{x}$ son sus $\mathbf{y}$ -coordenadas, entonces

$$N(\mathbf{t}) = \frac{1}{\Delta} \left(\sum_{i=1}^n \Delta_{0i} y_i^2 + \sum_{1 \leq i < j \leq n} (\Delta_{0i} + \Delta_{0j} - \Delta_{ij}) y_i y_j \right).$$

Definición 1.14. Un *politopo convexo* P en $\mathbb{R}^n$, es la envolvente convexa ¹ de un número finitos puntos de $\mathbb{R}^n$.

Dado que para un retículo las celdas de Voronoi son politopos congruentes a la celda de Voronoi centrada en cero, y teniendo presente que si P es un politopo en $\mathbb{R}^n$ entonces, su segundo momento no normalizado respecto al origen, que se denota por $U(P)$, está dado

¹La envolvente convexa es la intersección de todos los conjuntos convexos que contienen a un conjunto de puntos X de dimensión n . Dados k puntos $x_1, x_2, \dots, x_k$ su envolvente convexa C viene dada por la expresión:

$$C(X) = \left\{ \sum_{i=1}^k \alpha_i x_i \mid x_i \in X, \alpha_i \in \mathbb{R}, \alpha_i \geq 0; \sum_{i=1}^k \alpha_i = 1 \right\}$$

por:

$$U(P) = \int_P \mathbf{x} \cdot \mathbf{x} d\mathbf{x}.$$

El momento de inercia de P respecto al origen, el cual se va a denotar por $I(P)$, se expresa como:

$$I(P) = \frac{U(P)}{\text{vol}(P)},$$

donde $\text{vol}(P) = \int_P d\mathbf{x}$ es el volumen de P . Por último, el segundo momento normalizado de P respecto al origen es:

$$G(P) = \frac{1}{n} \frac{U(P)}{\text{vol}(P)^{1+2/n}} = \frac{1}{n} \frac{I(P)}{\text{vol}(P)^{2n}}. \quad (1.4)$$

La anterior es otra manera de representar (2).

Ya que la finalidad de este trabajo es encontrar el segundo momento normalizado de un politopo, celda de Voronoi para lattices en dimensión 5, y su cálculo sigue siendo engorroso, se dividirá este problema grande en varios problemas pequeños, es decir, se dividirá la celda de Voronoi en regiones más pequeñas, para las cuales su segundo momento no normalizado sea más sencillo de calcular. En efecto, al dividir la celda de Voronoi en regiones más pequeñas y disjuntas, el numerador de la expresión del segundo momento normalizado se puede expresar como una suma de integrales sobre estas regiones más pequeñas. Esto hace que el cálculo del segundo momento normalizado sea más manejable, utilizando el siguiente resultado, ver capítulo 21, página 456 de [8].

Definición 1.15. Un *simplex* o *n-simplex* es un politopo y es la envolvente convexa de un conjunto de $n + 1$ puntos independientes $\mathbf{u}_1, \dots, \mathbf{u}_{n+1} \in \mathbb{R}^n$ afines, es decir, que $\mathbf{u}_i - \mathbf{u}_j, 1 \leq i \leq n + 1, i \neq j$ son linealmente independientes para todo $j \in \{1, \dots, n + 1\}$.

Así, un 0-simplex es un punto, un 2-simplex es un triángulo, y al 3-simplex le corresponde un tetraedro.

Teorema 1.16. [4] Si $\mathbf{v}_i = (\mathbf{v}_{i1}, \mathbf{v}_{i2}, \dots, \mathbf{v}_{in})$, para $0 \leq i \leq n$, son los v rtices de un simplex n -dimensional T en $\mathbb{R}^n$, entonces:

- El centroide de T es el baricentro de los v rtices:

$$\mathbf{Ba} = \frac{1}{n+1} \sum_{i=0}^n \mathbf{v}_i. \quad (1.5)$$

- El volumen de T es:

$$\text{vol}(T) = \frac{1}{n!} \det \begin{bmatrix} 1 & \mathbf{v}_{01} & \cdots & \mathbf{v}_{0n} \\ 1 & \mathbf{v}_{11} & \cdots & \mathbf{v}_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \mathbf{v}_{n1} & \cdots & \mathbf{v}_{nn} \end{bmatrix}.$$

- El momento de inercia al rededor del origen es:

$$I(T) = \frac{n+1}{n+2} \|\mathbf{Ba}\|^2 + \frac{1}{(n+1)(n+2)} \sum_{i=0}^n \|\mathbf{v}_i\|^2.$$

De la definici n de $U(P)$ se puede ver que si Q es una partici n en n -simplices de un politopo P entonces, el segundo momento no normalizado de P se puede expresar de la siguiente forma:

$$U(P) = \sum_{T \in Q} U(T). \quad (1.6)$$

As  las cosas, usando (1.4) y (1.6), vamos a calcular la constante de cuantizaci n para lattices de primer tipo realizando una partici n  ptima de la celda en simplices.

1.5. Cuantización con Lattices

Un cuantizador es una relación $Q : \mathbb{R}^n \rightarrow H$ que mapea puntos en $\mathbb{R}^n$ a puntos en un subconjunto discreto $H \subseteq \mathbb{R}^n$. La función Q se define de tal manera que el punto en H más cercano al punto de entrada $\mathbf{x}$ es el valor de salida de $Q(\mathbf{x})$.

Ahora bien, si H consiste de un número finito de puntos del espacio euclídeo $\mathbb{R}^n$, el error cuadrático medio se expresa como

$$E = \frac{1}{n} \sum_{i=1}^M \int_{V(\mathbf{P}_i)} N(\mathbf{x} - \mathbf{P}_i) p(\mathbf{x}) d\mathbf{x}, \quad (1.7)$$

se puede notar que E depende de n , la dimensión del espacio, M , el número de puntos de H , y de la función de probabilidad p .

El problema del cuantizador consiste en encontrar el ínfimo de E , cuando se recorren todas las posibles distribuciones finitas de puntos H , en símbolos:

$$E(n, M, p) = \inf_{\{P_i\}} E.$$

Zador, [27], demostró que

$$\lim_{M \rightarrow \infty} M^{2/n} E(n, M, p) = G_n \left(\int_{\mathbb{R}^n} p(\mathbf{x})^{n/(n+2)} d\mathbf{x} \right)^{\frac{n+2}{n}}, \quad (1.8)$$

donde G_n , llamada *constante de cuantización*, sólo depende de n .

Al suponer que $\mathbf{x}$ se distribuye uniformemente en una región suficientemente grande de $\mathbb{R}^n$, es decir, $p(\mathbf{x})$ es la función de densidad uniforme, el error cuadrático medio se minimizará si cada punto $\mathbf{P}_i$ está en el centroide de su región de Voronoi, y (1.7) se puede ver como

$$E = \frac{\frac{1}{n} \sum_{i=1}^M \int_{V(\mathbf{P}_i)} N(\mathbf{x} - \mathbf{P}_i) d\mathbf{x}}{\sum_{i=1}^M \int_{V(\mathbf{P}_i)} d\mathbf{x}} \quad (1.9)$$

y el valor de la integral del lado derecho de la igualdad (1.8) es 1. En consecuencia, usando las ecuaciones (1.8) y (1.9), se tiene

$$G_n = \lim_{M \rightarrow \infty} \frac{1}{n} \frac{\frac{1}{M} \sum_{i=1}^M \int_{V(\mathbf{P}_i)} N(\mathbf{x} - \mathbf{P}_i) d\mathbf{x}}{\left(\frac{1}{M} \sum_{i=1}^M \text{vol}(V(\mathbf{P}_i)) \right)^{1 + \frac{2}{n}}}. \quad (1.10)$$

Ahora, se asume que M es suficientemente grande, de tal manera que la siguiente expresión se aproxime a G_n . El problema consiste en elegir los puntos $P_1, \dots, P_M$ en $\mathbb{R}^n$ de manera que se minimice

$$\frac{1}{n} \frac{\frac{1}{M} \sum_{i=1}^M \int_{V(\mathbf{P}_i)} N(\mathbf{x} - \mathbf{P}_i) d\mathbf{x}}{\left(\frac{1}{M} \sum_{i=1}^M \text{vol}(V(\mathbf{P}_i)) \right)^{1 + \frac{2}{n}}}, \quad (1.11)$$

proporcionando el cuantizador óptimo para entradas distribuidas uniformemente en una región muy grande de $\mathbb{R}^n$.

El lector puede inferir que debido a que los puntos pueden ser elegidos arbitrariamente, las celdas de Voronoi tendrán formas arbitrarias y se requerirá el cálculo de M integrales y volúmenes en $\mathbb{R}^n$. Esto hace que el estudio de la constante de cuantización sea una tarea difícil, ya que queremos que M sea muy grande. Para suavizar el problema, elegimos los puntos de H sobre un lattice, así, todas las celdas de Voronoi sean congruentes a $V(\mathbf{0})$, la celda de Voronoi que contiene al origen. En este caso, (1.10) se transforma en:

$$G_n(H) = \frac{1}{n} \frac{\int_{V(\mathbf{0})} \mathbf{x} \cdot \mathbf{x} d\mathbf{x}}{\text{vol}(V(\mathbf{0}))^{1 + \frac{2}{n}}}. \quad (1.12)$$

A esta última expresión se le conoce como *la constante de cuantización para H , el problema del cuantizador para un lattice*, consiste en minimizar la expresión (1.12) sobre lattices.

En particular, para esta investigación, se van a considerar solo los retículos de tipo I, es decir, aquellos a los que se puede asociar una *superbase obtusa*, debido a que la construcción y etiquetamiento (de vértices y caras) de la celda de Voronoi es cómoda y cuenta con mucha simetría, por ejemplo, como en el retículo hexagonal. Por lo tanto, se pretende calcular la constante de cuantización para retículos en dimensión 5, utilizando otro sistema de coordenadas que provienen de los productos internos de una superbase obtusa del lattice.

1.6. Constante de cuantización para lattices en dimensiones bajas

En esta sección, presentamos una descripción de cómo se representa la celda de Voronoi en lattices de primer tipo, siguiendo el enfoque propuesto por Conway y Sloane [13]. Este cálculo es de gran importancia en este trabajo porque resulta ser la inspiración para la generalización del cálculo de la constante de cuantización en dimensión n .

1.6.1. Descripción de la celda de Voronoi en dimensión 3

Consideremos Λ , un lattice en $\mathbb{R}^3$, con $B = \{\mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ como una superbase obtusa, que sin pérdida de generalidad podemos imaginar estricta, de este lattice. Definimos las $\mathbf{y}$ -coordenadas aumentadas como $(y_0, y_1, y_2, y_3)^T = (\mathbf{v}_0 \cdot \mathbf{t}, \mathbf{v}_1 \cdot \mathbf{t}, \mathbf{v}_2 \cdot \mathbf{t}, \mathbf{v}_3 \cdot \mathbf{t})^T$, donde $\mathbf{t} \in \mathbb{R}^3$. Dado que $\mathbf{v}_0 + \mathbf{v}_1 + \mathbf{v}_2 + \mathbf{v}_3 = 0$, se cumple $y_0 + y_1 + y_2 + y_3 = 0$. Se puede ver que existe la correspondencia de los vectores de la superbase que se suman con respecto a los subíndices de los F .

La celda de Voronoi $V(\mathbf{0})$ es fundamental para el cálculo de la constante de cuantización del lattice. Como hemos dicho, para describirla, nos basaremos en [13]. El Teorema (1.11) establece que los vectores de Voronoi del lattice son de la forma $\mathbf{v}_S = \sum_{i \in S} \mathbf{v}_i$, donde S es un subconjunto propio de $\{0, 1, 2, 3\}$. Esto implica que los siguientes vectores definen la celda de Voronoi:

$$\begin{aligned} &\mathbf{v}_0, \quad \mathbf{v}_1, \quad \mathbf{v}_2, \quad \mathbf{v}_3, \quad \mathbf{v}_0 + \mathbf{v}_1, \quad \mathbf{v}_0 + \mathbf{v}_2, \quad \mathbf{v}_0 + \mathbf{v}_3, \quad \mathbf{v}_1 + \mathbf{v}_2, \quad \mathbf{v}_1 + \mathbf{v}_3, \quad \mathbf{v}_2 + \mathbf{v}_3, \\ &\mathbf{v}_0 + \mathbf{v}_1 + \mathbf{v}_2, \quad \mathbf{v}_0 + \mathbf{v}_1 + \mathbf{v}_3, \quad \mathbf{v}_0 + \mathbf{v}_2 + \mathbf{v}_3, \quad \mathbf{v}_1 + \mathbf{v}_2 + \mathbf{v}_3. \end{aligned}$$

Cada vector de Voronoi determina una cara 2-dimensional de $V(\mathbf{0})$. Por ende, la celda de Voronoi tiene 14 caras, denotadas por F_S , donde S es un subconjunto propio de $\{0, 1, 2, 3\}$. Las caras correspondientes a los vectores de Voronoi mencionados son:

$$F_0, \quad F_1, \quad F_2, \quad F_3, \quad F_{01}, \quad F_{02}, \quad F_{03}, \quad F_{12}, \quad F_{13}, \quad F_{23}, \quad F_{012}, \quad F_{013}, \quad F_{023} \text{ y } F_{123},$$

donde se resalta la correspondencia de los vectores de la superbase que se suman con los subíndices de los F . Así por ejemplo F_{12} es la cara asociada al vector $\mathbf{v}_1 + \mathbf{v}_2$.

El razonamiento a continuación revela una característica importante de los puntos que pertenecen a una cara 2-dimensional de la celda de Voronoi y, al mismo tiempo, nos ayudará a encontrar las $\mathbf{y}$ -coordenadas aumentadas de los vértices de la celda.

Consideremos el conjunto $\bar{S} = \{0, 1, 2, 3\} \setminus S$. Según lo establecido en el Teorema (1.11), podemos concluir que $F_{\bar{S}} = -F_S$, lo que implica que las caras 2-dimensionales F_S y $F_{\bar{S}}$ son opuestas con respecto al origen. Adicionalmente, observamos que las caras adyacentes a F_i , es decir, aquellas que comparten una arista con F_i , son $F_{ij}, F_{ik}, F_{il}, F_{ijk}, F_{ijl}$ y F_{ikl} . En consecuencia, las caras del tipo F_i y sus opuestas tienen forma de hexágono, ya que tienen 6 caras cada una de ellas es paralela con otra, a modo de ejemplo los vectores $\mathbf{v}_i, \mathbf{v}_{ij}$ y $\mathbf{v}_{ikl} = -\mathbf{v}_j$ están en el mismo plano, es decir, las aristas que se generen de las intersecciones de $\mathbf{v}_i$ con $\mathbf{v}_{ij}$ y de $\mathbf{v}_i$ con $\mathbf{v}_{ikl}$ serán paralelas. Ahora, en lo que respecta a la cara F_{ij} , notamos que sus caras vecinas son F_i, F_j, F_{ijk} y F_{ijl} , lo que significa que las caras del tipo F_{ij} y sus opuestas tienen forma de cuadrilátero. Esto se puede observar en la figura 1.5.

Sabemos que un vértice de la celda se define mediante la intersección de tres caras, cada una de las cuales es vecina de las otras dos. Por lo tanto, si denotamos a un vértice de $V(\mathbf{0})$ con $\mathbf{P}_{ijkl}$, donde $ijkl$ es un reordenamiento de 0123, entonces este vértice se define mediante la intersección de las caras F_i, F_{ij} y F_{ijk} .

En resumen, para cada permutación de $\{0, 1, 2, 3\}$, obtenemos un vértice de la celda de Voronoi, lo que significa que $V(\mathbf{0})$ consta de 24 vértices. Además, tiene 8 caras con forma de hexágono y 6 con forma de cuadrilátero. Por lo tanto, para un lattice 3-dimensional Λ , su celda de Voronoi es un octaedro truncado o permutoedro Π_3 .

Cada vértice $\mathbf{p}_{ijkl} = F_i \cap F_{ij} \cap F_{ijk}$, pertenece a los hiperplanos (1.1) de los vectores de

Voronoi $\mathbf{v}_i, \mathbf{v}_{ij}, \mathbf{v}_{ijk}$, por lo tanto se cumplen las ecuaciones:

$$\begin{aligned} 2\mathbf{p} \cdot \mathbf{v}_i &= (\mathbf{v}_i)^2 \\ 2\mathbf{p} \cdot (\mathbf{v}_i + \mathbf{v}_j) &= (\mathbf{v}_i + \mathbf{v}_j)^2 \\ 2\mathbf{p} \cdot (\mathbf{v}_i + \mathbf{v}_j + \mathbf{v}_k) &= (\mathbf{v}_i + \mathbf{v}_j + \mathbf{v}_k)^2 \\ 2\mathbf{p} \cdot \mathbf{v}_l &= (\mathbf{v}_l)^2. \end{aligned}$$

Podemos darnos cuenta que del lado izquierdo de estas igualdades van quedando las $\mathbf{y}$ -coordenadas del vértice, entonces podemos tener que:

$$\begin{aligned} 2\mathbf{y}_i &= (\mathbf{v}_i)^2 \\ 2 \cdot (\mathbf{y}_i + \mathbf{y}_j) &= (\mathbf{v}_i + \mathbf{v}_j)^2 \\ 2 \cdot (\mathbf{y}_i + \mathbf{y}_j + \mathbf{y}_k) &= (\mathbf{v}_i + \mathbf{v}_j + \mathbf{v}_k)^2 \\ 2 \cdot \mathbf{y}_l &= (\mathbf{v}_l)^2. \end{aligned}$$

En consecuencia, por el Proposición (1.12), las $\mathbf{y}$ -coordenadas aumentadas del vértice $\mathbf{P}_{ijkl}$ son:

$$\begin{aligned} y_i &= \frac{1}{2} (p_{ij} + p_{ik} + p_{il}) \\ y_j &= \frac{1}{2} (-p_{ij} + p_{jk} + p_{jl}) \\ y_k &= \frac{1}{2} (-p_{ik} - p_{jk} + p_{kl}) \\ y_l &= \frac{1}{2} (-p_{il} - p_{jl} - p_{kl}). \end{aligned}$$

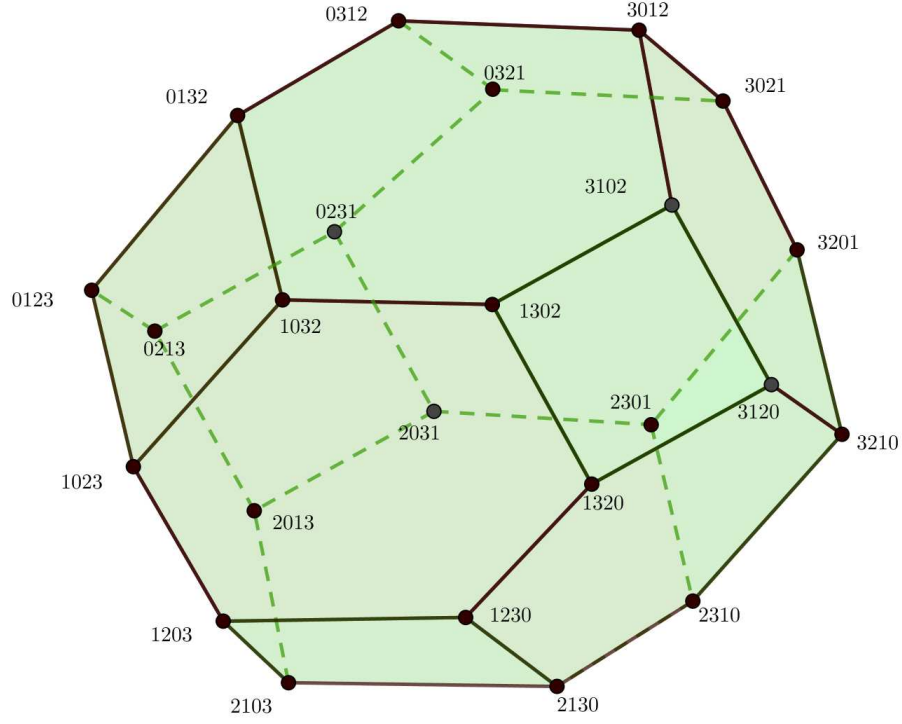


Figura 1.5: Representación de la celda de Voronoi en R^3 con los vértices etiquetados con elementos de S_4

Adicionalmente, la matriz de Gram del lattice es de la forma:

$$A = \begin{pmatrix} p_{01} + p_{12} + p_{13} & -p_{12} & -p_{13} \\ -p_{12} & p_{02} + p_{12} + p_{23} & -p_{23} \\ -p_{13} & -p_{23} & p_{03} + p_{13} + p_{23} \end{pmatrix}.$$

Luego, su determinante está dado por:

$$\begin{aligned} \Delta = & p_{01}p_{02}p_{03} + p_{01}p_{02}p_{13} + p_{01}p_{02}p_{23} + p_{01}p_{03}p_{12} + p_{01}p_{03}p_{23} + p_{01}p_{12}p_{13} + p_{01}p_{12}p_{23} \\ & + p_{01}p_{13}p_{23} + p_{02}p_{03}p_{12} + p_{02}p_{03}p_{13} + p_{02}p_{12}p_{13} + p_{02}p_{12}p_{23} + p_{02}p_{13}p_{23} + p_{03}p_{12}p_{13} \\ & + p_{03}p_{12}p_{23} + p_{03}p_{13}p_{23}. \end{aligned}$$

1.6.2. Cálculo de la constante de cuantización en dimensión 3

Nuestro objetivo es encontrar la fórmula de la constante de cuantización para lattices en $\mathbb{R}^3$ en términos de sus parámetros de Selling. Así las cosas consideremos un lattice tridimensional Λ con superbase obtusa estricta $B = \{\mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$. Para lograr esto, primero necesitamos calcular el segundo momento no normalizado de la celda de Voronoi centrada en el origen $V(\mathbf{0})$. Comenzaremos realizando una partición de esta celda en simplices, con el fin de utilizar el Teorema (1.16) y la fórmula (1.4), dividiendo el problema “difícil” de calcular el el segundo momento de un permutaedro, en varios problemas “fáciles” calculando los segundos momentos para simplices.

La celda de Voronoi tiene forma de octaedro truncado ver Figura 1.5. Podemos dividir cada cara hexagonal en 6 triángulos que tienen como vértice común el centro de la cara y se unen al origen. Esto genera 6 tetraedros en relación con cada cara hexagonal. Aplicando este procedimiento a todas las caras hexagonales, obtenemos un total de 48 tetraedros.

Además, cada cara con forma de cuadrilátero se puede dividir en cuatro triángulos con el centro de la cara y el origen como vértices comunes. Esto genera 4 tetraedros en cada una de estas caras. En total, las caras con forma de cuadrilátero generan 24 tetraedros. Por lo tanto, en la celda de Voronoi centrada en el origen, hay un total de 72 tetraedros.

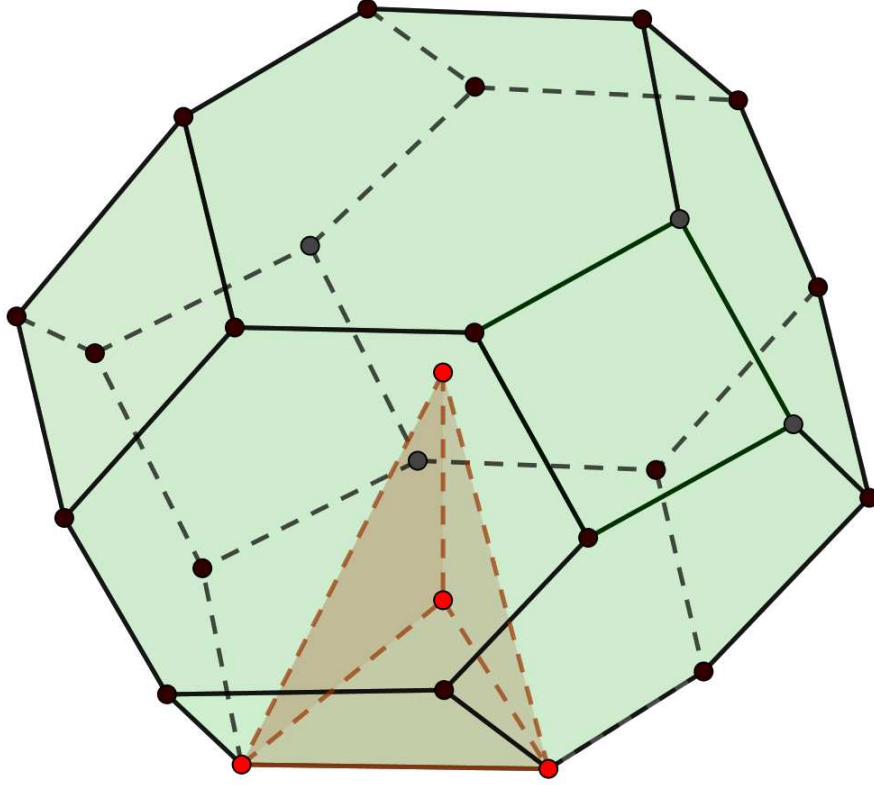


Figura 1.6: Partición en simplices de la celda de Voronoi.

