Universidad de **Valladolid**
Facultad de Ciencias

Trabajo de Fin de Grado
Grado en Matemáticas

Métodos algebraicos en la teoría de la fiabilidad

Autor: Miguel de los Ríos de Antonio
Tutor: Philippe Gimenez

Índice general

Introducción

La teoría de la fiabilidad estudia la probabilidad de fallo de máquinas complejas. Para esto, se toma una perspectiva sistémica, relacionando el funcionamiento de la máquina con el de sus componentes individuales. Durante este trabajo, se aplicarán métodos algebraicos para estudiar la fiabilidad de sistemas binarios. En concreto, se acota su fiabilidad por medio del K-polinomio del sistema. Para esto, se asigna a cada sistema binario un ideal monomial, de cuya graduación se puede definir un K-polinomio.

En el primer capítulo, se define y explora la estructura de retículo. Esta estructura se usa tanto para estudiar los sistemas binarios como para tratar con ideales monomiales. Pese a que no sea necesaria y en la literatura se suele tratar de forma implícita, se presenta aquí de forma explícita para clarificar y facilitar el temario.

Tras esto, en el segundo capítulo, se realiza una introducción a la teoría de la fiabilidad. Se definen los sistemas binarios como funciones monótonas entre retículos. Y se define su fiabilidad como la probabilidad de que el sistema esté en funcionamiento. Por último, usando la estructura de retículo, se obtienen cotas simples para la fiabilidad de un sistema.

En el tercer capítulo, se establece una correspondencia entre los ideales monomiales y los sistemas binarios. Se estudian las características básicas de estos ideales, tales como sus sistemas minimales de generadores, sus ideales radicales o la suma e intersección de ideales.

Por último, en el cuarto capítulo, se analiza a los ideales como módulos graduados. Para alcanzar este objetivo, se presentan ambas estructuras: en primer lugar la estructura de módulo sobre un anillo, y, tras esto, la estructura de módulo graduado sobre un anillo graduado. Una vez establecida esta estructura, se define el K-polinomio del ideal a partir de la serie de Hilbert de su graduación. Por último, se trunca este polinomio para acotar la fiabilidad del sistema.

Además, en el anexo, se estudian los ideales libres de cuadrados, ya que son aquellos que aparecen al asociar un ideal monomial a un sistema binario. Estos ideales están en correspondencia con complejos simpliciales, a partir

de los cuales se puede definir una homología que reflejará propiedades del K-polinomio. Esto ofrece una herramienta más para el estudio de la fiabilidad de sistemas binarios.

Capítulo 1

Retículos

En este capítulo presentaremos los retículos desde dos puntos de vista complementarios: como estructuras de orden y como estructuras algebraicas. Como demostraremos, ambos son equivalentes. Las referencias básicas para este capítulo son [3]y [1].

1.1. Retículos como posets

La teoría de orden estudia los conjuntos ordenados. Estos pueden ser parcial o totalmente ordenados.

Definición 1.1. Sea L un conjunto. Se dice $(L, \leq)$ es un poset[1] o conjunto parcialmente ordenado si la relación $\leq$ cumple las siguientes propiedades para todos $a, b \in L$:

1. Reflexividad: $a \leq a$.
2. Antisimetría: Si $a \leq b$ y $b \leq a$ entonces $a = b$.
3. Transitividad: Si $a \leq b$ y $b \leq c$ entonces $a \leq c$.

En tal caso se dice que $\leq$ es una relación de orden.

Además, si para todos $a, b \in L$ se cumple que $a \leq b$ ó $b \leq a$, se dice que L es un conjunto totalmente ordenado.

La estructura de poset es mucho más débil que la de conjunto totalmente ordenado. Sin embargo, esta última puede ser demasiado restrictiva. De esta forma, la estructura de retículo proporciona un punto intermedio entre ambas estructuras.

[1]La terminología *poset* proviene del juego de palabras ingles *Partially Ordered SET*

Definición 1.2. Sea $(L, \leq)$ un poset. Sea $S \subset L$ un subconjunto.

Un elemento $a \in L$ es una cota inferior de S si para todo $b \in S$ se cumple que $a \leq b$. Análogamente, es una cota superior si se cumple que $a \geq b$.

Un elemento $a \in L$ es el ínfimo de S, denotado por $\inf(S)$ si se cumple que a es una cota inferior de S y, si b es otra cota inferior de S, se tiene que $a \geq b$. Tal elemento puede existir o no.

Análogamente, a es supremo de S, denotado por $\sup(S)$ si a es una cota superior de S y $a \leq b$ para cualquier otra cota superior.

Definición 1.3. Un poset $(L, \leq)$ es un retículo si para cualquier $a, b \in L$ existen:

$$a \wedge b := \inf(\{a, b\}),$$
$$a \vee b := \sup(\{a, b\}).$$

El siguiente ejemplo explora uno de los ejemplos más típicos de retículos.

Ejemplo 1.4. Sea S un conjunto y $\mathcal{P}(S)$ su conjunto de partes. Entonces $(\mathcal{P}(S), \subset)$ es un retículo.

Si $A, B, C \in \mathcal{P}(S)$. Como $C \subset A$ y $C \subset B$ implican que $C \subset A \cap B$, se tiene que $A \wedge B = A \cap B$. Análogamente, como $A \subset C$ y $B \subset C$ implican que $A \cup B \subset C$, se tiene que $A \vee B = A \cup B$.

Ejemplo 1.5. Sea un anillo R y sea $\mathrm{Id}(R)$ su conjunto de ideales. Veamos que $(\mathrm{Id}(R), \subset)$ es un retículo.

Sean $I, J \in \mathrm{Id}(R)$. El ideal $I + J$ contiene a ambos. Además, si $I, J \subset K \in \mathrm{Id}(R)$ se tiene que $I + J \subset K$ pues K está cerrado bajo sumas. Por lo tanto, $I \vee J = I + J$.

Por otra parte, es fácil ver que $I \wedge J = I \cap J$.

Ejemplo 1.6. En el caso particular $R = \mathbb{Z}$, como es un dominio de ideales principales, cada ideal I es de la forma $\langle n \rangle$ para algún $n \in \mathbb{N}$. De este modo podemos identificar $\mathrm{Id}(\mathbb{Z})$ con $\mathbb{N}$.

Si definimos

$$n \leq m \quad \Longleftrightarrow \quad \langle n \rangle \supseteq \langle m \rangle,$$

esto equivale a la relación de divisibilidad $n \mid m$.

Con esta interpretación se tiene:

$$n \vee m = \mathrm{mcm}(n, m), \qquad n \wedge m = \mathrm{mcd}(n, m).$$

Así, la aritmética elemental de $\mathbb{N}$ puede entenderse como un retículo con las operaciones de mínimo común múltiplo y máximo común divisor.

Proposición 1.7. *Si $(L, \leq)$ es un conjunto totalmente ordenado, entonces también es un retículo.*

Demostración. Sean $a, b \in L$. Definamos $a \vee b$ y $a \wedge b$.

Supongamos que $a \leq b$, en tal caso $a \vee b = b$ y $a \wedge b = a$.

Igualmente, si $a \geq b$ se tiene que $a \vee b = a$ y $a \wedge b = b$.

□

Ejemplo 1.8. Los conjuntos $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ son retículos por ser totalmente ordenados.

La definición de retículos es equivalente a una condición más fuerte.

Proposición 1.9. *Un poset $(L, \leq)$ es un retículo si y solo si para cualquier $H \subset L$ finito existen tanto sup(H) como inf(H).*

Demostración.

$\Rightarrow$) Realizamos la demostración por inducción sobre la cardinalidad de H.

Suponemos que $H = \{h_1\}$ tiene solo un elemento. Entonces $\inf(H_1) = h_1$.

Supongamos ahora que todos los conjuntos de $n-1$ o menos elementos tienen inf bien definido. En este caso $H = \{h_1, \ldots, h_n\}$ tiene n elementos. Tomamos $a = \inf(\{h_1, \ldots, h_{n-1}\})$ que existe por hipótesis de inducción. Veamos que $b = \inf(\{a, h_n\})$ es el ínfimo de H.

Tenemos que $b \leq a \leq h_i$ para todo $i \in \{1, \ldots, n-1\}$. Además, $b \leq h_n$. Así que $b \leq h_i$ para todo $h_i \in H$.

Sea c una cota inferior de H. Entonces, $c \leq h_i$ para todo $i \in \{1, \ldots, n-1\}$ luego $c \leq a$. Además, $c \leq h_n$. Por lo que $c \leq b$.

La demostración de que sup(H) está bien definida es análoga.

$\Leftarrow$) Dado $a, b \in L$, si tomamos $H = \{a, b\}$ se tiene que $a \vee b = \sup(H)$ y $a \wedge b = \text{ínf}(H)$.

□

Observación 1.10. En la anterior proposición la hipótesis de H finito es indispensable, pues, tal y como vimos en el ejemplo 1.8, $\mathbb{R}$ es un retículo. Para $\mathbb{N} \subset \mathbb{R}$ se tendría que existe un elemento real $\infty = \sup(\mathbb{N})$ tal que $\infty \geq n$ para todo $n \in \mathbb{N}$.

Tal elemento no existe en la recta real. Sin embargo, sí que existe en la recta extendida$\mathbb{R} \cup \{-\infty, \infty\}$.

Ejemplo 1.11. $\mathbb{R}$ es un cuerpo ordenado. Esto es un cuerpo totalmente ordenado en el que para todo $x, y, z \in \mathbb{R}$ con $z > 0$ se cumple:

1. Si $x \leq y$, entonces $x + z \leq y + z$.

2. Si $x \leq y$, entonces $xz \leq yz$.

Esta estructura se pierde al pasar de $\mathbb{R}$ a $\mathbb{R}^n$, que no está completamente ordenado. Sin embargo, $\mathbb{R}^n$ sigue siendo un retículo. Para esto definimos la relación de orden:

$$(x_1, \ldots, x_n) \leq (y_1, \ldots, y_n) \iff x_i \leq y_i \quad \forall i \in \{1, \ldots, n\}.$$

Los operadores $\vee, \wedge$ resultantes son:

$$(x_1, \ldots, x_n) \vee (y_1, \ldots, y_n) = (x_1 \vee y_1, \ldots, x_n \vee y_n),$$

$$(x_1, \ldots, x_n) \wedge (y_1, \ldots, y_n) = (x_1 \wedge y_1, \ldots, x_n \wedge y_n).$$

Por ejemplo, en $\mathbb{R}^3$ se tiene que $(3, 7, 1) \vee (4, 6, 1) = (4, 7, 1)$.

En la siguiente sección definiremos la noción de morfismo de retículo. Por ahora, simplemente presentaremos la noción de morfismo de poset, que es una condición necesaria pero no suficiente para ser morfismo de retículo.

Definición 1.12. Sean $(L, \leq), (L', \leq')$ dos posets. Una aplicación $\phi : L \to L'$ es monótona si se cumple que para todo $a, b \in L$:

$$a \leq b \Longrightarrow \phi(a) \leq' \phi(b).$$

Ejemplo 1.13. Sea S un conjunto y $a \notin S$. Definimos el conjunto $S' = S \cup \{a\}$. La siguiente aplicación monótona ϕ es un morfismo entre $(\mathcal{P}(S), \subset)$ y $(\mathcal{P}(S'), \subset)$:

$$\phi : \mathcal{P}(S) \longrightarrow \mathcal{P}(S')$$
$$A \longmapsto A \cup \{a\}.$$

Por último, antes de proseguir con el punto de vista algebraico, definimos los subrretículos.

Definición 1.14. Sea $(L, \leq)$ un poset, $S \subset L$ y $\leq_S$ la restricción de $\leq$ a S. Se dice que $(S, \leq_S)$ es un subposet de $(L, \leq)$. Además, se dice que $(S, \leq_S)$ es un subrretículo de $(L, \leq)$ si es un retículo.

Ejemplo 1.15. Sea $2\mathbb{N} = \{0, 2, 4, \ldots\}$ el conjunto de números pares. Se tiene que $2\mathbb{N} \subset \mathbb{N}$ y, por tanto, que $\mathcal{P}(2\mathbb{N}) \subset \mathcal{P}(\mathbb{N})$. De hecho, $(\mathcal{P}(2\mathbb{N}), \subset)$ es un subrretículo de $(\mathcal{P}(\mathbb{N}), \subset)$.

Por otra parte, definamos $L = \{S \in \mathcal{P}(\mathbb{N}) : |S| \in 2\mathbb{N}\}$, donde $|S|$ representa la cardinalidad de S. Obviamente se tiene que $(L, \subset)$ es un subposet de $(\mathcal{P}(\mathbb{N}), \subset)$. Sin embargo, no es un subrretículo, puesto que $\sup(\{1, 2\}, \{2, 3\})$ no está bien definido. $\{1, 2, 3, n\}$ es una cota superior minimal de $\{1, 2\}$ y $\{2, 3\}$ para todo $n \in \mathbb{N} \setminus \{1, 2, 3\}$, por lo que no hay un supremo único.

1.2. Retículos como estructuras algebraicas

Desde el punto de vista algebraico, un retículo es un tipo de estructura algebraica. Se describen las leyes de las operaciones $\vee, \wedge$ que tal y como veremos en la siguiente sección, permiten recuperar la relación de orden.

Como ambas operaciones comparten gran parte de su comportamiento, resulta natural estudiar primero la noción más general de semirretículo que describe a ambas.

Definición 1.16. Un semirretículo algebraico es una estructura $(A, \circ)$ donde la operación $\circ : A \times A \to A$ cumple:

1. Idempotencia: $a \circ a = a$.
2. Conmutatividad: $a \circ b = b \circ a$.
3. Asociatividad: $a \circ (b \circ c) = (a \circ b) \circ c$.

Ejemplo 1.17. En la anterior sección vimos que si S es un conjunto, se tiene que $(\mathcal{P}(S), \subset)$ es un retículo de orden. Es fácil comprobar que $(\mathcal{P}(S), \cup)$ y $(\mathcal{P}(S), \cap)$ son semirretículos algebraicos.

Definición 1.18. $(A, \vee, \wedge)$ es un retículo algebraico si:

1. $(A, \vee)$ y $(A, \wedge)$ son semirretículos algebraicos.
2. Se cumplen las leyes de absorción: $a \vee (a \wedge b) = a, \qquad a \wedge (a \vee b) = a.$

El siguiente ejemplo comprueba que los retículos de la anterior sección siguen siendo retículo bajo esta nueva definición.

Ejemplo 1.19. Tal y como vimos en la anterior sección, el retículo de orden $(\mathbb{R}, \leq)$ produce dos operaciones $\vee, \wedge$ binarias. Se tiene que $(\mathbb{R}, \vee, \wedge)$ es un retículo algebraico.

Es obvio que $(\mathbb{R}, \vee)$ y $(\mathbb{R}, \wedge)$ son semirretículos algebraicos.

Para ver que son retículos algebraicos comprobamos las leyes de absorción por casos:

Sean $a, b \in \mathbb{R}$. Supongamos que $a \leq b$. En tal caso $a \vee b = b$ y $a \wedge b = a$. Por lo que $a \vee (a \wedge b) = a \vee (a) = a$ y $a \wedge (a \vee b) = a \wedge b = a$.

Y, si $a \geq b$, se tiene que $a \vee b = a$ y $a \wedge b = b$. Por lo cual $a \vee (a \wedge b) = a \vee (b) = a$ y $a \wedge (a \vee b) = a \wedge (a) = a$.

Ejemplo 1.20. El conjunto de dos elementos $F_2 = \{0, 1\}$, con $0 \leq 1$, forma un retículo de orden. Este también se puede definir como retículo algebraico a partir de la siguiente tabla de operación:

a	b	$a \vee b$	$a \wedge b$
0	0	0	0
0	1	1	0
1	0	1	0
1	1	1	1

Este retículo algebraico $(F_2, \vee, \wedge)$ aparece muy frecuentemente en informática, pues modela la lógica de los bits. En esta se interpretan los valores 0 como *Falso*, 1 como *Verdadero*; y las operaciones $\vee$ como *ó*, y $\wedge$ como *y*.

Al igual que en el ejemplo 1.11 podemos extender la estructura de retículo a $(F_2^n, \vee, \wedge)$.

Proposición 1.21. *Sea $(A, \vee, \wedge)$ un retículo y $a, b \in A$. Si se tiene:*

$$a \vee b = a \iff a \wedge b = b.$$

Demostración.

$\Rightarrow$) Sustituyendo $a = a \vee b$ obtenemos

$$a \wedge b = (a \vee b) \wedge b.$$

Pero, según la segunda ley de absorción

$$b \wedge (a \vee b) = b.$$

$\Leftarrow$) Sustituyendo $b = a \wedge b$ obtenemos

$$a \vee b = a \vee (a \wedge b).$$

Pero, según la primera ley de absorción

$$a \vee (a \wedge b) = a.$$

□

Ahora, partiendo de retículos algebraicos, sí que podemos definir un morfismo de retículos.

Definición 1.22. Sean $(A, \vee, \wedge), (A', \vee', \wedge')$ dos retículos algebraicos y $\phi : A \to A'$ una aplicación entre ellos. Se dice que ϕ es un morfismo de retículo si, para todo $a, b \in A$, se cumple:

1. $\phi(a \vee b) = \phi(a) \vee \phi(b)$.
2. $\phi(a \wedge b) = \phi(a) \wedge \phi(b)$.

Ejemplo 1.23. La siguiente figura 1.1 muestra dos retículos de orden. En ella los nodos representan elementos del retículo, las flechas discontinuas una aplicación ϕ y, las aristas desigualdades. Si un nodo x está conectado con un nodo y de forma que x está por encima de y se entiende que $x \geq y$.

El retículo de la izquierda $L = \{a, b, c, d\}$, tiene que $a \geq b, c$ y $b, c \geq d$. Y, el retículo de la derecha $L' = \{e, f, g\}$, tiene $e \geq f \geq g$.

Obsérvese que ϕ preserva el orden (es monótona), pero no preserva las operaciones $\vee, \wedge$ Pues $b \vee c = a$ pero $\phi(b) \vee \phi(c) = f \vee f = f \neq \phi(a)$.

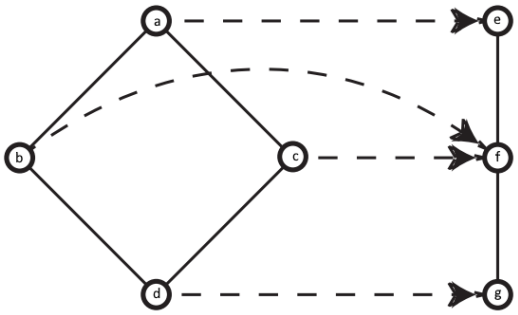

Figura 1.1: Ejemplo de morfismo de retículo. [3]

1.3. Equivalencia de definiciones

Como se mencionó en el anterior capítulo, ambas definiciones de retículo son equivalentes. En el lenguaje de categorías, se podría decir que existe un funtor de la categoría de los retículos algebraicos a la de los retículos de orden.

En un lenguaje más conjuntista, se puede decir que existe una biyección entre los retículos algebraicos y los retículos de orden. Además, cada homomorfismo de retículos es una aplicación monótona.

Teorema 1.24. *Existe una biyección entre el conjunto de retículos algebraicos y el conjunto de retículos de orden.*

Demostración. Construiremos una aplicación Φ del conjunto de retículos algebraicos al conjunto de retículos de orden. Tras esto construiremos otra aplicación Ψ en sentido contrario. Por último, demostraremos que $\Phi \circ \Psi = \mathrm{Id}$ y $\Psi \circ \Phi = \mathrm{Id}$.

