Sección de Matemáticas
Universidad de La Laguna

César Martín Ferrer

La Conjetura de la Sensibilidad y su demostración usando Teoría Espectral de Grafos

The Sensitivity Conjecture and its proof via Spectral Graph Theory

Trabajo Fin de Grado
Grado en Matemáticas
La Laguna, Julio de 2023

Dirigido por
Ignacio García Marco

Ignacio García Marco
Departamento de Matemáticas,
Estadística e I.O
Universidad de La Laguna
38200 La Laguna, Tenerife

Resumen · Abstract

Resumen

La Conjetura de la Sensibilidad era uno de los problemas abiertos más importantes en complejidad computacional. Tras 30 años de incertidumbre, Hao Huang (Emory, Atlanta, EE.UU) ha logrado demostrarla en poco más de una página [8].
Esta conjetura afirma que dos medidas de complejidad booleana: la sensibilidad y la sensibilidad por bloques son equivalentes, o, formalmente hablando, están polinómicamente relacionadas. La demostración de Huang usa con gran creatividad herramientas básicas del Álgebra Lineal, así como una reescritura de la conjetura en términos del grafo del hipercubo llevada a cabo por Gotsman y Linial [2]. El objetivo de esta memoria es presentar el contexto de la conjetura, así como su demostración e implicaciones.

Palabras clave: *Funciones booleanas, sensibilidad, grado máximo, hipercubo.*

Abstract

The Sensitivity Conjecture was one of the most important open problems in computational complexity. After 30 years of uncertainty, Hao Huang (Emory, Atlanta, USA) has succeeded in proving it in just over one page [8].
This conjecture states that two measures of boolean complexity: sensitivity and block sensitivity are equivalent, or, formally speaking, are polynomially related. Huang's proof makes creative use of basic tools of Linear Algebra, as well as a rewriting of the conjecture in terms of the hypercube graph by Gotsman and Linial [2].
The goal of this memory is to present the context of the conjecture as well as its proof and implications.

Agradecimientos

A mi tutor Nacho.
A mi familia.

La Laguna, 10 de julio de 2023

Introducción

Poco antes de la invención de los ordenadores en el siglo XX, diversos matemáticos trataban de encontrar un método universal de resolución de problemas a través de un conjunto de instrucciones lógicas definidas y ordenadas. Hoy en día, en términos de programación, llamamos a esto algoritmo. A raíz de este estudio, junto con el desarrollo de sistemas como cálculo Lambda (Alonzo Church), funciones recursivas (Kurt Godel) o la máquina de Turing (Alan Turing), aparece la teoría de la computación.

La teoría de la computación o teoría computacional se centra en estudiar y modelar los procesos de cálculo bajo el rigor de la Lógica, limitada por la capacidad de cálculo del sistema computacional con el que trabajemos. Es por ello que, esta teoría busca cuantificar los recursos requeridos por los sistemas para resolver estos problemas, con el fin de maximizar su eficiencia.

Al estudiar los circuitos y árboles de decisión, para poder analizar estos procesos y esquematizar las operaciones lógicas, fue necesario recurrir al álgebra de Boole (1854). Esta herramienta se desarrolla en el libro *Investigación sobre las leyes del pensamiento* publicado por George Boole [6]. La idea innovadora consiste en hacer uso del rigor del Álgebra, para estudiar la Lógica, donde cualquier número de afirmaciones o sentencias pueden ser clasificadas como verdadera o falsa. El primero en aplicar el álgebra de Boole fue Claude Shannon en 1948 [14] para el diseño de circuitos de conmutación eléctrica biestables y, posteriormente, se llevó a más campos como la automatización.

Debido a la codificación binaria de los ordenadores aplicada en el estudio sobre la validez y complejidad de los circuitos en la teoría de la computación, varios matemáticos se apoyaron en las funciones booleanas. Este tipo de funciones, son aquellas que toman como dominio $\{0,1\}^n$, es decir, cadenas de datos binarios de 0 o 1 con una cierta longitud n y como codominio únicamente los valores 1 y 0 (TRUE y FALSE).

Para cuantificar cuan compleja es una función booleana, Nisan y Szegedi [11] consideran varias medidas de complejidad, como son la sensibilidad puntual, por árbol de decisión, marginal o en bloques. Dándonos información sobre

lo compleja que es la función. En el mismo artículo Nisan y Szegedi demuestran relaciones polinómicas entre estas medidas de complejidad, excepto para la sensibilidad.

La Conjetura de la Sensibilidad es el problema matemático planteado por Nisan y Szegedy en 1989 [11], que afirma que existe una relación polinómica entre la sensibilidad en bloque y la sensibilidad marginal de una función booleana. Esta última prueba es necesaria para dar respuesta a la de pregunta de si todas las medidas de complejidad que enuncian son equivalentes. Hasta el momento de la prueba de Huang [8], sólo se sabía que la sensibilidad de una función booleana era una cota inferior de la sensibilidad por bloques y era necesaria hallar otra relación para poder concluir que estas son equivalentes.