Ahora, consideremos por ejemplo, la cara hexagonal F_1 y sea $\mathbf{m}_1$ su centro. En esta cara, uno de los seis tetraedros se forma con los vértices $\mathbf{0}$, $\mathbf{m}_1$, $\mathbf{P}_{1203}$ y $\mathbf{P}_{1230}$, que denotaremos como T_{12} . Vamos a determinar las $\mathbf{y}$ -coordenadas de estos vértices. Las coordenadas de $\mathbf{0}$ son $(0, 0, 0)^T$. Para $\mathbf{m}_1$, podemos observar que $\mathbf{m}_1 = \frac{1}{2}\mathbf{v}_1$. Dado que las $\mathbf{y}$ -coordenadas aumentadas de $\mathbf{v}_1$ son $(-p_{01}, p_{01} + p_{12} + p_{13}, -p_{12}, -p_{13})^T$, podemos inferir que las de $\mathbf{m}_1$ son $\frac{1}{2}(-p_{01}, p_{01} + p_{12} + p_{13}, -p_{12}, -p_{13})^T$.

Utilizando el Teorema (1.16) y la técnica vista en (1.6.1), podemos decir que la inercia de T_{12} está dada por

$$I(T) = \frac{4}{5} \|\mathbf{m}_1\|^2 + \frac{1}{(4)(5)} \|\mathbf{P}_{1230}\|^2 + \frac{1}{(4)(5)} \|\mathbf{P}_{1203}\|^2 + \frac{1}{(4)(5)} \|\mathbf{0}\|^2,$$

donde

$$\begin{aligned}
\mathbf{0} &: (0, 0, 0) \\
\mathbf{m}_1 &: \frac{1}{2} (p_{01} + p_{12} + p_{13}, -p_{12}, -p_{13}) \\
\mathbf{v}_{1203} &: \frac{1}{2} (p_{01} + p_{12} + p_{13}, p_{02} - p_{12} + p_{23}, -p_{03} - p_{13} - p_{23}) \\
\mathbf{v}_{1230} &: \frac{1}{2} (p_{01} + p_{12} + p_{13}, p_{02} - p_{12} + p_{23}, p_{03} - p_{13} - p_{23})
\end{aligned}$$

Utilizando (1.13) para calcular las normas y de nuevo el Teorema (1.16) para calcular el volumen de T_{12} concluimos que

$$\begin{aligned}
I(T_{12}) = & \frac{1}{40\Delta} \{ \Delta (6p_{01} + 3p_{02} + p_{03} + 6p_{12} + 6p_{13} + 3p_{23}) \\
& - p_{01}p_{02}p_{03} (3p_{12} + p_{13} + p_{23}) - 3p_{01}p_{02}p_{12} (p_{13} + p_{23}) \\
& - p_{01}p_{03} (p_{12}p_{13} + 4p_{12}p_{23} + p_{13}p_{23}) - p_{02}p_{03} (4p_{12}p_{13} + p_{12}p_{23} + p_{13}p_{23}) \\
& - 3p_{12}p_{13}p_{23}(p_{01} + p_{02} + p_{03}) \}
\end{aligned}$$

y el volumen de T_{12} es

$$\frac{1}{24\sqrt{\Delta}} p_{03} (p_{02} + p_{23}) (p_{01} + p_{12} + p_{13}).$$

Aplicando este mismo proceso para los demás tetraedros, un tetraedro por cada arista de la celda, y después sumándolos computacionalmente utilizando algoritmos en Sagemath, por (1.6), tenemos

$$U(P) = \sum_{T \in Q} U(T) = \sum_{T \in Q} I(T) \text{vol}(T)$$

Dado que sabiendo que $G(P) = \frac{1}{n} \frac{U(P)}{\text{vol}(P)^{1+2/n}} = \frac{1}{n} \frac{I(P)}{\text{vol}(P)^{2n}}$, como hemos dicho, Barnes y Sloane [4], concluyeron el siguiente resultado.

Teorema 1.17. [4] Sean $p_{ij} = -\mathbf{v}_i \cdot \mathbf{v}_j$, con $0 \leq i < j \leq 3$ los parámetros de Selling asociados a una superbase obtusa de un lattice 3-dimensional Λ , y sean

$$\begin{aligned}\Delta &= \sum^{(4)} p_{01}p_{02}p_{03} + \sum^{(3)} p_{01}p_{23} (p_{02} + p_{03} + p_{12} + p_{13}) \\ S_1 &= p_{01} + p_{02} + p_{03} + p_{12} + p_{13} + p_{23} \\ S_2 &= p_{01}p_{02}p_{13}p_{23} + p_{01}p_{03}p_{12}p_{23} + p_{02}p_{03}p_{12}p_{13} \\ K &= \sum^{(4)} p_{01}p_{02}p_{03} (p_{12} + p_{13} + p_{23})\end{aligned}$$

Entonces, la constante de cuantización de Λ es:

$$G_3(\Lambda) = \frac{\Delta S_1 + 2S_2 + K}{36\Delta^{4/3}}. \quad (1.13)$$

Utilizando este mismo proceso pero para lattices en dimensión 2 se puede calcular de manera muy sencilla la constante de cuantización para estos lattices, esto debido a que la cantidad de cálculos que se deben hacer son muchos menos que en dimensión 3.

Proposición 1.18. Sea Λ un lattice 2-dimensional con parámetros de Selling asociados p_{ij} , donde $0 \leq i < j \leq 2$. Si definimos a $S_1 = p_{01} + p_{02} + p_{12}$ y $K = p_{01}p_{02}p_{12}$, entonces la constante de cuantización de Λ está dada por la siguiente expresión:

$$G_2(\Lambda) = \frac{\Delta S_1 + K}{24\Delta^{3/2}}. \quad (1.14)$$

1.6.3. Constante de cuantización para lattice en dimensión 4

En esta sección, presentaremos algunos resultados sobre lattices de tipo I en dimensión 4, que se encuentran en [17].

Es importante destacar que en todas las dimensiones hay lattices primitivos de tipo I, en dimensión 2 y 3 es el único tipo de lattices existente, en dimensión 4, ver [25], [7] hay 3 tipos primitivos de lattices, a partir de la dimensión 5, que tiene 222 tipos primitivos, [14], la cantidad de tipos primitivos aumenta considerablemente en relación con la dimensión.

En el trabajo de J. Velásquez, se aplicó la técnica de Conway-Sloane [13] para describir la celda de Voronoi en lattices 4-dimensionales. Uno de los objetivos de ese trabajo fue calcular la constante de cuantización de un lattice Λ en $\mathbb{R}^4$ en términos de sus parámetros de Selling reducidos. Para los lattices de tipo I en dimensión 4 obtuvieron el siguiente resultado.

Teorema 1.19. [17](cap 4, pág 85) Sea Λ un lattice de Tipo I en $\mathbb{R}^4$ con parámetros de Selling reducidos $\rho = [p_{01}, p_{02}, \dots, p_{24}, p_{34}]$, entonces la constante de cuantización de Λ viene dada por:

$$G(\Lambda) = \frac{\Delta S_1 + 2S_2^{(I)} + K^{(I)}}{48\Delta^{5/4}} \quad (1.15)$$

donde

$$\begin{aligned} S_1 &= \sum^{(10)} p_{ij}, \\ S_2^{(I)} &= \sum^{(60)} p_{ij}p_{jk}p_{kl}p_{lm}p_{mj} + \sum^{(12)} p_{ij}p_{jk}p_{kl}p_{lm}p_{mi}, \\ K^{(I)} &= \sum^{(30)} p_{ij}p_{jk}p_{ki}p_{il}p_{im} + \sum^{(60)} p_{ij}p_{jk}p_{ki}p_{il}p_{jm} + \sum^{(60)} p_{ij}p_{jk}p_{ki}p_{il}p_{lm} + \\ &\quad \sum^{(12)} p_{ij}p_{jk}p_{kl}p_{lm}p_{mi}. \end{aligned}$$

Capítulo 2

Descripción de la celda de Voronoi

El Teorema (1.11) establece una correspondencia entre los vectores de Voronoi y los subconjuntos propios S de $\{0, 1, \dots, n\}$. Según este teorema, cada vector de Voronoi $\mathbf{v}_S$ está asociado a una cara $(n - 1)$ -dimensional de la celda de Voronoi, que denotamos como F_S .

En este capítulo, exploraremos a fondo dicho teorema para generar información detallada sobre las características combinatorias de la celda de Voronoi. Estos resultados no solo son significativos desde un punto de vista teórico, sino que también son esenciales para realizar los cálculos necesarios para determinar la constante de cuantización. La información derivada de este teorema será fundamental para optimizar y reducir la carga computacional en nuestras evaluaciones.

2.1. La celda de Voronoi para Lattices de primer tipo y el permutaedro

Es interesante observar que existe una relación simétrica entre los conjuntos S y su complemento $\bar{S} = \{0, \dots, n\} \setminus S$. En particular, si consideramos los vectores correspondientes $\mathbf{v}_{\bar{S}}$ y $\mathbf{v}_S$, podemos ver que $\mathbf{v}_{\bar{S}}$ es igual a $-\mathbf{v}_S$. Esto implica que las caras $F_{\bar{S}}$ y F_S son congruentes, pero opuestas con respecto al origen $\mathbf{0}$.

Observación 2.1. Del trabajo de Voronoi [25] y de Conway [13], se tiene que si $\{\mathbf{v}_0, \dots, \mathbf{v}_n\}$ es una superbase obtusa para un lattice de primer tipo, A, B son subconjuntos propios distintos de $\{0, 1, \dots, n\}$ entonces, F_A y F_B son caras vecinas (comparten una cara $(n - 2)$ -dimensional) de la celda de Voronoi centrada en el origen si y solo si $A \subset B$ o $B \subset A$.

Esta idea permite presentar desde una perspectiva más combinatoria una descripción de la celda de Voronoi en lattices de primer tipo. Para ello, estableceremos una correspondencia entre los vértices de la celda de Voronoi y los elementos del conjunto S_{n+1} . Además, caracterizaremos los elementos que se encuentran en una de las caras de dimensión $n - 1$ de la celda. Este razonamiento nos permitirá una comprensión más profunda y estructurada de la celda de Voronoi, resaltando las relaciones combinatorias en su geometría.

Con esta idea, en una celda de Voronoi de dimensión n , se puede observar que un vértice $\mathbf{p}$ es la intersección de n caras vecinas de dimensión $(n - 1)$. En virtud de la observación 2.1 los subconjuntos con los que se han etiquetado estas caras forman una cadena de subconjuntos únicos estrictamente encajados. Esto nos está diciendo que:

$$\mathbf{p} = F_{\sigma_0} \cap F_{\sigma_0\sigma_1} \cap \dots \cap F_{\sigma_0\dots\sigma_n}, \quad (2.1)$$

siendo $\sigma = (\sigma_0, \dots, \sigma_n)$, donde σ es una permutación de $\{0, \dots, n\}$, donde por simplicidad escribimos $\sigma_0 \dots \sigma_i$ en lugar de $\{\sigma_0, \dots, \sigma_i\}$.

Esta intersección es única para cada vértice, por lo tanto, cada vértice está en correspondencia biunívoca con las permutaciones del conjunto $\{0, \dots, n\}$, es decir, los vértices de la celda de Voronoi están en correspondencia biunívoca con los elementos del grupo S_{n+1} . De esta manera denotaremos un vértice dado por $\mathbf{p} = F_{\sigma_0} \cap F_{\sigma_0\sigma_1} \cap \dots \cap F_{\sigma_0\dots\sigma_n}$ como $\mathbf{p}_{\sigma_0\dots\sigma_n}$, también como $\mathbf{p}_\sigma$ o incluso simplemente como σ .

Nota. En adelante vamos a considerar que $F_{\sigma_0\dots\sigma_i}$ representa únicamente los vértices de la celda que están en esta cara.

Observación 2.2. Notemos que la $(n - 1)$ -cara $F_{\sigma_0\dots\sigma_i}$ contiene a todos los vértices $\mathbf{p}_{\sigma_0\dots\sigma_n}$ cuyos primeros $i + 1$ subíndices son un reordenamiento de $(\sigma_0, \dots, \sigma_i)$, y que los siguientes

$(n - i)$ subíndices son un reordenamiento de $(\sigma_{i+1}, \dots, \sigma_n)$, es decir, los vértices

$$\mathbf{p}_{\sigma'_0 \cdots \sigma'_i \sigma'_{i+1} \cdots \sigma'_n},$$

donde $\sigma'_0 \cdots \sigma'_i$ es una permutación de $\sigma_0 \cdots \sigma_i$, y de igual manera, $\sigma'_{i+1} \cdots \sigma'_n$ es una permutación de $\sigma_{i+1} \cdots \sigma_n$.

Ejemplo 2.3. Para $n = 3$, sea L un lattice con superbase obtusa $B = \{\mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$. Los vectores de Voronoi para L se obtienen al realizar la suma $\sum_S \mathbf{v}_S$ donde S recorre los subconjuntos propios de $\{0, 1, 2, 3\}$. Así pues, los vectores de Voronoi son:

$$\begin{array}{lll} \mathbf{v}_0 & \mathbf{v}_0 + \mathbf{v}_1 & \mathbf{v}_0 + \mathbf{v}_1 + \mathbf{v}_2 \\ \mathbf{v}_1 & \mathbf{v}_0 + \mathbf{v}_2 & \mathbf{v}_0 + \mathbf{v}_1 + \mathbf{v}_3 \\ \mathbf{v}_2 & \mathbf{v}_0 + \mathbf{v}_3 & \mathbf{v}_0 + \mathbf{v}_2 + \mathbf{v}_3 \\ \mathbf{v}_3 & \mathbf{v}_1 + \mathbf{v}_2 & \mathbf{v}_1 + \mathbf{v}_2 + \mathbf{v}_3 \\ & \mathbf{v}_1 + \mathbf{v}_3 & \\ & \mathbf{v}_2 + \mathbf{v}_3 & \end{array}$$

a cada uno de estos vectores, y en consecuencia a cada subconjunto propio S de $\{0, 1, 2, 3\}$, le corresponde una cara 2-dimensional, F_S , de la celda de Voronoi. Por ejemplo, como resultado de la Observación 2.2, notemos que la cara F_{02} que está dirigida por el vector $\mathbf{v}_{02} = \mathbf{v}_0 + \mathbf{v}_2$, dicha cara conti a los vértices cuyas etiquetas corresponden a:

$$0213, 0231, 2013, 2031.$$

De igual manera, los vértices en F_1 se corresponden con

$$1023, 1032, 1203, 1230, 1302, 1320. \quad (2.2)$$

y como último ejemplo los elementos de F_{023} , la cual es la cara opuesta de la cara F_1 debido a que sus vectores de Voronoi correspondientes son opuestos, son

$$3201, 2301, 3021, 0321, 2031, 0231. \quad (2.3)$$

Al analizar las palabras en el ejemplo (2.2) y (2.3), podemos notar una correspondencia estructural entre ellas: cada palabra tiene su permutación inversa ubicada en la cara opuesta. Esta similitud no es una coincidencia fortuita, sino que está relacionada con la simetría presente en la celda de Voronoi.

Este análisis nos conduce a un resultado clave, el cual se deriva de la observación anterior y establece una conexión directa entre la distribución de vértices y la estructura (tamaño) de las palabras generadas por esta división. Lo cual se puede resumir en la Proposición (2.4).

Proposición 2.4. La cantidad de vértices en $F_{\sigma_0 \dots \sigma_i}$ en una celda de Voronoi de un lattice de primer tipo es $(i+1)!(n-i)!$

Ahora, consideremos los vértices de dos caras $(n-1)$ -dimensionales, $F_{\sigma_0 \dots \sigma_i}$ y $F_{\sigma_0 \dots \sigma_j}$ vecinas, por la Observación (2.2) tenemos que los elementos de $F_{\sigma_0 \dots \sigma_i}$ son todos los vértices

$$\mathbf{P}_{\sigma'_0 \dots \sigma'_i \sigma'_{i+1} \dots \sigma'_n},$$

donde $\sigma'_0 \dots \sigma'_i$ sea una permutación de $\sigma_0 \dots \sigma_i$, y de igual manera, $\sigma'_{i+1} \dots \sigma'_n$ sea una permutación de $\sigma_{i+1} \dots \sigma_n$. Del mismo modo los vértices que están en la cara $F_{\sigma_0 \dots \sigma_j}$ son todos los vértices

$$\mathbf{P}_{\sigma'_0 \dots \sigma'_j \sigma'_{j+1} \dots \sigma'_n},$$

donde $\sigma'_0 \dots \sigma'_j$ y $\sigma'_{j+1} \dots \sigma'_n$ son una permutaciones de $\sigma_0 \dots \sigma_j$ y $\sigma_{j+1} \dots \sigma_n$ respectivamente.

Así pues, si $i < j$, entonces los vértices que están en la intersección $F_{\sigma_0 \dots \sigma_i} \cap F_{\sigma_0 \dots \sigma_j}$ están dados por

$$\mathbf{P}_{\sigma'_0 \dots \sigma'_i \sigma'_{i+1} \dots \sigma'_j \sigma'_{j+1} \dots \sigma'_n},$$

donde $\sigma'_0 \dots \sigma'_i$, $\sigma'_{i+1} \dots \sigma'_j$ y $\sigma'_{j+1} \dots \sigma'_n$ son una permutaciones de $\sigma_0 \dots \sigma_i$, $\sigma_{i+1} \dots \sigma_j$ y $\sigma_{j+1} \dots \sigma_n$ respectivamente.

Vemos que el resultado de interceptar los vértices de dos caras $(n-1)$ -dimensionales a las que pertenece σ , son todos los vértices que se pueden generar con la división de σ dos veces y realizar las todas las permutaciones de los elementos dentro de cada uno de los tres bloques

resultantes, el verde, el azul y el rojo. Esto nos conduce a la siguiente proposición, la cual es un análogo de la proposición (2.4).

Proposición 2.5. La cantidad de vértices en la intersección de $F_{\sigma_0 \dots \sigma_i}$ y $F_{\sigma_0 \dots \sigma_j}$ en una celda de Voronoi de un lattice de primer tipo es $(i+1)!(j-i)!(n-j)!$

Por supuesto, el impulso que tenemos ahora es generalizar esta idea. Si queremos caracterizar los vértices de una cara $(n-k)$ -dimensional, debemos interceptar los vértices de k caras vecinas dos a dos de dimensión $n-1$, es decir, se deben escoger k subconjuntos $S_0, \dots, S_{k-1}$ de $U = \{0, \dots, n\}$ de tal manera que estén encajados; sin pérdida de generalidad asumamos $S_0 \subset \dots \subset S_{k-1}$ y con ellos generamos los correspondientes $F_{S_0}, \dots, F_{S_{k-1}}$, con esta cadena de conjuntos podemos construir la siguiente partición de U

$$\{S_0, S_1 - S_0, \dots, S_{k-1} - S_{k-2}, U - S_{k-1}\}$$

De manera más específica, un vértice que pertenezca a la cara $(n-k)$ -dimensional, resultante de la intersección de las caras $F_{S_0}, \dots, F_{S_{k-1}}$ se encuentra representado con un reordenamiento de los elementos en el conjunto $\{0, \dots, n\}$, obtenido así: los elementos se distribuyen en $k+1$ subconjuntos ordenados, siguiendo una disposición tal que en el reordenamiento, los primeros $|S_0|$ elementos corresponden a un orden específico de los elementos en S_0 ; posteriormente, los siguientes $|S_1 - S_0|$ elementos son un reordenamiento del conjunto $S_1 - S_0$, y este proceso se repite sucesivamente hasta que los últimos $|U - S_{k-1}|$ elementos sean un reordenamiento del conjunto $U - S_{k-1}$. A este conjunto de vértices lo denotaremos por

$$F(B_0 | \dots | B_{k-1} | B_k) \tag{2.4}$$

donde

$$B_0 = S_0, B_1 = S_1 - S_0, \dots, B_{k-1} = S_{k-1} - S_{k-2}, B_k = U - S_{k-1}.$$

Proposición 2.6. Las caras k -dimensionales de la celda de Voronoi están en correspondencia biunívoca con las particiones ordenadas del conjunto $\{0, \dots, n\}$, en $n-k+1$ bloques no vacíos $B_0, \dots, B_{n-k}$.

Ahora bien, los v rtices en la cara correspondiente a la subdivisi n en bloques $B_0, \dots, B_{n-k}$ est n dados por las $n - k$ intersecciones de los conjuntos

$$F_{B_0}, F_{B_0 \cup B_1}, \dots, F_{B_0 \cup B_1 \dots \cup B_{n-k}},$$

es decir, resulta ser $F(B_0|B_1|\dots|B_{n-1-k})$.

Corolario 2.7. Una cara k -dimensional de la celda de Voronoi de un lattice tipo I dada por $F(B_0|B_1|\dots|B_{n-1-k})$ contiene $|B_0|! \cdot |B_1|! \dots |B_{n-1-k}|!$ v rtices.

Ejemplo 2.8. Hablemos de las caras 1 y 2-dimensionales de la celda de Voronoi de un lattice 3-dimensional L . consideremos la superbase obtusa $B = \{\mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ de L , as  los vectores de Voronoi son obtenidos al realizar la suma $\sum_S \mathbf{v}_S$ donde S son los subconjuntos propios de $\{0, 1, 2, 3\}$.

- Las caras 1-dimensionales est n en correspondencia biun voca con las particiones ordenadas del conjunto $\{0, 1, 2, 3\}$ en 3 bloques no vac os, se puede ver que necesariamente uno de estos bloques tiene que tener dos elementos y los bloques restantes uno.

Supongamos que una de las particiones de U en tres conjuntos no vac os es $\{B_0, B_1, B_2\}$, Por ejemplo se pueden tomar los elemento de la partici n como $B_0 = \{2, 1\}$, $B_1 = \{3\}$ y $B_2 = \{0\}$, de esta partici n salen $3!$ reordenaciones de los bloques que son unas de las particiones ordenadas que est n en correspondencia con las siguientes caras 1-dimensionales de la celda:

$$\begin{array}{ll} F(B_0|B_1|B_2) & F(B_0|B_2|B_1) \\ F(B_1|B_0|B_2) & F(B_1|B_2|B_0) \\ F(B_2|B_0|B_1) & F(B_2|B_1|B_0) \end{array}$$

De esta manera el n mero de caras 1 dimensionales en la celda es

$$3!(\mathbf{s}(4, 3)) = 6 * 6 = 36,$$

donde $\mathbf{s}(4, 3)$ es el n mero de Stirling de segunda especie de 4 en 3 que representa la

cantidad de particiones posibles de un conjunto de 4 elementos en un tres bloques no vacíos.

- Las caras 2-dimensionales están en correspondencia biunívoca con las particiones ordenadas del conjunto $\{0, 1, 2, 3\}$ en 2 bloques no vacíos, por tanto hay dos casos; uno de ellos es que en la partición exista un bloque de tres elementos y el restante de 1, o el otro caso que hayan dos bloques de dos elementos.

Supongamos que una de las particiones de U en tres conjuntos no vacíos es $\{B_0, B_1\}$, Por ejemplo se pueden tomar los elemento de la partición como $B_0 = \{2, 1\}$ y $B_1 = \{0, 3\}$, de esta partición salen $2!$ reordenaciones de los bloques que son unas de las particiones ordenadas que están en correspondencia con las siguientes caras 2 dimensionales de la celda:

$$F(B_0|B_1) \quad F(B_1|B_0)$$

De esta manera el número de caras 2 dimensionales en la celda es

$$2!(s(4, 2)) = 2 * 7 = 14,$$

donde $s(4, 3)$ es el número de Stirling de segunda especie de 4 en 2 que representa la cantidad de particiones posibles de un conjunto de 4 elementos en un dos bloques no vacíos.

Los números de Stirling de segunda especie, denotados como $s(m, d)$, se utilizan para contar de cuántas formas diferentes se pueden dividir m elementos en d conjuntos no vacíos. Son útiles para problemas de conteo que implican distribuir objetos en grupos, sin importar el orden dentro de los grupos, en este caso nos ayudan a contar la cantidad de caras de una dimensión determinada en la celda.

La fórmula general para los números de Stirling de segunda especie:

$$s(m, d) = \frac{1}{d!} \sum_{j=0}^d (-1)^{d-j} \binom{k}{j} j^m.$$

Estos números son una herramienta muy útil en la descripción que estamos haciendo y nos conduce al siguiente corolario.

Corolario 2.9. La celda de Voronoi para un lattice tipo I en dimensión n contiene $(n + 1 - k)!(s(n, n + 1 - k))$ caras k -dimensionales.