Durante la demostración, S será un conjunto, $L = (S, \leq)$ un retículo de orden y $A = (S, \vee, \wedge)$ un retículo algebraico.

Φ) Partiendo de $A = (S, \vee, \wedge)$, definimos en S la relación de orden $a \leq b \iff a \vee b = b$. Veamos que $(S, \leq)$ es un retículo de orden.

Empecemos por ver qué es un poset, es decir, que la relación es de orden. Sean $a, b, c \in S$:

1. **Reflexividad:** Por idempotencia se tiene que $a \vee a = a$. Por lo tanto, $a \leq a$.

2. **Antisimetría:** Partimos de $a \leq b$ y $b \leq a$. En un lenguaje algebraico esto se traduce por $a \vee b = b$ y $b \vee a = a$. Como $\vee$ es conmutativo, es necesario que $a = b$.

3. **Transitividad:** Partimos de $a \leq b$ y $b \leq c$. Es decir $a \vee b = b$ y $b \vee c = c$. Veamos que $a \leq c$. Por la asociatividad de $\vee$ se tiene que $a \vee c = a \vee (b \vee c) = (a \vee b) \vee c = b \vee c = c$. Luego $a \leq c$.

Nótese que para demostrar cada uno de los tres axiomas de orden, hemos tenido que usar un axioma de semirretículo algebraico diferente.

Ahora veamos que $a \vee b = \sup(\{a, b\})$ y $a \wedge b = \text{ínf}(\{a, b\})$. Comencemos por sup.

Veamos que $a, b \leq a \vee b$:

- $a \vee (a \vee b) = (a \vee a) \vee b = a \vee b$, por lo que $a \leq a \vee b$.

- $b \vee (a \vee b) = (a \vee b) \wedge b = a \vee (b \vee b) = a \vee b$, por lo que $b \leq a \vee b$.

Ahora, veamos que si $a, b \leq c$ entonces $a \vee b \leq c$. Partimos de $a \vee c = c$ y $a \vee b = b$. Aplicando esto:

$$(a \vee b) \vee c = a \vee (b \vee c) = a \vee c = c,$$

por lo que $a \vee b \leq c$.

Análogamente, demostremos que $a \vee b = \text{ínf}(\{a, b\})$.

Veamos que $a \wedge b \leq a, b$.

- $a \vee (a \wedge b) = a$ por la primera ley de absorción, por lo que se concluye que $a \vee b \leq a$.

- $b \vee (a \vee b) = b \vee (b \vee a) = b$ por la primera ley de absorción, por lo que se concluye que $a \vee b \leq b$.

Ahora, veamos que si $c \leq a, b$ entonces $c \leq a \wedge b$. Partimos de $a \vee c = a$ y $b \vee c = b$. Según la proposición 1.21 esto es equivalente a $a \wedge c = c$ y $b \wedge c = c$. Ahora computamos:

$$(a \wedge b) \wedge c = a \wedge (b \wedge c) = a \wedge c = c.$$

Y, volviendo a aplicar 1.21, vemos que $(a \wedge b) \vee c = a \wedge b$. De donde se concluye que $c \leq a \wedge b$.

Por tanto $\Phi(A) = (S, \leq)$ es un retículo.

Ψ) Partiendo de $L = (S, \leq)$, definimos en S las operaciones binarias $a \vee b := \sup(\{a, b\})$ y $a \wedge b := \text{ínf}(\{a, b\})$ Veamos que $(S, \vee, \wedge)$ es un retículo algebraico.

Para esto, comenzamos por ver que es un semirretículo algebraico:

1. **Idempotencia:** $a \vee a = \sup(\{a, a\}) = a$.
2. **Conmutatividad:** $a \vee b = \sup(\{a, b\}) = \sup(\{b, a\}) = b \vee a$.
3. **Asociatividad:** $a \vee (b \vee c) = \sup(\{a, b, c\}) = (a \vee b) \vee c$.

El caso de $\wedge$ es análogo.

Veamos ahora que se cumplen las leyes de absorción.

- $a \vee (a \wedge b) = \sup(\{a, \text{ínf}(\{a, b\})\})$. Como $\text{ínf}(\{a, b\}) \leq a$, se tiene que $\sup(\{a, \text{ínf}(\{a, b\})\}) = a$.
- $a \wedge (a \vee b) = \text{ínf}(\{a, \sup(\{a, b\})\})$. Como $\sup\{a, b\} \geq a$, se tiene que $\text{ínf}(\{a, \sup(\{a, b\})) = a$.

Por tanto, $\Psi(L) = (S, \vee, \wedge)$ es un retículo algebraico.

$\Phi \circ \Psi$) Partimos de un retículo de orden $L = (S, \leq)$ y aplicamos Ψ para obtener el retículo algebraico $(S, \vee, \wedge)$ con $a \vee b := \sup(\{a, b\})$ y $a \wedge b := \text{ínf}(\{a, b\})$.

Luego aplicamos Φ a este retículo algebraico para obtener la relación $\leq'$ en S definida por:

$$a \leq' b \iff a \vee b = b.$$

Queremos ver que $\leq = \leq'$, es decir, que para todo $a, b \in S$ se cumple:

$$a \leq b \iff a \leq' b.$$

Si $a \leq b$ entonces se tiene tanto $b \geq a$ como $b \geq b \vee a$. Por lo tanto, $a \vee b = \sup(\{a, b\}) = b$. Luego $a \leq' b$.

Si $a \leq' b$, se tiene que $\sup(\{a, b\}) = b$. Por lo que $b \geq a$.

$\Psi \circ \Phi$) Partimos de un retículo algebraico $A = (S, \vee, \wedge)$ y aplicamos Φ para obtener el retículo de orden $(S, \leq)$ con $a \leq b \iff a \vee b = b$.

Luego aplicamos Ψ a este retículo de orden para obtener las operaciones $\vee', \wedge'$ definidas en S como:

$$a \vee' b := \sup(\{a, b\}), \qquad a \wedge' b = \text{ínf}(\{a, b\}).$$

Queremos ver que $\vee = \vee'$ y $\wedge = \wedge'$. Es decir, que para todo $a, b \in S$ se cumple:

$$a \vee b = a \vee' b, \qquad a \wedge b = a \wedge' b.$$

Realizamos la demostración para $\vee = \vee'$ pues el caso de $\wedge = \wedge'$ es análogo. Procedemos en dos pasos: demostramos que $a \vee b$ es una cota superior de $\{a, b\}$, y demostramos que $a \vee b$ es la mínima cota superior de $\{a, b\}$.

(i) Queremos ver que $a \vee b \geq a, b$.

$$(a \vee b) \vee a = a \vee b \vee a = a \vee a \vee b = (a \vee a) \vee b = a \vee b.$$

Análogamente:

$$(a \vee b) \vee b = a \vee (b \vee b) = a \vee b.$$

(ii)Queremos ver que si $c \geq a, b$ entonces $c \geq a \vee b$. O, equivalentemente, si $a \vee c = b \vee c = c$ se tiene$(a \vee b) \vee c = c$.

$$(a \vee b) \vee c = a \vee (b \vee c) = a \vee c = c.$$

□

Observación 1.25. Recordemos que, por 1.21, se tiene que $a \vee b = b \iff a \wedge b = a$. Por lo cual, se tiene que $a \leq b \iff a \wedge b = a$. De hecho, se podría haber realizado la construcción partiendo de esta definición alternativa.

De ahora en adelante no distinguiremos entre retículos de orden y retículos algebraicos.

Proposición 1.26. *Sean $(A, \vee, \wedge), (A', \vee', \wedge')$ dos retículos y $\phi : A \to A'$ un homomorfismo de retículo. Entonces ϕ es monótono.*

Demostración. Sean $a, b \in A$ con $a \leq b$. Equivalentemente $a \vee b = b$.

Por lo tanto, se cumple $\phi(b) = \phi(a \vee b) = \phi(a) \vee \phi(b)$. Por lo tanto $\phi(a) \leq' \phi(b)$. □

Proposición 1.27. *Sean $(L, \leq), (L', \leq')$ dos retículos y $\phi : L \to L'$ una aplicación monótona biyectiva entre ellos. Entonces ϕ es homomorfismo de retículos.*

Demostración. Sean $a, b \in L$. Veamos primero que $\phi(a \vee b) = \phi(a) \vee' \phi(b)$. Para esto caracterizamos a $\phi(a) \vee' \phi(b) = \sup(\{\phi(a), \phi(b)\}$

Como $a \vee b \geq a, b$ y ϕ es monótona, se tiene que $\phi(a \vee b) \geq' \phi(a), \phi(b)$. Por lo tanto, $\phi(a \vee b)$ es una cota superior de $\{\phi(a), \phi(b)\}$.

Supongamos que $c \geq \phi(a), \phi(b)$ es otra cota superior. Entonces, como ϕ es monótona e invertible, se tiene que $\phi^{-1}(c) \geq a, b$. Y como $a \vee b = \sup(\{a, b\})$ se tiene que $\phi^{-1}(c) \geq a \vee b$. Ahora, por monotonía, se concluye que $c \geq' \phi(a \vee b)$.

Se puede argumentar de forma análoga para $\phi(a \wedge b)$. □

Capítulo 2

Fiabilidad de sistemas

Las máquinas y sistemas tecnológicos terminan malfuncionando con el tiempo: las correas de relojes se rompen, las ruedas de los coches se pinchan y los engranajes se engrasan. Aunque esto es inevitable, puede prevenirse o retrasarse para que los sistemas duren lo máximo.

La siguiente historieta informal nos muestra de forma intuitiva qué mentalidad tienen los ingenieros al diseñarlos.

Vamos a celebrar nuestro cumpleaños haciendo paracaidismo. Saltamos del avión y tiramos de la anilla...¡pero el paracaídas no se abre! ¿Qué hacemos? ¿Vamos a morir?

No. Hemos traído un paracaídas de repuesto. Tiramos de la anilla y funciona. Hemos sobrevivido gracias a la ***redundancia*** *en el paracaídas, que hace un sistema más* ***fiable****. Esta misma filosofía es la que siguen los ingenieros al diseñar sistemas tecnológicos.*

Sin embargo, esta mentalidad no siempre existió. En los orígenes del estudio de la fiabilidad (durante la Primera Guerra Mundial [5]) el enfoque predominante era mejorar la calidad de cada componente, estudiando su tiempo de vida medio mediante herramientas estadísticas tales como la esperanza matemática o distribuciones de fallo.

Con el tiempo, la experiencia mostró que, a partir de un punto, era más efectivo añadir componentes redundantes a los sistemas que aumentar la calidad de estos últimos. De este modo, la fiabilidad pasó de entenderse no solo como una propiedad de cada pieza, sino como una propiedad emergente del sistema en su conjunto.

Hoy en día, ambas perspectivas conviven y se complementan. En este capítulo exploraremos la teoría de fiabilidad desde un punto sistémico, introduciendo técnicas estadísticas de análisis de componentes allá cuando sea necesario[6].

2.1. Sistemas binarios

Un sistema representa una máquina. Estas máquinas son complejas y pueden estar formadas por una variedad de máquinas simples.

Ejemplo 2.1. Una bicicleta es una máquina compleja. Está formada por dos ruedas, un sillín, un esqueleto metálico, una cadena, un manillar, etc. Todos estos componentes son máquinas más simples. Por ejemplo, las ruedas también están formadas por componentes. Tienen: cubierta, llantas, radios, válvula, buje. Y, a su vez, una válvula está formada por aún más máquinas.

Durante el análisis de un sistema es necesario decidir en cuántas máquinas se subdivide este. ¿Es necesario tener en cuenta las llantas y los radios, o es suficiente con considerar las ruedas?

Analizar un sistema conlleva relacionar el estado de sus componentes con el estado del sistema. Por lo que, desde un punto de vista matemático, solo es necesario conocer el número de componentes y la dependencia que tiene el estado del sistema con estos.

Además, añadimos una hipótesis simplificadora, los componentes pueden funcionar o no funcionar. No existe ningún punto intermedio. De esta forma, basta con un bit para describir el estado de un componente. Este puede estar funcionando 1 o no estarlo 0.

Definición 2.2. Un sistema binario con n componentes es una función monótona[1] $\phi : F_2^n \to F_2$. Se llama orden del sistema al número de componentes n.

En esta definición F_2 codifica un bit. Por lo cual, la aplicación ϕ describe cuál es el estado del sistema para cada uno de los posibles estados de los componentes.

Además, hemos requerido que ϕ sea monótona. Pues, suponemos que el estado del sistema no empeorará si mejora el estado de sus componentes.

Observación 2.3. En la definición de sistema hemos partido de la hipótesis de que el estado de un componente se puede codificar como una variable en F_2. Los sistemas que no cumplen esta propiedad se llaman sistemas multiestado en vez de sistemas binarios.

Sea $F_q = \{1, \ldots, q\}$ con $1 \leq \ldots \leq q$. Un sistema multiestado está descrito por una función monótona $\phi : F_q^n \to F_q$.

Por ejemplo, un sistema multiestado con q estados puede ser un ventilador que pueda funcionar en q velocidades. O, en su lugar, podría ser un video de Youtube que puede mostrarse en calidades $\{360\text{p}, 480\text{p}, 720\text{p}, 1080\text{p}\}$.

[1] Los retículos F_2 y F_2^n se definieron en el ejemplo 1.20.

Durante este documento tratamos con sistemas binarios en vez de multiestado porque estos tienen una estructura combinatoria más rica. En concreto, como veremos posteriormente, generan un ideal libre de cuadrados y un complejo simplicial.

Ejemplo 2.4. Los sistemas binarios triviales son aquellos en los que ϕ es constante. Como ϕ toma valores en F_2, existen dos sistemas triviales: el "distópico"$\phi_0 = 0$ que nunca funciona, y el "utópico"$\phi_1 = 1$ que siempre funciona.

A priori, estos sistemas no parecen tener un gran interés. Sin embargo, pueden ser muy útiles estructuralmente. Pues, como veremos posteriormente, son los elementos máximos y mínimos del retículo de sistemas binarios.

Ejemplo 2.5. Otro ejemplo de sistemas binarios son los $k-n$, llamados "k sobre n". Estos sistemas funcionan si al menos k de sus n componentes están funcionando. Por ejemplo, un coche con una rueda de repuesto es un sistema $4-5$. Pues, para funcionar, necesita que cuatro de sus cinco ruedas no estén pinchadas, da iguales qué cuatro de las cinco sean.

Denotamos un sistema $k-n$ por $\phi_{k,n}$. De esta forma, en el ejemplo del coche tendríamos que $\phi_{4,5}((1,1,0,1,1)) = 1$ y $\phi_{4,5}((1,1,0,0,1)) = 0$.

Inspirados por los circuitos eléctricos, los sistemas $n-n$ se llaman sistemas secuenciales, y los sistemas $1-n$ se llaman sistemas paralelos.

Ejemplo 2.6 (Códigos Correctores)**.** Como ya se ha mencionado anteriormente, los ordenadores almacenan y comunican información por medio de bits. Un mensaje a través de la web se puede interpretar como dos vectores $e, r \in F_q$. El vector e representa la información enviada y el vector r la información recibida.

Estos vectores no tienen por qué coincidir, puesto que puede darse errores durante la comunicación. De hecho, es común que se den errores. Para prevenir esto se aplican códigos correctores de errores.

Supongamos que q es primo o potencia de primo y, por tanto, $F_q = \mathbb{F}_q$ es un cuerpo. Sea $n, m \in \mathbb{N}$ con $0 < n < m$. Entonces tanto $\mathbb{F}_q^n$ como $\mathbb{F}_q^m$ son espacios vectoriales. Se puede definir un código lineal como una aplicación lineal inyectiva $C : \mathbb{F}_q^n \to \mathbb{F}_q^m$.

Esta aplicación añade $m-n$ bits de redundancia al sistema. Por ejemplo, un código lineal puede ser:

$$C : \mathbb{F}_q^1 \longrightarrow \mathbb{F}_q^3$$

$$(1) \longmapsto (1,1,1)$$

$$(0) \longmapsto (0,0,0)$$

De esta forma, si recibimos $(1, 0, 1)$ podemos suponer que ha habido un error en el segundo bit y que el mensaje original era $(1, 1, 1)$.

Para que el mensaje sea interpretado correctamente necesitamos que dos de los tres bits sean comunicados sin errores. Por lo tanto, este sistema sería un sistema $k - n$. En concreto, sería $\phi_{2,3}$.

Además de sistemas binarios, nos interesan sistemas coherentes. Estos son aquellos que no tienen componentes irrelevantes. Es decir, que ninguna de sus componentes es innecesaria.

Definición 2.7. Sea $i, n \in \mathbb{N}$ con $0 < i \leq n$. Se define la aplicación substitución í-ésima como:

$$s_i : F_2^n \times F_2 \longrightarrow F_2^n$$

$$((a_1, \dots a_i, \dots, a_n), b) \longmapsto (a_1, \dots, b, \dots, a_n).$$

Ejemplo 2.8. Sea $v = (1, 0) \in F_2^2$. Entonces, al aplicar la sustitución en cada coordenada:

$$s_1(v, 0) = (0, 0), \qquad s_2(v, 1) = (1, 1).$$

Obsérvese que si el valor que sustituimos coincide con el original, el vector no cambia:

$$s_1(v, 1) = s_2(v, 0) = (1, 0).$$

Definición 2.9. Sea $\phi : F_2^n \to F_2$ un sistema binario. Sea $i \in \mathbb{N}$ con $0 < i \leq n$. Se dice que la i-ésima componente de ϕ es relevante si existe $v \in F_2^n$ con $\phi(s_i(v, 1)) = 1$ y $\phi(s_i(v, 0)) = 0$.

Se dice que una componente es irrelevante si no es relevante.

Decimos que ϕ es coherente si todas sus componentes son relevantes.

Ejemplo 2.10. Sea $i, n \in \mathbb{N}$ con $0 < i < n$. Definimos el sistema binario X_i como:

$$X_i(a_1, \dots, a_n) = a_i.$$

En este sistema, la única componente relevante es la i-ésima.

Ejemplo 2.11. Los sistemas triviales no son coherentes, ya que ninguna de sus componentes es relevante. En cambio, los sistemas $k-n$ sí son coherentes: el estado del sistema depende efectivamente de todas sus componentes.

2.2. Retículo de sistemas binarios

Los sistemas binarios forman un retículo. Esto nos va a permitir construir sistemas binarios a partir de otros sistemas binarios.

Teorema 2.12. *El conjunto de los sistemas binarios de orden n, L_n, puede ser dotado de estructura de retículo.*

Demostración. Una función $f : F_2^n \to F_2$ puede ser interpretada como una 2^n-tupla de $F_2^{2^n}$. En efecto, F_2^n tiene 2^n elementos, por lo que para determinar la imagen de una función es necesario determinar su imagen en cada uno de estos.

El conjunto de funciones de $F_2^n \to F_2$ hereda la estructura de retículo de $F_2^{2^n}$. Según esta estructura, si f, g son dos funciones y $a \in F_2^n$:

$$(f \vee g)(a) := f(a) \vee g(a),$$

$$(f \wedge g)(a) := f(a) \wedge g(a),$$

$$f \leq g \iff f(b) \leq g(b) \quad \forall b \in F_2^n.$$

Por lo tanto, solo es necesario demostrar que L_n es un subrretículo. Es decir, que si ϕ, ψ son monótonas, entonces $\phi \vee \psi$ y $\phi \wedge \psi$ también lo son.