Tras 30 años, el matemático Hao Huang (Univ. Emory, Atlanta, EE. UU) [8] ha resuelto esta propuesta en poco más de una página, mejorando en el proceso un resultado anterior probado por Chung, Füredi, Graham, y Seymour [5] en 1988. Para el desarrollo de la demostración, usa una reescritura del enunciado de la conjetura en términos de la Teoría de Grafos debida a Gotsman y Linial [2]. Esta reescritura traduce el problema original, formulando bajo el punto de vista de la teoría computacional y funciones booleanas, trabajando sobre un grafo que conoceremos como el hipercubo y un cierto parámetro combinatorio del mismo que denominaremos sensibilidad de un grafo.

Nuestro objetivo será enunciar y demostrar la Conjetura de la Sensibilidad en tres capítulos, donde profundizaremos en el trabajo de Huang, sus antecedentes y sus consecuencias. En el primer capítulo, introduciremos los resultados necesarios para llegar a comprender el enunciado de la versión equivalente de la conjetura en términos de la Teoría de Grafos, que demuestra Huang. Dentro de la Teoría de Grafos daremos pie a algunos conceptos necesarios para poder enunciar la conjetura. Primero, introduciremos los conceptos fundamentales, como el grado de un vértice o los conjuntos independientes, con el fin de presentar qué es la sensibilidad de un grafo. Posteriormente, estudiaremos en detalle los grafos bipartitos y regulares. En particular demostraremos que el número de independiencia (el número de vértices del mayor independiente) de estos grafos coincide con la mitad del número de vértices. Esta conclusión, se obtendrá como consecuencia de los famosos Teoremas de Hall 1.24, y Teorema del matrimonio 1.26.

Posteriormente, definiremos la sensibilidad de un grafo como el menor valor que puede tomar el grado máximo de un subgrafo inducido con más vértices que el grado de independencia. Tras esto, presentaremos el grafo del hipercubo Q^n, que es un grafo bipartito y $n-$regular con 2^n vértices. Finalmente, enunciaremos la Conjetura de la Sensibilidad, que versa sobre el valor de la sensibilidad de los grafos del hipercubo.

En el segundo capítulo, procedemos a demostrar la reescritura de la Conjetura de la Sensibilidad en términos de la Teoría de Grafos en el Teorema 2.14. Para ello, necesitaremos recordar herramientas del Álgebra Lineal, como el cálculo de autovalores aplicado a matrices simétricas, dando lugar a resultados como el Teorema espectral 2.7 y el principio de Rayleigh 2.8. Estos resultados nos permiten demostrar el Teorema del entrelazamiento de Cauchy 2.10. Este es un ingrediente usado por Huang en su demostración de la reescritura de la Conjetura de la Sensibilidad en términos de la Teoría de Grafos 2.14, que nos dice que cualquier grafo inducido por el hipercubo Q^n con al menos $2^{n-1}+1$ vértices tendrá al menos un vértice con grado mayor o igual a 0. En otras palabras, que la sensibilidad del hipercubo Q^n es al menos $\sqrt{n}$. En este capítulo también presentamos la corta y elegante demostración de este resultado aportado por Huang.

En el tercer capítulo, trasladamos los resultados obtenidos en la Teoría de Grafos a las funciones booleanas. Realizaremos un repaso histórico sobre las medidas de complejidad fundamentales para esta prueba, el grado, la sensibilidad y la sensibilidad por bloques de una función booleana con el fin de demostrar que estas son equivalentes, de forma que podamos explicar la formulación original de la Conjetura de la Sensibilidad.

La Conjetura de la Sensibilidad, en su versión original dice que la sensibilidad en bloques y la sensibilidad de una función booleana son equivalentes o, como diremos nosotros están polinómicamente relacionadas. Veremos como este resultado se sigue como un corolario directo del Teorema de equivalencia de Gotsman y Linial 3.37 y la conjetura de la sensibilidad en términos de la Teoría de Grafos 2.14.

Contenido

1

Teoría de Grafos: independencia y sensibilidad

En este capítulo buscamos introducir las herramientas necesarias para poder enunciar y entender el enunciado de una reescritura de la Conjetura de la Sensibilidad [8], en términos de la Teoría de Grafos.

1.1. Sensibilidad de un grafo

El objetivo en esta primera sección es definir el concepto de sensibilidad de un grafo y calcularlo en algunas familias de grafos. Para ello comenzaremos introduciendo algunos elementos básicos de la teoría de grafos.

Definición 1.1. *Un grafo no dirigido es un par ordenado $G = (V, E)$, donde $V = \{v_1, \ldots, v_n\}$ será un conjunto finito no vacío al que llamamos conjunto de vértices y $E = \{e_1, \ldots, e_m\}$ con $e_i = \{v_j, v_k\} \subseteq V$, un conjunto finito de aristas. En nuestro estudio consideraremos únicamente grafos simples, es decir, no encontramos lazos, osea que, $|e_i| = 2$, ni aristas múltiples, de forma que, $e_i \neq e_j$ para $i \neq j$.*

En los grafos hablaremos muchas veces de los vecinos de uno o más vértices, es por ello que definiremos el concepto de vecindad.