Siguiendo la Proposición (2.6), estos vértices están en correspondencia con las subdivisiones ordenadas de $U = \{0, \dots, n\}$ en $n + 1$ bloques ordenados no vacíos. Dado que la cantidad de bloques de la división coincide con la cantidad de elementos en U , cada bloque debe contener solo un elemento. Por lo tanto, como se mostró anteriormente en (2.1), los vértices pueden representarse como permutaciones del conjunto U .

Observación 2.10. Siguiendo la misma observación, podemos deducir que las caras de dimensión 1 de la celda también están relacionadas con las subdivisiones ordenadas de $U = \{0, \dots, n\}$ en n bloques ordenados no vacíos. En esta instancia, es importante notar que en la división debe existir un bloque que contenga exactamente dos elementos. Como resultado, podemos afirmar que la representación de los vértices como elementos de S_{n+1} en una cara de dimensión 1 difieren únicamente en una transposición de dos caracteres consecutivos.

Con estos resultados vamos a presentar como ejemplo la descripción asociada a la combinatoria de la estructura de todas las caras en todas las dimensiones de la celda de Voronoi en dimensión 5.

2.2. Caracterización combinatoria de la celda de Voronoi para lattices de tipo I en dimensión 5

Sea $n = 5$ y sea L un lattice con superbase obtusa $B = \{\mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4, \mathbf{v}_5\}$, los vectores de Voronoi son obtenidos al realizar las sumas $\sum_S \mathbf{v}_S$ donde S recorre todos los subconjuntos propios de $\{0, 1, 2, 3, 4, 5, 6\}$.

2.2.1. Caras 0-dimensionales de la celda

Los vértices de la celda son caras de dimensión 0, como hemos visto, los podemos representar como $F(\sigma_0|\sigma_1|\sigma_2|\sigma_3|\sigma_4|\sigma_5)$ donde $\sigma_i \in \{0, 1, 2, 3, 4, 5, 6\}$. Y por lo tanto existen $(n + 1)!$ vértices en la celda.

2.2.2. Caras 1-dimensionales de la celda

Por otro lado las caras de dimensión 1 de la celda de Voronoi están en correspondencia con las subdivisiones ordenadas del conjunto $U = \{0, 1, 2, 3, 4, 5\}$ en 5 subconjuntos disjuntos no vacíos.

Por la Observación (2.10), las caras de dimensión 1 corresponden a segmentos de recta en los cuales los vértices en los extremos se diferencian únicamente por una transposición de dos elementos consecutivos. Esto se ilustra claramente en la siguiente figura.



Figura 2.1: Ejemplo de cara 1 dimensional de la celda de Voronoi, donde $\sigma_i \in \{0, 1, 2, 3, 4, 5, 6\}$.

De esta manera el número de caras 1 dimensionales en la celda es

$$5!(s(6, 5)) = 120 * 15 = 1800.$$

2.2.3. Caras 2-dimensionales de la celda

Las caras de dimensión 2 de la celda de Voronoi están en correspondencia con las subdivisiones ordenadas del conjunto $U = \{0, 1, 2, 3, 4, 5\}$ en 4 subconjuntos disjuntos no vacíos. Lo cual nos indica que en las particiones pueden pasar dos cosas, tener un conjunto de 3 elementos y tres conjuntos de 1 elemento o tener dos conjuntos de 2 elementos y dos de 1.

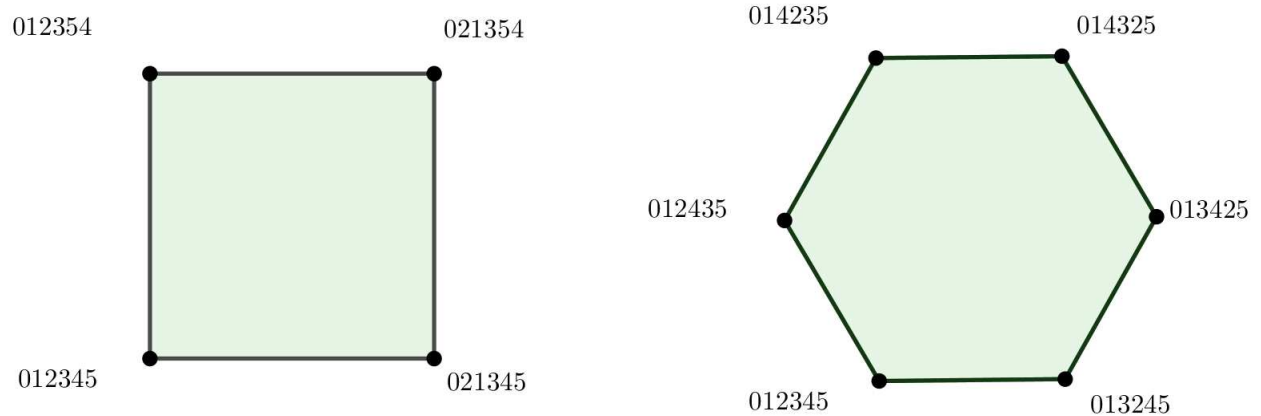


Figura 2.2: Ejemplo de dos caras 2-dimensionales de la celda de Voronoi, $F(0|12|3|45)$ y $F(0|1|234|5)$ respectivamente.

2.2.4. Caras 3-dimensionales de la celda

Hablemos ahora de las caras tridimensionales de la celda de Voronoi. Siguiendo la Observación (2.6), estas caras están relacionadas con las particiones ordenadas de U en 3 bloques. En consecuencia, existen tres posibilidades para lograr esto. A continuación, presentaremos un ejemplo de cada una de estas posibilidades y la estructura gráfica resultante.

La primera posibilidad implica que el conjunto U se divide en tres subconjuntos, cada uno con dos elementos. En otras palabras, los vértices en una cara tridimensional con esta característica se pueden representar como $F(\sigma_0\sigma_1|\sigma_2\sigma_3|\sigma_4\sigma_5)$.

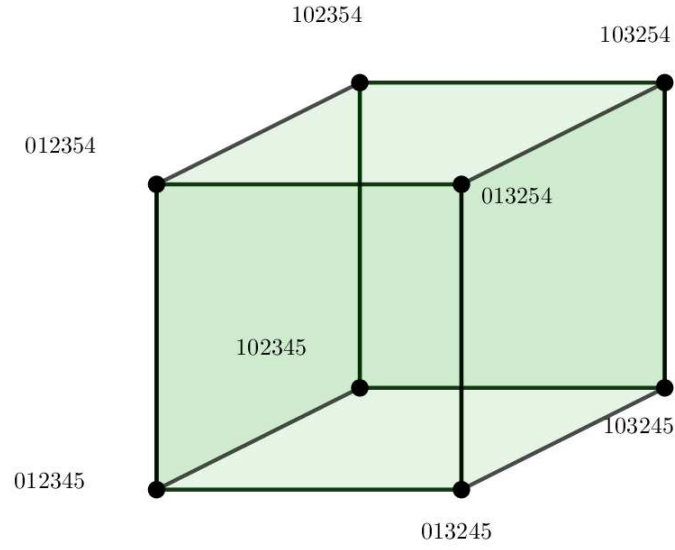


Figura 2.3: Ejemplo $F(01|23|54)$ de cara tridimensional de la celda de Voronoi.

La segunda posibilidad implica tomar un subconjunto de tres elementos, otro de dos elementos y finalmente uno de un elemento. De esta manera, los vértices en una de estas caras pueden ser de la forma $F(\sigma_0\sigma_1\sigma_2|\sigma_3|\sigma_4\sigma_5)$ y obtenemos una cara así:

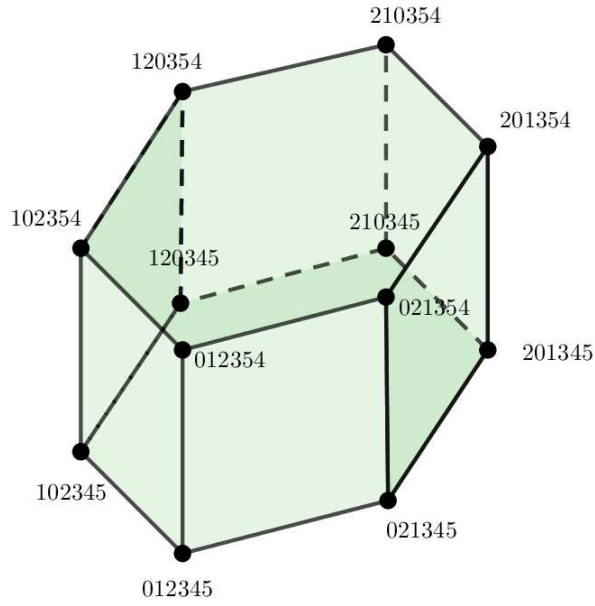


Figura 2.4: Ejemplo $F(012|3|54)$ de cara tridimensional de la celda de Voronoi

Por último, la última posibilidad para realizar esta división de U en subconjuntos no vacíos es tener un conjunto de 4 elementos y el resto de conjuntos de un elemento. Por ejemplo, la siguiente figura muestra una de estas caras con esta estructura, y los vértices están dados por: $F(\sigma_0\sigma_1\sigma_2\sigma_3|\sigma_4|\sigma_5)$.

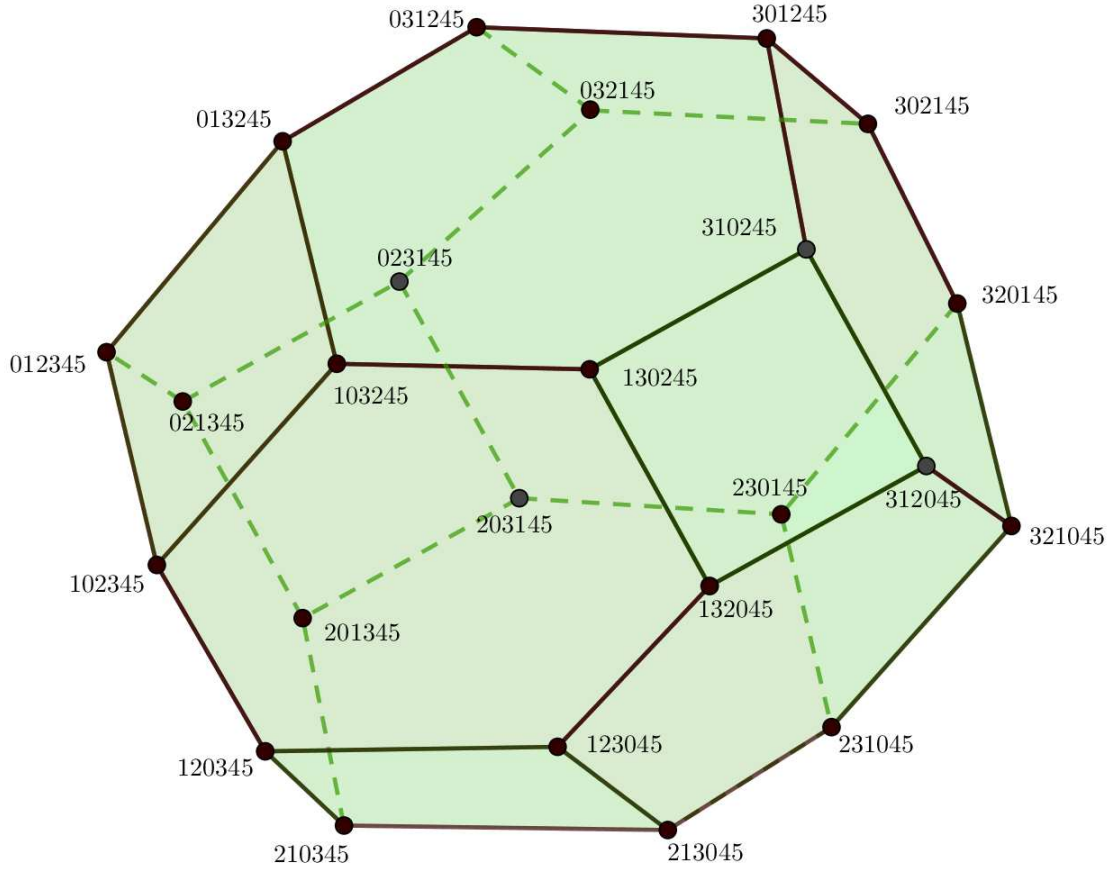


Figura 2.5: Permutaedro como ejemplo de cara tridimensional de la celda de Voronoi de dimensión 5, $F(0123|4|5)$.

2.3. Caracterización vectorial del la celda de Voronoi

Hasta este punto, hemos obtenido un conocimiento valioso sobre el comportamiento de los vértices en la celda de Voronoi y también sobre las características de sus caras. Sin embargo, esta ha sido una presentación netamente combinatoria, nos enfocaremos en una presentación específica vectorial de los vértices en la celda de Voronoi en función de los parámetros de Selling del lattice. Esta presentación nos permitirá comprender aún más los aspectos de esta estructura geométrica y revelar posibles patrones y propiedades que puedan estar ocultos

en su configuración.

2.3.1. Vértices de la Celda

Como hemos visto cada vértice $\mathbf{p}_{\sigma_0 \dots \sigma_n} = F_{\sigma_0} \cap F_{\sigma_0 \sigma_1} \cap \dots \cap F_{\sigma_0 \dots \sigma_{n-1}}$, pertenece a los Hiperplanos (1.1) de los Vectores de Voronoi $\mathbf{v}_{\sigma_0}, \mathbf{v}_{\sigma_0 \sigma_1}, \dots, \mathbf{v}_{\sigma_0 \dots \sigma_{n-1}}$, por lo tanto se cumplen las ecuaciones:

$$\begin{aligned} 2\mathbf{p} \cdot \mathbf{v}_{\sigma_0} &= (\mathbf{v}_{\sigma_0})^2 \\ 2\mathbf{p} \cdot \mathbf{v}_{\sigma_0 \sigma_1} &= (\mathbf{v}_{\sigma_0 \sigma_1})^2 \\ &\vdots \\ 2\mathbf{p} \cdot \mathbf{v}_{\sigma_0 \dots \sigma_{n-1}} &= (\mathbf{v}_{\sigma_0 \dots \sigma_{n-1}})^2 \\ -2\mathbf{p} \cdot \mathbf{v}_{\sigma_n} &= (\mathbf{v}_{\sigma_n})^2 \end{aligned}$$

Podemos darnos cuenta que del lado izquierdo de estas igualdades van quedando las $\mathbf{y}$ -coordenadas del vértice. Y restando ecuaciones consecutivas finalmente obtenemos:

$$\begin{aligned} 2\mathbf{y}_{\sigma_0} &= (\mathbf{v}_{\sigma_0})^2 \\ 2\mathbf{y}_{\sigma_1} &= (\mathbf{v}_{\sigma_0} + \mathbf{v}_{\sigma_1})^2 - (\mathbf{v}_{\sigma_0})^2 \\ &\vdots \\ 2\mathbf{y}_{\sigma_i} &= (\mathbf{v}_{\sigma_0} + \dots + \mathbf{v}_{\sigma_i})^2 - (\mathbf{v}_{\sigma_0} + \dots + \mathbf{v}_{\sigma_{i-1}})^2 \\ &\vdots \\ 2\mathbf{y}_{\sigma_{n-1}} &= (\mathbf{v}_{\sigma_0} + \dots + \mathbf{v}_{\sigma_{n-1}})^2 - (\mathbf{v}_{\sigma_0} + \dots + \mathbf{v}_{\sigma_{n-2}})^2 \\ -2\mathbf{y}_{\sigma_0} &= (\mathbf{v}_{\sigma_0})^2 \end{aligned}$$

Veamos la coordenada

$$\begin{aligned}
2\mathbf{y}_{\sigma_i} &= (\mathbf{v}_{\sigma_0} + \cdots + \mathbf{v}_{\sigma_i})^2 - (\mathbf{v}_{\sigma_0} + \cdots + \mathbf{v}_{\sigma_{i-1}})^2 \\
&= (\mathbf{v}_{\sigma_0} + \cdots + \mathbf{v}_{\sigma_{i-1}}) + 2(\mathbf{v}_{\sigma_0} + \cdots + \mathbf{v}_{\sigma_{i-1}}) \cdot \mathbf{v}_{\sigma_i} + \mathbf{v}_{\sigma_i}^2 - (\mathbf{v}_{\sigma_0} + \cdots + \mathbf{v}_{\sigma_{i-1}})^2 \\
&= 2(\mathbf{v}_{\sigma_0} + \cdots + \mathbf{v}_{\sigma_{i-1}}) \cdot \mathbf{v}_{\sigma_i} + \mathbf{v}_{\sigma_i}^2 \\
&= -2 \sum_{j < i} p_{\sigma_j \sigma_i} + \mathbf{v}_{\sigma_i}^2,
\end{aligned}$$

por la Proposición (1.12) tenemos que $\mathbf{v}_{\sigma_i}^2 = \sum_{\sigma_j \neq \sigma_i} p_{\sigma_i \sigma_j}$, por tanto

$$2\mathbf{y}_{\sigma_i} = -2 \sum_{j < i} p_{\sigma_j \sigma_i} + \sum_{\sigma_j \neq \sigma_i} p_{\sigma_i \sigma_j}.$$

Así concluimos el siguiente resultado.

Proposición 2.11. Sea $\sigma \in S_{n+1}$, un vértice de la celda de Voronoi, tal que $\sigma = (\sigma_0, \sigma_1, \dots, \sigma_n)$, con $\sigma_i \in \{0, 1, \dots, n\}$ y $0 \leq i \leq n$. Entonces, la coordenada σ_i de las $\mathbf{y}$ - coordenadas aumentadas del vértice σ están dadas por:

$$\mathbf{y}_{\sigma_i} = -\frac{1}{2} \sum_{j=0}^{i-1} p_{\sigma_i \sigma_j} + \frac{1}{2} \sum_{j=i+1}^n p_{\sigma_i \sigma_j} = -\frac{1}{2} p_{\sigma_i | \sigma_0 \dots \sigma_{i-1}} + \frac{1}{2} p_{\sigma_i | \sigma_{i+1} \dots \sigma_n}, \quad (2.5)$$

donde $p_{\sigma_i \sigma_j} = p_{\sigma_j \sigma_i}$.

Observación 2.12.

- El término $p_{\sigma_i \sigma_j}$ aparece en dos de las coordenadas del vértice dado por σ , en la coordenada σ_i y σ_j .
- El signo de $p_{\sigma_i \sigma_j}$ en cada coordenada depende de si $\sigma_i > \sigma_j$ o si $\sigma_j > \sigma_i$.

Definición 2.13. Sean $\sigma_i, \sigma_j \in \{0, 1, \dots, n\}$ y $\sigma_i < \sigma_j$. A los vectores que sus componentes son cero, excepto en las posiciones σ_i, σ_j , las cuales le corresponden p_{σ_i, σ_j} y $-p_{\sigma_i, \sigma_j}$

respectivamente, se denominarán *vectores principales* y los denotaremos por $e_{\sigma_i\sigma_j}$ o $e_{\sigma_j\sigma_i}$.

Haciendo uso de la Observación (2.12) y la Definición (2.13), podemos notar que las $\mathbf{y}$ -coordenadas de los vértices de la celda de Voronoi se pueden expresar en términos de los vectores principales, es decir, como la suma de todos los vectores principales $e_{\sigma_i\sigma_j}$ multiplicado por el signo de $\sigma_j - \sigma_i$, esto es:

$$\mathbf{P}(\sigma) = \frac{1}{2} \sum_{i < j} sg(\sigma_j - \sigma_i) e_{\sigma_i\sigma_j}, \quad (2.6)$$

donde sg es la función signo.

Ejemplo 2.14. Sea $n = 2$, entonces tenemos $3!$ vértices etiquetados con permutaciones de $\{0, 1, 2\}$. En particular, consideremos la permutación $\sigma = (2, 0, 1)$. Entonces, la descomposición del vértice en términos de los vectores principales es:

$$\begin{aligned} \mathbf{P}(2, 0, 1) &= \frac{1}{2}sg(0 - 2)e_{02} + \frac{1}{2}sg(1 - 0)e_{01} + \frac{1}{2}sg(2 - 1)e_{12} \\ &= -\frac{1}{2}e_{02} + \frac{1}{2}e_{01} - \frac{1}{2}e_{12} \\ &= -\frac{1}{2} \begin{pmatrix} -p_{02} \\ 0 \\ -p_{02} \end{pmatrix} + \frac{1}{2} \begin{pmatrix} p_{01} \\ -p_{01} \\ 0 \end{pmatrix} - \frac{1}{2} \begin{pmatrix} 0 \\ p_{12} \\ -p_{12} \end{pmatrix} \\ &= \frac{1}{2} \begin{pmatrix} p_{01} - p_{02} \\ -p_{01} - p_{12} \\ p_{02} + p_{12} \end{pmatrix}. \end{aligned}$$

2.4. Aristas de la celda

Ejemplo 2.15. Consideremos la dimensión $n = 5$, y un lattice con superbase obtusa $\{\mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4, \mathbf{v}_5\}$, los vértices que están en $F(5|2|43|0|1)$, que son los vértices de una

cara 1- dimensional de la celda de Voronoi del lattice son

$$\begin{aligned}\mathbf{P}(524301) &= \frac{1}{2}(e_{01} - e_{02} - e_{03} - e_{04} - e_{05} - e_{12} - e_{13} - e_{14} - e_{15} \\ &\quad + e_{23} + e_{24} - e_{25} - \textcolor{red}{e}_{34} - e_{35} - e_{45}) \\ \mathbf{P}(523401) &= \frac{1}{2}(e_{01} - e_{02} - e_{03} - e_{04} - e_{05} - e_{12} - e_{13} - e_{14} - e_{15} \\ &\quad + e_{23} + e_{24} - e_{25} + \textcolor{red}{e}_{34} - e_{35} - e_{45}).\end{aligned}$$

Podemos notar que solo cambia de signo el vector principal e_{34} , con esto en mente, la arista que va del vértice 523401 al vértice 524301 está dado simplemente por

$$\mathbf{P}(523401) - \mathbf{P}(524301) = e_{34}.$$

Por otro lado, el baricentro de esta cara, está determinado por la mitad de la suma de estos dos vértices por lo tanto, pasa lo contrario que lo hecho anteriormente

$$\begin{aligned}\mathbf{P}(523401) + \mathbf{P}(524301) &= e_{01} - e_{02} - e_{03} - e_{04} - e_{05} - e_{12} - e_{13} \\ &\quad - e_{14} - e_{15} + e_{23} + e_{24} - e_{25} - e_{35} - e_{45}\end{aligned}$$

Una de las ideas destacadas en el ejemplo anterior resulta especialmente interesante, ya que señala la existencia de una relación entre los vectores principales y las aristas de la celda de Voronoi. Ahora exploraremos este concepto de manera más general.

Consideremos un lattice L de primer tipo en $\mathbb{R}^n$. Según la Observación (2.10), las caras 1-dimensionales de la celda de Voronoi contienen exactamente dos vértices ubicados en sus extremos. Lo interesante aquí es que estos dos vértices solo difieren en una transposición de dos elementos consecutivos. Supongamos que estos vértices se denotan como $\sigma = \sigma_0 \cdots \sigma_i \sigma_{i+1} \cdots \sigma_n$ y $\sigma' = \sigma_0 \cdots \sigma_{i+1} \sigma_i \cdots \sigma_n$, donde la única diferencia radica en la transposición entre σ_i y σ_{i+1} . Con esta observación en mente, por la ecuación (2.6), tenemos

$$\mathbf{P}(\sigma) = \frac{1}{2} \sum_{\substack{k < j, \\ k \neq i, \\ j \neq i+1}} sg(\sigma_j - \sigma_k) e_{\sigma_k \sigma_j} + \frac{1}{2} sg(\sigma_{i+1} - \sigma_i) e_{\sigma_i \sigma_{i+1}},$$

$$\mathbf{P}(\sigma') = \frac{1}{2} \sum_{\substack{k < j, \\ j \neq i, \\ k \neq i+1}} sg(\sigma_j - \sigma_k) e_{\sigma_k \sigma_j} + \frac{1}{2} sg(\sigma_i - \sigma_{i+1}) e_{\sigma_i \sigma_{i+1}},$$

El signo del vector principal $e_{\sigma_i \sigma_{i+1}}$ es diferente para cada v rtice, as  que.

$$\mathbf{P}(\sigma') - \mathbf{P}(\sigma) = sg(\sigma_{i+1} - \sigma_i) e_{\sigma_i \sigma_{i+1}}$$

Supongamos, sin p rdida de generalidad, que $\sigma_i < \sigma_{i+1}$. Al ordenar adecuadamente la resta, aseguramos que $\sigma_{i+1} - \sigma_i > 0$. De esta manera, obtenemos una caracterizaci n vectorial de las aristas con los vectores principales de la celda de Voronoi.