$\phi \vee \psi$) Sea $a, b \in F_2^n$ con $a \leq b$. Veamos que $\phi(a) \vee \psi(a) \leq \phi(b) \vee \psi(b)$. O, lo que es equivalente, $(\phi(a) \vee \psi(b)) \vee (\phi(b) \vee \psi(b)) = \phi(b) \vee \psi(b)$.

Para esto, usamos la asociatividad y conmutatividad.

$$(\phi(a) \vee \psi(a)) \vee (\phi(b) \vee \psi(b)) = (\phi(a) \vee \phi(b)) \vee (\psi(a) \vee \psi(b)) = \phi(b) \vee \psi(b).$$

Donde hemos usado que $\phi(a) \leq \phi(b) \Rightarrow \phi(a) \vee \phi(b) = \phi(b)$ y $\psi(a) \leq \psi(b) \Rightarrow \psi(a) \vee \psi(b) = \psi(b)$.

$\phi \wedge \psi$) Sea $a, b \in F_2^n$ con $a \leq b$. Veamos que $\phi(a) \wedge \psi(a) \leq \phi(b) \wedge \psi(b)$. Según la observación 1.25, se tiene que esto es equivalente a $(\phi(a) \wedge \psi(a)) \wedge (\phi(b) \wedge \psi(b)) = \phi(a) \wedge \psi(a)$. Llegado a este punto se puede realizar un razonamiento análogo al empleado en el anterior caso. □

Este teorema nos dice que si ϕ, ψ son sistemas binarios, entonces podemos construir otro sistema $\phi \vee \psi$ ó $\phi \wedge \psi$ a partir de ellos. A continuación veremos que todos los sistemas binarios no triviales se pueden construir a partir de X_i.

Definición 2.13. Sea ϕ un sistema binario. Su conjunto de cortes se define como $C_\phi^0 = \phi^{-1}(\{0\})$ y su conjunto de caminos $C_\phi^1 = \phi^{-1}(\{1\})$.

Además, se define su generador de caminos como el conjunto de caminos minimales, es decir:

$$G_\phi^1 = \{a \in C_\phi^1 : \nexists b \in C_\phi^1, b \leq a\}.$$

Observación 2.14. Esta notación está inspirada por los sistemas eléctricos. En estos, la electricidad parte de una batería y ha de recorrer el circuito a través de cables y componentes para volver a la batería. Si cualquiera de estos componentes está dañado, cortocircuitado o apagado, la electricidad es incapaz de cruzarlo y tiene que buscar un camino alternativo a través de otros componentes.

Por esto, aquellos estados en los cuales el sistema funciona se llaman caminos, y aquellos en los que no funcionan se llaman cortes (cortocircuito).

El primer paso es construir, para cada camino, un sistema que lo represente a partir de los X_i.

Definición 2.15. Sea $(a_1, \ldots, a_n) \in F_2^n$ una lista de elementos de F_2. Se denota:

$$\bigwedge_i a_i := a_1 \wedge \ldots \wedge a_n,$$

$$\bigvee_i a_i := a_1 \vee \ldots \vee a_n.$$

Esta notación generaliza los sumatorios Σ y los productorios Π para las operaciones $\wedge, \vee$.

Ejemplo 2.16. En el caso de F_2 se tiene:

$$\bigwedge_i a_i = \text{ínf}(\{a_1, \ldots, a_n\}) = \begin{cases} 1, & \text{si todos los } a_i = 1, \\ 0, & \text{si existe un } a_i = 0. \end{cases}$$

$$\bigvee_i a_i = \sup(\{a_1, \ldots, a_n\}) = \begin{cases} 1, & \text{si existe un } a_i = 1, \\ 0, & \text{si todos los } a_i = 0. \end{cases}$$

Definición 2.17. Sea $v = (v_1, \ldots, v_n) \in F_2^n$ se define su soporte como

$$\text{sop}(v) = \{i : v_i \neq 0\}.$$

Observación 2.18. El soporte se puede usar para definir una métrica llamada la métrica de Hamming. Esta métrica dicta $\|v\| = |\text{sop}(v)|$.

Es muy común en el ámbito de los códigos correctores de errores. También se puede usar para simplificar la definición de los sistemas $k - n$.

$$\phi_{k,n}(a) = \begin{cases} 1, & \text{si } \|a\| \geq k, \\ 0, & \text{si } \|a\| < k. \end{cases}$$

Definición 2.19. Sea $v = (v_1, \ldots, v_n) \in F_2^n$. Es posible asignarle un sistema de orden n:

$$\phi_v := \bigwedge_{i \in \text{sop}(v)} X_i.$$

Proposición 2.20. *Sea $v = (v_1, \ldots, v_n) \in F_2^n$. Se tiene que:*

$$\phi_v(a) = \begin{cases} 1, & \textit{si } v \leq a, \\ 0, & \textit{en caso contrario.} \end{cases}$$

Demostración. Sea $a \in F_2^n$.

Si $v \leq a$, entonces $v_i \leq a_i$. Por lo tanto, $\text{sop}(v) \subset \text{sop}(a)$. Y, en consecuencia $X_i(a) = 1$ para cada $i \in \text{sop}(v)$.

En caso contrario, existe al menos una coordenada i para la que $v_i > a_i$. Para que se cumple esta desigualdad es necesario que $v_i = 1$ y $a_i = 0$. Por tanto, $i \in \text{sop}(v)$. Y, tenemos que $X_i(a) = 0$. □

Ahora, podemos dar la expresión de un sistema a partir de los X_i.

Teorema 2.21. *Sea $\phi \in L_N$ un sistema binario. Se tiene que:*

$$\phi = \bigvee_{v \in C_\phi^1} \phi_v.$$

Demostración. Llamemos ψ a la nueva expresión $\psi = \bigvee_{v \in C_\phi^1} \phi_v$. Queremos ver que $\psi = \phi$.

1) Sea $a \in C_\phi^1$, veamos que $\psi(a) = 1$.

Tenemos que $\psi \geq \phi_v$ para todo $v \in C_\phi^1$. Como $\phi_a(a) = 1$ se tiene que $\psi(a) = 1$.

0)Sea $a \in C_\phi^0$, veamos que $\psi(a) = 0$.

Basta con ver que $\phi_v(a) = 0$ para todo $v \in C_\phi^1$. Supongamos que existe $v \in C_\phi^1$ tal que $\phi_v(a) = 1$. Entonces, se tendría que $v \leq a$. Y, como ϕ es monótona, $\phi(a) = 1$. Lo cual es absurdo, pues habíamos supuesto que $a \in C_\phi^0$. □

Ejemplo 2.22. Tomemos el sistema $\phi_{2,3}$. Sus caminos son

$$C_\phi^1 = \{(1,1,0),(1,0,1),(0,1,1),(1,1,1)\}.$$

Por lo tanto, su construcción a través de X_i es:

$$\phi_{2,3} = (X_1 \wedge X_2) \vee (X_1 \wedge X_3) \vee (X_2 \wedge X_3) \vee (X_1 \wedge X_2 \wedge X_3).$$

Podemos observar que el último término no es necesario. Esto es porque su estado no pertenece al conjunto de generadores de caminos G_ϕ^1.

$$\phi_{2,3} = (X_1 \wedge X_2) \vee (X_1 \wedge X_3) \vee (X_2 \wedge X_3).$$

El retículo de sistemas binarios tiene aún más propiedades especiales.

Definición 2.23. Un retículo $(L, \vee, \wedge)$ es distributivo si se cumplen las siguientes ecuaciones para todo $a, b, c \in L$:

1. $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.
2. $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$.

Proposición 2.24. *El retículo de sistemas binarios L_n es distributivo.*

Demostración. Mostramos dos estrategias de demostración diferentes.

a) Podemos realizar la demostración mediante fuerza bruta. Sean $\phi, \psi \in L_n$ y $a \in F_2^n$. Tenemos que $(\phi \vee \psi)(a) = \phi(a) \vee \psi(a)$ y $(\phi \wedge \psi)(a) = \phi(a) \wedge \psi(a)$. Como $\phi(a), \psi(a) \in F_2$. Si las ecuaciones 1,2 se cumplen en F_2, entonces también se cumplen en L_n.

F_2 tiene una cantidad finita de elementos, luego es posible comprobar que todas las combinaciones de valores de a, b, c cumplen ambas ecuaciones. Esto equivale a realizar 16 cálculos simples.

Se dejan estos cálculos como ejercicio al lector.

b) L_n es un subrretículo de $F_2^{2^n}$. Por tanto, si las ecuaciones 1,2 se cumplen en $F_2^{2^n}$ también se cumplirán en L_n.

Recordemos que se pueden identificar los subconjuntos de F_2^n con las aplicaciones $F_2^n \to \{0,1\} = F_2$ con la siguiente aplicación:

$$\begin{aligned} \mathcal{P}(F_2^n) &\longrightarrow F_2 \\ S &\longmapsto f_S(a) = \begin{cases} 1, & \text{si } a \in S, \\ 0, & \text{si } a \notin S. \end{cases} \end{aligned}$$

En este caso se llama a f_S la función indicatriz del conjunto S.

Es fácil ver que si $S, T \subset F_2^n$ entonces $f_S \vee f_G = f_{S \cup G}$ y $f_S \wedge f_G = f_{S \cap G}$. Además, como esta identificación es biyectiva, genera un isomorfismo de retículos.

Se sabe que las operaciones $\cup, \cap$ sobre los conjuntos cumplen las ecuaciones 1,2. Por lo tanto, también se cumplen en F_2^n.

□

Observación 2.25. Se llama retículo booleano a un retículo con máximo y mínimo en el cual cada elemento a tiene un único complementario $\bar{a}$ que cumple:

$$a \wedge \bar{a} = 0, \qquad a \vee \bar{a} = 1.$$

El complementario de un elemento, generaliza el concepto de complementariedad de conjuntos. De hecho, se puede ver en [1, Thm. 5.5] que todo retículo booleano finito es isomorfo a un álgebra de conjuntos. Es decir, que si L es un retículo booleano finito, existe un conjunto S tal que L es isomorfo como retículo a $\mathcal{P}(S)$.

En el caso infinito el resultado es más débil. En lugar de ser L isomorfo a $\mathcal{P}(S)$, es isomorfo a un subrretículo $L' \subset \mathcal{P}(S)$.

Se tiene que $F_2^{2^n}$ es un retículo booleano, pero L_n no lo es. Pues, pese a que una función ϕ sea monótona, $\bar{\phi}$ no tiene por qué serlo.

2.3. Cotas de sistemas binarios

En este retículo, hay dos elementos de especial importancia.

Definición 2.26. Sea L un retículo. Si existe, $1 \in L$ es el (único) máximo de L si $1 \geq a$ para todo $a \in L$.

Análogamente, si existe, $0 \in L$ es el (único) mínimo de L si $0 \leq a$ para todo $a \in L$.

Proposición 2.27. *Si L admite un máximo, para todo $a \in L$ se tiene:*

$$a \vee 1 = 1, \quad a \wedge 1 = a.$$

Análogamente, si L admite un mínimo, para todo $a \in L$ se tiene:

$$a \vee 0 = a, \quad a \wedge 0 = 0.$$

Ejemplo 2.28. El retículo F_2^n admite un máximo y un mínimo. Estos son:

$$1 = (1, 1, \ldots), \quad 0 = (0, 0, \ldots).$$

Además, L_n también admite máximo y mínimo. Estos son los sistemas triviales:

$$1 = \phi_1, \quad 0 = \phi_0.$$

Ejemplo 2.29. El retículo $\mathbb{R}$ carece de máximos o mínimos.

Sin embargo, como vimos en el ejemplo 1.10. Se puede extender $\mathbb{R}$ a la recta real extendida $\mathbb{R} \cup (-\infty, +\infty)$. Esta sí que tiene tanto máximo como mínimo. Estos son $+\infty, -\infty$.

Desde este punto de vista podemos obtener cotas para el comportamiento de los sistemas binarios.

Proposición 2.30. *Sea ϕ un sistema binario de orden n. Si ϕ no es trivial, entonces $\phi(1) = 1$ y $\phi(0) = 0$.*

Demostración. ϕ no es trivial, es decir, no es una función constante. Luego existen $a, b \in F_2^n$ tales que $\phi(a) \neq \phi(b)$. Como ϕ solo puede tomar dos valores, escogemos, sin pérdida de generalidad, que $\phi(a) = 0$ y $\phi(b) = 1$.

Al ser ϕ monótona, $0 \leq a$ implica $\phi(0) \leq \phi(a)$. Por lo que $\phi(0) = 0$.

Análogamente, $b \leq 1$ implica $\phi(b) \leq \phi(1)$. Por lo que $\phi(1) = 1$. □

La siguiente proposición muestra que el conjunto de sistemas binarios no triviales, $L_n \setminus \{0, 1\}$, tiene máximo y mínimo.

Proposición 2.31. *Sea ϕ un sistema binario no trivial de orden n. Entonces se cumple:*

$$\phi_{n,n} \leq \phi \leq \phi_{1,n}.$$

Demostración. Sea $a \in F_2^n$.

$\leq$) Si $\phi_{n,n}(a) = 0$, entonces $\phi_{n,n}(a) \leq \phi(a)$ trivialmente.

Por otro lado, si $\phi_{n,n}(a) = 1$, entonces $a = 1$. Y, como hemos visto en la anterior proposición, $\phi(1) = 1$.

$\geq$) Análogamente, si $\phi_{1,n}(a) = 1$ entonces $\phi(a) \leq \phi_{1,n}(a)$.

Y, si $\phi_{1,n}(a) = 0$, entonces $a = 0$, por lo que $\phi(0) = 0$. □

La siguiente desigualdad compara el comportamiento de un sistema binario, es decir, de una aplicación monótona, con el de un homomorfismo de retículo. Además, caracteriza cuándo las aplicaciones monótonas de F_2^n a F_2 son homomorfismos de retículos.

Proposición 2.32. *Sea ϕ un sistema binario de orden n. Se tiene para todo $a, b \in F_2^n$:*

1. $\phi(a \vee b) \geq \phi(a) \vee \phi(b)$.

2. $\phi(a \wedge b) \leq \phi(a) \wedge \phi(b)$.

Además, $\phi_{1,n}$ es el único sistema coherente que alcanza esta cota.

Demostración.

1) Como se tiene que $a \vee b \geq a, b$ y ϕ es monótona, también se tiene que $\phi(a \vee b) \geq \phi(a), \phi(b)$.

Por lo que $\phi(a \vee b) \geq \sup(\{\phi(a), \phi(b)\}) = \phi(a) \vee \phi(b)$.

2) Este caso es análogo al anterior.

$\phi_{1,n}$**)** Un simple cálculo permite demostrar que $\phi_{1,n}$ alcanza esta cota.

$$\phi_{1,n}(a \vee b) = \bigvee_{i=1}^{n}(a_i \vee b_i) = (\bigvee_{i=1}^{n} a_i) \vee (\bigvee_{i=1}^{n} b_i) = \phi_{1,n}(a) \vee \phi_{1,n}(b),$$

$$\phi_{1,n}(a \wedge b) = \bigwedge_{i=1}^{n}(a_i \wedge b_i) = (\bigwedge_{i=1}^{n} a_i) \wedge (\bigwedge_{i=1}^{n} b_i) = \phi_{1,n}(a) \wedge \phi_{1,n}(b).$$

Sea ϕ cualquier otro sistema binario coherente que cumpla ambas igualdades. Veamos que $\phi = \phi_{1,n}$.

Como el sistema es coherente, la primera coordenada es relevante. Es decir, existe $v \in F_2^n$ con $\phi(s_1(v, 1)) = 1$ y $\phi(s_1(v, 0)) = 0$.

Pero, se tiene que, si $x \in F_2$

$$s_1(v, x) = s_1(v, 0) \vee s_1(0, x).$$

Por lo que al aplicar la igualdad, tenemos que:

$$x = \phi(s_1(v, x)) = \phi(s_1(v, 0) \vee s_1(0, x)) = \phi(s_1(v, 0)) \vee \phi(s_1(0, x)).$$

Por lo tanto:

$$x = \phi(s_1(0, x)).$$

Luego $X_1 \leq \phi$ y $\phi = \phi \vee X_1$.

Podemos realizar este mismo proceso con $v_2, v_3, \ldots$ hasta llegar a:

$$\phi = \phi \vee \bigvee_{i=1}^{n} X_i = \bigvee_{i=1}^{n} X_i = \phi_{1,n}.$$

□

A partir de esta última cota podemos proporcionar una estructura extra al conjunto de caminos y cortes.

Proposición 2.33. *Sea ϕ un sistema binario de orden n. Entonces $(C_\phi^0, \wedge)$ y $(C_\phi^1, \vee)$ son semirretículos.*

Demostración.

C_ϕ^0) Queremos ver que $(C_\phi^0, \wedge)$ es un semirretículo. Esto equivale a ver que si x, y son dos cortes del sistema, $x \wedge y$ también lo es.

Por la segunda desigualdad de la Proposición 2.32 tenemos que:

$$\phi(x \wedge y) \leq \phi(x) \wedge \phi(y) = 0 \wedge 0 = 0.$$

Y, por tanto, $\phi(x \wedge y) = 0$. Por lo que $x \wedge y \in C_\phi^0$.

C_ϕ^1) Queremos ver que $(C_\phi^1, \vee)$ es un semirretículo. Al igual que en el caso anterior, veremos que si x, y son dos caminos del sistema, $x \vee y$ también lo es.

Por la primera desigualdad de la Proposición 2.32 tenemos que:

$$\phi(x \vee y) \geq \phi(x) \vee \phi(y) = 1 \vee 1 = 1.$$

Y, por tanto, $\phi(x \vee y) = 1$. Por lo que $x \vee y \in C_\phi^1$.

□

Observación 2.34. En los sistemas multiestado se define el conjunto de i-caminos como $C_\phi^i = \{a \in F_2^n : \phi(a) \leq i\}$, de esta forma no se pierde la estructura de semirretículo.

2.4. Fiabilidad

La fiabilidad de un sistema informa de la probabilidad de que esté funcionando.

Definición 2.35. Sea ϕ un sistema binario de orden n y sea P una probabilidad sobre F_2^n. Se define la fiabilidad de ϕ dado P como:

$$h_P(\phi) = E[\phi(X)],$$

donde E denota la esperanza matemática.

Observación 2.36. F_2^n tiene un número finito de elementos, por lo tanto, todos sus subconjuntos son medibles. Por esta razón, $\phi : F_2^n \to F_2$ es trivialmente medible y su esperanza matemática está bien definida.

Observación 2.37. Tenemos que $E[\phi(X)] = 1 \cdot P(\phi(X) = 1) + 0 \cdot P(\phi(X) = 0) = P(\phi(X) = 1)$. Por lo que la fiabilidad de un sistema es la probabilidad de que este esté en funcionamiento.

Como nuestro espacio es finito, si conocemos P se puede calcular la fiabilidad de un sistema mediante técnicas de fuerza bruta.

Ejemplo 2.38. Calculemos la fiabilidad de $\phi_{2,3}$ de forma manual con probabilidad uniforme $P(a) = \frac{1}{8}$.

$$h_P(\phi) = P(\phi(X) = 1) = \frac{4}{8} = \frac{1}{2},$$

pues de los 2^3 casos totales el sistema funciona en 4 de ellos.