Podemos notar que la cara 1-dimensional determinada por estos v rtices se representa como:

$$F(B_0|B_1|\cdots|B_i|\cdots|B_n)$$

donde $B_0 = \{\sigma_0\}$, $B_1 = \{\sigma_1\}$, ..., $B_i = \{\sigma_i, \sigma_{i+1}\}$, ..., $B_{n-1} = \sigma_n$. Entonces el baricentro de cada arista se puede expresar como:

$$\frac{1}{2}(\mathbf{P}(\sigma') + \mathbf{P}(\sigma)) = \frac{1}{2} \sum_{\substack{k < j, \\ k \neq i, \\ j \neq i+1}} sg(\sigma_j - \sigma_k) e_{\sigma_k \sigma_j} \quad (2.7)$$

$$= \frac{1}{2} \sum_{k < j} sg(\sigma_j - \sigma_k) e_{\sigma_k \sigma_j} - \frac{1}{2} \sum_{B_i} \sum_{\substack{k < j, \\ \sigma_k, \sigma_j \in B_i}} sg(\sigma_j - \sigma_k) e_{\sigma_k \sigma_j} \quad (2.8)$$

$$= \frac{1}{2} \sum_{l < m} \sum_{\substack{\sigma_k \in B_l, \\ \sigma_j \in B_m}} sg(\sigma_j - \sigma_k) e_{\sigma_k \sigma_j} \quad (2.9)$$

Nota. En adelante vamos a denotar como $e_{C_0|C_1}$, donde C_0 y C_1 son subconjuntos disjuntos de $U = \{0, \dots, n\}$ al vector

$$e_{C_0|C_1} = \sum_{\substack{\sigma_k \in C_0, \\ \sigma_j \in C_1}} sg(\sigma_j - \sigma_k) e_{\sigma_k \sigma_j}$$

Entonces (2.9) se puede ver como:

$$\frac{1}{2} \sum_{l < m} e_{B_l|B_m}. \quad (2.10)$$

Observación 2.16. Podemos notar que la coordenada i de $e_{C_0|C_1}$ está dada por:

- $p_{i|C_1}$ si $i \in C_0$,
- $-p_{i|C_1}$ si $i \in C_1$,
- o por 0 en otro caso.
- Además, si sumamos las coordenadas de $e_{C_0|C_1}$ dadas por el conjunto $C_0 \cup C_1$ tenemos como resultado 0, y si sumamos las coordenadas indexadas por el conjunto C_0 (C_1 respectivamente) vamos a tener como resultado $p_{C_0|C_1}$ ($-p_{C_0|C_1}$ respectivamente).

Como preámbulo podemos decir que la expresión (2.10) representa la suma pero solo tomando en cuenta los términos que se obtienen entre dos elementos los cuales viven en bloques diferentes, en otras palabras, captura las contribuciones de los vectores principales que conectan elementos de distintos bloques de la partición.

Por otro lado, la expresión con signo $-$ de (2.8) representa la suma pero solo de los términos obtenidos por dos elementos dentro de un mismo bloque, es decir, captura las contribuciones de los vectores principales que conectan elementos de un mismo bloque de la partición.

En la celda de Voronoi existen muchas aristas iguales, es decir, dadas por el mismo vector principal, incluso podemos decir que existen $\binom{n+1}{2}$ aristas diferentes en la celda, las cuales son, la cantidad de posibilidades de hacer transposición de dos elementos consecutivos en

una reordenación cualquiera de el conjunto $\{0, 1, \dots, n\}$.

Por otro lado, podemos calcular cuánto mide cada arista, esto es, calcular las normas de los vectores principales. De la Definición (2.13) recordemos que el vector principal e_{ij} , con $i < j$, está dado por un vector desde la componente 0 hasta la componente n para el cual sus posiciones σ_i, σ_j , las cuales le corresponden p_{σ_i, σ_j} y $-p_{\sigma_i, \sigma_j}$ respectivamente. Utilizando la Proposición (1.13) obtenemos:

$$|e_{ij}| = p_{ij} \sqrt{\frac{\Delta_{ij}}{\Delta}}.$$

Ejemplo 2.17. Para asentar las ideas, vamos a presentar como ejemplo los vértices que son adyacentes al vértice 140253, esto puede ser representado gráficamente como sigue

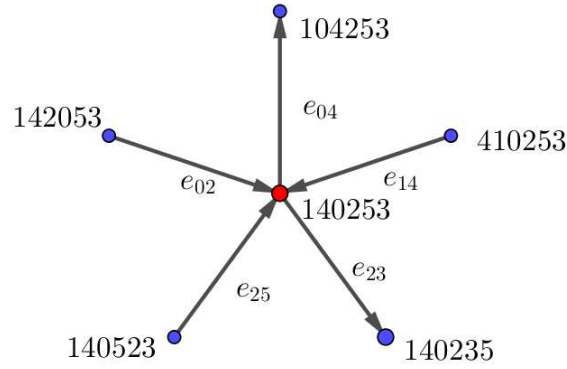


Figura 2.6: Vértices adyacentes al vértice 140253

Por otro lado, por ejemplo las y -coordenadas del vértice 012345 y del vértice 012435 según

(2.6) de manera explicita son

$$\begin{aligned}
\mathbf{P}(012435) &= \frac{1}{2}(e_{01} + e_{02} + e_{03} + e_{04} + e_{05} + e_{12} + e_{13} + e_{14} + e_{15} \\
&\quad + e_{23} + e_{24} + e_{25} - e_{34} + e_{35} + e_{45}) \\
&= \frac{1}{2} \begin{pmatrix} p_{01} + p_{02} + p_{03} + p_{04} + p_{05} \\ -p_{01} + p_{12} + p_{23} + p_{14} + p_{15} \\ -p_{02} - p_{12} + p_{23} + p_{24} + p_{25} \\ -p_{03} - p_{13} - p_{23} - p_{34} + p_{35} \\ -p_{04} - p_{14} - p_{24} + p_{34} + p_{45} \\ -p_{05} - p_{15} - p_{25} - p_{35} - p_{45} \end{pmatrix} \\
\mathbf{P}(012345) &= \frac{1}{2}(e_{01} + e_{02} + e_{03} + e_{04} + e_{05} + e_{12} + e_{13} + e_{14} + e_{15} \\
&\quad + e_{23} + e_{24} + e_{25} + e_{34} + e_{35} + e_{45}) \\
&= \frac{1}{2} \begin{pmatrix} p_{01} + p_{02} + p_{03} + p_{04} + p_{05} \\ -p_{01} + p_{12} + p_{23} + p_{14} + p_{15} \\ -p_{02} - p_{12} + p_{23} + p_{24} + p_{25} \\ -p_{03} - p_{13} - p_{23} + p_{34} + p_{35} \\ -p_{04} - p_{14} - p_{24} - p_{34} + p_{45} \\ -p_{05} - p_{15} - p_{25} - p_{35} - p_{45} \end{pmatrix}.
\end{aligned}$$

El baricentro de la cara que definen estos dos v rtices seg n (2.10) expl citamente est  dado por

$$\begin{aligned}
\mathbf{Ba}(F(0|1|2|43|5)) &= (\mathbf{P}(012435) + \mathbf{P}(012345)) \\
&= \frac{1}{2}(e_{01} + e_{02} + e_{03} + e_{04} + e_{05} + e_{12} + e_{13} + e_{14} + e_{15} \\
&\quad + e_{23} + e_{24} + e_{25} + e_{35} + e_{45}) \\
&= \frac{1}{2} \begin{pmatrix} p_{01} + p_{02} + p_{03} + p_{04} + p_{05} \\ -p_{01} + p_{12} + p_{23} + p_{14} + p_{15} \\ -p_{02} - p_{12} + p_{23} + p_{24} + p_{25} \\ -p_{03} - p_{13} - p_{23} + p_{35} \\ -p_{04} - p_{14} - p_{24} + p_{45} \\ -p_{05} - p_{15} - p_{25} - p_{35} - p_{45} \end{pmatrix}
\end{aligned}$$

Es interesante notar que esta idea nos permite contar todas las aristas de la celda de Voronoi. Dado que tenemos $6!$ vértices en total, cada vértice está conectado a otros 5 vértices adyacentes. Sin embargo, debemos considerar que cada vértice en el extremo de una arista se cuenta dos veces. Por lo tanto, el número total de aristas en la celda de Voronoi es $6! \times \frac{5}{2} = 1800$. Esto coincide con la estrategia que desarrollamos previamente para contar las aristas, como se mencionó en 2.9.

Esta observación nos proporciona una forma eficiente de calcular el número total de aristas en la celda de Voronoi, y refuerza la relación entre la combinatoria y la geometría que estamos explorando en nuestro trabajo.

2.5. Caras de dimensión 2 de la celda

Como vimos en la Proposición (2.6), cada cara dos dimensional de una celda de Voronoi para un lattice de primer tipo en $\mathbb{R}^n$, esta en correspondencia con una partición ordenada de $\{0, \dots, n\}$ en $n - 1$ bloques. Lo cual nos indica, como en (2.2.3), que en las particiones pueden pasar dos cosas, tener un conjunto de 3 elementos y $n - 2$ conjuntos de 1 elemento o tener dos conjuntos de 2 elementos y $n - 3$ de 1. Esto se puede apreciar en el ejemplo

escogido que se muestra en la siguiente figura.

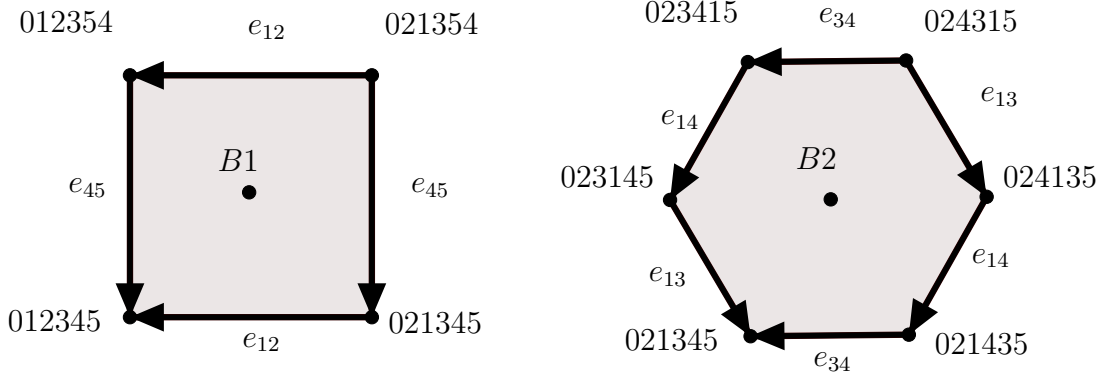


Figura 2.7: Caras 2 dimensionales

Aquí se puede ver que, las $\mathbf{y}$ -coordenadas de los baricentros B_1 y B_2 , se encuentran con la suma de uno de los vértices de la cara del respectivo baricentro con la mitad de sumas o restas de los vectores principales involucrados en las aristas de estas caras, estos vectores acompañados de un signo conveniente.

Por ejemplo, podemos llegar al baricentro B_1 sumando el vértice $\mathbf{P}(021345)$ con $\frac{1}{2}(e_{12} - e_{45})$, explícitamente:

$$\begin{aligned}
 \mathbf{Ba}(F(0|21|3|45)) &= \mathbf{P}(021345) + \frac{1}{2}(e_{12} - e_{45}) \\
 &= \frac{1}{2}(e_{01} + e_{02} + e_{03} + e_{04} + e_{05} - e_{12} + e_{13} + e_{14} + e_{15} \\
 &\quad + e_{23} + e_{24} + e_{25} + e_{34} + e_{35} + e_{45}) + \frac{1}{2}(e_{12} - e_{45}) \\
 &= \frac{1}{2} \begin{pmatrix} p_{01} + p_{02} + p_{03} + p_{04} + p_{05} \\ -p_{01} + p_{13} + p_{14} + p_{15} \\ -p_{02} + p_{23} + p_{24} + p_{25} \\ -p_{03} - p_{13} - p_{23} + p_{34} + p_{35} \\ -p_{04} - p_{14} - p_{24} - p_{34} \\ -p_{05} - p_{15} - p_{25} - p_{35} \end{pmatrix}.
 \end{aligned}$$

Notemos que, los índices de los vectores principales, e_{12} y e_{45} , que se sumaron al vértice $P(021345)$, representan las transposiciones que se deben hacer en la permutación que determina a dicho vértice 021345 para llegar a su vértice *opuesto* $P(012354)$ en $F(0|21|3|45)$ con relación al centro de la cara, es decir el baricentro buscado.

Calculemos ahora este mismo baricentro utilizando la formula (1.5) para comprobar que se obtiene el mismo resultado

$$\begin{aligned} \mathbf{Ba}(F(0|21|3|45)) &= \frac{1}{4}(\mathbf{P}(021345) + \mathbf{P}(012345) + \mathbf{P}(012354) + \mathbf{P}(021354)) \\ &= \frac{1}{2}(e_{01} + e_{02} + e_{03} + e_{04} + e_{05} + e_{13} + e_{14} + e_{15} + e_{23} + e_{24} + e_{25} + e_{34} + e_{35}) \\ &= \frac{1}{2} \begin{pmatrix} p_{01} + p_{02} + p_{03} + p_{04} + p_{05} \\ -p_{01} + p_{13} + p_{14} + p_{15} \\ -p_{02} + p_{23} + p_{24} + p_{25} \\ -p_{03} - p_{13} - p_{23} + p_{34} + p_{35} \\ -p_{04} - p_{14} - p_{24} - p_{34} \\ -p_{05} - p_{15} - p_{25} - p_{35} \end{pmatrix}. \end{aligned}$$

Notemos que $F(0|12|3|45)$ representa los vértices en la cara determinada por la partición $B_0 = \{0\}$, $B_1 = \{2, 1\}$, $B_3 = \{3\}$ y $B_4 = \{4, 5\}$. De este modo, como en (2.10), el baricentro también se puede ver como

$$\frac{1}{2} \sum_{l < m} e_{B_l | B_m}.$$

Lo cual está sumando solo las contribuciones de los vectores principales e_{ij} generados por índices que viven en diferentes bloques.

De la misma manera se puede hacer el mismo proceso para el otro caso de cara dos dimensional. Por ejemplo, podemos llegar al baricentro B_2 sumando el vértice 023145 más $\frac{1}{2}(e_{13} - e_{14} - e_{34})$, explícitamente como sigue:

$$\begin{aligned}
\mathbf{Ba}(F(0|2|143|5)) &= \mathbf{P}(023145) + \frac{1}{2}(e_{13} - e_{14} - e_{34}) \\
&= \frac{1}{2}(e_{01} + e_{02} + e_{03} + e_{04} + e_{05} - e_{12} - e_{13} + e_{14} + e_{15} \\
&\quad + e_{23} + e_{24} + e_{25} + e_{34} + e_{35} + e_{45}) + \frac{1}{2}(e_{13} - e_{14} - e_{34}) \\
&= \frac{1}{2} \begin{pmatrix} p_{01} + p_{02} + p_{03} + p_{04} + p_{05} \\ -p_{01} - p_{12} + p_{15} \\ -p_{02} + p_{12} + p_{23} + p_{24} + p_{25} \\ -p_{03} - p_{23} + p_{35} \\ -p_{04} - p_{24} + p_{45} \\ -p_{05} - p_{15} - p_{25} - p_{35} - p_{45} \end{pmatrix}.
\end{aligned}$$

De nuevo, los índices de los vectores principales que se sumaron al vértice, e_{13} , e_{14} y e_{34} , como debe ocurrir, representan las transposiciones que se deben hacer en el vértice 023145 para llegar a su *opuesto* 024135 en $F(0|2|143|5)$, es decir, el vértice también en $F(0|2|143|5)$ tal que su suma con 021345 da como resultado el centro de la cara, es decir, el baricentro.

Y se puede calcular este mismo baricentro utilizando la formula (1.5) y se comprueba que tienen el mismo resultado.

$$\frac{1}{2} \sum_{l < m} e_{B_l|B_m}.$$

que de nuevo, está sumando solo las contribuciones de los vectores principales e_{ij} generados por índices que viven en diferentes bloques.

Estos ejemplos proporcionan una intuición clave sobre cómo podemos calcular el baricentro de manera general en cualquier cara y en cualquier dimensión. Además, nos ayudan a identificar qué vértices son opuestos en cada cara.

2.6. Caras k -dimensionales de la celda

Definición 2.18. En una celda de Voronoi correspondiente a un lattice de primer tipo, el *vértice opuesto* σ' de un vértice σ en una cara de dimensión k se define como aquel vértice tal que la semisuma $\frac{1}{2}(\sigma' + \sigma)$ resulta en el baricentro de la cara mencionada.

Teorema 2.19. Sea L un lattice de primer tipo y sea $\mathbf{F}$ una cara k -dimensional de la celda de Voronoi, correspondiente a la partición ordenada $B_0, B_1, \dots, B_{n-1-k}$ de $U = \{0, 1, \dots, n\}$, entonces el baricentro de $\mathbf{F}$ en $\mathbf{y}$ -coordenadas aumentadas está dado por

$$\mathbf{Ba}(\mathbf{F}) = \frac{1}{2} \sum_{l < m} \sum_{\substack{\sigma_k \in B_l, \\ \sigma_j \in B_m}} sg(\sigma_j - \sigma_k) e_{\sigma_k \sigma_j} = \frac{1}{2} \sum_{l < m} e_{B_l | B_m},$$

donde $sg(\sigma_k - \sigma_j)$ es la función de signo, igual a 1 si $\sigma_k > \sigma_j$ y -1 si $\sigma_k < \sigma_j$.

Demostración. Consideremos $\mathbf{F}$, la cara k -dimensional de la celda de Voronoi, correspondiente a la partición ordenada $B_0, B_1, \dots, B_{n-1-k}$ de $U = \{0, 1, \dots, n\}$. Sabemos que el baricentro de un politopo se define como el promedio de sus vértices, es decir,

$$\mathbf{Ba} = \frac{1}{m} \sum_{i=1}^m \mathbf{v}_i,$$

donde m es la cantidad de vértices en el politopo y $\mathbf{v}_i$ son los vértices. En nuestro caso, el baricentro de la cara $\mathbf{F}$ se calcula de la misma manera, pero considerando $m = |B_0|! \cdot |B_1|! \cdots |B_{n-1-k}|!$. Recordemos que los vértices están representados por un reordenamiento de $\{0, \dots, n\}$ en $n-1-k$ subconjuntos ordenados. Estos subconjuntos se organizan de forma que los primeros $|B_0|$ elementos corresponden al orden específico de B_0 , seguidos por $|B_1|$ elementos reordenados de B_1 , y así sucesivamente hasta que los últimos $|B_{n-1-k}|$ elementos sean un reordenamiento de B_{n-1-k} .

De esta manera, las $\mathbf{y}$ -coordenadas de todos los vértices σ , denotados como $\mathbf{P}(\sigma)$, se expresan como:

$$\mathbf{P}(\sigma) = \frac{1}{2} \sum_{\sigma_i < \sigma_j} sg(\sigma_j - \sigma_i) e_{\sigma_i \sigma_j},$$

en $\mathbf{F}$. Observamos que cada contribución de los vectores principales, representados por índices σ_i, σ_j que pertenecen a bloques diferentes, tienen el mismo signo, ya que los bloques tienen un orden específico. Dado que hay m vértices, hay también m contribuciones idénticas de estos vectores principales. Así, el baricentro de $\mathbf{F}$ se puede expresar como:

$$\mathbf{Ba}(\mathbf{F}) = \frac{1}{m} \frac{1}{2} \sum_{B_i} \sum_{\beta \in S_{B_i}} \sum_{\beta_k < \beta_j} sg(\beta_j - \beta_k) e_{\beta_k \beta_j} + \frac{1}{m} \left(m \frac{1}{2} \sum_{l < h} \sum_{\substack{\sigma_k \in B_l, \\ \sigma_j \in B_h}} sg(\sigma_j - \sigma_k) e_{\sigma_k \sigma_j} \right) \quad (2.11)$$

Donde S_{B_i} es el conjunto de permutaciones del conjunto B_i , y $\beta_k, \beta_j \in \beta$. Notamos que la expresión anterior (2.11) ya nos proporciona el resultado del teorema. Solo resta demostrar que

$$\sum_{B_i} \sum_{\beta \in S_{B_i}} \sum_{\beta_k < \beta_j} sg(\beta_j - \beta_k) e_{\beta_k \beta_j} = 0. \quad (2.12)$$

Podemos observar que (2.12) representa la suma de las contribuciones de todos los vértices de los vectores principales, los cuales tienen índices pertenecientes al mismo bloque de la partición. Esta suma tiene en cuenta todas las permutaciones dentro de cada bloque.

Sin pérdida de generalidad, demostraremos para B_i que

$$\sum_{\beta \in S_{B_i}} \sum_{\beta_k < \beta_j} sg(\beta_j - \beta_k) e_{\beta_k \beta_j} = 0.$$

Es necesario que $|B_i| = r > 1$, para que se puedan seleccionar dos índices y generar un vector principal. Tomemos $\beta = \beta_0 \cdots \beta_i \cdots \beta_j \cdots \beta_{r-1} \in S_{B_i}$. De esta permutación se genera

el vector principal $sg(\beta_j - \beta_i)e_{\beta_i\beta_j}$, el cual está incluido en la suma mencionada. Por otro lado, la permutación $(\beta_i\beta_j)\beta = \beta_0 \cdots \beta_j \cdots \beta_i \cdots \beta_{r-1}$ también está en S_{B_i} porque este consta de todas las permutaciones de B_i . Por lo tanto, también está presente el vector principal $sg(\beta_i - \beta_j)e_{\beta_i\beta_j}$ en la suma, lo que significa que este vector principal se cancela. Este proceso es repetible para cualquier par de elementos de cualquier permutación de B_i , lo que nos lleva a concluir que

$$\sum_{\beta \in S_{B_i}} \sum_{\beta_k < \beta_j} sg(\beta_j - \beta_k)e_{\beta_k\beta_j} = 0,$$

y, finalmente,

$$\mathbf{Ba}(\mathbf{F}) = \frac{1}{2} \sum_{l < m} \sum_{\substack{\sigma_k \in B_l, \\ \sigma_j \in B_m}} sg(\sigma_j - \sigma_k)e_{\sigma_k\sigma_j} = \frac{1}{2} \sum_{l < m} e_{B_l|B_m}.$$

□

El grupo simétrico S_m es el conjunto de todas las permutaciones posibles de un conjunto con m elementos. Una permutación simplemente implica una reorganización de estos elementos.

Regresemos a $\mathbf{F}$, la cara k -dimensional de la celda de Voronoi, asociada con la partición ordenada $B_0, B_1, \dots, B_{n+1-k}$ de $U = \{0, 1, \dots, n\}$. Desde la perspectiva de S_n , un vértice σ puede ser representado por la concatenación en orden de las palabras obtenidas a partir de las permutaciones σ_{B_i} con $\sigma_{B_i} \in S_{B_i}$, para cada $i \in \{0, 1, \dots, n+1-k\}$. Así,

$$\sigma = \sigma_{B_0} || \sigma_{B_1} || \cdots || \sigma_{B_{n+1-k}},$$

donde $||$ denota la operación de concatenación de palabras.

Dado que S_m es un grupo, cada permutación tiene su inversa. El inverso de una permutación es aquella que deshace los intercambios realizados por la permutación original. Por ende, si σ es una permutación en S_m , su inversa, denotada como σ^{-1} , se define como la permutación

que deshace los intercambios realizados por σ . Específicamente, si $\sigma = \sigma_1\sigma_2\ldots\sigma_m$, donde σ_i es el elemento en la posición i , entonces su inversa σ^{-1} está dada por:

$$\sigma^{-1} = \sigma_m\sigma_{m-1}\ldots\sigma_2\sigma_1.$$

Tomando en consideración este concepto, el siguiente resultado demostrará la relación entre los vértices opuestos en una cara de la celda de Voronoi y los inversos en el grupo simétrico.

Corolario 2.20. Sea L un lattice de primer tipo en $\mathbb{R}^n$ y sea $\mathbf{F}$ una cara k -dimensional de la celda de Voronoi, correspondiente a la partición ordenada $B_0, B_1, \ldots, B_{n-1-k}$ de $U = \{0, 1, \ldots, n\}$, entonces, dado un vértice $\sigma = \sigma_{B_0}||\sigma_{B_1}||\cdots||\sigma_{B_{n+1-k}}$, su opuesto en la cara $\mathbf{F}$, denotado por $op_{\mathbf{F}}(\sigma)$, está dado por

$$op_{\mathbf{F}}(\sigma) = \sigma_{B_0}^{-1}||\sigma_{B_1}^{-1}||\cdots||\sigma_{B_{n+1-k}}^{-1}.$$

Donde $\sigma_{B_i}^{-1}$ es el inverso de σ_{B_i} en S_{B_i}

Capítulo 3

Cálculo de la constante de cuantización

La metodología para calcular la constante de cuantización en dimensión 5 en este capítulo se basa en la técnica que se presentó en la Sección (1.6). En ese capítulo, particionamos la celda de Voronoi en simples. La idea central es dividir la celda de Voronoi en estas piezas más manejables y calcular su inercia y su volumen.