Ejemplo 2.39. Supongamos que tanto $\phi(a)$ como $P(a)$ son difíciles de computar. Por ejemplo:

$$\phi(a) = a_1 \vee (a_2 \wedge ((a_3 \wedge a_4) \vee (a_5 \wedge a_6))),$$
$$P(a) = \prod_i (\frac{1}{i+1})^{a_i}.$$

En tal caso, si se escoge un algoritmo de fuerza bruta, habría que calcular 2^n valores de ϕ. Y, para aquellos que sean caminos, también habría que calcular P. Esto es inviable para sistemas con muchos componentes.

Ejemplo 2.40. Para simplificar los cálculos, se suele suponer que las diferentes componentes son independientes e igualmente distribuidas. Pero, incluso así el cálculo teórico de la fiabilidad puede ser difícil.

Supongamos que la probabilidad de que cada componente funcione es p y que estamos tratando con un sistema $\phi_{k,n}$. En dicho caso, la probabilidad de un estado es $P(a) = p^{\|a\|}(1-p)^{n-\|a\|}$ donde $\|a\|$ es el número de componentes de a en funcionamiento..

En tal caso, basta con sumar las aportaciones de todos los estados con $\|a\| \geq k$:

$$h_P(\phi_{k,n}) = \sum_{m=k}^{n} \binom{n}{m} p^m (1-p)^{n-m}.$$

Tomemos $k = 2, n = 4, p = \frac{1}{3}$.

$$\begin{aligned} h_P(\phi_{2,4}) &= \sum_{m=2}^{4} \binom{4}{m} (\frac{1}{3})^m (\frac{2}{3})^{4-m} = \\ &= \binom{4}{2} (\frac{1}{3})^2 (\frac{2}{3})^2 + \binom{4}{3} (\frac{1}{3})^3 (\frac{2}{3})^1 + \binom{4}{4} (\frac{1}{3})^4 (\frac{2}{3})^0 = \\ &= 6\frac{4}{81} + 4\frac{2}{81} + \frac{1}{81} = \frac{24+8+1}{81} = \frac{33}{81} = \frac{11}{27}. \end{aligned}$$

Dada la dificultad de calcular la fiabilidad, se suele recurrir a acotarla. Para esto es necesario recurrir a la estructura de retículo de $\mathbb{R}$, teniendo en cuenta que si $p, q \in [0,1] \subset \mathbb{R}$ representan probabilidades, entonces $p \vee q, p \wedge q \in [0,1] \subset \mathbb{R}$ también representan probabilidades.

Proposición 2.41. *Sean $\phi, \psi \in L_n$ sistemas binarios y sea P una probabilidad sobre F_2^n. Se tiene que*

1. $h_P(\phi \vee \psi) \geq h_P(\phi) \vee h_P(\psi)$.
2. $h_P(\phi \wedge \psi) \leq h_P(\phi) \wedge h_P(\psi)$.

Demostración. Sea f un sistema binario. Como $h_P(f) = P(f(X) = 1)$. Se tiene que $h_P(f) = P(C_f^1)$. Recordemos que la probabilidad es una aplicación monótona de $(\mathcal{P}(F_2^n), \subset)$ a $(\mathbb{R}, \leq)$, es decir, que si $A \subset B$ entonces $P(A) \leq P(B)$.

1) Tenemos que $\phi \vee \psi \geq \phi, \psi$. Sea $a \in F_2^n$. Si $\phi(a) = 1$ ó $\psi(a) = 1$ entonces $\phi(a) \vee \psi(a) = 1$. Por tanto, $C_\phi^1, C_\psi^1 \subset C_{\phi \vee \psi}^1$.

En consecuencia, se tiene que $P(C_\phi^1), P(C_\psi^1) \leq P(C_{\phi \vee \psi}^1)$. Lo cual implica $P(C_\phi^1) \vee P(C_\psi^1) \leq P(C_{\phi \vee \psi}^1)$, que era lo que queríamos demostrar.

2) Análogamente, $\phi \wedge \psi \leq \phi, \psi$. Sea $a \in F_2^n$. Si $\phi(a) \vee \psi(a) = 1$ entonces $\phi(a) = 1$ ó $\psi(a) = 1$. Por tanto, $C_{\phi \wedge \psi}^1 \subset C_\phi^1, C_\psi^1$.

En consecuencia, se tiene que $P(C_{\phi \wedge \psi}^1) \leq P(C_\phi^1), P(C_\psi^1)$. Lo cual implica $P(C_{\phi \wedge \psi}^1) \leq P(C_\phi^1) \wedge P(C_\psi^1)$, que era lo que queríamos demostrar.

□

Capítulo 3

Ideales y sistemas binarios

En este capítulo exploraremos el papel del álgebra conmutativa en la combinatoria algebraica. Para ello, comenzamos construyendo ideales monomiales a partir de sistemas binarios [9]. A continuación, analizaremos estos ideales con mayor profundidad [4]. Esto permitirá aplicar el álgebra combinatoria al estudio de la fiabilidad.

3.1. Correspondencia entre caminos y monomios

Vamos a asociar a cada sistema binario un objeto algebraico, en concreto un ideal monomial.

Para ello, utilizamos una técnica habitual en combinatoria, consistente en codificar la información de un objeto en el exponente de un monomio (véase, por ejemplo, [2] para un tratamiento analítico de esta idea).

Definición 3.1. Un *monomio* en $\mathbb{R}[x_1, \ldots, x_n]$ es una expresión de la forma:

$$x^{\bar{a}} = \prod_i x_i^{a_i}$$

donde $\bar{a} = (a_1, \ldots, a_n) \in \mathbb{N}^n$. Se dice que $\bar{a}$ es el exponente del monomio.

Denotamos por $\mathcal{N}_n$ al conjunto de monomios en n variables.

Observación 3.2. A partir de este punto denotaremos a vectores mediante una barra. De forma que $\bar{a}_i$ denota el i-ésimo vector de una lista, mientras que a_i denota la i-ésima componente de un vector. Con esta notación, se representaría a la j-ésima componente del i-ésimo vector de una lista como $a_{i,j}$.

La multiplicación de monomios se traduce en la suma de exponentes:

$$x^{\bar{a}} \cdot x^{\bar{b}} = x^{\bar{a}+\bar{b}}.$$

Esta ley algebraica nos permite establecer una equivalencia entre la relación de orden de los monomios y la de los exponentes.

Definición 3.3. $\mathcal{N}_n$ tiene la relación de orden de *divisivilidad*. $x^{\bar{a}} \leq x^{\bar{b}}$ si existe $w \in \mathcal{N}_n$ tal que $x^{\bar{b}} = wx^{\bar{a}}$. En este caso denotamos $x^{\bar{a}} \mid x^{\bar{b}}$.

Por otro lado, $\mathbb{N}^n$ tiene la relación de orden por *coordenadas*. Es decir, $\bar{a} \leq \bar{b}$ si y solo si $a_i \leq b_i \quad \forall i$.

Proposición 3.4. *Sean $x^{\bar{a}}, x^{\bar{b}}$ dos monomios. Se tiene que $x^{\bar{a}} \leq x^{\bar{b}}$ si y solo si $\bar{a} \leq \bar{b}$.*

Demostración.

$\Rightarrow$) Supongamos que $x^{\bar{a}} \leq x^{\bar{b}}$. Entonces existe $w \in \mathcal{N}_n$ con $x^{\bar{b}} = wx^{a}$. Escribiendo $w = x^{\bar{c}}$, con $\bar{c} \in \mathbb{N}^n$, se obtiene:

$$x^{\bar{b}} = x^{\bar{c}}x^{\bar{a}} = x^{\bar{c}+\bar{a}}.$$

Por tanto, $\bar{b} = \bar{a} + \bar{c}$. Lo que implica $\bar{a} \leq \bar{b}$.

$\Leftarrow$) Supongamos ahora que $\bar{a} \leq \bar{b}$. Entonces $\bar{b} - \bar{a} \in \mathbb{N}^n$ y, por tanto, es un exponente válido. Por lo que podemos tomar su monomio asociado $w = x^{\bar{b}-\bar{a}}$.

Para este monomio se tiene que:

$$wx^{\bar{a}} = x^{\bar{b}-\bar{a}}x^{\bar{a}} = x^{\bar{b}}.$$

Luego, $x^{\bar{a}} \leq x^{\bar{b}}$. □

A partir de los conceptos de caminos, monomios, y minimalidad ya definidos, podemos construir la correspondencia clave: asignar a cada sistema binario un ideal monomial.

El primer paso consiste en asociar a cada estado de un sistema un monomio. De forma que la estructura algebraica del ideal refleje la estructura combinatoria del sistema.

Definición 3.5. A cada estado $\bar{a} = (a_1, \ldots, a_n)$ de un sistema binario ϕ de orden n se le puede asignar un monomio mediante la siguiente aplicación.

$$\begin{aligned} \Psi_n : F_2^n &\longrightarrow \mathcal{N}_n \subset \mathbb{R}[x_1, \ldots, x_n] \\ \bar{a} &\longmapsto x^{\bar{a}} \end{aligned}$$

Definición 3.6. El ideal de caminos de un sistema binario ϕ de orden n , denotado por I_ϕ se define como:[1]

$$I_\phi = \langle \Psi_n(C_\phi^1) \rangle.$$

Ejemplo 3.7. Tomemos el sistema de orden 2, $\phi(x_1, x_2) = x_1 \wedge x_2$. Tiene como conjunto de caminos $C_\phi^1 = \{(1,1)\}$. Luego, su ideal asociado es

$$I_\phi = \langle \Psi_2((1,1)) \rangle = \langle x_1 x_2 \rangle.$$

No son necesarios todos los caminos del sistema para generar el ideal. Es suficiente el conjunto mínimo de generadores G_ϕ^1 definido en 2.13.

Proposición 3.8. *Dado un sistema binario ϕ de orden n, se tiene que $I_\phi = \langle \Psi_n(G_\phi^1) \rangle$.*

Demostración. Sea $\bar{a} \in C_\phi^1$ un camino cualquiera. Si $\bar{a} \in G_\phi^1$. Entonces, $x^{\bar{a}} \in \langle \Psi_n(G_\phi^1) \rangle$.

Al contrario, si $\bar{a} \notin G_\phi^1$, existe un $\bar{b} \in G_\phi^1$ con $\bar{b} \leq \bar{a}$. Como $x^{\bar{b}} \mid x^{\bar{a}}$, se concluye que $x^{\bar{a}} \in \langle \Psi_n(G_\phi^1) \rangle$. □

Ejemplo 3.9. Si tomamos el sistema $\phi(x_1, x_2) = x_1 \vee x_2$ veremos que sus caminos son $\{(1,0), (0,1), (1,1)\}$. De estos solo $(1,0)$ y $(0,1)$ son caminos minimales, pues $(1,1) \geq (1,0), (0,1)$.

Al aplicar Ψ_2 se transforman en $\{x_1, x_2, x_1x_2\}$. Por lo tanto $I_\phi = \langle x_1, x_2, x_1x_2 \rangle$. Donde vemos que $x_1x_2 \in \langle x_1, x_2 \rangle$ por lo que era un generador innecesario.

3.2. Ideales monomiales

Los ideales asociados a sistemas resultan ser ideales monomiales, una clase con propiedades computacionales muy favorables. Aunque no profundizaremos aquí en dichos aspectos algorítmicos, sí exploraremos su estructura algebraica. Además, en el caso de los sistemas binarios, son además ideales monomiales libres de cuadrados.

Definición 3.10. $I \subset \mathbb{R}[x_1, \ldots, x_n]$ es un ideal monomial si está generado por monomios: $I = \langle x^{\bar{a}_1}, \ldots, x^{\bar{a}_m} \rangle$.

$\mathbb{R}[x_1, \ldots, x_n]$ es un $\mathbb{R}$-espacio vectorial de dimensión infinita. Su base canónica son los monomios $\mathcal{N}_n$. Es posible obtener un resultado análogo para los ideales monomiales.

[1] Recordemos que el ideal generado por un conjunto S es el mínimo ideal que contiene a S y se denota por $\langle S \rangle$.

Definición 3.11. El conjunto de monomios de un ideal I se denota como $\mathcal{N}_I = \mathcal{N} \cap I$.

Proposición 3.12. *Si $I \subset \mathbb{R}[x_1, \ldots, x_n]$ es un ideal monomial. El conjunto $\mathcal{N}_I$ forma una base de I como $\mathbb{R}$-espacio vectorial.*

Demostración. Dado que los monomios forman una base de $\mathbb{R}[x_1, \ldots, x_n]$, basta ver que $\mathcal{N}_I$ genera I como $\mathbb{R}$-espacio vectorial..

Si $I = \langle x^{\bar{a}_1}, \ldots, x^{\bar{a}_m} \rangle$, cualquier $f \in I$ puede escribirse como

$$f = \sum_{i=1}^{m} f_i x^{\bar{a}_i}, \quad f_i \in \mathbb{R}[x_1, \ldots, x_n].$$

Descomponiendo cada f_i en monomios, obtenemos que f es combinación lineal de monomios de la forma $x^{\bar{a}_i} g$, que pertenecen a I, es decir, a $\mathcal{N}_I$.

Así, $\mathcal{N}_I$ genera I, y como sus elementos son linealmente independientes, forman una base. □

Esta propiedad permite verificar rápidamente si un polinomio está en el ideal. Basta con comprobar si sus monomios lo están.

De hecho, esta propiedad de verificación caracteriza totalmente a los ideales monomiales. El siguiente corolario y su definición auxiliar los demuestran.

Definición 3.13. Sea f un polinomio. Denotamos como $\mathrm{sop}(f)$ y llamamos soporte de f, al conjunto de monomios en los que se descompone f.

Ejemplo 3.14. Por ejemplo, la cuádrica $f = x^2 + xy + y^2$ tiene $\mathrm{sop}(f) = \{x^2, xy, y^2\}$.

Corolario 3.15. *Son equivalentes:*

1. *I es un ideal monomial.*
2. *Para $f \in \mathbb{R}[x_1, \ldots, x_n]$, se tiene que $f \in I \iff sop(f) \subset I$.*

Demostración.

$\Rightarrow$) Si I es monomial, entonces como espacio vectorial tiene por base a $\mathcal{N}_I$. Por tanto, un polinomio f pertenece a I si y solo si todos sus monomios están en $\mathcal{N}_I \subset I$, es decir, $\mathrm{sop}(f) \subset I$.

$\Leftarrow$) Supongamos que la condición sobre el soporte se cumple. Consideramos $\{f_1, \ldots, f_m\}$ un sistema de generadores de I. Para cada f_i, tenemos $\mathrm{sop}(f_i) \subset I$. Por lo que, f_i pertenece al ideal generado por su soporte: $f_i \in \langle \mathrm{sop}(f_i) \rangle$.

Sustituyendo cada f_i por los monomios de su soporte, obtenemos un sistema de generadores constituido únicamente por monomios. Así, I es un ideal monomial. □

3.3. Sistemas de generadores

Los ideales monomiales admiten una infinidad de sistemas generadores monomiales. Pues, si G es un sistema generador y g un monomio del ideal, entonces $G \cup \{g\}$ es otro sistema generador monomial. Sin embargo, existe un único sistema de generadores monomiales minimal. Lo construiremos en esta sección.

Lema 3.16. *Sea $\{u_1, \ldots, u_m\}$ un sistema de generadores monomiales del ideal I. Un monomio v pertenece a I si y solo si $\exists i, u_i \mid v$.*

Demostración.

$\Leftarrow$) Obvio.

$\Rightarrow$) Como v pertenece al ideal se puede expresar como:

$$v = \sum_i f_i u_i, \quad f_i \in \mathbb{R}[x_1, \ldots, x_n].$$

Aplicamos el operador soporte sobre esta expresión. Y vemos que:

$$\operatorname{sop}(v) = \operatorname{sop}(\sum_i f_i u_i) \subset \bigcup_i \operatorname{sop}(f_i u_i).$$

Y, como v es un monomio, se tiene que $v \in \bigcup_i \operatorname{sop}(f_i u_i)$. En concreto, $v \in \operatorname{sop}(f_i u_i)$ para algún u_i particular.

Ahora, expresando f_i como suma de monomios g_{ij}:

$$\operatorname{sop}(f_i u_i) = \operatorname{sop}(\sum_j g_{ij} u_i) \subset \bigcup_i \operatorname{sop}(g_{ij} u_i).$$

Por lo que se tiene que $v \in \operatorname{sop}(g_{ij} u_i)$. Lo cual es equivalente a $v = g_{ij} u_i$. Así que $u_i \mid v$.

□

Los sistemas de generadores monomiales de I son subconjuntos de $\mathcal{N}_I$. Por lo cual, al tratar con ellos usamos la relación de orden de contención de conjuntos. Es decir, $A \leq B$ si $A \subset B$. Buscamos el sistema de generadores mínimo bajo esta relación.

Proposición 3.17. *Cada ideal monomial I tiene un único sistema de generadores monomial minimal G_I.*

Demostración.

$\exists$) Sea $C_I \subset \mathbb{N}$ el conjunto de cardinalidades de sus sistemas generadores. Este conjunto no está vacío, pues por definición, I admite al menos un sistema de generadores finito.

Como $\mathbb{N}$ está bien ordenado, se tiene que C_I tiene un mínimo. Basta con coger un sistema de generadores que alcance dicho mínimo.

$\exists!$) Sean $G_1 = \{u_1, \ldots, u_m\}$ y $G_2 = \{v_1, \ldots, v_s\}$ dos sistemas generadores minimales.

Como $u_1 \in \langle G_2 \rangle$, por el anterior lema tenemos que $v_i \mid u_1$ para algún v_i. Pero, a su vez, existe un u_j tal que $u_j \mid v_i$, puesto que $v_i \in \langle G_1 \rangle$. Por transitividad, $u_j \mid u_1$.

Si $j \neq 1$, entonces $G_1 \setminus \{u_1\}$ es sistema de generadores. Por lo que G_1 no es minimal. Absurdo.

Si $j = 1$, se tiene que $u_1 \mid v_i$ y que $v_i \mid u_1$. Por lo cual $v_i = u_1$. Repetimos ahora este mismo procedimientos sobre u_2. Inductivamente, llegamos a $G_1 = G_2$ □

Como vimos en el ejemplo 1.5, los ideales de un anillo forman un retículo Este retículo se da con las operaciones $I \wedge J := I \cap J$,$I \vee J := \langle I \cup J \rangle = I + J$ y con la relación de orden de contención de conjuntos.

Los ideales monomiales heredan esta estructura de retículo, formando un subrretículo.

Proposición 3.18. *El conjunto de ideales monomiales forma un subrretículo del conjunto de ideales de* $\mathbb{R}[x_1, \ldots, x_n]$.

Demostración. Veamos que el conjunto de ideales monomiales está cerrado bajo $\wedge$ y $\vee$. En concreto, veamos que si I, J son ideales monomiales, entonces $I \cap J$ y $I + J$ también lo son.

Para esto construimos un nuevo sistema de generadores a partir de los de I, J. Sean $\{u_i\}$ los generadores r de I, y $\{v_j\}$ los s generadores de J.

$\wedge$) Sea g un monomio. Si $g \in I \cap J$, entonces $\exists i, j$, con $u_i \mid g, v_j \mid g$. Luego su mínimo común múltiplo (mcm) también lo divide. Como esto ocurre para todo $g \in I \cap J$, el sistema $\{\text{mcm}(u_i, v_j)\}$ genera $I \wedge J$.

$\vee$) Si f es un polinomio de $I + J$ entonces $f = \sum w_i v_i + \sum w_j v_j$. Por lo que $\{u_i, v_j\}$ genera $I \vee J$.

□

3.4. Ideal radical

Históricamente, el álgebra conmutativa tiene sus raíces en dos campos principales: la teoría de números y la geometría algebraica. Cada una de

ellas ofrece una perspectiva distinta sobre el concepto de radical de un ideal.