Este proceso de descomposición nos permite calcular el segundo momento no normalizado para cada uno de estos simples. El segundo momento no normalizado es esencial para determinar la constante de cuantización, ya que solo restaría dividir este segundo momento por una potencia específica del volumen. La idea es calcular la contribución de cada simplex y luego sumar todas estas contribuciones para obtener el segundo momento no normalizado de la celda de Voronoi en su totalidad.

Una vez que tengamos el segundo momento no normalizado de la celda de Voronoi, podemos calcular la constante de cuantización en el lattice. Esta construcción nos llevará a encontrar patrones para así dar una idea de como sería una fórmula generalizada para la constante de cuantización que sea aplicable a cualquier lattice de primer tipo en cualquier dimensión.

3.1. Motivación

Analizando las ecuaciones (1.14), (1.13) y (1.15), en primera instancia podríamos percibir que no tienen relación entre sí. Sin embargo, es importante destacar que los coeficientes en todas estas ecuaciones están estrechamente relacionados con su dimensión. Para destacar que estas ecuaciones siguen un patrón, vamos a representar cada término del numerador de las ecuaciones, así como el determinante, utilizando grafos.

Un grafo no dirigido es un tipo de grafo en el cual las aristas representan relaciones simétricas y no tienen un sentido definido.

Formalmente, se definen por un par de conjuntos $G = (V, E)$, donde:

- $V \neq \emptyset$ es el conjunto no vacío de vértices o nodos.
- $E \subseteq \{(a, b) \in V \times V\}$ es el conjunto de aristas, tal que $(a, b) = (b, a)$.

Un grafo es simple si a lo más existe una arista uniendo dos vértices cualesquiera. De esta manera, un grafo completo es un grafo simple no dirigido donde cada par de vértices está conectado por una arista.

El grafo completo de $n + 1$ vértices tiene $\frac{n(n+1)}{2}$ aristas, y se denota con K_{n+1} .

En este caso, siendo Λ un lattice con superbase obtusa $B = \{\mathbf{v}_0, \mathbf{v}_1 \dots, \mathbf{v}_n\}$, vamos a tomar el grafo K_{n+1} con vértices etiquetados con los elementos de B y se etiqueta la arista que une a $\mathbf{v}_i$ con $\mathbf{v}_j$ con el parámetro de Selling p_{ij} .

Ejemplo 3.1.

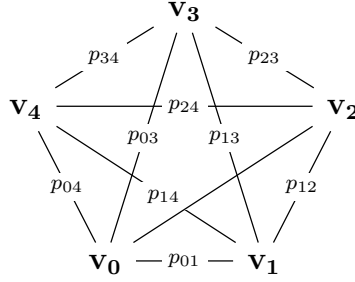


Figura 3.1: El grafo K_5 etiquetado con los parámetros de Selling e índices vectores de la superbase obtusa.

Un árbol es un grafo en el que cualquier par de vértices están conectados por exactamente un camino, o alternatively, es un grafo conexo sin ciclos. Sea G un grafo simple. Un árbol generador de G es un subgrafo de G que es un árbol y contiene todos los vértices de G .

El siguiente resultado se presenta sin demostración y describe cómo calcular el determinante en cualquier dimensión de un lattice. Este teorema y su demostración se pueden encontrar en la Sección 1.6 de [17].

Teorema 3.2. Sea Λ un lattice n -dimensional, y $B = \{\mathbf{v}_0, \mathbf{v}_1, \dots, \mathbf{v}_n\}$ una superbase para Λ . Si $p_{i|jk\dots l} = p_{ij} + p_{ik} + \dots + p_{il}$, con $p_{ij} = -\mathbf{v}_i \cdot \mathbf{v}_j$ para $0 \leq i < j \leq n$. Entonces el determinante del lattice, $\det(L)$, viene dado por:

$$\det(L) = \sum_T \prod_{[\mathbf{v}_i, \mathbf{v}_j] \in T} p_{ij}$$

donde T recorre todos los árboles generadores de K_{n+1} son los vértices etiquetados con B y las aristas con p_{ij} , y $[\mathbf{v}_i, \mathbf{v}_j]$ denota la arista entre los vértices $\mathbf{v}_i$ y $\mathbf{v}_j$.

Ejemplo 3.3. Un lattice en dimensión 3 con una superbase obtusa $B = \{\mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$, tiene asociado el grafo completo

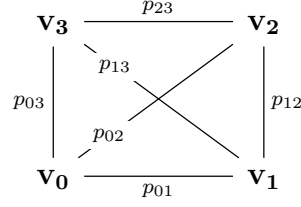


Figura 3.2: K_4 .

Tiene grafos generadores que se pueden obtener de uno de los dos siguientes grafos.

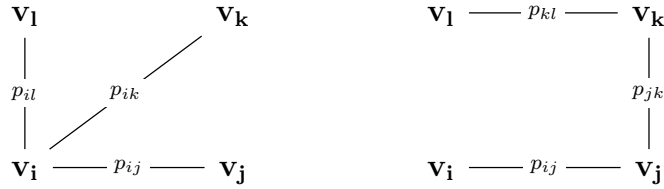


Figura 3.3: Generadores de los árboles generadores de K_4 . Variando i, j, k, l en $\{0, 1, 2, 3\}$.

Entonces por el Teorema (3.2), cada uno de estos grafos corresponde a un sumando de:

$$\begin{aligned} \det(\Lambda) = & p_{01}p_{02}p_{03} + p_{01}p_{02}p_{13} + p_{01}p_{03}p_{12} + p_{02}p_{03}p_{12} + p_{02}p_{03}p_{13} + \\ & p_{01}p_{02}p_{23} + p_{01}p_{12}p_{13} + p_{01}p_{03}p_{23} + p_{02}p_{12}p_{13} + p_{03}p_{12}p_{13} + p_{01}p_{12}p_{23} + \\ & p_{01}p_{13}p_{23} + p_{02}p_{12}p_{23} + p_{02}p_{13}p_{23} + p_{03}p_{12}p_{23} + p_{03}p_{13}p_{23}. \end{aligned}$$

Por otro lado si tenemos un lattice en dimensión 5, que tiene superbase $B = \{\mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4, \mathbf{v}_5\}$, entonces el grafo completo K_6 con los vértices etiquetados con B y las aristas etiquetadas con los parámetros de Selling, tiene la forma

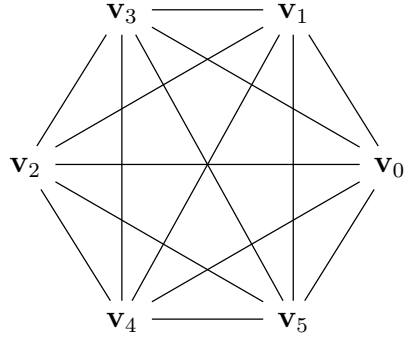


Figura 3.4: K_6 .

Los árboles generadores son obtenidos por los siguientes grafos

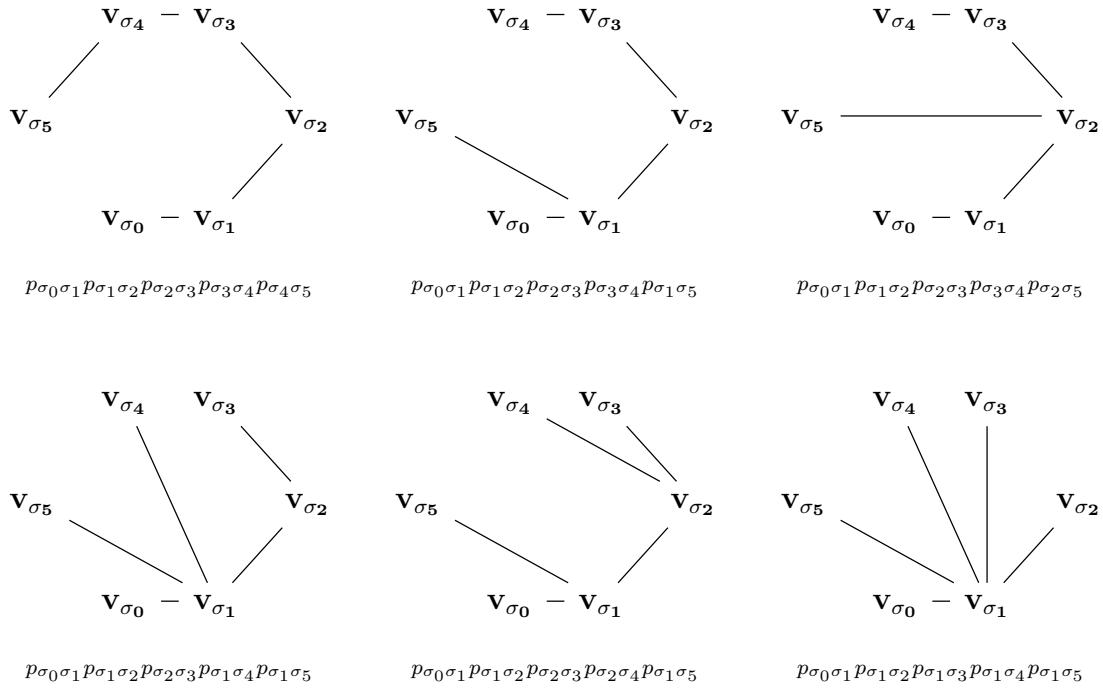


Figura 3.5: Generadores de los árboles generadores de K_6 . Variando los σ_i con $0 \leq i \leq 5$ en $\{0, 1, 2, 3, 4, 5\}$.

De esta manera, en virtud del Teorema (3.2), el volumen del lattice en dimensión 6 es la suma de todos los árboles generadores obtenidos de la Figura (3.5).

Así, con esta información, disponemos de una herramienta poderosa para determinar el volumen de un lattice sin necesidad de calcular explícitamente el determinante de la matriz de Gram. Además, esta metodología nos permite expresar el volumen de un lattice de forma concisa y eficiente, evitando la necesidad de una escritura explícita.

A la luz de los árboles generadores y la representación de términos dados por multiplicaciones de parámetros de Selling, el numerador de las ecuaciones (1.14), (1.13) y (1.15), sí cumplen un patrón, al menos en estas tres dimensiones, veamos que si tomamos a C_i como la representación de la suma de todos los términos obtenidos al multiplicar las etiquetas de los grafos que son árboles generadores del grafo completo a los cuales se les ha añadido una arista para formar un ciclo de longitud i .

Ejemplo 3.4. Es decir, C_2 representa la suma de todos los términos obtenidos de árboles como los siguientes

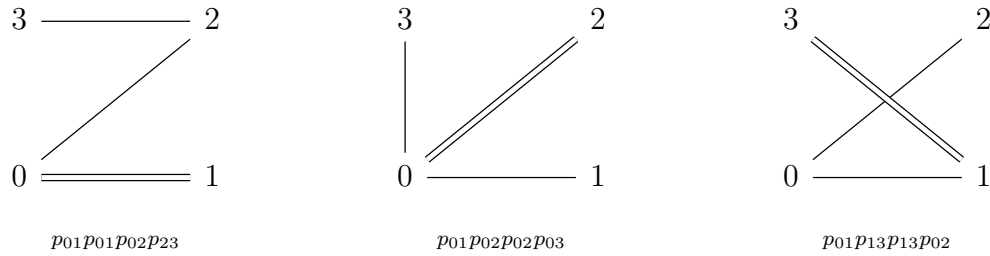


Figura 3.6: Ejemplo de algunos terminos de C_2 en dimensión 3.

C_3 representa la suma de todos los términos obtenidos de árboles como los siguientes

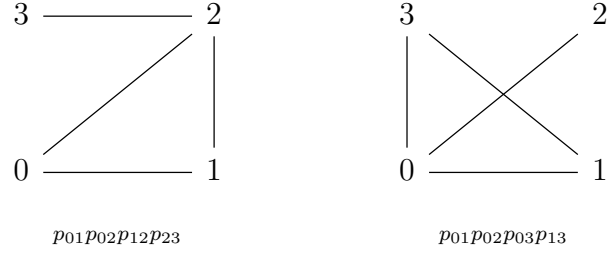


Figura 3.7: Ejemplo de algunos términos de C_3 en dimensión 3.

Y como último ejemplo en esta dimensión, C_4 representa la suma de todos los términos obtenidos de árboles como los siguientes

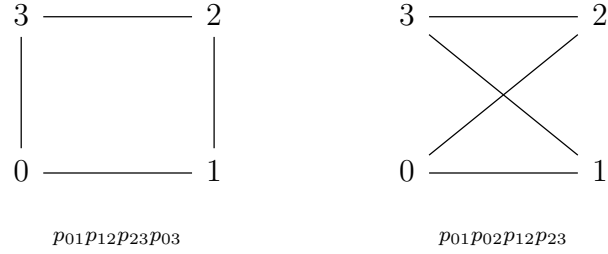


Figura 3.8: Ejemplo de algunos términos de C_4 en dimensión 3.

Con esta idea en mente, el numerador de la expresión (1.14), que es la constante de cuantización para un lattice en dimensión 2, se puede expresar utilizando estos “ciclos” y queda de la forma

$$G_2(\Lambda) = \frac{C_2 + 4C_3}{24\Delta^{3/2}}. \quad (3.1)$$

Por otro lado, con la misma idea pero ahora en dimensión 3, la ecuación (1.13) se puede expresar como

$$G_3(\Lambda) = \frac{C_2 + 4C_3 + 6C_4}{36\Delta^{4/3}}, \quad (3.2)$$

No solo es interesante que también se puede expresar la constante de cuantización para lattices de primer tipo en dimensión 4 utilizando estos ciclos, sino que también lo es y mucho más, la confirmación de un patrón que venían siguiendo las dos expresiones anteriores, la expresión en dimensión (1.15) queda de la forma

$$G_4(\Lambda) = \frac{C_2 + 4C_3 + 6C_4 + 8C_5}{48\Delta^{5/4}}. \quad (3.3)$$

El patrón que siguen las ecuaciones para la constante de cuantización es uno de nuestros principales aportes en este trabajo, porque se convierte en nuestra conjetura para calcular la constante de cuantización para lattices de primer tipo en cualquier dimensión, esta conjetura esta enunciada como sigue.

Conjetura 3.5. Sea Λ un lattice de Tipo I en $\mathbb{R}^n$ con superbase obtusa $B = \{\mathbf{v}_0, \dots, \mathbf{v}_n\}$, con parámetros de Selling reducidos p_{ij} con i, j en $\{0, \dots, n\}$ y determinante Δ , entonces la constante de cuantización de Λ viene dada por:

$$G_n(\Lambda) = \frac{C_2 + 2 \sum_{k=2}^n k C_{k+1}}{12n\Delta^{n+1/n}},$$

donde C_i representa la suma de todos los términos obtenidos al multiplicar las etiquetas de los grafos que son árboles generadores del grafo completo a los cuales se les ha añadido una arista para formar un ciclo de longitud i .

La finalidad de el resto de este capítulo es demostrar que esta conjetura se cumple para lattices de primer tipo en dimensión 5, lo cual se convierte en el aporte más importante de este trabajo de investigación.

3.2. Partición de la celda de Voronoi

Como hemos mencionado, vamos a presentar una partición de la celda de Voronoi en simples, de manera general. Recordemos que un simplex es la envolvente convexa de un conjunto de $n + 1$ puntos distintos $\mathbf{u}_1, \dots, \mathbf{u}_{n+1} \in \mathbb{R}^n$. En este caso, estos puntos serán seleccionados de la siguiente manera:

- En primer lugar elegimos un vértice $\sigma = \sigma_0\sigma_1 \cdots \sigma_n$ en la celda de Voronoi, para este caso es la intersección de las n caras $C = \{F_{\sigma_0}, F_{\sigma_0\sigma_1}, \dots, F_{\sigma_0 \cdots \sigma_{n-1}}\}$.
- El vértice cero del simplex coincide con el centro de la celda, $\mathbf{0}$, que corresponde al baricentro de la celda de Voronoi. Hacemos notar que el primer baricentro coincide con $\mathbf{Ba}(F(U))$, donde $U = \{0, 1, \dots, n\}$ tal como se definió en (2.4).
- El vértice uno del simplex que estamos construyendo será el baricentro de una de las caras $n - 1$ dimensionales de la celda a la que pertenece el vértice. Específicamente, tenemos n posibilidades de escoger esta cara. Llamémosla $F_{\sigma_0 \cdots \sigma_{\tau_0}}$, así las cosas el segundo vértice será $\mathbf{Ba}(F_{\sigma_0 \cdots \sigma_{\tau_0}})$, siendo $\tau_0 \in \{0, 1, \dots, n - 1\}$.
- El vértice dos del simplex que estamos construyendo será el baricentro de una de las caras $(n - 2)$ -dimensionales de la celda a la que pertenece el vértice, la cual está contenida en la cara previamente escogida $F_{\sigma_0 \cdots \sigma_{\tau_0}}$. Sabemos que las caras $(n - 2)$ -dimensionales son la intersección de dos caras $(n - 1)$ -dimensionales. Por lo tanto, necesitamos escoger otro elemento de C diferente de $F_{\sigma_0 \cdots \sigma_{\tau_0}}$. Tal elección las podemos hacer entre $n - 1$ posibilidades. Supongamos que esta cara es $F_{\sigma_0 \cdots \sigma_{\tau_1}}$. Entonces, el vértice dos del simplex es $\mathbf{Ba}(F_{\sigma_0 \cdots \sigma_{\tau_0}} \cap F_{\sigma_0 \cdots \sigma_{\tau_1}})$, siendo τ_1 un elemento en $\{0, 1, \dots, n - 1\} \setminus \{\tau_0\}$.

En general,

- El i -ésimo vértice del simplex será el baricentro de una de las caras $(n - i)$ -dimensionales de la celda a la que pertenece el vértice, la cual está contenida en la cara obtenida en el paso anterior: $F_{\sigma_0 \cdots \sigma_{\tau_0}} \cap F_{\sigma_0 \cdots \sigma_{\tau_1}} \cap \cdots \cap F_{\sigma_0 \cdots \sigma_{\tau_{i-2}}}$. Dado que las caras $(n - i)$ -dimensionales son la intersección de i caras $(n - 1)$ -dimensionales, necesitamos escoger otro elemento de C diferente a previamente elegidos para realizar la intersección con la cara obtenida en el paso anterior. Para lo cual tenemos $n - i + 1$ posibilidades. Supongamos que esta cara es $F_{\sigma_0 \cdots \sigma_{\tau_{i-1}}}$. Entonces, el i -ésimo vértice es $\mathbf{Ba}(F_{\sigma_0 \cdots \sigma_{\tau_0}} \cap F_{\sigma_0 \cdots \sigma_{\tau_1}} \cap \cdots \cap F_{\sigma_0 \cdots \sigma_{\tau_{i-1}}})$ con $\tau_{i-1} \notin \{\tau_0, \tau_1, \dots, \tau_{i-2}\}$.

Note que el proceso anterior termina después de n cuando se llega al vértice σ , que es el baricentro de la cara 0-dimensional, la cual es la intersección de todos los elementos de C .

Esto nos revela varias observaciones importantes. Primero, para cada vértice hay $n!$ formas de construir un simplex. Segundo, bajo esta construcción, no hay simples repetidos; todos son disjuntos, y su unión resulta en la celda. Esto significa que la partición está bien definida. Es decir, la cantidad total de simples construidos siguiendo este procedimiento es el producto de $(n+1)!$, que es el número de vértices, con $n!$, que es el número de simples que se pueden construir para un vértice dado. Finalmente, estos simples se pueden etiquetar con elementos de $S_{n+1} \times S_n$.

Existe una correspondencia biunívoca entre el conjunto de simples generados por la partición descrita y $S_{n+1} \times S_n$. Una pareja ordenada (σ, τ) en $S_{n+1} \times S_n$ representa los vértices del simplex determinado por el proceso descrito en los ítems anteriores. Tomando σ como el vértice y τ como el conjunto ordenado resultante $\{\tau_0, \tau_1, \dots, \tau_{i-2}\}$, que representa los baricentros resultantes en dicho proceso.

Ejemplo 3.6. Sea Λ un lattice en $\mathbb{R}^3$ con superbase obtusa $B = \{\mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ entonces el simplex asociado a la pareja $(\sigma, \tau) = (2301, 210)$ está delimitado por los siguientes vértices:

Vértice 0: este vértice está determinado por el $\mathbf{Ba}(F(2301)) = \mathbf{0}$, el cual es el baricentro de la celda.

Vértice 1: ya que el primer elemento de τ es 2 este vértice está determinado por el baricentro de la cara F_{230} ya que según el proceso, se toman los índices desde la posición 0 hasta la posición 2 del vértice, esto es

$$2\mathbf{Ba}(F(230|1)) = -e_{12} - e_{13} + e_{01} \quad (3.4)$$

$$= \begin{pmatrix} p_{01} \\ -p_{01} - p_{12} - p_{13} \\ p_{12} \\ p_{13} \end{pmatrix}. \quad (3.5)$$

En general, en cualquier dimensión, el vértice 1 está siempre determinado por la mitad de un vector de Voronoi.

Vértice 2: ya que el segundo elemento de τ es 1 este vértice está determinado por el baricentro de la cara $F_{230} \cap F_{23}$, esto es

$$2\mathbf{Ba}(F(23|0|1)) = -e_{12} - e_{13} + e_{01} - e_{02} - e_{03} \quad (3.6)$$

$$= \begin{pmatrix} p_{01} - p_{02} - p_{03} \\ -p_{01} - p_{12} - p_{13} \\ p_{12} + p_{02} \\ p_{13} + p_{03} \end{pmatrix}. \quad (3.7)$$

Vértice 3: finalmente como es de esperarse ya que el último elemento de τ es 0 este vértice está determinado por el baricentro de la cara $F_{230} \cap F_{23} \cap F_2$, el cual es justamente el vértice σ , esto es

$$2\mathbf{Ba}(F(2|3|0|1)) = -e_{12} - e_{13} + e_{01} - e_{02} - e_{03} + e_{23} \quad (3.8)$$

$$= \begin{pmatrix} p_{01} - p_{02} - p_{03} \\ -p_{01} - p_{12} - p_{13} \\ p_{12} + p_{02} + p_{23} \\ p_{13} + p_{03} - p_{23} \end{pmatrix}. \quad (3.9)$$

Por lo tanto el simplex está determinado por el conjunto de vértices

$$\Delta(\sigma, \tau) = \{\mathbf{0}, e_{12} - e_{13} + e_{01}, e_{12} - e_{13} + e_{01} - e_{02} - e_{03}, e_{12} - e_{13} + e_{01} - e_{02} - e_{03} + e_{23}\}$$

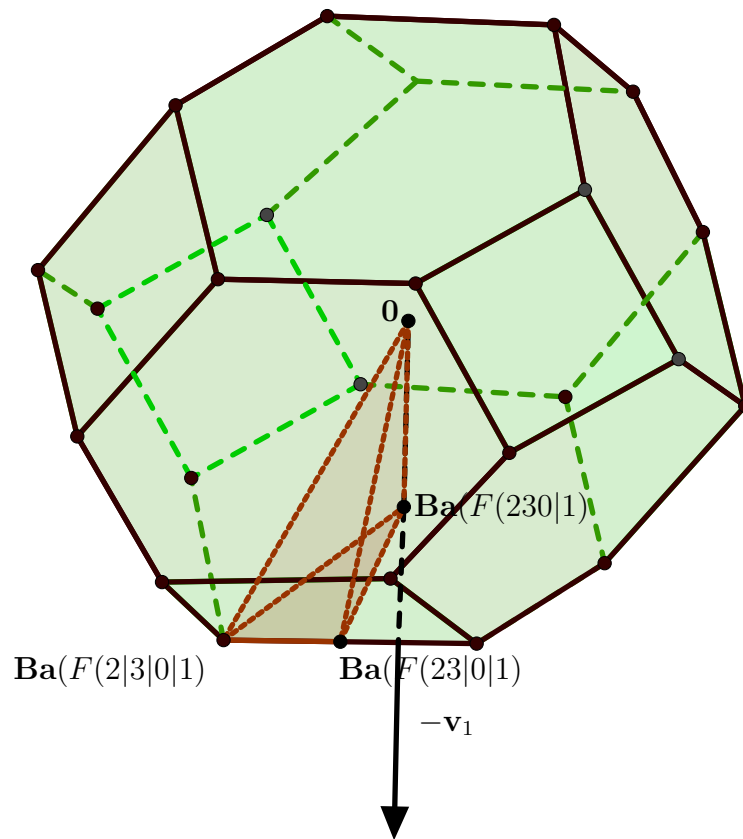


Figura 3.9: Simplex $\Delta(2301, 210)$.

Ya que vamos a concentrarnos en dimensión 5 conviene presentar un ejemplo de la construcción de un simplex de dicha dimensión.

Ejemplo 3.7. Sea Λ un lattice en $\mathbb{R}^5$ con superbase obtusa $B = \{\mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4, \mathbf{v}_5\}$ entonces el simplex dado por $(\sigma, \tau) = (234051, 32140)$ está determinado por los siguientes vértices:

- **Vértice 0:** este vértice está determinado por el $\mathbf{Ba}(F(234051)) = \mathbf{0}$, el cual es el baricentro de la celda.
- **Vértice 1:** ya que el primer elemento de τ es 3 este vértice está determinado por el baricentro de la cara F_{2340} ya que según el proceso, se toman los índices desde la

posición 0 hasta la posición 3 del vértice, esto es

$$2\mathbf{Ba}(F(2340|51)) = -e_{12} - e_{13} - e_{14} + e_{01} + e_{25} + e_{35} + e_{45} + e_{05} \quad (3.10)$$

Este es el vector de Voronoi $\mathbf{v}_2 + \mathbf{v}_3 + \mathbf{v}_4 + \mathbf{v}_0$.

- **Vértice 2:** ya que el segundo elemento de τ es 2 este vértice está determinado por el baricentro de la cara $F_{2340} \cap F_{234}$, esto es

$$\begin{aligned} 2\mathbf{Ba}(F(234|0|51)) = & -e_{12} - e_{13} - e_{14} + e_{01} + e_{25} + e_{35} + e_{45} + e_{05} \\ & - e_{02} - e_{03} - e_{04} \end{aligned}$$

- **Vértice 3:** debido a que el tercer elemento de τ es 1 este vértice está determinado por el baricentro de la cara $F_{2340} \cap F_{234} \cap F_{23}$, el cual es justamente el vértice σ , esto es

$$\begin{aligned} 2\mathbf{Ba}(F(23|4|0|51)) = & -e_{12} - e_{13} - e_{14} + e_{01} + e_{25} + e_{35} + e_{45} + e_{05} \\ & - e_{02} - e_{03} - e_{04} + e_{24} + e_{34} \end{aligned}$$

- **Vértice 4:** el cuarto elemento de τ es 4 este vértice está determinado por el baricentro de la cara $F_{2340} \cap F_{234} \cap F_{23} \cap F_{23405}$,

$$\begin{aligned} 2\mathbf{Ba}(F(23|4|0|5|1)) = & -e_{12} - e_{13} - e_{14} + e_{01} + e_{25} + e_{35} + e_{45} + e_{05} \\ & - e_{02} - e_{03} - e_{04} + e_{24} + e_{34} - e_{15} \end{aligned}$$

- **Vértice 5**, finalmente como el último elemento de τ es 0 este vértice está determinado por el baricentro de la cara $F_{2340} \cap F_{234} \cap F_{23} \cap F_{23405} \cap F_2$, el cual es justamente el vértice σ , esto es $+20+$

$$\begin{aligned} 2\mathbf{Ba}(F(2|3|4|0|5|1)) = & -e_{12} - e_{13} - e_{14} + e_{01} + e_{25} + e_{35} + e_{45} + e_{05} \\ & - e_{02} - e_{03} - e_{04} + e_{24} + e_{34} - e_{15} + e_{23} \end{aligned}$$

Por lo tanto el simplex está determinado por el conjunto de vértices

$$\begin{aligned} \Delta(\sigma, \tau) = & \{\mathbf{0}, e_{2340|51}, e_{2340|51} + e_{234|0}, e_{2340|51} + e_{234|0} + e_{23|4}, \\ & e_{2340|51} + e_{234|0} + e_{23|4} + e_{5|1}, e_{2340|51} + e_{234|0} + e_{23|4} + e_{5|1} + e_{2|3}\} \end{aligned}$$

Del Teorema (2.19) que nos dice que si tenemos a L un lattice de primer tipo y sea $\mathbf{F}$ una cara k -dimensional de la celda de Voronoi, correspondiente a la partición ordenada $B_0, B_1, \dots, B_{n-1-k}$ de $U = \{0, 1, \dots, n\}$, entonces el baricentro de $\mathbf{F}$ en $\mathbf{y}$ -coordenadas aumentadas está dado por

$$\mathbf{Ba}(\mathbf{F}) = \frac{1}{2} \sum_{l < m} e_{B_l|B_m},$$

tomando el simplex como el conjunto ordenado de vértices $\Delta(\sigma, \tau) = \{\mathbf{d}_0, \dots, \mathbf{d}_n\}$ donde $\sigma = (\sigma_0, \dots, \sigma_n)$ y $\tau = (\tau_0, \dots, \tau_{n-1})$ en $S_{n+1} \times S_n$, el proceso para la obtención de los vértices de dicho simplex puede ser descrito de la siguiente manera.

Dado que el primer vértice $\mathbf{d}_0$ del simplex es $\mathbf{Ba}(F_{\sigma_0 \dots \sigma_n}) = \mathbf{0}$ la partición de $U = \{0, \dots, n\}$ correspondiente a esta cara es U mismo.

Por otro lado el segundo vértice $\mathbf{d}_1$ del simplex es $\mathbf{Ba}(F_{\sigma_0 \dots \sigma_{\tau_0}})$ la partición de U es $B_0 = \{\sigma_0, \dots, \sigma_{\tau_0}\}$ y $B_1 = \{\sigma_{\tau_0+1}, \dots, \sigma_n\}$, esto es

$$\mathbf{d}_1 = \mathbf{Ba}(F(B_0|B_1)) = \frac{1}{2} e_{B_0|B_1},$$

Ahora, el tercer vértice $\mathbf{d}_2$ del simplex es $\mathbf{Ba}(F_{\sigma_0 \dots \sigma_{\tau_0}} \cap F_{\sigma_0 \dots \sigma_{\tau_1}})$, sin pérdida de generalidad supongamos que $\tau_0 < \tau_1$, la partición de U es $B_0 = \{\sigma_0, \dots, \sigma_{\tau_0}\}$, $B_1 = \{\sigma_{\tau_0+1}, \dots, \sigma_{\tau_1}\}$ y $B_2 = \{\sigma_{\tau_1+1}, \dots, \sigma_n\}$, esto es

$$\mathbf{d}_2 = \mathbf{Ba}(F(B_0|B_1|B_2)) = \frac{1}{2} \sum_{l < m}^2 e_{B_l|B_m},$$

$$\mathbf{d}_2 = \frac{1}{2} e_{B_1|B_2} + \frac{1}{2} e_{B_0|B_1 \cup B_2},$$

$$\mathbf{d}_2 = \frac{1}{2} e_{B_1|B_2} + \mathbf{d}_1.$$

El vértice $\mathbf{d}_i$ del simplex será el es $\mathbf{d}_i = \mathbf{Ba}(F_{\sigma_0 \dots \sigma_{\tau_0}} \cap F_{\sigma_0 \dots \sigma_{\tau_1}} \cap \dots \cap F_{\sigma_0 \dots \sigma_{\tau_{i-1}}})$. Si la partición de U correspondiente a la cara $F_{\sigma_0 \dots \sigma_{\tau_0}} \cap F_{\sigma_0 \dots \sigma_{\tau_1}} \cap \dots \cap F_{\sigma_0 \dots \sigma_{\tau_{i-2}}}$ correspondiente al vértice anterior $\mathbf{d}_{i-1}$ es $T = \{B_0, B_1, \dots, B_{i-1}\}$, debido a que

$$\mathbf{d}_{i-1} = \mathbf{Ba}(F(B_0 | \dots | B_i)) = \frac{1}{2} \sum_{l < m}^{i-1} e_{B_l|B_m},$$

entonces

$$\mathbf{d}_i = \frac{1}{2} e_{C_0|C_1} + \mathbf{d}_{i-1}, \quad (3.11)$$

donde $\{C_0, C_1\}$ es una partición de algún elemento de T

Observación 3.8. Esto nos muestra que dado el conjunto ordenado de vértices que determinan los vértices de un simplex $\Delta(\sigma, \tau) = \{\mathbf{d}_0, \dots, \mathbf{d}_n\}$, podemos inferir que, ya que cada uno de esos vértices son baricentros de caras que están en correspondencia con una partición ordenada de U , la diferencia $\mathbf{d}_{i+1} - \mathbf{d}_i$ de dos vértices consecutivos $\mathbf{d}_i$ y $\mathbf{d}_{i+1}$ da como resultado la suma de los vectores principales correspondientes a una partición en dos conjuntos C_0 y C_1 de uno de los elementos B_i de la partición de correspondiente a la cara a la que pertenece $\mathbf{d}_i$.

De esta manera, con las diferencias $\mathbf{d}_{i+1} - \mathbf{d}_i$ tendríamos unos vectores que representan el camino que va desde el origen hasta el vértice.

Ejemplo 3.9. Los vértices del simplex $\Delta(42301, 0321)$ están dados por las sumas de los siguientes vectores:

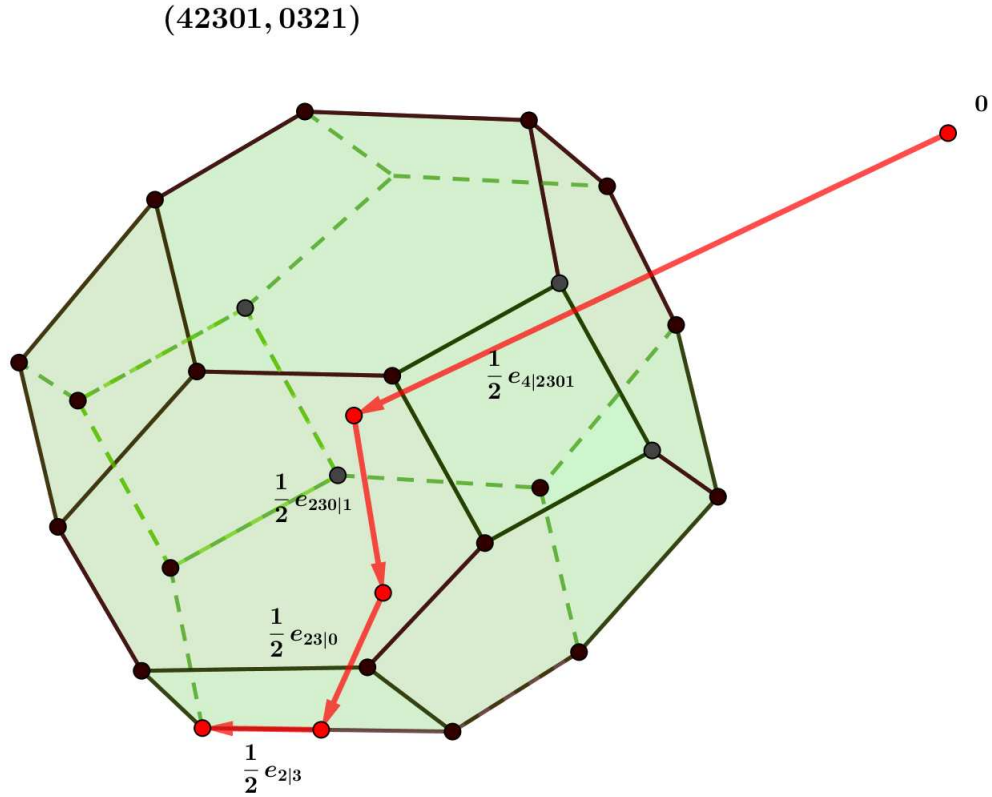


Figura 3.10: Camino desde el centro de la celda de Voronoi hasta el vértice 42301, recorriendo los vértices del simplex $\Delta(42301, 0321)$.

Paso seguido a la obtención de la partición de la celda de Voronoi en simpleses, debemos calcular para cada simplex, el volumen y el momento de inercia, esto haciendo uso del Teorema (1.16).

3.3. Árboles de búsqueda binarios

Para facilitar el entendimiento de los cálculos que vamos a mostrar, es necesario presentar algunos conceptos sobre árboles binarios ya que estos son una gran herramienta de representación de los simplices construidos.

Un árbol binario plano, es un árbol en el que cada nodo puede tener como máximo dos hijos. En ciencias de la computación, un árbol binario es una estructura de datos en la cual cada nodo puede tener un hijo izquierdo y un hijo derecho. No pueden tener más de dos hijos, de ahí su nombre “binario”. Llamaremos raíz del árbol binario al vértice que no tiene padre.

El tamaño de un árbol es el número de sus nodos. El número de árboles binarios planos de tamaño n es el número catalán C_n definido como:

$$C_n = \frac{1}{n+1} \binom{2n}{n} = \frac{2n!}{n!(n+1)!}$$

Un árbol etiquetado es un árbol con una etiqueta adjunta a cada nodo. En nuestro caso, en primera medida vamos a tomar las etiquetas sobre todo el conjunto $\{0, \dots, n-1\}$, que son los elementos con los que vamos a formar τ .

Un subárbol de un árbol binario es una porción del árbol que se forma tomando un nodo específico, junto con todos sus descendientes (nodos que están conectados a él en niveles inferiores), y las aristas que los conectan. En otras palabras, un subárbol se genera al seleccionar un nodo y “recortar” todo el subconjunto de nodos y aristas que cuelgan de él.

Definición 3.10. Un árbol de búsqueda binario es una estructura de datos en forma de árbol en la que cada nodo tiene como máximo dos hijos, denominados hijo izquierdo y derecho. Además, para cada nodo, todos los elementos en el subárbol izquierdo son menores que el nodo, y todos los elementos en el subárbol derecho son mayores que el nodo.

Para construir un árbol de búsqueda binario $T(w)$ con una palabra w , seguimos estos pasos:

1. Leer la palabra w : Recorre la palabra w de izquierda a derecha y toma cada carácter.
2. Inserción en el árbol: Inserta cada carácter en el árbol siguiendo estas reglas:

- Si el árbol está vacío, crea un nodo raíz con el primer carácter de w .
- Si el carácter es menor que el nodo actual, se inserta en el subárbol izquierdo recursivamente.
- Si el carácter es mayor que el nodo actual, se inserta en el subárbol derecho recursivamente.

Ejemplo 3.11. El árbol binario de búsqueda $T(6412530)$ que representa la palabra 6412530 es construido de la siguiente manera:

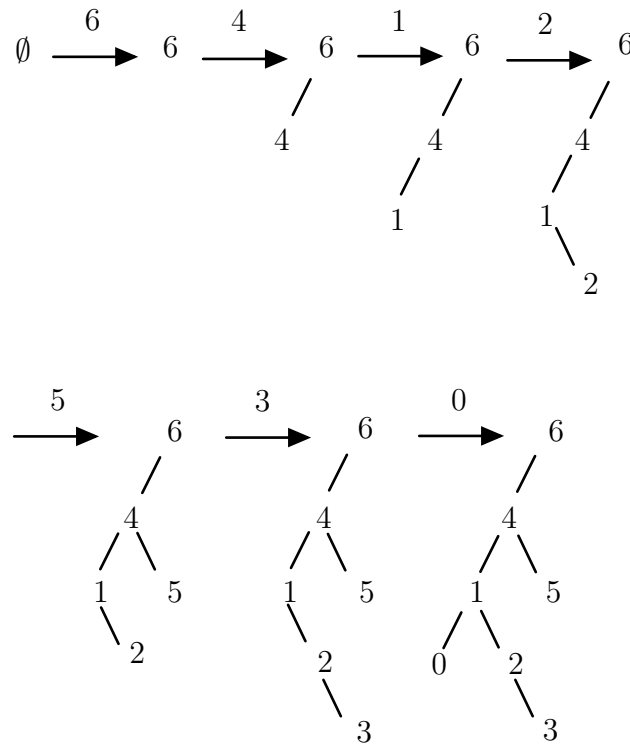


Figura 3.11: Construcción del árbol de búsqueda binario $T(6412530)$, el cual tiene como raíz al 6.

La idea es usar estos árboles de búsqueda binarios tanto para representar los simplices, como para representar el volumen de ellos.

Sean $\sigma = (\sigma_0 \cdots \sigma_n) \in S_{n+1}$ y $\tau = (\tau_0 \cdots \tau_{n-1}) \in S_n$, donde los elementos de τ van a representar permutaciones de los espacios entre los elementos de σ , es decir,

$$\begin{array}{ccccccc} \sigma = (\sigma_0 & \sigma_1 & \cdots & \sigma_i & \sigma_{i+1} & \cdots & \sigma_n) \\ \downarrow & \downarrow & & \downarrow & \downarrow & & \downarrow \\ 0 & 1 & i-1 & i & i+1 & n-1 \end{array}$$

Definición 3.12. Para $(\sigma, \tau) \in S_{n+1} \times S_n$, se construye el árbol de búsqueda binario $T(\sigma, \tau)$ siguiendo estos pasos:

1. Se inicia el proceso de construcción del árbol binario generando un nodo raíz, el cual se obtiene etiquetando los espacios de σ de 0 a $n-1$, tal como se ilustra a continuación.

$$\begin{array}{ccccccc} \sigma = (\sigma_0 & \sigma_1 & \cdots & \sigma_i & \sigma_{i+1} & \cdots & \sigma_n) \\ \downarrow & \downarrow & & \downarrow & \downarrow & & \downarrow \\ 0 & 1 & i-1 & i & i+1 & n-1 \end{array}$$

Y sustituyendo el espacio τ_0 por una subdivisión $|$, creándose así dos palabras, una a la izquierda y otra a la derecha del espacio τ_0 .

2. Para i desde 1 hasta $n-1$ se genera un nuevo nodo subdividiendo la palabra que contiene al espacio τ_i en el nodo N más inferior donde dicho espacio aparece; este nuevo nodo será un hijo a la izquierda o a la derecha de N según la palabra que lo contenga sea la izquierda o la derecha de N .
3. El proceso termina cuando recorremos τ .

Ejemplo 3.13. El árbol de búsqueda $T(03264751, 6412530)$ se construye de la siguiente manera.

Observación 3.15. Para el árbol $T(\sigma, \tau)$, cada nodo N representa una subdivisión en dos palabras de una palabra σ' donde σ' es una sub-palabra de σ . Por lo tanto, podemos concluir que el conjunto de caracteres de cualquier nodo en el subárbol con raíz en N dentro de $T(\sigma, \tau)$ no contiene caracteres que no estén presentes en σ' .

En la siguiente sección, demostraremos el siguiente teorema. Gracias a la representación de los simplices en árboles binarios, podemos enunciar este teorema de una manera más concisa.

Teorema 3.16. Sea $\Delta(\sigma, \tau)$ la representación de un simplex proveniente de la partición (3.2) de una celda de Voronoi para un lattice de primer tipo. Entonces el volumen de este simplex está dado por:

$$\text{vol}(\sigma, \tau) = \frac{1}{2^n n! \Delta^{1/2}} \prod_{v \in V} p_v, \quad (3.12)$$

donde V es el conjunto de nodos del árbol binario de búsqueda $T(\sigma, \tau)$

3.4. Volumen de un simplex

Si $\mathbf{v}_i = (\mathbf{v}_{1i}, \mathbf{v}_{2i}, \dots, \mathbf{v}_{ni})^t$, para $0 \leq i \leq n$, son los vértices de un simplex n -dimensional (σ, τ) en coordenadas euclídeas en $\mathbb{R}^n$, entonces el volumen de $\Delta(\sigma, \tau)$ es:

$$\text{vol}(\sigma, \tau) = \frac{1}{n!} \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \mathbf{v}_{10} & \mathbf{v}_{11} & \cdots & \mathbf{v}_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{v}_{n0} & \mathbf{v}_{n1} & \cdots & \mathbf{v}_{nn} \end{vmatrix}. \quad (3.13)$$

Como podemos ver, si tenemos los vértices en las $\mathbf{y}$ -coordenadas aumentadas, no podremos calcular este determinante de esta manera, debemos encontrar una manera de calcular este volumen cuando las coordenadas sean $\mathbf{y}$ -coordenadas.

Recordemos que las $\mathbf{y}$ -coordenadas de un vértice están dadas por $\mathbf{d} = M^T \mathbf{v}_i$ donde $\mathbf{v}_i$ está en coordenadas euclídeas en $\mathbb{R}^n$ y M es la matriz generadora del lattice, podemos ver que

$$(M^T)^{-1}\mathbf{d} = \mathbf{v}_i.$$

Si añadimos a la matriz $(M^T)^{-1}$ una columna cero y una fila cero las cuales en su primera componente tengan un 1 y el resto sean ceros, de la forma

$$(M^{-1})' = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & (M^T)^{-1} & & \\ 0 & & & \end{pmatrix},$$

podemos decir que $\det(M^{-1})' = \det(M^T)^{-1}$ y que si añadimos a $\mathbf{d}$ una coordenada cero con un 1, de la forma,

$$\mathbf{d}' = \begin{bmatrix} 1 \\ \mathbf{y}_1 \\ \vdots \\ \mathbf{y}_n \end{bmatrix}$$

las columnas de la matriz en la ecuación (3.13) para los vértices de un simplex dado por (σ, τ) en orden, son iguales a $(M^{-1})'\mathbf{d}'_i$ donde $\mathbf{d}'_i$ es el vector en $\mathbf{y}$ -coordenadas correspondiente a $\mathbf{v}_i$ agregándole un uno. De esta manera la ecuación (3.13) se puede ver como

$$\text{vol}(\sigma, \tau) = \frac{1}{n!} \left| (M^{-1})' \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \mathbf{d}_{10} & \mathbf{d}_{11} & \cdots & \mathbf{d}_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{d}_{n0} & \mathbf{d}_{n1} & \cdots & \mathbf{d}_{nn} \end{bmatrix} \right| \quad (3.14)$$

$$= \frac{1}{n! \Delta^{1/2}} \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \mathbf{d}_{10} & \mathbf{d}_{11} & \cdots & \mathbf{d}_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{d}_{n0} & \mathbf{d}_{n1} & \cdots & \mathbf{d}_{nn} \end{vmatrix}. \quad (3.15)$$

Debido a que el primero de los vértices del simplex es $\mathbf{d}_0 = \mathbf{0}$ (3.14) queda de la forma:

$$\frac{1}{n!\Delta^{1/2}} \begin{vmatrix} \mathbf{d}_{11} & \cdots & \mathbf{d}_{1n} \\ \vdots & \ddots & \vdots \\ \mathbf{d}_{n1} & \cdots & \mathbf{d}_{nn} \end{vmatrix}. \quad (3.16)$$

Hemos logrado que las filas de esta matriz estén dadas por las $\mathbf{y}$ -coordenadas **No** aumentadas de los vértices del simplex $\Delta(\sigma, \tau)$, son no aumentadas porque no tienen la componente 0 de las coordenadas aumentadas.

Haciendo la operación $C_i - C_{i-1} \rightarrow C_i$ siguiendo el orden descendente desde $i = n$ hasta $i = 2$ a la matriz en (3.16), por la observación (3.8) tenemos

$$A = \frac{1}{2} \begin{bmatrix} \uparrow & \cdots & \uparrow & \cdots & \uparrow \\ e_{C_0^1|C_1^1} & \cdots & e_{C_0^i|C_1^i} & \cdots & e_{C_0^n|C_1^n} \\ \downarrow & \cdots & \downarrow & \cdots & \downarrow \end{bmatrix}, \quad (3.17)$$

donde $\{C_0^1, C_1^1\}$ es una partición de $U = \{0, \dots, n\}$, y $\{C_0^i, C_1^i\}$ es una partición de C_k^j para algún $j < i$, y $k \in \{0, 1\}$.

Se puede ver que cada columna e_N se corresponde con un nodo N del árbol de búsqueda binario $T(\sigma, \tau)$. Este nodo N representa una subdivisión de una palabra σ' en dos palabras.

Por las Observaciones (2.16) y (3.15), podemos concluir que cualquier columna representada por un nodo en el subárbol con raíz en N dentro del árbol $T(\sigma, \tau)$ tendrá un valor de 0 en las coordenadas que no estén indexadas por elementos presentes en la palabra σ' .

Para calcular el valor absoluto del determinante de la matriz (3.17), realizamos operaciones que nos lleven a una fila específica en la que solo hay un elemento P distinto de cero. Una vez que logramos esto, podemos calcular el determinante de la matriz sobre esa fila particular.

Cuando tenemos una fila en la que solo un elemento, P , es diferente de cero, el valor absoluto del determinante de la matriz se simplifica. Podemos calcularlo tomando $|P|$ y multiplicándolo por el determinante de la matriz que resulta cuando eliminamos la fila y la

columna a la que pertenece P . Después de calcular el determinante de la matriz resultante al seleccionar una fila con un único elemento P , repetiremos este proceso de manera recursiva con cada nueva matriz resultante.

El proceso se hará de la siguiente manera:

Tomamos la primera columna $e_{C_0^1|C_1^1}$, debido a que los vectores dados por cada columna de esta matriz no contienen la coordenada cero de las coordenadas aumentadas, sin pérdida de generalidad, vamos a sumar las filas indexadas por el conjunto C^1 el cual es el conjunto de $\{C_0^1, C_1^1\}$ que no contiene al 0, y esta suma la vamos a ubicar en la fila indexada por el primer elemento de C^1 , $C^1[0]$. Al realizar esta operación, por la Observación (2.16), la fila $C^1[0]$ consiste de ceros en todas las posiciones excepto en la posición uno, la cual va a estar determinada por $\pm p_{C_0^1|C_1^1}$, entonces el valor absoluto del determinante (3.17) el producto de $p_{C_0^1|C_1^1}$ con el determinante de la matriz $A_1 = A[1, C^1[0]]$ resultante de eliminar la columna uno y la fila $C^1[0]$.