En teoría de números, los ideales surgieron como una extensión de la noción de número, introducidos por Kummer y Dedeking para restaurar la factorización única en anillos en los que esta propiedad fallaba. Así, los ideales primos desempeñan el papel de "factores elementales" y el radical de un ideal $\sqrt{I}$ puede entenderse como una generalización de los operadores $\sqrt[n]{}$, pero trasladados al lenguaje de los ideales. En contraste, en la geometría algebraica, los ideales radicales cumplen un papel geométrico fundamental. Allí, la correspondencia entre polinomios y curvas se generaliza a una correspondencia entre variedades e ideales radicales. De manera que estos últimos son considerados como "n-superficies" en el espacio.

Definición 3.19. Sea un ideal I de un anillo R. Se define su ideal radical $\sqrt{I}$ como:

$$\sqrt{I} = \{f \in A : \exists n \geq 1, f^n \in I\}.$$

Nótese que si $f \in I$ es un elemento del ideal, entonces todas sus raíces $\sqrt[2]{f}, \sqrt[3]{f}, \ldots$ pertenecen al ideal radical, siempre que estas existan en el anillo R. De esta forma, el ideal radical $\sqrt{I}$ contiene a todas sus raíces algebraicas".

Para demostrar que el radical de un ideal monomial también es monomial son necesarias algunas definiciones auxiliares. Estas permiten trabajar geométricamente con el conjunto de exponentes.

Definición 3.20. Sean $\{\bar{a}_i\}$ una familia de exponentes en $\mathbb{N}^n$. Se denota por $\langle \bar{a}_i \rangle$ y se llama politopo generado por $\{\bar{a}_i\}$ a:

$$\langle \bar{a}_i \rangle := \{\bar{b} \in \mathbb{N}^n : \bar{b} = \sum_i \lambda_i \bar{a}_i, \quad \lambda_i \in \mathbb{Q}, 0 \leq \lambda_i \leq 1\}.$$

Se dice que un generador $\bar{a}_j \in \{\bar{a}_i\}$ es un vértice si no pertenece a $\langle \bar{a}_i \rangle_{i \neq j}$,.

Los politopos generalizan a los polígonos y a los poliedros.

Proposición 3.21. *Si I es un ideal monomial, entonces $\sqrt{I}$ también es un ideal monomial.*

Demostración. Sea $f = \sum_i c_i x^{\bar{a}_i}$ un polinomio de $\sqrt{I}$. Existe $k \geq 0$ tal que $f^k \in I$. Como I es monomial, cada monomio de su soporte pertenece a I:

$$f^k = (\sum_i c_i x^{\bar{a}_i})^k = \sum_{k_1+\ldots+k_n}^{k} \binom{k}{k_1, \ldots, k_n} \prod_i^n (c_i x^{\bar{a}_i})^{k_i}.$$

Sea $x^{\bar{a}} \in \text{sop}(f)$. Supongamos que $k\bar{a}$ es un vértice de $\langle k\bar{a}_i \rangle$. Y, a su vez, supongamos que el término $(x^{\bar{a}})^k \notin \text{sop}(f)$ por cancelarse con otros términos en

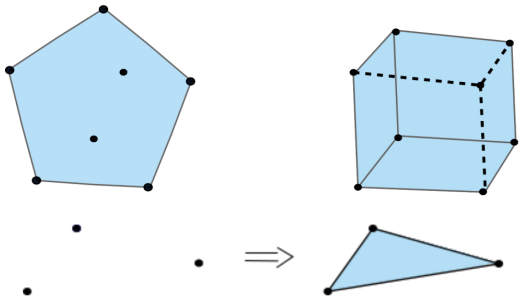

Figura 3.1: Ejemplos de politopos. Arriba-izquierda un pentágono, arriba-derecha un cubo, y abajo un triángulo. [10]

la anterior expresión. Decir que se cancela con otros términos es equivalente a decir: $x^{k\bar{a}} = (x^{\bar{a}_1})^{k_1} \dots (x^{\bar{a}_n})^{k_n}$ con $k = k_1 + \dots + k_n$.

Sin pérdida de generalidad, suponemos que $\bar{a} = \bar{a}_1$ y que $k \neq k_1$. Entonces:

$$(k - k_1)\bar{a}_1 = k_2\bar{a}_2 + \dots + k_n\bar{a}_n.$$

Por tanto:

$$\bar{a}_1 = \frac{k_2}{k - k_1}\bar{a}_2 + \dots + \frac{k_n}{k - k_1}\bar{a}_n, \qquad \frac{k_i}{k - k_1} \in [0, 1].$$

Lo cual es absurdo, pues $k\bar{a}_1$ es vértice. Por lo cual, si $k\bar{a}_1$ es vértice, entonces $x^{k\bar{a}_1} \in \text{sop}(f) \subset I$ y, por lo tanto, $x^{\bar{a}_1} \in \sqrt{I}$.

Por otra parte, si $\bar{a}$ no es vértice, se puede expresar como suma de vértices:

$$k\bar{a} = k_1(k\bar{a}_1) + \dots + k_n(k\bar{a}_n) \quad k_i \in [0, 1].$$

Que es a su vez producto de monomios: $x^{ka} = (x^{ka^1})^{k_1} \dots (x^{ka^n})^{k_n}$. Y, aplicando la raíz k-ésima, resulta $x^a = (x^{\bar{a}_1})^{k_1} \dots (x^{\bar{a}_n})^{k_n}$.

Como los $k_i \in \mathbb{Q}$ los podemos denotar por $k_i = \frac{p_i}{q_i}$. Ahora definimos $q = \prod_{i=1}^{n} q_i$, de forma que $qk_i \in \mathbb{Z}$. Elevando la ecuación a la potencia q-ésima obtenemos $x^{q\bar{a}} = (x^{\bar{a}_1})^{qk_1} \dots (x^{\bar{a}_n})^{qk_n}$.

Cada uno de los $x^{q\bar{a}_i}$ pertenece al ideal $\sqrt{I}$, pues sus exponentes son potencias de vértices. Luego, $x^{q\bar{a}}$ también lo hace por ser producto monomios del ideal. Y, $x^{\bar{a}} \in \sqrt{I}$ por ser raíz de $x^{q\bar{a}}$.

De esta forma, se ve que $\sqrt{I}$ es monomial. Pues si $f \in \sqrt{I}$, entonces $x^{\bar{a}} \in \text{sop}(f)$ también pertenece al ideal.

□

Durante la demostración de que los ideales monomiales forman un subrretículo, construimos un sistema de generadores explícitos para $I \vee J, I \wedge J$. Se puede realizar una construcción similar para el caso del ideal radical. Pero, esto requiere introducir un operador auxiliar sobre monomios que nos permita describir el nuevo sistema de generadores.

Definición 3.22. Sea $x^{\bar{a}}$ un monomio con exponente $\bar{a} = (a_1, \ldots, a_n)$ Se define su radical como:

$$\sqrt{x^{\bar{a}}} = \prod_{a_i \neq 0} x_i,$$

en otras palabras, $\sqrt{x^{\bar{a}}} = x^{\bar{b}}$ con exponente $\bar{b} = (b_1, \ldots, b_n)$ dado por:

$$b_i = \begin{cases} 1 & \text{si } a_i \geq 1, \\ 0 & \text{si } a_i = 0. \end{cases}$$

Proposición 3.23. *Si I es un ideal monomial generado por $\{u_i\}$. Entonces el ideal radical $\sqrt{I}$ está generado por $\{\sqrt{u_i}\}$*

Demostración. Dividimos la demostración en dos pasos.

1) Cada $\sqrt{u_i}$ pertenece a $\sqrt{I}$

Sea $u_i = x^{\bar{a}}$ con exponente $\bar{a} = (a_1, \ldots, a_n)$ y $\sqrt{u_i} = x^{\bar{b}}$. Definimos $k = \max_j a_j$. Consideremos $x^{k\bar{b}} = (\sqrt{u_i})^k$. Para cada coordenada j:

- Si $a_j \geq 1$, entonces $b_j = 1$ y $kb_j = k \geq a_j$.
- Si $a_j = 0$, entonces $b_j = 0$ y por tanto $a_j = kb_j = 0$.

De aquí se deduce que $\bar{a} \leq k\bar{b}$, es decir, $x^{\bar{a}} \mid x^{k\bar{b}}$. Como $x^{\bar{a}} = u_i \in I$, se concluye que $x^{k\bar{b}} \in I$, y por definición $x^{\bar{b}} = \sqrt{u_i} \in \sqrt{I}$.

2) Los $\{\sqrt{u_i}\}$ generan todo $\sqrt{I}$.

Sea $v = x^{\bar{c}} \in \sqrt{I}$ un monomio cualquiera. Entonces $v^k \in I$ para algún $k \geq 1$. En particular, existe un $u_i = x^{\bar{a}}$ tal que $u_i \mid v^k$, es decir, $v^k = x^{\bar{d}} u_i$ para algún monomio $x^{\bar{d}}$. Esto es:

$$x^{k\bar{c}} = x^{\bar{d}} x^{\bar{a}} = x^{\bar{d}+\bar{a}}.$$

Igualando los exponentes:

$$k\bar{c} = \bar{d} + \bar{a}.$$

Analizando por coordenadas:

- Si $a_j \geq 1$, necesariamente $c_j \geq 1$, de modo que $c_j \geq b_j$.

- Si $a_j = 0$, entonces $b_j = 0$ y se tiene trivialmente $c_j \geq b_j$.

Así, $\bar{c} \geq \bar{b}$, lo que implica $x^{\bar{b}} \mid x^{\bar{c}}$. En consecuencia, $\sqrt{u_i}$ divide a v, y por tanto v pertenece al ideal generado por los $\sqrt{u_i}$.

Esto prueba que $\sqrt{I} = \langle \sqrt{u_i} \rangle$. □

Es posible distinguir los ideales monomiales radicales de los que no lo son a partir de sus sistemas de generadores. En efecto, un ideal monomial es radical si y solo si puede generarse mediante monomios "radicales", es decir, libres de cuadrados.

Definición 3.24. Sea $x^{\bar{a}}$ un monomio con exponente $\bar{a} = (a_1, \ldots, a_n) \in \mathbb{N}^n$. Decimos que $x^{\bar{a}}$ es libre de cuadrados si $\bar{a} \leq 1$, es decir, si $a_i = 0$ ó 1 para todo $i \in \{1, \ldots, n\}$.

Nótese que $\sqrt{v}$ es libre de cuadrados para cualquier monomio v.

Definición 3.25. Un ideal monomial es libre de cuadrados si admite un sistema de generadores formados únicamente por monomios libres de cuadrados.

Proposición 3.26. *Sea I un ideal monomial. Entonces:*

$$I = \sqrt{I} \iff I \text{ es libre de cuadrados.}$$

Demostración.

⇒) Supongamos que $I = \sqrt{I}$. Si $\{u_i\}$ es un sistema de generadores de I, entonces, por la proposición anterior, I también está generado por $\{\sqrt{u_i}\}$ que son libres de cuadrados.

⇐) Supongamos ahora que I es libre de cuadrados, generado por $\{u_i\}$ libres de cuadrados. Como vimos, $\sqrt{I}$ está generado por $\{\sqrt{u_i}\}$. Pero, al ser los u_i libres de cuadrados, se cumple $u_i = \sqrt{u_i}$. Por lo tanto, $I = \sqrt{I}$. □

Veamos ahora que los sistemas binarios generan ideales libres de cuadrados.

Proposición 3.27. *Sea ϕ un sistema binario de orden n. I_ϕ es un ideal monomial libre de cuadrados.*

Demostración. Recordemos que $I_\phi := \langle \Psi_n(C^1_\phi) \rangle$ y que, si $\bar{a} \in F_2^n$ es un estado, $\Psi_n(\bar{a}) = x^{\bar{a}}$.

Se tiene que $1 = (1, \ldots, 1)$ es el máximo de F_2^n, luego todo $\bar{a} \in F_2^n$ cumple $\bar{a} \leq 1$. Por tanto, $x^{\bar{a}}$ es libre de cuadrados. □

Capítulo 4

K-polinomios y fiabilidad

Los ideales monomiales admiten una estructura de módulo graduado sobre $\mathbb{K}[x_1, \ldots, x_n]$ [9] . A partir de esta estructura se pueden construir invariantes algebraicos como la serie de Hilbert y el K-polinomio[9, 8].

Cuando el ideal proviene de un sistema binario, dichos invariantes pueden emplearse para estudiar propiedades de fiabilidad del sistema. En particular, el K–polinomio proporciona cotas para la función de fiabilidad asociada [9, 7].

4.1. Módulos

La estructura de módulo sobre un anillo R generaliza el concepto de espacio vectorial sobre un cuerpo $\mathbb{K}$. Además, los ideales también poseen esta estructura.

Cómo sería de esperar, un módulo se define de forma análoga a un espacio vectorial.

Definición 4.1. Sea R un anillo conmutativo con unidad 1. Un R-módulo es un grupo abeliano $(M, +)$ junto con una aplicación

$$R \times M \longrightarrow M,$$

$$(r, x) \longmapsto rx,$$

llamada acción escalar, que satisface para todo $r, s \in R$ y $x, y \in M$:

1. $r(x + y) = rx + ry$.
2. $(r + s)x = rx + sx$.
3. $(rs)x = r(sx)$.

4. $1x = x$.

Al visitar los primeros ejemplos de módulos encontraremos construcciones análogas a las realizadas para construir espacios vectoriales.

Ejemplo 4.2. Si $\mathbb{K}$ es un cuerpo, entonces $\mathbb{K}^n$ es un espacio vectorial con las operaciones:

$$k(x_1, \ldots, x_n) = (kx_1, \ldots, kx_n),$$
$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n).$$

Estas mismas operaciones se pueden extender a R^n cuando R es un anillo. De esta forma, cuando $R = \mathbb{Z}$, $\mathbb{Z}^n$ es un módulo sobre $\mathbb{Z}$.

Ejemplo 4.3. Sea S un conjunto. El conjunto de aplicaciones de S a R, denotado por R^S es un módulo. Pues, si $f, g \in R^S$, $r \in R$, $s \in S$, se puede definir:

$$(rf)(s) = rf(s),$$
$$(f + g)(s) = f(s) + g(s).$$

A este módulo se le da el nombre de módulo de funciones sobre S.

Proposición 4.4. *Todo ideal I de un anillo R es un módulo sobre R.*

Demostración. El ideal hereda las operaciones de R.

Como $(I, +)$ es un subgrupo abeliano de $(R, +)$, y $rI \subseteq I$ para todo $r \in R$ por la definición de ideal, basta notar que la acción $R \times I \to I$, $(r, x) \mapsto rx$, es la restricción de la multiplicación de R, la cual ya satisface los axiomas de módulo. □

Observación 4.5. En el campo del álgebra no conmutativa los ideales se definen como subconjuntos $I \subset R$ que, con las operaciones heredadas de este, son módulos sobre R.

Sin embargo, como R es un anillo no conmutativo, se distingue entre dos tipos de módulos: por la izquierda, $(r, x) \mapsto r \cdot x$; y por la derecha, $(r, x) \mapsto x \cdot r$. Por lo tanto, esta noción de lateralidad también se extiende a ideales.

Ejemplo 4.6. En particular, si $I \subset \mathbb{R}[x_1, \ldots, x_n]$ es un ideal monomial, es un módulo sobre $\mathbb{R}[x_1, \ldots, x_n]$.

Los módulos pierden algunas propiedades al generalizar los espacios vectoriales a anillos. Una de las más importantes es la de las bases. Pues, todo espacio vectorial admite una base, pero no todo módulo la admite.

A continuación, veremos la subclase de módulos que sí admite una base.

Definición 4.7. Dado un módulo M sobre un anillo R, se dice que un conjunto $L \subset M$ es linealmente independiente si $0 = \sum_{i=1}^{m} \lambda_i l_i, \quad \lambda_i \in R, l_i \in L$ implica que $\lambda_i = 0$ para todo i.

Se dice que un conjunto $G \subset M$ es un sistema de generadores si el mínimo módulo que lo contiene, $\langle G \rangle$, es M.

Se dice que M es un módulo libre si admite un sistema de generadores $B \subset M$ que es a su vez linealmente independiente.

Ejemplo 4.8. En $\mathbb{R}[x, y]$ el ideal $I = \langle x, y \rangle$ no es libre, pues $\{x, y\}$ no son linealmente independientes. Existe una combinación lineal $(y) \cdot x + (-x) \cdot y = 0$.

Definición 4.9. Sea R un anillo y M un módulo. Se dice que M está finitamente generado si existe un conjunto finito $G \subset M$ tal que $M = \langle G \rangle$.

Ejemplo 4.10. Sea $I = \langle xyz \rangle \subset \mathbb{R}[x, y, z]$. I tiene estructura de módulo sobre $\mathbb{R}[x, y, z]$. Como tal, I está finitamente generado, pues si $p \in I$ entonces $p = q(xyz)$ con $q \in \mathbb{R}[x, y, z]$.

Sin embargo, I también tiene estructura de módulo sobre $\mathbb{R}$. Como tal, I no está finitamente generado. El conjunto $\{x^n yz\} \subset I$ es infinito y linealmente independiente sobre $\mathbb{R}$.

En efecto, que un módulo esté finitamente generado depende de en qué anillo vivan sus coeficientes.

Las obstrucciones que impiden que un módulo M sea libre pueden proporcionar mucha información sobre este módulo. La siguiente definición codifica estas obstrucciones en objetos.

Definición 4.11. Sea $M = \langle G \rangle$ un módulo sobre R, generado por un sistema $G = \{g_1, \ldots, g_n\}$. Una sizigia es un vector $s = (s_1, \ldots, s_n) \in R^n$ tal que:

$$\sum_i s_i g_i = 0.$$

El conjunto de sizigias se denota $\mathrm{Syz}(G)$.

Proposición 4.12. *Si M es un módulo sobre R generado por G. El conjunto $Syz(G)$ también es un módulo sobre R.*

Demostración. Como $\mathrm{Syz}(G)$ es un subconjunto de R^n, basta comprobar que es cerrado bajo suma y multiplicación escalar.

+) Sea $x, y \in \mathrm{Syz}(M_G)$ con $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n)$. Veamos que $x + y \in \mathrm{Syz}(M_G)$:

$$\sum_i (x_i + y_i)g_i = \sum_i x_i g_i + \sum_i y_i g_i = 0 + 0 = 0.$$

·) Sean $x \in \mathrm{Syz}(M_G), r \in R$. Veamos que $rx \in \mathrm{Syz}(M_G)$:

$$\sum_i (rx_i)g_i = r\sum_i x_i g_i = r0 = 0.$$

□

Ejemplo 4.13. En el ejemplo 4.8 vimos que $(y, -x)$ es una sizigia de $\langle x, y\rangle$. De hecho, $\mathrm{Syz}(\{x, y\}) = \langle (y, -x)\rangle$.

Como módulo $\mathrm{Syz}(\{x, y\})$ podría tener a su vez sizigias. Pero, como está generado por un único elemento, y su anillo $R = \mathbb{R}[x_1, \ldots, x_n]$ es un dominio de integridad, esto es imposible. $\mathrm{Syz}(\{(y, -x)\}) = \{0\}$.

Los morfismos de módulos son aplicaciones lineales, al igual que en el caso vectorial.

Definición 4.14. Una aplicación $f : M \to N$ entre dos módulos sobre R es homomorfismo de R-módulos si es lineal. Es decir, si para todo $r, s \in R$ y $x, y \in M$ se tiene que:

$$f(rx + sy) = rf(x) + sf(y).$$

Ejemplo 4.15. Definimos el homomorfismo de módulos sobre $\mathbb{R}[x, y]$:

$$\langle x, y\rangle \longrightarrow \langle x, y\rangle$$

$$rx + sy \longmapsto ry + sx$$

Al igual que en el caso de espacios vectoriales, esta aplicación se puede representar mediante una matriz:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Ejemplo 4.16. En el caso de módulos que no son libres, una matriz no siempre representa una aplicación lineal bien definida. Por ejemplo, sean los módulos $\langle x, y\rangle, \langle 1\rangle \subset \mathbb{R}[x, y]$.

La matriz $\begin{pmatrix} 1 & 1 \end{pmatrix}$ no representa ninguna aplicación lineal. Supongamos que lo hiciera:

$$f : \langle x, y\rangle \longrightarrow \langle 1\rangle$$

$$rx + sy \longmapsto rf(x) + sf(y) = r + s$$

Calculemos $f(xy)$ de dos formas distintas:

$$f(xy) = xf(y) = x,$$

$$f(xy) = yf(x) = y,$$

lo que es absurdo, pues $x \neq y$.

Los submódulos toman rol similar al de los subespacios vectoriales en el álgebra lineal.

Definición 4.17. Sea M un módulo sobre R. Un subconjunto $N \subset M$ es un submódulo de M si está cerrado bajo sumas y productos por elementos de R.

Ejemplo 4.18. El conjunto $\{(r, r, r) : r \in \mathbb{Z}\}$ es un submódulo de $\mathbb{Z}^3$.

Ejemplo 4.19. $\langle x \rangle$ es un submódulo de $\langle x, y \rangle \subset \mathbb{R}[x, y]$. Obsérvese que $\langle x \rangle$ es libre pese a $\langle x, y \rangle$ no serlo.

4.2. Módulos graduados

La noción de anillo graduado generaliza la idea del grado de un polinomio.

Definición 4.20. Sea $(R, +, \cdot)$ un anillo. Se dice que R es graduado si se puede descomponer de la forma:

$$R = \bigoplus_{k \in \mathbb{N}} R_k$$

donde:

1. R_k son subgrupos aditivos de R,
2. se tiene que $R_k \cdot R_q \subset R_{k+q}$.

Definición 4.21. Sea R un anillo graduado y $r \in R$. Como $R = \bigoplus_{k \in \mathbb{N}} R_k$ se puede expresar r como una suma finita:

$$r = \sum_{k \in \mathbb{N}} r_k, \quad r_k \in R_k,$$

donde solo un número finito de r_k no son nulos.

En tal caso, se define su proyección k-ésima como $\pi_k(r) = r_k$. Además, se llama el soporte de r a:

$$\text{sop}(r) = \{k \in \mathbb{N} : \pi_k(r) \neq 0\}.$$

Como el soporte de r es un conjunto finito, es posible definir el grado y el cograd de r:

$$\deg(r) = \sup(\text{sop}(r)), \qquad \text{codeg}(r) = \text{ínf}(\text{sop}(r)).$$

Ejemplo 4.22. Sea R un anillo, entonces $R[x]$ es un anillo graduado. En efecto, si definimos:

$$R[x]_k = \{rx^k : r \in R\}.$$

Se tiene que $R[x] = \bigoplus_{k\in\mathbb{N}} R[x]_k$ y que $R_k \cdot R_q \subset R_{k+q}$, puesto que si $r, s \in R$ se tiene que $(rx^k) \cdot (sx^q) = (rs)x^{k+q}$.

En consecuencia, cada polinomio p se puede descomponer como $\sum_{k\in\text{sop}(p)} r_k x^k$.

Por ejemplo, si $p = x^3 + 2x^2 + 3x$ entonces se tiene que:

$$\text{sop}(p) = \{1, 2, 3\}, \quad \deg(p) = 3, \quad \text{codeg}(p) = 1.$$

Ejemplo 4.23. El anterior ejemplo se puede extender al caso de polinomios de varias variables $R[x_1, \ldots, x_n]$. Para esto definimos la 1-norma de los exponentes:

$$|(v_1, \ldots, v_n)| = v_1 + \ldots + v_n.$$

A partir de ella, se puede descomponer $R[x_1, \ldots, x_n]$ como:

$$R[x_1, \ldots, x_n]_k = \{\sum_{|v|=k} r_{\bar{v}} x^{\bar{v}} : r_{\bar{v}} \in R\}.$$

Por lo tanto, se tendría que $R[x_1, \ldots, x_n] = \bigoplus_{k\in\mathbb{N}} R[x_1, \ldots, x_n]_k$ y que $R[x_1, \ldots, x_n]_k \cdot R[x_1, \ldots, x_n]_q \subset R[x_1, \ldots, x_n]_{k+q}$. Pues sí $r, s \in R$ y $\bar{v}, \bar{w} \in \mathbb{Z}^n$ se tiene que $(rx^{\bar{v}})(sx^{\bar{w}}) = (rs)x^{\bar{v}+\bar{w}}$ con $|\bar{v} + \bar{w}| = |\bar{v}| + |\bar{w}|$.

Por ejemplo, si $p = 2xy^2 + 3x^2y + 7x$ en $R[x, y]$ se tiene que:

$$\text{sop}(p) = \{1, 3\}, \quad \deg(p) = 3, \quad \text{codeg}(p) = 1, \quad \pi_1(p) = 7x, \quad \pi_3(p) = 2xy^2 + 3x^2y.$$

A partir de un anillo graduado se puede definir un módulo graduado.

Definición 4.24. Sea R un anillo graduado y M un módulo sobre R. Se dice que M es graduado si se puede descomponer como:

$$M = \bigoplus_{k\in\mathbb{N}} M_k$$

donde:

1. M_k son subgrupos aditivos de M,
2. se tiene que $R_q \cdot M_k \subset M_{q+k}$.

Los ideales monomiales son módulos graduados.

Proposición 4.25. *Sea $I = \langle x^{\bar{a}_1}, \ldots, x^{\bar{a}_n}\rangle \subset \mathbb{R}[x_1, \ldots, x_m]$ un ideal monomial. I tiene estructura de módulo graduado sobre $\mathbb{R}[x_1, \ldots, x_m]$.*

Demostración. Definimos $I_k = I \cap \mathbb{R}[x_1, \ldots, x_m]_k = \{rx^{\bar{v}} \in I : |\bar{v}| = k\}$. Y veamos que $I = \bigoplus_{k\in\mathbb{N}} I_k$ es un módulo graduado.

Si $rx^{\bar{v}}, sx^{\bar{w}} \in I_i$ se tiene que $rx^{\bar{v}} + sx^{\bar{w}} \in I$ por ser el ideal cerrado por sumas. Además, $rx^{\bar{v}} + sx^{\bar{w}} \subset \mathbb{R}[x_1, \ldots, x_m]_k$ por ser este un subgrupo. En consecuencia, $rx^{\bar{v}} + sx^{\bar{w}} \in I_k$, lo que significa que I_k es un subgrupo aditivo de I.

Sea $rx^{\bar{v}} \in \mathbb{R}[x_1, \ldots, x_m]_k$ un monomio y sea $sx^{\bar{w}} \in I_q$ otro monomio del ideal. Se tiene que $(rx^{\bar{v}})(sx^{\bar{w}}) = (rs)x^{\bar{v}+\bar{w}}$ es un monomio de $\mathbb{R}[x_1, \ldots, x_m]_{k+q}$ y además pertenece al ideal, pues es cerrado por productos por elementos de $\mathbb{R}[x_1, \ldots, x_m]$. Por lo que $\mathbb{R}[x_1, \ldots, x_m]_k \cdot I_q \subset I_{k+q}$.

Por último, veamos que se da la igualdad $I = \bigoplus_{k\in\mathbb{N}} I_k$. Como $I \supset \bigoplus_{k\in\mathbb{N}} I_k$ es obvio, solo es necesario demostrar $I \subset \bigoplus_{k\in\mathbb{N}} I_k$.

Sea $p \in I$ un polinomio. Puede ser descompuesto en monomios:

$$p = \sum_{k\in \mathrm{sop}(p)} \pi_k(p), \quad \pi_k(p) \in \mathbb{R}[x_1, \ldots, x_m]_k.$$

Como I es monomial, por el corolario 3.15, los monomios $\pi_k(p)$ también pertenecen al ideal. Por consecuente:

$$p = \sum_{k\in \mathrm{sop}(p)} \pi_k(p), \quad \pi_k(p) \in I \cap \mathbb{R}[x_1, \ldots, x_m]_k = I_k.$$

□

Observación 4.26. Es posible generalizar los ideales monomiales a través de la estructura de módulo graduado.

Sea $R = \bigoplus_{k\in\mathbb{N}} R_k$ un anillo graduado. Se dice que un ideal $I \subset R$ es homogéneo si se cumple que la descomposición:

$$I = \bigoplus_{k\in\mathbb{N}} I_k, \quad I_k := I \cap R_k,$$

le otorga estructura de módulo graduado sobre R.

Además, se dice que un elemento $r \in R$ es homogéneo si $r \in R_k$ para algún $k \in \mathbb{N}$.

Al igual que en los ideales monomiales, se cumple que un ideal es homogéneo si y solo si se puede generar por elementos homogéneos.

Definición 4.27. Sea R un anillo graduado y M, N dos módulos graduados sobre R. La aplicación $\phi : M \to N$ es un homomorfismo de módulos graduados de grado $d \in \mathbb{N}$ si:

1. ϕ es lineal.
2. Se tiene que $\phi(M_k) \subset N_{k+d}$.

Ejemplo 4.28. Sea $I = \langle xy, yz\rangle$ un ideal monomial del anillo $\mathbb{R}[x, y, z]$. La familia de aplicaciones:

$$\phi_n : I \longrightarrow I$$
$$p \longmapsto x^n \cdot p$$

Cada ϕ_n es un homomorfismo de módulos graduados de grado n.

4.2.1. Módulos multigraduados

Al igual que los anillos graduados generalizan el anillo de polinomios $R[x]$, los anillos multigraduados generalizan el anillo de polinomios en varias variables $R[x_1, \ldots, x_n]$.

Definición 4.29. Sea $(R, +, \cdot)$ un anillo. Se dice que R es multigraduado si se puede descomponer de la forma:

$$R = \bigoplus_{\bar{v}\in\mathbb{N}^n} R_{\bar{v}}$$

donde:

1. $R_{\bar{v}}$ son subgrupos aditivos de R,

2. se tiene que $R_{\bar{v}} \cdot R_{\bar{w}} \subset R_{\bar{v}+\bar{w}}$.

Definición 4.30. Sea R un anillo graduado y $r \in R$. Como $R = \bigoplus_{\bar{v}\in\mathbb{N}^n} R_{\bar{v}}$ se puede expresar r como una suma finita:

$$r = \sum_{\bar{v}\in\mathbb{N}^n} r_{\bar{v}}, \quad r_{\bar{v}} \in R_{\bar{v}},$$

donde solo un número finito de $r_{\bar{v}}$ son no nulos.

En tal caso, se define su proyección $\bar{v}$-ésima como $\pi_{\bar{v}}(r) = r_{\bar{v}}$. Además, se llama el soporte de r a:

$$\operatorname{sop}(r) = \{\bar{v} \in \mathbb{N}^n : \pi_{\bar{v}}(r) \neq 0\}.$$

Ejemplo 4.31. Sea R un anillo, entonces $R[x_1, \ldots, x_n]$ es un anillo multigraduado. En efecto, si definimos:

$$R[x_1, \ldots, x_n]_{\bar{v}} = \{rx^{\bar{v}} : r \in R\}$$

Se tiene que $R[x] = \bigoplus_{\bar{b}\in\mathbb{N}^n} R[x]_{\bar{v}}$ y que $R_{\bar{v}} \cdot R_{\bar{w}} \subset R_{\bar{v}+\bar{w}}$, puesto que si $r, s \in R$ se tiene que $(rx^{\bar{v}}) \cdot (sx^{\bar{w}}) = (rs)x^{\bar{v}+\bar{w}}$.

En consecuencia, cada polinomio p se puede descomponer como $\sum_{\bar{v}\in\operatorname{sop}(p)} r_{\bar{v}}x^{\bar{v}}$.

Por ejemplo, si $p = 2xy^2 + 3x^2y + 7x$ en $R[x, y]$ se tiene que:

$$\operatorname{sop}(p) = \{(1,2),(2,1),(1,0)\}, \quad \pi_{(1,2)}(p) = 3x^2y, \quad \pi_{(2,1)}(p) = 2xy, \quad \pi_{(1,0)}(p) = 7x.$$

De forma análoga a los módulos graduados, se pueden definir los módulos multigraduados.

Definición 4.32. Sea R un anillo multigraduado y M un módulo sobre R. Se dice que M es multigraduado si se puede descomponer como:

$$M = \bigoplus_{\bar{v}\in\mathbb{N}^n} M_{\bar{v}}$$

donde:

1. $M_{\bar{v}}$ son subgrupos aditivos de M,

2. se tiene que $R_{\bar{v}} \cdot M_{\bar{w}} \subset M_{\bar{v}+\bar{w}}$.

.

Ejemplo 4.33. Sea $R = \mathbb{R}[x_1, \ldots, x_n]$. Siguiendo el ejemplo 4.23 se puede definir una graduación en R como:

$$R[x_1, \ldots, x_n]_k = \{\sum_{|v|=k} r_{\bar{v}} x^{\bar{v}} : r_{\bar{v}} \in R\}.$$

Esta graduación se puede extender a una multigraduación en el módulo R^m, de forma que tenemos:

$$R^m = \bigoplus_{\bar{v} \in \mathbb{N}^m} R^m_{\bar{v}}$$

con $R^m_{\bar{v}}$ definido como:

$$R^m_{\bar{v}} = R_{v_1} \oplus \ldots \oplus R_{v_m}.$$

Por ejemplo, en el caso R^3 tenemos que el vector $(x, xy, xyz) \in R^3_{(1,2,3)}$.

La siguiente proposición se demuestra de forma análoga al caso graduado 4.25 .

Proposición 4.34. *Sea $I = \langle x^{\bar{a}_1}, \ldots, x^{\bar{a}_n} \rangle \subset \mathbb{R}[x_1, \ldots, x_m]$ un ideal monomial. I tiene estructura de módulo multigraduado sobre $\mathbb{R}[x_1, \ldots, x_m]$.*

Observación 4.35. Al igual que en el caso graduado, I hereda la graduación de $\mathbb{R}[x_1, \ldots, x_m]$, es decir:

$$I_{\bar{v}} = I \cap \mathbb{R}[x_1, \ldots, x_m]_{\bar{v}} = \{r x^{\bar{v}} : r \in \mathbb{R}\}.$$

4.3. Serie de Hilbert

La serie de Hilbert de un módulo graduado almacena información de su estructura graduada. En concreto, sus coeficientes almacenan la dimensión de los espacios en los que se descompone.

Para poder definirla, es necesario definir previamente el anillo de series formales, que extiende al anillo de polinomios.

Definición 4.36. Sea $\mathbb{K}$ un cuerpo. Denotamos por $\mathbb{K}[[x_1, \ldots, x_n]]$ al anillo de series formales sobre $\mathbb{K}$ en n variables. Este conjunto se define como:

$$\mathbb{K}[[x_1, \ldots, x_n]] = \{f : \mathbb{N}^n \to \mathbb{K}\}.$$

Su suma es la suma usual de funciones:

$$(f + g)(\bar{v}) = f(\bar{v}) + g(\bar{v}),$$

mientras que su producto de funciones es el producto de convolución:

$$(f \cdot g)(\bar{v}) = \sum_{\bar{a}+\bar{b}=\bar{v}} f(\bar{a}) \cdot g(\bar{b}).$$

Una serie formal f se denota como:

$$\sum_{\bar{v}\in\mathbb{N}^n} f(\bar{v})x^{\bar{v}}.$$

Observación 4.37. Su definición es análoga a la de los polinomios en varias variables. La única diferencia es que al definir polinomios se pide que la función sea nula siempre salvo en una cantidad finita de valores.

En concreto, una consecuencia es que $\mathbb{K}[x_1, \ldots, x_n] \subset \mathbb{K}[[x_1, \ldots, x_n]]$.

Observación 4.38. La serie formal $\sum_{n\in\mathbb{N}} x^n = 1 + x + x^2 + \ldots$ del anillo $\mathbb{R}[[x]]$ tiene como inversa la serie $1 - x$. Puesto que:

$$(\sum_{n\in\mathbb{N}} x^n)(1-x) = \sum_{n\in\mathbb{N}} x^n - \sum_{n\in\mathbb{N}} x^{n+1} = 1.$$

Durante el desarrollo de las series de Hilbert aparecerá el término:

$$\frac{1}{1-x} = \sum_{n\in\mathbb{N}} x^n, \qquad (1-x) = \frac{1}{\sum\limits_{n\in\mathbb{N}} x^n}.$$

A partir de esta noción es posible definir la serie de Hilbert. Esta puede verse como aplicación $\mathbb{N}^n \to \mathbb{N}$ ó como serie formal. En su definición daremos una notación diferente a cada una de estas dos perspectivas.

Definición 4.39. Sea $M = \bigoplus_{k\in\mathbb{N}} M_k$ un módulo graduado sobre $\mathbb{R}[x_1, \ldots, x_n]$. Su función de Hilbert es:

$$HF_M : \mathbb{N} \longrightarrow \mathbb{R}$$
$$k \longmapsto \dim_{\mathbb{R}}(M_k)$$

donde $\dim_{\mathbb{R}}(M_k)$ denota la dimensión de M_k como $\mathbb{R}$-espacio vectorial.

Asociamos a la función de Hilbert, la serie de Hilbert, que se define como:

$$HS_M(x) = \sum_{n\geq 0} HF_M(k)x^k.$$

Análogamente, si $M = \bigoplus_{\bar{v}\in\mathbb{N}^n} M_{\bar{v}}$ es multigraduado, se define su función Hilbert multigraduada:

$$HF_M : \mathbb{N}^n \longrightarrow \mathbb{R}$$

$$\bar{v} \longmapsto \dim_{\mathbb{R}}(M_{\bar{v}})$$

y su serie de Hilbert multigraduada:

$$HS_M(x_1, \ldots, x_n) = \sum_{\bar{v} \geq 0} HF_M(\bar{v}) x^{\bar{v}}.$$

Los siguientes ejemplos muestran cómo calcular la serie de Hilbert de algunos ideales monomiales.

Ejemplo 4.40. Tomemos el ideal monomial $I = \langle x \rangle$ sobre el anillo $\mathbb{R}[x]$. Entonces se tiene que:

$$I = \langle x \rangle_{\mathbb{R}} + \langle x^2 \rangle_{\mathbb{R}} + \ldots$$

donde $\langle v \rangle_{\mathbb{R}}$ denota el $\mathbb{R}$-subespacio vectorial generado por $\bar{v}$.