Procedemos de manera similar con la matriz A_1 , tomando su primera columna $e_{C_0^2|C_1^2}$, la cual no contiene coordenada 0 ni coordenada $C^1[0]$, y vamos a sumar las filas de la matriz indexadas por el conjunto C^2 el cual es el elemento de $\{C_0^2, C_1^2\}$ que no contiene a 0 ni a $C^1[0]$, y esta suma la vamos a ubicar en la fila indexada por el primer elemento de C^2 , $C^2[0]$. Al realizar esta operación, la fila $C^2[0]$ de A_1 consistirá de ceros en todas las posiciones excepto en la posición uno, la cual va a estar determinada por $\pm p_{C_0^2|C_1^2}$, entonces el valor absoluto del determinante de A_1 es el producto de $p_{C_0^2|C_1^2}$ con el determinante de la matriz $A_2 = A_1[1, C^2[0]]$ resultante de eliminar la columna uno y la fila $C^2[0]$.

Este proceso se hace de manera recursiva, así que en el paso i vamos a tener una matriz A_{i-1} la cual es una matriz que se le han eliminado las primeras $i - 1$ columnas y $i - 1$ filas dadas por los $i - 1$ pasos anteriores. Así que la primera columna de A_{i-1} es $e_{C_0^i|C_1^i}$, vamos a sumar las filas de la matriz indexadas por el conjunto C^i el cual es el elemento de $\{C_0^i, C_1^i\}$ que no contiene a los índices de las filas eliminadas en los $i - 1$ pasos anteriores, y esta suma la vamos a ubicar en la fila indexada por el primer elemento de C^i , esta operación está descrita por

$$\sum_{j \in C^i} F_j \rightarrow F_{C^i[0]},$$

donde $C^i[0]$ es el primer elemento de C^i .

Al realizar esta operación, la fila $C^i[0]$ de $A_{i-1} = [1, C^{i-1}[0]]$ consistirá de ceros en todas las posiciones excepto en la posición uno, la cual va a estar determinada por $\pm p_{C_0^i|C_1^i}$, entonces el valor absoluto del determinante de $A_{i-1}[1, C^i[0]]$ es el producto de $p_{C_0^i|C_1^i}$ con el determinante de la matriz $A[1, C^i[0]]$ resultante de eliminar la columna uno y la fila $C^i[0]$.

En consecuencia el determinante de la matriz A es:

$$\det(A) = \frac{1}{2^n} \prod_i^n P_{C_0^i|C_1^i},$$

y como cada $C_0^i|C_1^i$ está determinado por un nodo del árbol de búsqueda $T(\sigma, \tau)$ tenemos que

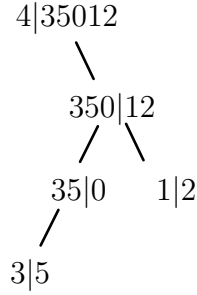
$$\text{vol}(\sigma, \tau) = \frac{1}{2^n n! \Delta^{1/2}} \prod_{v \in V} p_v, \quad (3.18)$$

donde V es el conjunto de nodos del árbol binario de búsqueda $T(\sigma, \tau)$. Lo cual demuestra el Teorema (3.16).

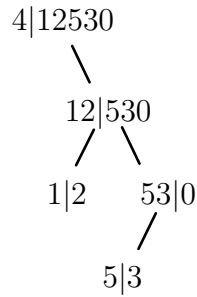
Surge ahora la pregunta, ¿para un simplex dado $\Delta(\sigma, \tau)$ cuántos y cuáles otros simples dados por σ' y τ' tienen volumen igual?

Veamos que $p_{C_1|C_0} = p_{C_0|C_1}$, así que si hacemos a (σ, τ) una operación adecuada para que alguno de sus nodos $N = C_0|C_1$ sea intercambiado por $N' = C_1|C_0$ y a su vez se intercambia el subárbol izquierdo por el subárbol derecho de N tendríamos otro (σ', τ') con igual volumen que (σ, τ) .

Ejemplo 3.17. El simplex $\Delta(435012, 03421)$ representado en el árbol binario $T(435012, 03421)$ está dado por:



Y el simplex $\Delta(412530, 02143)$ representado en el árbol binario $T(412530, 02143)$ está dado por:



Podemos notar que la diferencia entre los dos árboles que se han intercambiado el orden de la división en los nodos 12|350 y 3|5 y por consiguiente sus respectivos subárboles izquierdo por el derecho. Aún así, por el Teorema (3.16) estos simples tienen el mismo volumen.

Definición 3.18. Siendo $(\sigma, \tau) \in S_{n+1} \times S_n$, llamaremos como r_i a la transformación que convierte al simplex $\Delta(\sigma, \tau)$ en el único simplex $\Delta(\sigma', \tau')$ de manera que:

- r_i toma el árbol binario $T(\sigma, \tau)$ y lo transforma en otro árbol binario $T(\sigma', \tau')$ aplicando el intercambio entre palabra derecha e izquierda y a su vez el intercambio entre el subárbol derecho e izquierdo del i -ésimo nodo N^i que aparece en la construcción de $T(\sigma, \tau)$,
- y que no modifica el orden de aparición de los nodos de $T(\sigma, \tau)$, donde el lugar de N^i será tomado por el nodo resultante de la transformación aplicada a el.

Observación 3.19.

- Las transformaciones r_i no modifican ningún otro nodo del árbol original salvo precisamente N^i , de aquí podemos decir que si dos árboles $T(\sigma, \tau)$ y $T(\sigma', \tau')$ cumplen que uno se puede obtener con una transformación r_i aplicada al otro, entonces los simplices $\Delta(\sigma, \tau)$ y $\Delta(\sigma', \tau')$ tienen el mismo volumen.
- Si tomamos el nodo N^i del árbol $T(\sigma, \tau)$ y el nodo $N^{i'}$ del árbol $T(\sigma', \tau')$, podemos darnos cuenta por la Observación (2.16) que los vectores e_{N^i} y $e_{N^{i'}}$ tienen signo opuesto.

3.5. Segundo momento de un simplex

Según el Teorema (1.16) Si $\mathbf{d}_i = (\mathbf{d}_{1i}, \mathbf{d}_{2i}, \dots, \mathbf{d}_{ni})^t$, para $0 \leq i \leq n$, son los vértices de un simplex n -dimensional (σ, τ) en $\mathbf{y}$ -coordenadas no aumentadas, entonces el momento de inercia al rededor del origen es:

$$I(\sigma, \tau) = \frac{1}{(n+1)(n+2)} \left(\left\| \sum_{i=0}^n \mathbf{d}_i \right\|^2 + \sum_{i=0}^n \|\mathbf{d}_i\|^2 \right) \quad (3.19)$$

por la Observación (3.14) y sabiendo que $\mathbf{d}_0 = 0$ tenemos que

$$I(\sigma, \tau) = \frac{1}{(n+1)(n+2)} \left(\left\| \frac{1}{2} \sum_{i=1}^n \sum_{j=1}^i e_{N^j} \right\|^2 + \sum_{i=1}^n \left\| \frac{1}{2} \sum_{j=1}^i e_{N^j} \right\|^2 \right) \quad (3.20)$$

Notemos que se cumple que

$$\left\| \sum_{i=1}^n \sum_{j=1}^i e_{N^j} \right\|^2 = \left\| \sum_{i=1}^n (n+1-i) e_{N^i} \right\|^2,$$

de esta manera

$$I(\sigma, \tau) = \frac{1}{4(n+1)(n+2)} \left(\underbrace{\left(\sum_{i=1}^n (n+1-i) e_{N^i} \right)^2}_{S_1} + \underbrace{\sum_{i=1}^n \left(\sum_{j=1}^i e_{N^j} \right)^2}_{S_2} \right) \quad (3.21)$$

Por lo tanto, expandiendo cada S_1 y S_2 de (3.21) y luego sumando dentro de los paréntesis, vamos a tener sumandos de la forma $\alpha_{kl} e_{N^k} \cdot e_{N^l}$ con $l, k \in \{1, \dots, n\}$ obtenidos de la siguiente manera:

Si $k = l$, de S_1 obtenemos $(n+1-k)^2 e_{N^k}^2$, por otro lado de S_2 obtenemos $(n+1-k) e_{N^k}^2$ por lo tanto en este caso el coeficiente α_{kl} de $e_{N^k}^2$ es

$$\alpha_{kl} = (n+1-k)(n+2-k) \quad (3.22)$$

Sin perdida de generalidad si $k < l$, de S_1 obtenemos $2(n+1-k)(n+1-l) e_{N^k} \cdot e_{N^l}$. Por otro lado de S_2 , obtenemos $2(n+1-l) e_{N^k} \cdot e_{N^l}$ por lo tanto en este caso el coeficiente α_{kl} de $e_{N^k} \cdot e_{N^l}$ es

$$\alpha_{kl} = 2(n+2-k)(n+1-l). \quad (3.23)$$

Por lo tanto (3.21) queda de la forma

$$I(\sigma, \tau) = \frac{1}{4(n+1)(n+2)} \left(\sum_{k=1}^n (n+1-k)(n+2-k) e_{N^k}^2 \right) \quad (3.24)$$

$$+ \sum_{k < l}^n 2(n+2-k)(n+1-l) e_{N^k} \cdot e_{N^l} \quad (3.25)$$

Sabemos que existen n transformaciones r_i , una por cada nodo, que le podemos aplicar a $\Delta(\sigma, \tau)$. Para cada nodo N^i tenemos dos opciones aplicar o no aplicar la transformación r_i (debe ser claro que aplicar dos veces la transformación deja todo igual que antes), por

ende, de $\Delta(\sigma, \tau)$ obtenemos 2^n simplices dados por la elección en cada nodo si aplicar o no la transformación.

Veamos ahora que sucede si aplicamos a $\Delta(\sigma, \tau)$ una transformación r_i , de manera que $r_i(\Delta(\sigma, \tau)) = \Delta(\sigma', \tau')$. Por la Observación (3.19), la expresión $I(\sigma, \tau)$ solo se va a diferenciar de $I(\Delta(\sigma', \tau'))$ en el signo de los términos $\alpha_{kl}e_{N^k} \cdot e_{N^l}$, cuando $k = i \vee l = i$.

De esta manera si sumamos todas las inercias de todos los 2^n simplices obtenidos de $\Delta(\sigma, \tau)$ al decidir si aplicar o no r_i a cada nodo N^i del árbol $T(\sigma, \tau)$, sobreviven solamente los términos $\alpha_{kl}e_{N^k} \cdot e_{N^l}$, con $k = l$. Por lo tanto, si tomamos el conjunto de simplices

$$R = \{r_i(\Delta(\sigma, \tau)) : i \in \{1, \dots, n\}\}$$

tenemos que:

$$\sum_{\delta \in R} (I(\delta)) = \frac{2^n}{4(n+1)(n+2)} \left(\sum_{k=1}^n (n+1-k)(n+2-k)e_{N^k}^2 \right) \quad (3.26)$$

Es de gran relevancia que todos los simplices de R tengan el mismo volumen, debido a que nuestro objetivo era calcular el segundo momento no normalizado

$$U(\Delta(\sigma, \tau)) = I(\sigma, \tau) \cdot \text{vol}(\Delta(\sigma, \tau))$$

para cada simplex. Con lo hecho anteriormente no solo podemos calcular U para cada simplex si no que también podemos calcular la suma de los U para todos los simplices en el conjunto R de la siguiente manera.

Teorema 3.20. Sea $\Delta(\sigma, \tau)$ la representación de un simplex proveniente de la partición (3.2) de una celda de Voronoi para un lattice de primer tipo y sea $R = \{r_i(\Delta(\sigma, \tau)) : i \in \{1, \dots, n\}\}$ el conjunto de simplices obtenidos al aplicar las transformaciones r_i dadas por la Definición (3.18) a $\Delta(\sigma, \tau)$. Entonces la suma de los segundos momentos no normalizados

de los simplices en R está dada por:

$$\sum_{\delta \in R} U(\delta) = \frac{1}{4(n+2)!\Delta^{1/2}} \left(\sum_{k=1}^n (n+1-k)(n+2-k)e_{N^k}^2 \right) \prod_{k=1}^n p_{N^k}, \quad (3.27)$$

donde N^k es el k -ésimo nodo insertado en árbol binario de búsqueda $T(\sigma, \tau)$

Por (3.26) y el Teorema (3.16) el resultado es inmediato.

El Teorema que hemos desarrollado en este trabajo ha demostrado ser fundamental para reducir drásticamente el número de cálculos necesarios para validar nuestra conjetura en dimensiones más altas. Sin este teorema, el número de cálculos requeridos sería muy grande, creciendo de manera exponencial con cada dimensión adicional como $(n+1)!$. Por ejemplo, en el caso de una dimensión 5, el número de cálculos necesarios ascendería a 86400, sin tener en cuenta que cada uno de estos cálculos implica la evaluación de al menos 4 normas y el almacenamiento de estos resultados para su posterior comparación. Esto no solo sería computacionalmente prohibitivo, sino que también consumiría una cantidad significativa de memoria.

Sin embargo, gracias a nuestro teorema, hemos logrado reducir significativamente la carga computacional. Al dividir el trabajo por 2^5 , pudimos reducir el número total de cálculos a 2700. Esta optimización nos permitió verificar la conjetura en dimensión 5 con los recursos computacionales disponibles. En resumen, el teorema ha sido crucial para hacer factible la validación de nuestra conjetura en dimensiones más altas, proporcionando un enfoque más eficiente y manejable para abordar el problema.

Teorema 3.21. Sea Λ un lattice de Tipo I en $\mathbb{R}^5$ con superbase obtusa $B = \{\mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4, \mathbf{v}_5\}$, con parámetros de Selling reducidos p_{ij} con i, j en $\{0, 1, 2, 3, 4, 5\}$ y determinante Δ , entonces la constante de cuantización de Λ viene dada por:

$$G_5(\Lambda) = \frac{C_2 + 2 \sum_{k=2}^5 k C_{k+1}}{60 \Delta^{6/5}},$$

donde C_i representa la suma de todos los términos obtenidos al multiplicar las etiquetas de los grafos que son árboles generadores del grafo completo a los cuales se les ha añadido una

arista para formar un ciclo de longitud i .

Los algoritmos utilizados para la verificación de este teorema serán puestos en el apéndice del trabajo.

Capítulo 4

Conclusiones y propuestas futuras

En este capítulo final del trabajo, presentaremos una serie de conclusiones y exploraremos posibles nuevos caminos que podrían continuar después de este proyecto.

En primer lugar, es importante destacar los numerosos puentes que se han tendido entre diferentes áreas de las matemáticas, así como entre las matemáticas y la computación. Por ejemplo, hemos logrado proporcionar una descripción combinatoria sintética (3.21) para una expresión totalmente analítica (1.12) de la constante de cuantización en lattices de primer tipo en dimensión 5. Al hacerlo, hemos establecido conexiones entre elementos combinatorios, como las caras de la celda de Voronoi, y conceptos más abstractos como los grafos y árboles binarios. Estas conexiones nos han permitido formular ecuaciones analíticas de manera combinatoria (3.27), (3.26), (3.12) y (3.24), lo que a su vez ha enriquecido nuestra comprensión de la estructura subyacente de los lattices y sus propiedades.

Además, al explorar estas interrelaciones, hemos abierto la puerta a nuevas líneas de investigación que podrían profundizar aún más en estos temas. Por ejemplo, podríamos investigar cómo las técnicas combinatorias utilizadas en este trabajo podrían aplicarse a otros problemas en teoría de lattices o en áreas relacionadas de la matemática discreta. También podríamos explorar cómo estas conexiones entre combinatoria y análisis podrían generalizarse a dimensiones superiores o a diferentes tipos de lattices.

El siguiente paso natural en la continuación de este trabajo de investigación es validar la conjetura planteada (3.5) en dimensiones superiores a 5, y, si somos más ambiciosos, buscar demostrarla.

Por otro lado, enfocándonos en el caso de lattices en dimensión 5, se puede continuar tratando el problema de encontrar el lattice óptimo que minimice la constante de cuantización para lattices de primer tipo en dimensión 5. Como primer paso, podríamos utilizar la fórmula proporcionada por (3.21), realizando evaluaciones sobre diferentes familias de lattices en esta dimensión. De esta manera, con las ideas que resulten de estas evaluaciones, se podrían aplicar métodos de optimización para determinar la constante de cuantización de manera precisa, tomando los parámetros de Selling como variables de la ecuación, sabiendo la dificultad de esta tarea, porque tendríamos 15 variables diferentes. Además, vale la pena recalcar que este trabajo ha representado un avance significativo en esta dirección, ya que hemos desarrollado la capacidad de calcular la constante de cuantización para cualquier lattice de primer tipo.

El aporte realizado en este trabajo de investigación es predominantemente teórico, siendo el resultado más importante el Teorema (3.21) reforzando la posible veracidad de la Conjetura (3.5). Por otro lado, aunque se pudiera demostrar la conjetura planteada, lo cual podría significar un gran impulso en la cuantización vectorial, su aplicación sigue teniendo dificultad, una de las razones detrás de esta condición es la relación directa entre el problema del lattice cuantizador y la dificultad de resolver problemas fundamentales en teoría de lattices.

4.1. Problemas asociados a lattices y una posible aplicación en Criptografía

El proceso de cuantización vectorial utilizando un lattice está intrínsecamente vinculado al desafío de encontrar el vector más cercano en dicho lattice, el cual es uno de los problemas fundamentales en la teoría de lattices. A su vez este problema está relacionado con otros problemas de lattices tales como el Problema del vector más corto, Problema de la base de vectores cortos, Problema del gap o distancia más corta entre vectores, entre otros [3].

La resolución de estos problemas no solo es fundamental para comprender en profundidad el

proceso de cuantización vectorial con lattices, sino que también tiene aplicaciones prácticas significativas en campos como la comunicación digital [1, 2, 9] y la criptografía ([5] capítulo 3).

Definición 4.1. (Problema del Vector Más Corto (SVP)). Dado como entrada una base B de un lattice Λ , calcular un vector no nulo $\mathbf{v} \in \Lambda$ de norma $|\mathbf{v}|$ mínima sobre Λ .

El Problema del Vector Más Cercano podría interpretarse como una versión de SVP.

Definición 4.2. (Problema del Vector Más Cercano (CVP)). Dado como entrada una base B de un lattice Λ en $\mathbb{R}^n$, y un vector objetivo $\mathbf{t} \in \text{span}(\Lambda)$, calcular un vector del retículo $\mathbf{c} \in \Lambda$ más cercano a $\mathbf{t}$, es decir, $|\mathbf{t} - \mathbf{c}| = \text{dist}(\Lambda, \mathbf{t})$.

El problema del punto del lattice más cercano y la celda de Voronoi están relacionados en el sentido de que $\mathbf{x} \in \Lambda$ es un punto de retícula más cercano a $\mathbf{y}$ si y solo si $\mathbf{y} - \mathbf{x} \in \text{Vor}(\Lambda)$.

El Problema del Vector Más Cercano (CVP) y el Problema del Vector Más Corto (SVP) son conocidos por ser difíciles de resolver en general, y su dificultad está estrechamente relacionada con la complejidad computacional asociada a su resolución. La determinación del vector del lattice más cercano a un vector objetivo puede ser computacionalmente intensiva, especialmente en dimensiones altas.

Aunque no somos expertos en teoría de la complejidad computacional, entendemos que tanto el CVP como el SVP son problemas NP-difíciles [19], lo que sugiere que es improbable que exista un algoritmo polinomial capaz de encontrar la solución exacta en un tiempo razonable, a menos que P sea igual a NP. Por lo tanto, la búsqueda de soluciones eficientes para estos problemas sigue siendo un desafío importante en la investigación en teoría de lattices y áreas relacionadas [21].

Dejamos referencias sobre el tratamiento de estos problemas y su complejidad debido a nuestras limitaciones en este campo [19]. Sin embargo, reconocemos la importancia de comprender la complejidad computacional asociada con el CVP y el SVP para abordar eficazmente estos problemas en la práctica y en futuras investigaciones.

Es interesante destacar que las referencias propuestas se encuentran en publicaciones relacionadas con la criptografía. Esto se debe a que la dificultad de resolver problemas como el

CVP y el SVP brinda una oportunidad significativa en el campo de la criptografía.

Un criptosistema de clave pública implica la generación de un par de claves, una pública y una privada, relacionadas matemáticamente. La clave pública se comparte abiertamente para cifrar mensajes, mientras que la clave privada se mantiene en secreto y se utiliza para descifrar los mensajes cifrados. La seguridad de un criptosistema de clave pública depende de la dificultad computacional de resolver ciertos problemas matemáticos asociados con la generación de claves y el proceso de cifrado-descifrado. En general, estos problemas deben ser lo suficientemente difíciles de resolver como para que un atacante no pueda deducir la clave privada a partir de la clave pública o descifrar mensajes cifrados sin conocer la clave privada. Esto se aplica en seguridad en línea, autenticación de usuarios y firma digital.

Las construcciones criptográficas basadas en retículos emergen como candidatos prometedores en el contexto de la criptografía post-cuántica. A diferencia de los esquemas de clave pública convencionales, como RSA o la criptografía de curva elíptica, que pueden ser vulnerables a ataques cuánticos ([5] capítulo 4), los sistemas de lattices ofrecen una alternativa más resistente.

El CVP y SVP son fundamentales en la construcción de sistemas de seguridad criptográfica debido a las siguientes razones:

Seguridad criptográfica basada en lattices: La dificultad en la resolución del CVP y el SVP proporciona una base sólida para el diseño de esquemas criptográficos basados en lattices. Estos problemas se utilizan en la construcción de protocolos de seguridad que posiblemente puedan garantizar la confidencialidad y la integridad de la información, así como en el diseño de sistemas de autenticación y firma digital.

Resistencia contra ataques criptográficos: Los problemas de lattices como el CVP y el SVP se utilizan en la construcción de criptosistemas resistentes a diversos ataques, incluidos los ataques de búsqueda exhaustiva y los ataques basados en técnicas de reducción de problemas difíciles a problemas más simples. La dificultad de resolver estos problemas puede garantizar la seguridad y la robustez de los sistemas criptográficos basados en lattices.

En un criptosistema basado en lattices, la generación de claves implica la selección de bases del lattice. Una buena clave privada se basa en una base que contiene vectores cortos,

como una superbase obtusa para lattices de primer tipo. Estos vectores cortos hacen que la resolución de problemas como CVP y SVP sea más factible ([5] sección 11, [22,24]). Por otro lado, una buena clave pública se basa en una base que contiene vectores largos con ángulos agudos entre ellos, lo que dificulta la resolución de los problemas antes mencionados.

De nuevo como no somos expertos en el campo de la criptografía, dejamos referencias sobre esta interesante aplicación [5,18].

En resumen, es posible que el impacto práctico del trabajo de investigación tardará en materializarse debido a la dificultad del Problema del Vector Más Cercano (CVP), el cual está estrechamente relacionado con el proceso de cuantización vectorial con lattices. Sin embargo, como hemos observado, la dificultad puede ser una oportunidad. El aporte de este trabajo proporciona una idea del comportamiento de una familia de lattices, específicamente los del primer tipo.

4.2. Lattices de primer tipo como cuantizadores

En el contexto de esta investigación, hay dos artículos fundamentales que merecen ser destacados [22] y [24], donde se logra resolver el Problema del Vector Más Cercano (CVP) en tiempo polinomial para lattices de primer tipo y una generalización de este algoritmo para lattices zonotopales, respectivamente. Estos avances evidencian un progreso significativo en la resolución de problemas relacionados con lattices, lo que potencialmente abre nuevas posibilidades para la aplicación práctica de la cuantización vectorial en áreas como la criptografía post-cuántica.

Una pregunta que surge en la discusión del artículo en mención es: ¿existen lattices del primer tipo que sean eficaces como cuantizadores? Este interrogante abre la puerta a explorar la manipulación y optimización de la fórmula en la conjetura (3.5), utilizándola con el fin de responder esta cuestión.

Como se menciona en [22], existe un método relativamente sencillo para construir una retícula del primer tipo de manera “arbitraria”. Este enfoque implica la construcción de una matriz simétrica A de tamaño $(n + 1) \times (n + 1)$, conocida como la matriz de Gram aumentada (1.3). En esta matriz, las entradas son los parámetros de Selling, los cuales son

números positivos. Una vez obtenida la matriz A , se puede aplicar un método de Cholesky para recuperar una matriz B tal que $BB' = A$. Las filas de esta matriz B representan los vectores de la superbase obtusa del lattice del primer tipo. Este procedimiento sugiere que la construcción de lattices de primer tipo es factible utilizando únicamente una serie de números positivos que servirán como parámetros de Selling.

Los autores de [22] concluyen su artículo destacando que su algoritmo tiene potencial aplicación en problemas de ingeniería de comunicaciones, como la codificación y la cuantización. Un área de investigación interesante para el futuro sería encontrar lattices del primer tipo que sean efectivas en la generación de buenos códigos, cuantizadores eficientes o criptosistemas robustos. Además, la manipulación y optimización de la fórmula en la conjetura (3.5) podría ser un indicador de la eficiencia de los lattices de primer tipo en dichas aplicaciones.

Apéndice

En esta sección vamos a adjuntar todos los programas que se utilizaron para realizar el cálculo de G_5 . Los paquetes utilizados fueron:

```
from itertools import product
import numpy as np
import itertools
from itertools import combinations
from copy import deepcopy
from operator import add,mul
from collections import defaultdict
from collections import Counter
from sage.combinat.cartesian_product import CartesianProduct_iters
import time
```

La siguiente función toma como entrada una lista y un elemento de esa lista. Devuelve los índices, de izquierda a derecha, de los elementos anteriores más cercanos en la lista, uno mayor y otro menor que el elemento dado. En caso de que no exista un elemento menor, se considera el índice 0. Si no hay un elemento mayor, se considera el índice como el tamaño de la lista.

Este programa es útil para obtener la subcadena de una cadena (denotada como sigma) donde se necesita realizar una división. Esta subcadena es crucial para construir los nodos de los árboles binarios, proporcionando los índices del primer y último elemento de esta subcadena.

```

def intervalo(numbers, target):
    smaller = None
    larger = None

    for num in numbers:

        if num == target:
            break
        if num < target:
            if smaller is None or num >= smaller:
                smaller = num+1
        elif num > target:
            if larger is None or num < larger:
                larger = num+1

    if smaller==None:
        smaller=0
    if larger ==None:
        larger=len(numbers)+1
    return [smaller, larger]

```

Una vez obtenida la subcadena utilizando los índices proporcionados por el programa anterior, procedemos a realizar de manera recursiva las divisiones necesarias.

```

def conjuntos(sigma,tau):
    particiones_recursivas=[]
    for t in tau:
        I=intervalo(tau,t)

        #con intervalo se obtiene la subpalabra de sigma que
        #se va a dividir, se procede a ello en el espacio t

        particion_t=[sigma[I[0]:t+1],sigma[t+1:I[1]]]

```

```

    particiones_recurativas.append(particion_t)
return particiones_recurativas

```

Este programa toma como entrada una lista grande y dos sublistas conexas de ella. El objetivo es dividir una de estas sublistas en dos sublistas contiguas. Utilizando este programa, determinaremos los índices en la lista grande donde ocurren estas subdivisiones.

Este enfoque nos permite identificar los puntos de partición en la lista grande, lo que es esencial para realizar operaciones más complejas o análisis detallados de sus elementos. Este programa nos ayudará a determinar qué sucede con los índices de los espacios en una cadena, denotada como σ , cuando obtenemos otra cadena, σ_{prima} , a partir de σ y una aplicación r_i 3.18. Este proceso implica una transformación en la cadena original, lo que puede afectar la ubicación de los espacios dentro de ella.

```

def ind_espacio(sigma_prima,nodo):
    #ordena los elementos a cada lado de la división del nodo.
    A=sorted(nodo[0])
    B=sorted(nodo[1])

    lista1=sigma_prima.copy()

    #crea una lista de indices de los elementos a la izquierda
     #(resp der) de la division del nodo
    C=[lista1.index(izq) for izq in nodo[0]]
    D=[lista1.index(der) for der in nodo[1]]
    #ordena los elementos de la palabra sigma_prima
    #preparandolas para compararse con A y B.

    lista1[min(C):max(C)+1]=sorted(lista1[min(C):max(C)+1])
    lista1[min(D):max(D)+1]=sorted(lista1[min(D):max(D)+1])

    #finalmente se compara para averiguar en que indice está
    #el espacio de la division del nodo.

```

```

division=0
if A+B ==lista1[min(C):max(D)+1] or A+B ==lista1[min(D):max(C)+1]:
    division=lista1.index(A[-1])
elif B+A ==lista1[min(C):max(D)+1] or B+A ==lista1[min(D):max(C)+1]:
    division=lista1.index(B[-1])

return division

```

Este programa crea todos los elementos de la clase (sigma,tau) dadas por las aplicaciones r_i , 3.18.

```

def r_(sigma , tau,i):
    sigma_prima=sigma.copy()

    #toma el i-esimo nodo de T(sigma,tau).
    N=conjuntos(sigma,tau)[i]

    #hace el respectivo intercambio de la palabra izquierda
#del nodo por la de la derecha
    sigma_prima[sigma_prima.index(N[0][0]):sigma_prima.index(N[0][0])+
        len(N[0]+N[1])]=N[1]+N[0]

    #va llenando tau_prima a medida que va encontrando donde
#quedaron los índices de los espacios en sigma_prima,
#esto con la función ind_espacio para cada nodo.
    tau_prima =[]
    for nodo in conjuntos(sigma, tau):
        tau_prima.append(ind_espacio(sigma_prima,nodo))

    return [sigma_prima,tau_prima]

```

```

def clase(sigma,tau):

    n=len(tau)
    opciones=[0,1]

    #crea todas las listas de n elementos solamente con
#entradas ceros y unos, es claro que son 2^n.
    combinaciones=list(itertools.product(opciones,repeat=n))

    #con cada lista de ceros y unos se aplica r_i cuando i sea el indice con un 1
    clase_s_t=[]
    for list_0_1 in combinaciones:
        L=np.array(list_0_1)
        representante=[sigma, tau]

        # toma los indices de Lis_0_1 de los elementos que
#son 1
        for k in list(np.nonzero(L)[0]):
            representante=r_(representante[0],representante[1],k)
        clase_s_t.append(representante)
    return clase_s_t

```

Este programa crea la lista de todas las clases dadas por los r_i que particionan $S_{n+1} \times S_n$.

```

def clases(n):
    permutaciones_n = list(itertools.permutations(range(n + 1)))
    # Permutaciones de 0 a n
    listas_n_1 = list(itertools.permutations(range(n)))
    # Permutaciones de 0 a n-1

    pares_de_listas = [[list(perm_n), list(perm_n_1)] for
        perm_n in permutaciones_n for perm_n_1 in listas_n_1]

```

```

clases=[]
suma_clases=[]
for i in pares_de_listas:
    if i not in suma_clases :
        clasei=clase(i[0],i[1])
        clases.append(clasei)
        suma_clases=suma_clases+clasei

return clases

```

Vamos a mostrar como se calculan, la matriz de Gram `gram(n)`, los vectores principales `vector_principal(i,j,n)`, sumas de vectores principales `e_conjuntos(sigma,tau)`, volumen de un simplex `volumen(sigma,tau)`, norma de vectores en y -coordenadas `norma1(n,vector1)`, suma de inercia de simplex en la misma clase `suma_inercias(sigma,tau)`.

```

def vector_principal(i,j,n):
    w = zero_vector(SR, n+1)
    w[min(i,j)]=var('p{}{}'.format(min(i,j),max(i,j)))
    w[max(i,j)]=-var('p{}{}'.format(min(i,j),max(i,j)))

    return w

```

```

def gram(n):
    P=matrix(SR,n)
    for i in range(1,n+1):
        for j in range(1,n+1):
            if i==j:
                s=0
                for l in range(n+1):
                    if l!=i:

```

```

        s=s+var('p{}'.format(min(i,l),max(i,l)))
    P[i-1,j-1]=s
    else:
        P[i-1,j-1]=-var('p{}'.format(min(i,j),max(i,j)))
        P[j-1,i-1]=P[i-1,j-1]
return P

def volumen(sigma,tau):
    volum=1
    for i in conjuntos(sigma,tau):
        C = [[x, y] for x in i[0] for y in i[1]]
        factor_volumen = sum([var('p{}'.format(min(c[0],c[1]),max(c[0],c[1]))) for c
        C])
        volum *= factor_volumen
    return volum.expand()

def DERIVADAS1(dimension,D):
    Derivadas=matrix(SR,dimension+1)

    for i in range(dimension+1):
        for j in range(dimension+1):
            if i==j:
                Derivadas[i,j]=0
            else:
                Derivadas[i,j]=D.diff(var('p{}'.format(min(i,j),max(i,j))))
    return(Derivadas)

def DERIVADAS2(dimension,D):
    Derivadas=matrix(SR,dimension+1)

```

```

for i in range(dimension+1):
    for j in range(dimension+1):
        if i==j:
            Derivadas[i,j]=0
        else:
            Derivadas[i,j]=D.diff(var('D{}{}'.format(min(i,j),max(i,j)))) )
return(Derivadas)

def DERIVADAS(dimension):
    Derivadas=matrix(SR,dimension+1)

    for i in range(dimension+1):
        for j in range(dimension+1):
            if i==j:
                Derivadas[i,j]=0
            else:
                Derivadas[i,j]=var('D{}{}'.format(min(i,j),max(i,j)))
    return(Derivadas)

#La norma de un vector en y-coordenadas

def norma1(n,vector1):
    N1=0
    dif=DERIVADAS(n)
    for i in range(1,n+1):
        N1=N1+(dif[0][i])*(vector1[i]*vector1[i]).expand()
    N2=0
    for i in range(1,n+1):
        for j in range(1,n+1):
            if i<j:

```

```

N2=N2+((dif[0][i])+(dif[0][j])
        -(dif[i][j]))*(vector1[i]*vector1[j]).expand()

norma=(N1+N2)
return norma

def e_conjuntos(sigma,tau):

    n=len(tau)

    suma_sobre_clase=[]
    A=conjuntos(sigma,tau)
    for i in range(n):
        C = [[x, y] for x in A[i][0] for y in A[i][1]]
        sumanorma= sum([sgn(c[1]-c[0])*vector_principal(c[0],c[1],len(tau)) for c in
            C])
        suma_sobre_clase.append(sumanorma)
    return suma_sobre_clase

def suma_inercias(sigma,tau):

    n=len(tau)

    suma_sobre_clase=0
    A=e_conjuntos(sigma,tau)
    for i in range(n):
        suma_sobre_clase+=(n-i)*(n+1-i)*norma1(n,A[i])

    return suma_sobre_clase.expand()

```

Este siguiente programa calcula $G_conj(n)$, que es el calculo de la conjetura 3.5 en dimensión n .

```
def M(n):

    M = [[0]*(n)]*(n)
    for i in range(n):
        M[i] = [-var('p%d%d' % tuple(sorted((i+1,j+1)))) for j in range(n)]
        M[i][i] = sum([var('p%d%d' % tuple(sorted((i+1,k))))
                        for k in range(0,n+1)]) - var('p%d%d' % (i+1,i+1))

    return(Matrix(M))

def d(n):

    lis=list(combinations(list(range(n+1)), 2))
    c=0
    for j in lis:
        i=list(j)
        c+=var('D%d%d' % tuple(sorted((i[0],i[1]))))*var('p%d%d' %
            tuple(sorted((i[0],i[1]))))
    return c/n

def G_conj(n):
    G = 0
    Ck = C_k(n+1)

    for g in Ck:
        k = Graph(g,multiedges=True).girth()
        if k == 2:
            G += mono(g)
        if k > 2:
            G += 2*(k-1)*mono(g)
```

```

return(expand(G))

def mono(g):
    mono = 1
    for e in g:
        mono = mono*var('p%d%d' % (sorted(e)[0],sorted(e)[1]))
    return(mono)

def C_k(n):
    P = prufer(n)
    C = []
    for ps in P:
        for i in range(n):
            for j in range(i+1,n):
                c = prufer_to_tree(ps)
                c.append([i,j])
                if sorted(c) not in C:
                    C.append(sorted(c))

    return(C)

def prufer_to_tree(ps):

    n = len(ps)+2
    ps = list(ps)
    N = list(range(n))
    T = []
    while len(N) > 2:
        j = min(set(N)-set(ps))
        T.append(sorted([j,ps[0]]))
        N.remove(j)

```

```

        ps.remove(ps[0])
    T.append([N[0],N[1]])
    return(T)

```

```
def pruver(n):
```

```

    return(itertools.product(range(n), repeat=n-2))

```

Estos últimos programas hacen uso del paquete multiprocessing debido a la gran cantidad de cálculos que se debe realizar (2700 en dimensión 5), tomando en cuenta que cada calculo es muy grande. El proceso que realizan es calcular la conjetura y U por separado, para después, hacer la resta de las dos cosas. En el proceso se sacan como factor común las derivadas provenientes de la matriz adjunta y finalmente se expande todo. De esta manera como el resultado fue cero, podemos concluir que G_n y G_{conj} son lo mismo, como se muestra en la imagen para dimensión 5 queda demostrada la conjetura.

```

    from concurrent.futures import ProcessPoolExecutor
    import multiprocessing

```

```
def calcular_contribucion(i):
```

```

    return (suma_inercias(i[0], i[1]) * volumen(i[0], i[1])).expand()

```

```
def U_paralelo(n):
```

```

    start_time = time.time()
    A = representantes_de_clase(n)
    print("--- %s seconds U1 ---" % (time.time() - start_time))
    with ProcessPoolExecutor(max_workers=multiprocessing.cpu_count()) as executor:
        contribuciones = list(executor.map(calcular_contribucion, A))
    print("--- %s seconds U2 ---" % (time.time() - start_time))
    suma_total = sum(contribuciones)
    print("--- %s seconds U3 ---" % (time.time() - start_time))

```

```

return (suma_total / (factorial(n + 2)) * 3)

def calcular_contribucion2(i,dif,gif):
    start_tim = time.time()
    F=(dif[i[0]][i[1]] * gif[i[0]][i[1]]).expand()
    print("--- %s seconds un cálculo ---" % (time.time() - start_tim))
    return F

def final(n):
    start_time = time.time()
    a=U_paralelo(n)

    print("--- %s seconds para U ---" % (time.time() - start_time))

    G=((G_conj(n)*d(n)).expand()-a)

    print("--- %s seconds para Gconj-U ---" % (time.time() - start_time))

    deter=det(gram(n)).expand()

    dif=DERIVADAS1(n,deter)
    gif=DERIVADAS2(n,G)
    print("--- %s seconds U1 ---" % (time.time() - start_time))

    lis=list(combinations(list(range(n+1)), 2))
    suma=0
    for j in lis:
        i=list(j)
        suma+=(dif[i[0]][i[1]]*gif[i[0]][i[1]]).expand()
        print("--- %s seconds para un cálculo ---" % (time.time() - start_time))

```

```
return suma
```

Finalmente mostramos los resultados en cada dimensión hasta 5, donde podemos evidenciar que cada resultado da cero, lo que verifica la conjetura en todas estas dimensiones:

```
In [8]: final(2)
```

```
--- 0.009526968002319336 seconds U1 ---  
--- 3.046579360961914 seconds U2 ---  
--- 3.0468263626098633 seconds U3 ---  
--- 3.047044038772583 seconds para U ---  
--- 3.0491206645965576 seconds para Gconj-U ---  
--- 3.052523374557495 seconds U1 ---  
--- 3.0534517765045166 seconds para un cálculo ---  
--- 3.053845167160034 seconds para un cálculo ---  
--- 3.055269956588745 seconds para un cálculo ---
```

```
Out[8]: 0
```

```
In [7]: final(3)
```

```
--- 0.023230791091918945 seconds U1 ---  
--- 3.202615976333618 seconds U2 ---  
--- 3.204921007156372 seconds U3 ---  
--- 3.206153631210327 seconds para U ---  
--- 3.2296347618103027 seconds para Gconj-U ---  
--- 3.2794253826141357 seconds U1 ---  
--- 3.283360004425049 seconds para un cálculo ---  
--- 3.2868282794952393 seconds para un cálculo ---  
--- 3.290329694747925 seconds para un cálculo ---  
--- 3.2939274311065674 seconds para un cálculo ---  
--- 3.2970869541168213 seconds para un cálculo ---  
--- 3.300110101699829 seconds para un cálculo ---
```

```
Out[7]: 0
```

In [9]: `final(4)`

```
--- 0.03208422660827637 seconds U1 ---  
--- 5.500671625137329 seconds U2 ---  
--- 5.624651908874512 seconds U3 ---  
--- 5.634766101837158 seconds para U ---  
--- 5.920592546463013 seconds para Gconj-U ---  
--- 15.39533281326294 seconds U1 ---  
--- 15.857349634170532 seconds para un cálculo ---  
--- 16.36398720741272 seconds para un cálculo ---  
--- 16.8989520072937 seconds para un cálculo ---  
--- 17.45855951309204 seconds para un cálculo ---  
--- 18.09280776977539 seconds para un cálculo ---  
--- 18.663387298583984 seconds para un cálculo ---  
--- 19.24356722831726 seconds para un cálculo ---  
--- 19.81760048866272 seconds para un cálculo ---  
--- 20.405921936035156 seconds para un cálculo ---  
--- 20.98069739341736 seconds para un cálculo ---
```

Out[9]: 0

```
In [2]: final(5)
```

```
--- 0.18421602249145508 seconds U1 ---  
--- 40.7701735496521 seconds U2 ---  
--- 95.06309723854065 seconds U3 ---  
--- 95.36862754821777 seconds para U ---  
--- 283.92514848709106 seconds para Gconj-U ---  
--- 327.43474411964417 seconds U1 ---  
--- 1326.5927267074585 seconds para un cálculo ---  
--- 2024.696287870407 seconds para un cálculo ---  
--- 2751.6424293518066 seconds para un cálculo ---  
--- 3494.9460804462433 seconds para un cálculo ---  
--- 4252.603781223297 seconds para un cálculo ---  
--- 5028.807729244232 seconds para un cálculo ---  
--- 5795.239112615585 seconds para un cálculo ---  
--- 6573.074412107468 seconds para un cálculo ---  
--- 7352.284101486206 seconds para un cálculo ---  
--- 8135.137571334839 seconds para un cálculo ---  
--- 8908.958705425262 seconds para un cálculo ---  
--- 9682.519746303558 seconds para un cálculo ---  
--- 10450.310079097748 seconds para un cálculo ---  
--- 11225.957651138306 seconds para un cálculo ---  
--- 12008.713238954544 seconds para un cálculo ---
```

```
Out[2]: 0
```

Bibliografía

- [1] ALLEN, B; AGRELL, E. (Apr 20, 2021), The Optimal Lattice Quantizer in Nine Dimensions, *Annalen Phys.* <https://doi.org/10.48550/arXiv.2104.10107>
- [2] AGRELL, E; ERIKSSON, T. (1998) Optimization of lattices for quantization. **44** 5, 1814–1828, *IEEE Transactions on Information Theory*, doi: 10.1109/18.705561
- [3] AJTAI, M. (1996), Generating Hard Instances of Lattice Problems. *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, ACM Press, New York City. 99-108. <https://doi.org/10.1145/237814.237838>
- [4] BARNES, E. S.; SLOANE, N. J. A. (1983). The optimal lattice quantizer in three dimensions. *SIAM J. Algebraic Discrete Methods* **4** no. 1, 30–41. <https://doi.org/10.1137/0604005>
- [5] BOAZ BARAK (November, 2021) An intensive introduction to cryptography. *Creative Commons “Attribution-NonCommercial- NoDerivatives 4.0 International”* . 99-108. <https://github.com/boazbk/crypto>
- [6] Charve, L (1882) De la réduction des formes quadratiques quaternaires positives. *Annales scientifiques de l'École normale supérieure* 2 . tome 11 , pp 119-134. <https://eudml.org/doc/80877>
- [7] CONWAY, J. H. (with the assistance of F.Y.C. FUNG), (1997) The sensual (quadratic) form, *Carus Mathematical Monographs*, **26** Math. Assoc. of America, Washington, DC . <https://www.jstor.org/stable/10.4169/j.ctt5hh92j>

- [8] CONWAY, J. H.; SLOANE, N. J. A. (1999) Sphere Packing, Lattices and Groups. *Springer-Verlag 3rd Edition*.
- [9] CONWAY, J. H.; SLOANE, N. J. A. (1985) A Lower Bound on the Average Error of Vector Quantizers, *IEEE Transactions on Information Theory*, **31** (2) , 106–109. DOI: 10.1109/TIT.1985.1056993
- [10] CONWAY, J. H.; SLOANE, N. J. A. (1992). Low-dimensional lattices. VI. Voronoi reduction of three-dimensional lattices. *Proceedings: Mathematical and Physical Sciences*, 436(1896) **436** , 55–68. <http://www.jstor.org/stable/52019>
- [11] CONWAY J.H.; SLOANE, N. J. A. (March 1982) Voronoi regions of lattices, second moments of polytopes, and quantization, *IEEE Transactions on Information Theory* **28**(1982), 211–226, doi: 10.1109/TIT.1982.1056483
- [12] CONWAY J.H.; SLOANE, N. J. A.(1984) On the Voronoi regions of certain lattices, *SIAM Journal on Algebraic and Discrete Methods*, **5** (3) , 294–305. <https://doi.org/10.1137/0605031>
- [13] CONWAY, J. H., AND N. J. A. SLOANE. (1992) Low-Dimensional Lattices. VI. Voronoi Reduction of Three-Dimensional Lattices, *Mathematical and Physical Sciences*, vol. 436, no. 1896, pp. 55–68. JSTOR, <http://www.jstor.org/stable/52019>
- [14] ENGEL, P; GRISHUKHIN, V.P.(2002) There are exactly 222 L -types of primitive five-dimensional lattices. *European J. Combin.* **23** , no. 3, 275–279. <https://doi.org/10.1006/eujc.2001.0551>
- [15] FEJES TÓTH, G. (1959) Sur la représentation d’une population infinie par un nombre fini d’elements, *Acta Mathematica Academiae Scientiarum Hungaricae*, **10** , 307–313. <https://doi.org/10.1007/BF02024494>
- [16] F. HIVERT AND J. -C. NOVELLI AND J. -Y. THIBON. (2004). The Algebra of Binary Search Trees *arXiv*. <https://arxiv.org/abs/math/0401089v2>
- [17] VELÁSQUEZ, J.M.; ROSSETTI, J.P. (2012). Retículos en $\mathbb{R}^4$ y el pro-

blema del cuantizador óptimo. *Universidad Nacional de Cordoba*, .
<https://www.famaf.unc.edu.ar/documents/1146/DMat72.pdf>

- [18] MANOJ KUMAR AND PRATAP PATTNAIK. (2020) Post Quantum Cryptography(PQC) - An overview, IBM Thomas J. Watson Research Center. *IEEE High Performance Extreme Computing Conference (HPEC), Waltham, MA, USA*. doi: 10.1109/HPEC43674.2020.9286147
- [19] D. MICCIANCIO. (2001). The hardness of the closest vector problem with preprocessing, *IEEE Trans. Inform. Theory*, *47* . pp. 1212-1215. doi: 10.1109/18.915688
- [20] D. MICCIANCIO AND O. REGEV. (2009). Lattice-based Cryptography. In: Bernstein, D.J., Buchmann, J., Dahmen, E. (eds) Post-Quantum Cryptography. *Springer, Berlin, Heidelberg*. . https://doi.org/10.1007/978-3-540-88702-7_5
- [21] D. MICCIANCIO AND P. VOULGARIS. (2009). A deterministic single exponential time algorithm for most lattice problems based on Voronoi cell computations, *42nd ACM Symposium on Theory of Computing*, <https://doi.org/10.1137/100811970>
- [22] ROBBY G. MCKILLIAM, ALEX J. GRANT AND I. VAUGHAN L. CLARKSON (2014). Finding a closest point in a lattice of Voronoi's first kind, <https://arxiv.org/abs/1405.7014v1>
- [23] SCHÜRMANN, A. (2009). Computational Geometry of Positive Definite Quadratic Forms: Polyhedral Reduction Theories, Algorithms, and Applications, *AMS*, DOI: <https://doi.org/10.1090/ulect/048>
- [24] S. THOMAS MCCORMICK, BRITTA PEIS, ROBERT SCHEIDWEILER, FRANK VALLENTIN. (2021) A polynomial time algorithm for solving the closest vector problem in zonotopal lattices, <https://arxiv.org/abs/2004.07574v3>
- [25] VORONOI, G.F. (1909). Nouvelles applications des paramètres continus à la théorie des formes quadratiques. *J. Reine Angew. Math.* **133** (1908), 97–178; **134** 198–287; **136**, 67–181 [2,21]. <https://doi.org/10.1515/crll.1908.133.97>

- [26] WALDIR AND SILVA, CARVALHO, EDSON AND SOARES, EDUARDO (2021). Topological Quantum Codes from Lattices Partition on the n-Dimensional Flat Tori. *Entropy* **23**, 959. doi= 10.3390/e23080959
- [27] ZADOR, P.L. (1982). Asymptotic quantization error of continuous signals and their quantization dimension, *Institute of Electrical and Electronic Engineers, Transactions on Information Theory*. **28** , 139–149.