En consecuencia, su función de Hilbert es:

$$HF_I(k) = \begin{cases} 1, & \text{si } k \geq 1, \\ 0, & \text{si } k = 0. \end{cases}$$

Y su serie de Hilbert:

$$HS_I(x) = \sum_{k \geq 1} x^k.$$

Ejemplo 4.41. Tomemos el ideal monomial $I = \langle x, y \rangle$ sobre el anillo $\mathbb{R}[x, y]$. Entonces se tiene que:

$$I = \langle x, y \rangle_{\mathbb{R}} + \langle x^2, xy, y^2 \rangle_{\mathbb{R}} + \langle x^3, x^2y, xy^2, y^3 \rangle_{\mathbb{R}} + \ldots$$

Se pueden construir $k+1$ monomios de grado k en I. Estos son $x^k, x^{k-1}y, x^{k-2}y^2$, $\ldots, xy^{k-1}, y^k$. Por lo tanto, la función de Hilbert del ideal I es:

$$HF_I(k) = \begin{cases} k+1, & \text{si } k \geq 1, \\ 0, & \text{si } k = 0. \end{cases}$$

Y su función de Hilbert:

$$HS_I(x) = \sum_{k \geq 1} (k+1) x^k.$$

Ejemplo 4.42. Sea $I = \langle x, y\rangle$ ideal monomial del anillo $\mathbb{R}[x, y]$. I se descompone como:

$$I = \langle x\rangle_{\mathbb{R}} + \langle y\rangle_{\mathbb{R}} + \langle x^2\rangle_{\mathbb{R}} + \langle xy\rangle_{\mathbb{R}} + \langle y^2\rangle_{\mathbb{R}} + \dots$$

Por lo que su función de Hilbert multigraduada será:

$$HF_I(\bar{v}) = \begin{cases} 1, & \text{si } \bar{v} \geq 1, \\ 0, & \text{en caso contrario.} \end{cases}$$

Y su serie de Hilbert:

$$HS_I(x, y) = \sum_{a+b\geq 1} x^a y^b.$$

Como podemos observar, esta no coincide con su serie de Hilbert.

Los K-polinomios permiten representar la información de las series de Hilbert de forma más compacta. Para definirlo, será necesario recurrir al anillo de series formales en el que viven las series de Hilbert.

Definición 4.43. Sea M un $\mathbb{R}[x_1, \dots, x_n]$ módulo graduado. Se define su K-polinomio como:

$$K_M(x) = HS_M(x)(1 - x)^n.$$

Y, en caso de que M sea multigraduado se define como:

$$K_M(x_1, \dots, x_n) = HS_M(x_1, \dots, x_n) \prod_{i=1}^{n} (1 - x_i).$$

Observación 4.44. Despejando en la definición de K-polinomio se tiene que:

$$HS_M(x_1, \dots, x_n) = \frac{K_M(x_1, \dots, x_n)}{\prod_{i=1}^{n}(1 - x_i)}.$$

Así que el K-polinomio se puede interpretar como el numerador de la serie de Hilbert.

Los siguientes ejemplos muestran el cálculo del K-polinomio de un ideal monomial.

Ejemplo 4.45. Sea $I = \langle x\rangle$ ideal monomial del anillo $\mathbb{R}[x]$. En ejemplos anteriores hemos calculado su serie de Hilbert:

$$HS_I(x) = \sum_{k\geq 1} x^k.$$

Calculemos su K-polinomio:

$$K_I(x) = (\sum_{k\geq 1} x^k)(1-x) = \sum_{k\geq 1} x^k - \sum_{k\geq 1} x^{k+1}.$$

Realizando un cambio de índice en el segundo sumatorio:

$$\sum_{k\geq 1} x^k - \sum_{k\geq 2} x^k = x.$$

Ejemplo 4.46. Sea $I = \langle x, y\rangle$ ideal monomial del anillo $\mathbb{R}[x, y]$. En ejemplos anteriores hemos calculado su serie de Hilbert:

$$HS_I(x) = \sum_{k\geq 1}(k+1)x^k.$$

Por lo que su K-polinomio es:

$$(\sum_{k\geq 1}(k+1)x^k)(1-x)^2 = (\sum_{k\geq 1}(k+1)x^k - \sum_{k\geq 1}(k+1)x^{k+1})(1-x).$$

Realizamos la primera multiplicación:

$$(\sum_{k\geq 1}(k+1)x^n)(1-x) = \sum_{k\geq 1}(k+1)x^n - \sum_{k\geq 1}(k+1)x^{k+1}.$$

Realizando un cambio de índice en el segundo sumatorio.

$$\sum_{k\geq 1}(k+1)x^k - \sum_{k\geq 2} kx^k = 2x + \sum_{k\geq 2} x^k.$$

Realizando la segunda multiplicación:

$$(2x + \sum_{k\geq 2} x^k)(1-x) = 2x + \sum_{k\geq 2} x^k - 2x^2 - \sum_{k\geq 2} x^{k+1}.$$

Y, con otro cambio de índice:

$$2x + \sum_{k\geq 2} x^k - 2x^2 - \sum_{k\geq 3} x^k = 2x - x^2.$$

Ejemplo 4.47. Sea $I = \langle x, y\rangle$ el ideal monomial del anillo $\mathbb{R}[x, y]$. En ejemplos anteriores hemos calculado su serie de Hilbert multigraduada:

$$HS_I(x, y) = \sum_{a+b\geq 1} x^a y^b.$$

Por lo que su K-polinomio multigraduado es:

$$K_I(x,y) = (\sum_{a+b\geq 1} x^a y^b)(1-x)(1-y).$$

Para simplificar el cálculo, usamos la igualdad:

$$\sum_{a+b\geq 1} x^a y^b = (\sum_{a\geq 1} x^a)(\sum_{b\geq 1} y^b) + \sum_{c\geq 1} x^c + \sum_{d\geq 1} y^d.$$

Recordemos de los anteriores ejemplos que:

$$(\sum_{k\geq 1} x^k)(1-x) = x.$$

Por tanto, cada sumando del producto sería:

$$(\sum_{a\geq 1} x^a)(\sum_{b\geq 1} y^b)(1-x)(1-y) = (\sum_{a\geq 1} x^a)(1-x)(\sum_{b\geq 1} y^b)(1-y) = xy,$$

$$(\sum_{c\geq 1} x^c)(1-x)(1-y) = x(1-y) = x - xy,$$

$$(\sum_{d\geq 1} y^d)(1-x)(1-y) = (\sum_{d\geq 1} y^d)(1-y)(1-x) = y(1-x) = y - xy.$$

Sumándolos:

$$K_I(x,y) = xy + x - xy + y - xy = x + y - xy.$$

Ejemplo 4.48. Sea $I\langle x, yz\rangle$ en $\mathbb{R}[x,y,z]$. Su serie de Hilbert multigraduada es:

$$HS_I = x\sum_{a,b,c} x^a y^b z^c + yz\sum_{d,e} y^d z^e.$$

Y su K-polinomio:

$$K_I = HS_I(1-x)(1-y)(1-z).$$

Como su serie de Hilbert tiene dos términos, realizamos el producto en dos partes:

$$x(\sum_{a,b,c} x^a y^b z^c)(1-x)(1-y)(1-z.)$$

Si tenemos en cuenta que

$$\sum_{a,b,c} x^a y^b z^c = (\sum x^a)(\sum y^b)(\sum z^c),$$

y que

$$(\sum x^k)(1-x) = 1,$$

se tiene que

$$x(\sum_{a,b,c} x^a y^b z^c)(1-x)(1-y)(1-z) = x(\sum x^a)(\sum y^b)(\sum z^c)(1-x)(1-y)(1-z) = x.$$

De forma análoga, podemos realizar el cómputo del otro término

$$yz(\sum_{d,e} y^d z^e)(1-x)(1-y)(1-z) = yz(\sum y^d)(\sum z^e)(1-x)(1-y)(1-z) = yz(1-x).$$

Juntando estos dos sumandos:

$$K_I(x,y,z) = x + yz - yzx.$$

4.4. Cotas para la fiabilidad

Las cotas de la fiabilidad se obtienen truncando el K-polinomio del ideal. Sin embargo, el método de truncamiento no es el usual. Para introducirlo es necesario introducir antes un método simple para obtener el K-polinomio del ideal.[11]

Teorema 4.49. *Sea I un ideal monomial de $\mathbb{R}[x_1, \ldots, x_n]$ y G_I su conjunto minimal de generadores. Se tiene que:*

$$K_I = \sum_{J \subset G_I} (-1)^{|J|} MCM(J),$$

donde MCM representa el mínimo común múltiplo y $|J|$ la cardinalidad del conjunto J.

Observación 4.50. Esta fórmula resulta práctica para sistemas de tamaño reducido, aunque el crecimiento exponencial del número de subconjuntos la hace poco eficiente en casos generales. En la literatura se emplean resoluciones graduadas mínimas para calcular el K-polinomio del ideal, ya que permiten un cálculo más estructurado y están estrechamente relacionadas con la teoría homológica.

Comprobemos este teorema con un ejemplo.

Ejemplo 4.51. Tomemos el ideal $I = \langle x, y\rangle$ de $\mathbb{R}[x, y]$. En el anterior ejemplo calculamos su K-polinomio:

$$K_I(x, y) = x + y - xy.$$

Veamos que obtenemos el mismo resultado utilizando la fórmula del teorema.

Su conjunto minimal de generadores es $G_I = \{x, y\}$. De este conjunto se pueden obtener tres subconjuntos no nulos:

$$J_1 = \{x\}, \qquad J_2 = \{y\}, \qquad J_3 = \{x, y\}.$$

Aplicando ahora la fórmula del teorema:

$$K_I(x, y) = (-1)^{|J_1|}\text{MCM}(J_1)+(-1)^{|J_2|}\text{MCM}(J_2)+(-1)^{|J_3|}\text{MCM}(J_3) = x+y-xy,$$

como esperábamos.

Definición 4.52. Sea $m \in \mathbb{N}$, I un ideal monomial de $\mathbb{R}[x_1, \ldots, x_n]$ y $K_I = \sum_{J\subset G_I}(-1)^{|J|}\text{MCM}(J)$ su K-polinomio. Se define el K-polinomio truncado en orden m como:

$$K_{I,m} = \sum_{J\subset G_I, |J|\leq m} (-1)^{|J|}\text{MCM}(J).$$

Ejemplo 4.53. Continuemos con el anterior ejemplo. Teníamos que:

$$K_I(x, y) = x + y - xy.$$

Por lo tanto, sus truncamientos son:

$$K_{I,0}(x, y) = 0, \qquad K_{I,1}(x, y) = x + y, \qquad K_{I,2}(x, y) = x + y - xy.$$

Llegado este punto ya estamos preparados para enunciar el teorema.

Teorema 4.54. *Sea ϕ un sistema binario de orden n y P una probabilidad sobre F_2^n. Si las componentes son independientes con probabilidad p_i se tiene que:*

$$K_{I_\phi,m}(p_1, \ldots, p_n) \leq h_P(\phi), \qquad \textit{si } m \textit{ es par.}$$
$$K_{I_\phi,m}(p_1, \ldots, p_n) \geq h_P(\phi), \qquad \textit{si } m \textit{ es impar.}$$

Corolario 4.55. *Sea ϕ un sistema binario de orden n y P una probabilidad sobre F_2^n. Si las componentes son independientes con probabilidad p_i se tiene que:*

$$K_{I_\phi,m}(p_1, \ldots, p_n) = h_P(\phi).$$

Demostración. Tenemos que:

$$K_I = \sum_{J \subset G_I} (-1)^{|J|} \text{MCM}(J),$$

y que:

$$K_{I,m} = \sum_{J \subset G_I, |J| \leq m} (-1)^{|J|} \text{MCM}(J).$$

Como G_I es finito, podemos tomar $m \geq |G_I|$. En tal caso, se cumple para todos los $J \subset G_I$ que $|J| \leq m$. Y, en consecuencia, todos los términos que aparecen en el sumatorio de $K_{I,m}$ aparecen también en el de K_I. Por lo que $K_I = K_{I,m}$ si $m \geq |G_I|$.

Supongamos sin pérdida de generalidad que m es par. Entonces, al aplicar el anterior teorema tenemos que:

$$K_I(p_1, \ldots, p_n) = K_{I,m}(p_1, \ldots, p_n) \leq h_P(\phi).$$

Aplicando ahora el teorema a $m+1$, que es impar:

$$K_I(p_1, \ldots, p_n) = K_{I,m+1}(p_1, \ldots, p_n) \geq h_P(\phi).$$

Por lo que se puede concluir que:

$$K_I(p_1, \ldots, p_n) = h_P(\phi).$$

□

A continuación, veamos algunos ejemplos:

Ejemplo 4.56. Sea $\phi_{1,2} = \phi(x, y) = x \vee y$ sistema binario de orden dos. Su conjunto de caminos es:

$$C_\phi^1 = \{(1,0), (0,1), (1,1)\}.$$

De los cuales, solo $G_\phi^1 = \{(1,0), (0,1)\}$ son minimales. Por lo tanto, su ideal monomial es:

$$I_\phi = \langle \Psi(G_\phi^1) \rangle = \langle x, y \rangle.$$

Ya habíamos calculado su K-polinomio en los anteriores ejemplos.

$$K_{I_\phi} = x + y - xy.$$

Sus truncamientos serían:

$$MT_0(K_{I_\phi}) = 0, \qquad MT_1(K_{I_\phi}) = x + y, \qquad MT_2(K_{I_\phi}) = x + y - xy.$$

Podemos calcular su fiabilidad manualmente:

$$h_P(\phi) = p_1(1-p_2) + (1-p_1)p_2 + p_1p_2.$$

Supongamos que $p_1 = p_2 = \frac{1}{2}$. Entonces $h_P(\phi) = \frac{3}{4}$. Veamos que se cumplen las cotas:

$$\frac{3}{4} \geq 0, \qquad \frac{3}{4} \leq \frac{1}{2} + \frac{1}{2} = 1, \qquad \frac{3}{4} \geq \frac{1}{2} + \frac{1}{2} - \frac{1}{2}\frac{1}{2} = \frac{3}{4}.$$

$$MT_0(K_{I_\phi}) = 0 \leq \frac{3}{4},$$

$$MT_1(K_{I_\phi}) = \frac{1}{2} + \frac{1}{2} = 1 \geq \frac{3}{4},$$

$$MT_2(K_{I_\phi}) = \frac{1}{2} + \frac{1}{2} - \frac{1}{2}\frac{1}{2} = \frac{3}{4}.$$

Ejemplo 4.57. Sea $\phi_{1,3} = \phi(x,y,z) = x \vee y \vee z$ sistema binario de orden tres. Su conjunto de caminos es:

$$C^1_\phi = \{(1,0,0),(1,1,0),(1,0,1),(1,1,1),(0,1,1),(0,1,0),(0,0,1)\}.$$

Y el conjunto minimal es:

$$G^1_\phi = \{(1,0,0),(0,1,0),(0,0,1)\}.$$

Por lo tanto, su sistema de generadores minimal es:

$$G_{I_\phi} = \{x,y,z\}.$$

Sus subconjuntos no vacíos son:

$$J_1 = \{x\}, \qquad J_2 = \{y\}, \qquad J_3 = \{z\},$$

$$J_4 = \{x,y\}, \qquad J_5 = \{x,z\}, \qquad J_6 = \{y,z\},$$

$$J_7 = \{x,y,z\}.$$

A partir de ellos podemos calcular el K-polinomio del ideal.

$$K_{I_\phi}(x,y,z) = (x+y+z) - (xy+xz+yz) + (xyz).$$

Y sus truncamientos son:

$$K_{I_\phi,0}(x,y,z) = 0,$$

$$K_{I_\phi,1}(x,y,z) = (x+y+z),$$

$$K_{I_\phi,2}(x,y,z) = (x+y+z) - (xy+xz+yz),$$
$$K_{I_\phi,3}(x,y,z) = (x+y+z) - (xy+xz+yz) + (xyz).$$

Supongamos que las probabilidades son $p_1 = \frac{1}{2}, p_2 = \frac{1}{3}, p_3 = \frac{1}{4}$. Entonces, la fiabilidad del sistema es:

$$h_P(\phi) = P(\phi(X,Y,Z) = 1) = 1 - P(\phi(X,Y,Z) = 0) = 1 - P((X,Y,Z) =$$

$$= (0,0,0)) = 1 - \frac{1}{2}\frac{2}{3}\frac{3}{4} = \frac{3}{4}.$$

Comparémoslo con las cotas generadas por los truncamientos del K-polinomio.

$$K_{I_\phi,0}(\frac{1}{2},\frac{1}{3},\frac{1}{4}) = 0 \leq \frac{3}{4},$$

$$K_{I_\phi,1}(\frac{1}{2},\frac{1}{3},\frac{1}{4}) = (\frac{1}{2}+\frac{1}{3}+\frac{1}{4}) = \frac{13}{12} \geq \frac{3}{4},$$
$$K_{I_\phi,2}(\frac{1}{2},\frac{1}{3},\frac{1}{4}) = \frac{13}{12} - (\frac{1}{2}\frac{1}{3}+\frac{1}{2}\frac{1}{4}+\frac{1}{3}\frac{1}{4}) = \frac{13}{12} - \frac{3}{8} = \frac{17}{24} \leq \frac{3}{4},$$
$$K_{I_\phi,3}(\frac{1}{2},\frac{1}{3},\frac{1}{4}) = \frac{17}{24} + (\frac{1}{2}\frac{1}{3}\frac{1}{4}) = \frac{3}{4}.$$

Conclusión

A lo largo de este documento se ha presentado un método algebraico para obtener una familia de cotas de la fiabilidad de un sistema binario. El procedimiento seguido puede resumirse en los siguientes pasos:

1. Dado un sistema binario ϕ, se construye su ideal monomial asociado $I_\phi = \Psi(\phi)$.
2. A continuación, se obtiene el K-polinomio K_{I_ϕ} correspondiente.
3. Finalmente, se consideran sus truncamientos y se evalúan en las probabilidades p_i de los componentes.

Este enfoque es aplicable a cualquier sistema binario y proporciona cotas superiores e inferiores de su fiabilidad mediante un procedimiento sistemático. Sin embargo, el cálculo del K-polinomio presentado en esta memoria resulta ineficiente para sistemas con muchas componentes. Por ello, en la práctica, sus coeficientes suelen obtenerse a través de resoluciones graduadas del ideal [9], concepto que no se ha desarrollado en esta memoria al exceder el marco de contenidos previsto. Dichas resoluciones forman parte del temario de la asignatura de máster *Álgebra Combinatoria*.

Apéndice A

Complejos simpliciales

Los ideales libres de cuadrados añaden una estructura geométrica a los ideales monomiales. Esta estructura geométrica les permite codificar un complejo simplicial en los exponentes de sus generadores minimales. En esta subsección analizamos esta correspondencia entre complejos simpliciales e ideales libres de cuadrados, y estudiamos las características topológicas de estos complejos por medio de homología simplicial.

A.1. Correspondencia de Stanley-Reisner

En el campo de la topología algebraica los complejos sirven de ejemplos fundamentales. Estos permiten construir espacios básicos en los que obtener intuición sobre la maquinaria algebraica usada. Principalmente, dos tipos de complejos son estudiados: los complejos simpliciales y los complejos celulares. Ambos se construyen como cadenas de objetos de menor dimensión, sin embargo, los primeros muestran un comportamiento combinatorio, mientras los segundos muestran un comportamiento más geométrico.

Definición A.1. Un complejo simplicial Δ con n vértices $\{1, 2, \ldots, n\}$ es una colección de subconjuntos $\Delta \subset \mathcal{P}(\{1, \ldots, n\})$ cumpliendo: que si $\sigma \in \Delta$ y $\tau \subset \sigma$ entonces $\tau \in \Delta$.

Cada uno de los $\sigma \in \Delta$ se llama símplice[1].

Definición A.2. Sea Δ un complejo simplicial y $\sigma \in \Delta$ un símplice.

Se define la dimensión de σ como $\dim(\sigma) = |\sigma| - 1$ donde $|\sigma|$ es la cardinalidad de σ como conjunto.

A su vez, se define la dimensión de Δ como $\dim(\Delta) = \max_{\sigma \in \Delta}(\dim(\sigma))$ salvo si $\Delta = \{\}$, en tal caso $\dim(\Delta) = -\infty$.

[1] En la literatura también se llama cara.

El subconjunto de símplices de Δ de dimensión n se denota como $\Delta_n = \{\sigma \in \Delta : \dim(\sigma) = n\}$.

Ejemplo A.3. La imagen A.1 muestra un complejo simplicial Δ sobre cinco vértices. Analizamos la imagen sistemáticamente para deducir los símplices de Δ.

En dimensión 2 se puede observar que contiene al triángulo $\{1, 2, 3\}$ por tanto también contiene a los segmentos $\{1, 2\}, \{2, 3\}, \{1, 3\}$ y a los puntos $\{1\}, \{2\}, \{3\}$.

En dimensión 1 tenemos además a las rectas $\{3, 4\}, \{2, 4\}$ y por tanto al punto $\{4\}$.

Por último tenemos un punto aislado en dimensión 0: $\{5\}$.

Juntando toda esta información, tenemos:

$$\Delta = \{\{1, 2, 3\}, \{1, 2\}, \{2, 3\}, \{1, 3\}, \{3, 4\}, \{2, 4\}, \{1\}, \{2\}, \{3\}, \{4\}, \{5\}\}.$$

El complejo es de dimensión 2, pues su máximo símplice es bidimensional.

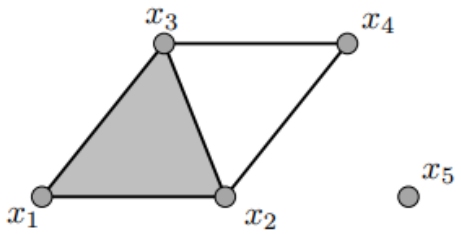

Figura A.1: Ejemplo de complejo simplicial. [8]

Una vez más, antes de construir la correspondencia de ideales, la construiremos sobre monomios para poder extenderla a ideales a partir de estos.

Definición A.4. Se define la correspondencia Φ_n entre símplices con n vértices y monomios libres de cuadrados en n variables:

$$\Phi_n : \mathcal{P}(\{1, \ldots, n\}) \longrightarrow \mathcal{N}$$

$$\sigma \longmapsto x^\sigma = \prod_{i \in \sigma} x_i$$

Proposición A.5. *La aplicación Φ_n es un isomorfimo de retículo..*

Demostración. Como es obvio que Φ_n es biyectiva, solo es necesario demostrar que es monótona.

Supongamos que $\tau \subset \sigma$. Si se da $i \in \tau$ se tiene que $i \in \sigma$. Por lo que si $x_i \mid x^\tau$ entonces $x_i \mid x^\sigma$ y, en conclusión, $x^\tau \mid x^\sigma$. Por lo que la aplicación es monótona. □

Teorema A.6. *Existe una correspondencia biyectiva entre el conjunto de ideales monomiales libres de cuadrados en n variables y el conjunto de complejos simpliciales en n vértices. Esta correspondencia se llama correspondencia de Stanley-Reisner.*

Demostración. Está demostración será constructiva. A partir de un complejo simplicial Δ obtendremos su ideal I_Δ y a partir de un ideal I obtendremos su complejo Δ_I.

Una vez construida esta correspondencia, demostraremos que es biyectiva.

$\Leftarrow$) Sea Δ un complejo simplicial. Definimos su imagen:

$$I_\Delta := \langle x^\sigma : \sigma \notin \Delta \rangle.$$

Como está generado por monomios libres de cuadrados, I_Δ es un ideal monomial libre de cuadrados.

$\Rightarrow$) Sea I un ideal monomial libre de cuadrados. Definimos su imagen:

$$\Delta_I := \{\sigma : x^\sigma \notin I\}.$$

Sea $\sigma \in \Delta_I$ y $\tau \subset \sigma$. Supongamos que $\tau \notin \Delta_I$, o, equivalentemente, $x^\tau \in I$. Como Φ_n es monótona, y $\tau \subset \sigma$, se tiene que $x^\tau \mid x^\sigma$. Lo cual es absurdo, porque implicaría que $x^\sigma \in I$.

$\Longleftrightarrow$) Veamos ahora que es biyectiva.

Tomamos un ideal libre de cuadrados I, queremos ver que $I_{\Delta_I} = I$. Para esto, realicemos la construcción por pasos:

$$\Delta_I := \{\sigma : x^\sigma \notin I\},$$

$$I_{\Delta_I} := \langle x^\sigma : \sigma \notin \Delta_I \rangle.$$

Como $\sigma \in \Delta_I$ si $x^\sigma \notin I$. Se tiene que $\sigma \notin \Delta_I$ implica que $x^\sigma \in I$. Por lo tanto, $I_{\Delta_I} = I$.

Partiendo de un complejo simplicial Δ se puede realizar un razonamiento análogo.

□

A.2. Homología simplicial

La homología es una herramienta algebraica que permite analizar un espacio por medio de una cadena de espacio vectoriales, a partir de los cuales se construyen los grupos de homología, cuyos invariantes reflejan la presencia de "agujeros.[en] el espacio.

Definición A.7. Definición. Sea Δ un complejo simplicial y $\mathbb{K}$ un cuerpo.El módulo de n-cadenas de Δ, denotado $C_n(\Delta, \mathbb{K})$, es el $\mathbb{K}$-espacio vectorial:

$$C_n(\Delta, \mathbb{K}) = \bigoplus_{\sigma \in \Delta} \mathbb{K}.$$

Es decir, es el conjunto de sumas formales finitas:

$$\sum_i k_i \sigma_i, \quad k_i \in \mathbb{K}, \sigma_i \in \Delta_n.$$

Ejemplo A.8. La imagen A.2 muestra un complejo simplicial Δ. Este es uno de los ejemplos con los que trabajaremos a lo largo de esta sección. Por ahora, simplemente daremos ejemplos de varias cadenas.

Las cadenas $\{2\} - \{3\}$ y $\pi\{4\}$ pertenecen a $C_0(\Delta, \mathbb{R})$. Por otra parte, las cadenas $\{2, 5\} + 3\{1, 2\}$ pertenecen a $C_1(\Delta, \mathbb{Q})$.

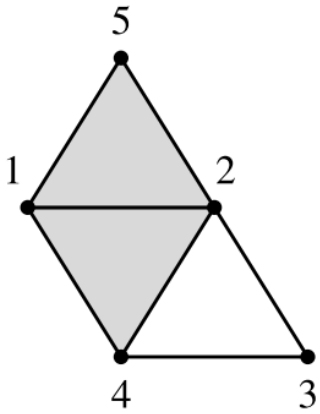

Figura A.2: Ejemplo de complejo simplicial. [8]

A continuación, definiremos el operador que relaciona los diferentes módulos de cadenas entre sí. Para ello, necesitaremos una definición auxiliar.

Definición A.9. Sean Δ un complejo simplicial, $\sigma \in \Delta_n$ un símplice, y $j \in \sigma$ un vértice. Denotamos por σ^j al símplice $\sigma \setminus \{j\}$.

Ejemplo A.10. En la figura A.2 el símplice $\sigma = \{1, 2\}$ representa a la arista que une a los puntos $\sigma^2 = \{1\}$ y $\sigma^1 = \{2\}$.

Por otro lado, el símplice $\sigma = \{1, 2, 4\}$ es un triángulo relleno con lados $\sigma^1 = \{2, 4\}, \sigma^2 = \{1, 4\}, \sigma^4 = \{1, 2\}$.

Definición A.11. Como $\Delta = \{1, \ldots, m\}$ todos sus subconjuntos $\sigma \subset \Delta$ se pueden expresar como subconjuntos ordenados $\{j_1, \ldots, j_r, \ldots, j_s\}$. Si $j \in \sigma$ y j ocupa la r-ésima posición, se dice que su signo es: $\text{sign}(j, \sigma) = (-1)^{r-1}$.

Ejemplo A.12. En la figura A.2 tomamos la arista $\{1, 4\}$, $\text{sign}(1, \{1, 4\}) = +1$ y $\text{sign}(4, \{1, 4\}) = -1$. Sin embargo, en el triángulo relleno $\{1, 2, 4\}$ se tiene que $\text{sign}(1, \{1, 2, 4\}) = +1$, $\text{sign}(2\{1, 2, 4\}) = -1$ y $\text{sign}(4, \{1, 2, 4\}) = +1$. Por lo que, al añadir el vértice $\{2\}$ entre $\{1\}$ y $\{4\}$, el signo de este último cambia.

Definición A.13. Sean Δ un complejo simplicial y $\mathbb{K}$ un cuerpo. La aplicación lineal frontera se define como:

$$\partial_n : C_n(\Delta, \mathbb{K}) \longrightarrow C_{n-1}(\Delta, \mathbb{K})$$

$$\sum_i k_i \sigma_i \longmapsto \sum_{i,j} \text{sign}(j, \sigma_i) k_i \sigma_i^j$$

Ejemplo A.14. Continuemos con el anterior ejemplo.

El borde de la arista $\{1, 2\}$ es $\partial_1(\{1, 2\}) = \{2\} - \{1\}$ pues esta parte de $\{1\}$ y llega a $\{2\}$.

El borde del triángulo $\{1, 2, 4\}$ es

$$\partial_2(\{1, 2, 4\}) = \{1, 2\} - \{1, 4\} + \{2, 4\},$$

que representa el perímetro del triángulo recorrido en sentido horario.

Proposición A.15. *Los operadores borde son nilpotentes. Es decir* $\partial_{n-1} \circ \partial_n = 0$.

Demostración. Sea $l = \sum_i k_i \sigma_i \in C_n(\Delta, \mathbb{K})$ una n-cadena. A aplicarle ∂_n

$$\partial_n(l) = \sum_{i,j} \text{sign}(j, \sigma_i) k_i \sigma_i^j.$$

Volviendo a aplicar el operador frontera.

$$\partial_{n-1}(\partial_n(l)) = \sum_{i,j,k} \text{sign}(k, \sigma_i^j) \text{sign}(j, \sigma_i) k_i \sigma_i^{j,k}.$$

Se tiene que $\sigma_i^{j,k} = \sigma_i^{k,j}$ por lo tanto basta con ver que $\text{sign}(k, \sigma_i^j)\text{sign}(j, \sigma_i) = -\text{sign}(j, \sigma_i^k)\text{sign}(k, \sigma_i)$.

Supongamos, sin pérdida de generalidad, que $j < k$. Si retiramos j de σ_i la posición de k se reduce en 1 y su signo cambia. Si retiramos primero k esto no pasa. Por tanto, hay un cambio de signo entre los dos órdenes. □

Corolario A.16. *Se tiene que $Im(\partial_n) \subset Ker(\partial_{n-1})$.*

Ejemplo A.17. Continuamos con la figura A.2. Sea $\sigma = \{1, 2, 4\}$. Como vimos anteriormente $\partial_2(\{1, 2, 4\} = \{1, 2\} - \{1, 4\} + \{2, 4\}$. Y, también tenemos que:

$$\partial_1(\{1, 2\}) = \{2\} - \{1\},$$
$$\partial_1(\{2, 4\}) = \{4\} - \{2\},$$
$$\partial_1(\{1, 4\}) = \{4\} - \{1\}.$$

Por lo que, al sumarlas

$$\partial_1(\partial_2(\{1, 2, 4\})) = (\{2\} - \{1\}) - (\{4\} - \{1\}) + (\{4\} - \{2\}) = 0,$$

esta expresión se anula tal y como esperábamos.

De esta forma obtenemos una cadena de espacios:

$$\ldots \xrightarrow{\partial_3} C_2(\Delta, \mathbb{K}) \xrightarrow{\partial_2} C_1(\Delta, \mathbb{K}) \xrightarrow{\partial_1} C_0(\Delta, \mathbb{K}) \xrightarrow{\partial_0} 0.$$

Y podemos definir la homología.

Definición A.18. Dado un complejo simplicial Δ. Llamamos grupo de homología en dimensión n al grupo:

$$H_n(\Delta, \mathbb{K}) := \ker(\partial_n)/\text{Im}(\partial_{n+1}).$$

Se definen los números de Betti como:

$$\beta_n := \dim_{\mathbb{K}}(H_n(\Delta, \mathbb{K}).$$

como $\mathbb{K}$-espacio vectorial.

Los números de Betti contienen información topológica del sistema. En concreto β_0 contiene el número de componentes conexas, β_1 contiene el número de agujeros, β_2 contiene el número de agujeros bidimensional, β_3 contiene el número de agujeros tridimensionales...

Ejemplo A.19. Volvemos a la figura A.2. En primer lugar, ordenamos los símplices de cada Δ_n. Denotamos por $g_1, \ldots, g_m$ a los generadores de $C_n(\Delta, \mathbb{K})$, cada uno corresponde a un símplice de Δ_n siguiendo el orden dado.

$$\Delta_0 = \{\{1\}, \{2\}, \{3\}, \{4\}, \{5\}\},$$
$$\Delta_1 = \{\{1,2\}, \{1,4\}, \{1,5\}, \{2,3\}, \{2,4\}, \{2,5\}, \{3,4\}\},$$
$$\Delta_2 = \{\{1,2,4\}, \{1,2,5\}\}.$$

A partir de los g_i generados por este orden de elementos, obtenemos la representación matricial de los operadores borde:

$$\partial_2 = \begin{pmatrix} 1 & 1 \\ -1 & 0 \\ 0 & -1 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix},$$

$$\partial_1 = \begin{pmatrix} -1 & -1 & -1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & -1 & -1 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix},$$

$$\partial_0 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Ahora calculamos las dimensiones de las imágenes y kernels a partir de su representación matricial.

$$\dim(\mathrm{Im}(\partial_2)) = 2, \qquad \dim(\mathrm{Ker}(\partial_2)) = 5,$$
$$\dim(\mathrm{Im}(\partial_1)) = 4, \qquad \dim(\mathrm{Ker}(\partial_1)) = 3,$$
$$\dim(\mathrm{Im}(\partial_0)) = 0, \qquad \dim(\mathrm{Ker}(\partial_0)) = 5.$$

Ahora, podemos calcular los grupos de homología mediante cocientes:

$$H_1 = \ker(\partial_1)/\mathrm{Im}(\partial_2) = \mathbb{K}^3/\mathbb{K}^2 = \mathbb{K},$$
$$H_0 = \ker(\partial_0)/\mathrm{Im}(\partial_1) = \mathbb{K}^5/\mathbb{K}^4 = \mathbb{K}.$$

Esto significa que el complejo es conexo ($\beta_0 = 1$) y posee exactamente un agujero unidimensional ($\beta_1 = 1$), correspondiente al hueco delimitado por el triángulo $\{2, 3, 4\}$.

A.3. Fórmula de Hochster

La fórmula de Hochster relaciona los números de Betti de un complejo simplicial con los de su ideal. En nuestro caso, nos permite obtener el K-polinomio de un ideal monomial libre de cuadrados a partir de su complejo simplicial.

Para introducirla, son necesarias dos definiciones previas.

Definición A.20. Sea Δ un complejo simplicial con n vértices y $\sigma \in \mathcal{P}(\{1,\dots,n\})$. Se define el complejo:

$$\Delta_\sigma = \{\tau \in \Delta : \tau \subset \sigma\}.$$

Ejemplo A.21. Sea Δ el complejo de A.1. Recordemos que este complejo es:

$$\Delta = \{\{1,2,3\},\{1,2\},\{2,3\},\{1,3\},\{3,4\},\{2,4\},\{1\},\{2\},\{3\},\{4\},\{5\}\}.$$

Si tomamos el símplice $\sigma = \{1,2,3\} \in \Delta$, que es un triángulo, se induce el complejo:

$$\Delta_\sigma = \{\{1,2,3\},\{1,2\},\{1,3\},\{2,3\},\{1\},\{2\},\{3\}\}.$$

Mientras que si tomamos $\tau = \{3,4,5\} \notin \Delta$, pese a que no pertenezca al complejo de partida induce otro complejo:

$$\Delta_\tau = \{\{3,4\},\{3\},\{4\},\{5\}\}.$$

Usaremos la fórmulas de Hochster [8]para definir los números de Betti de un ideal monomial libre de cuadrados a partir de los números de Betti de su complejo simplicial. Antes de esto será necesario definir los números de Betti reducidos.

Definición A.22. Sea Δ un complejo simplicial y $n \in \mathbb{N}$. Su n-ésimo número de Betti se define como:

$$\tilde{\beta}_n(\Delta) := \begin{cases} \beta_n(\Delta), & \text{si } n \geq 1, \\ \beta_n(\Delta) - 1, & \text{si } n = 0. \end{cases}$$

Definición A.23. Sea I un ideal monomial libre de cuadrados del anillo $\mathbb{R}[x_1,\dots,x_n]$, $k \in \mathbb{N}, \sigma \in \mathcal{P}(\{1,\dots,n\}) = \{0,1\}^n$. Se definen sus números de Betti como:

$$\beta_{k,\sigma}(I) = \tilde{\beta}_{|\sigma|-k-1}(\Delta_\sigma),$$

donde $|\sigma|$ representa la cardinalidad de σ como conjunto.

Además, según [7] se tiene el siguiente resultado:

Teorema A.24. *Sea I un ideal monomial libre de cuadrados del anillo $\mathbb{R}[x_1, \ldots, x_n]$. Entonces se tiene que:*

$$K_I(x_1, \ldots, x_n) = \sum_{k \in \mathbb{N}} (-1)^k \Big(\sum_{\sigma \in \{0,1\}^n} \beta_{k,\sigma}(I) x^\sigma \Big).$$

No computamos ejemplos de estos constructos porque tienen una eficiencia significativamente peor que el método ilustrado en el cuarto capítulo.

Bibliografía

[1] Brian Davey e Hilary Priestly. *Introduction to Lattices and Order*. Cambridge University Press, 2002.

[2] Philippe Flajolet y Robert Sedgewick. *Analytic combinatorics*. Cambridge University Press, 2009.

[3] George Grätzer. *Lattice Theory: Foundation*. Birkhauser, 2011.

[4] Jürguen Herzog y Takayuki Hibi. *Monomial Ideals*. Springer, 2011.

[5] Arnljot Hsyland y Marvin Rausand. *System Reliability Theory Models, Statistical Methods,and Applications*. Willey Interscience, 2004.

[6] Arne Bang Huseb y Kristina Rognlien Dahl. *Risk and reliability analysis with applications*. Apuntes personales, 2017.

[7] Rodrigo Iglesias et al. «Una introducción a la fiabilidad algebraica de sistemas multiestado». En: *La Gaceta de la RSME, Vol. 27, Número 3* (2024).

[8] Ezra Miller y Bernd Sturmfels. *Combinatorial Commutative Algebra*. Springer, 2005.

[9] Patricia Pascual-Ortigosa. «Algebraic Reliability. Monomial ideals applied to multi-state system reliability». Tesis doct. Universidad de la Rioja, 2022.

[10] Felipe Rincón y Simón Soto. «Introducción a la teoría de politopos». En: *Lecturas Matemáticas* 40.2 (2019), págs. 117-215. URL: `https://dialnet.unirioja.es/descarga/articulo/7215102.pdf`.

[11] Jan Snellman. *Generalized Hilbert Numerators II*. arXiv:math/0003097 [math.CO]. Accessed: 2025-09-14. 2000. URL: `https://arxiv.org/abs/math/0003097`.