Definición 1.2. *Sea un grafo $G = (V, E)$ y un vértice $v \in V$, llamamos conjunto de vecinos de v a $N(v) = \{u \in V \mid \{u, v\} \in E\}$. De forma general para $V' \subset V$ lo definiremos como $N(V') = \cup_{u \in V'} N(u)$.*

Asimismo, se define el grado de un vértice $v \in V$, y se denota por $\deg(v)$ como el número de aristas adyacentes al vértice. Al ser G un grafo simple, el grado coincide con el número de vecinos de este, es decir, $\deg(v) = |N(v)|$.

Definición 1.3. *Sea un grafo $G = (V, E)$, llamamos grado máximo del grafo al mayor grado de un vértice, es decir:*

$$\Delta(G) = \max\{\deg(v) \mid v \in V\}.$$

Definición 1.4. *Sean $G = (V, E)$ y $G' = (V', E')$ dos grafos, decimos que G' es un subgrafo de G si $V' \subset V$ y $E' \subset E$. Decimos además que G' es el subgrafo inducido por V' si $E' = \{e \in E \,|\, e \subset V'\}$; en tal caso lo denotamos $G' = [V']$.*

Veamos un ejemplo:

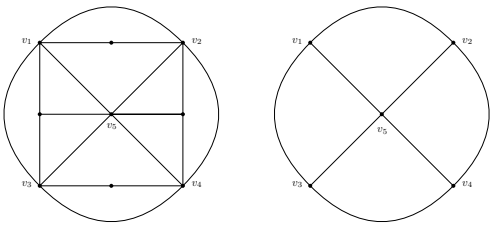

Figura 1.1: Grafo y un subgrafo inducido.

La Figura 1.1 muestra un grafo y su correspondiente subgrafo inducido por $V' = \{v_1, v_2, v_3, v_4, v_5\}$, observando el grafo G nos damos cuenta que $\deg(v_1) = 5$ y $\Delta(G) = 6$.

Definición 1.5. *Sea un grafo $G = (V, E)$ y $V' \subset V$ un conjunto no vacío, llamamos a V' independiente si para todo $v_1, v_2 \in V'$, $\{v_1, v_2\} \notin E$. En otras palabras, V' es un conjunto independiente si y solo si el subgrafo inducido por V' no tiene ninguna arista. Se observa entonces que $V' \subseteq V$ es un independiente si y solo si $\Delta([V']) = 0$. Denotaremos por $\alpha(G)$ al tamaño del independiente máximo, es decir:*

$$\alpha(G) = \text{máx}\{\, |V'| \mid \ V' \subset V \text{ independiente}\}.$$

En general, el cálculo de $\alpha(G)$ es un problema difícil desde el punto de vista de la complejidad computacional (ver, por ejemplo, [7, Problem GT20]). Sin embargo, existen familias de grafos donde sí es fácil determinar el valor de $\alpha(G)$.

Por ejemplo, para $k \geq 2$ el grafo estrella S_k es el grafo con vértices $\{v_1, \ldots, v_k, u\}$ y aristas $\{u, v_i\}$, para cualquier $i \in \{1, \ldots, k\}$ (ver Figura 1.2). Se comprueba que $\{v_1, \ldots, v_k\}$ es independiente y por tanto $\alpha(S_k) = k$.

Una familia que generaliza a los grafos estrella son los grafos bipartitos completos.

Definición 1.6. *Llamamos grafo bipartito completo $K_{r,s}$ al grafo formado por dos conjuntos disjuntos de vértices y todas las posibles aristas que unen los vértices de ambos conjuntos entre sí, es decir: $K_{r,s} = (A \sqcup B, E)$ siendo $|A| = r$, $|B| = s$ donde para todo $v_1 \in A$, $v_2 \in B$, existe $\{v_1, v_2\} \in E$.*

Se observa que, para todo $v \in A$ tendremos que $\deg(v) = s$, para todo $u \in B$ tendremos que $deg(u) = r$, y $|V| = r + s$ (ver Figura 1.3 para un ejemplo).

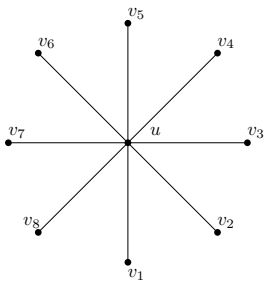

Figura 1.2: Grafo estrella $\mathcal{S}_8$.

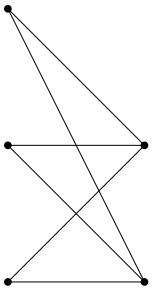

Figura 1.3: Grafo bipartito completo $K_{3,2}$.

Proposición 1.7. *Sean $r, s \geq 1$, entonces $\alpha(K_{r,s}) = \max\{r, s\}$.*

Demostración. Supongamos sin pérdida de generalidad que $r \geq s$ y, vamos a demostrar que $\alpha(K_{r,s}) = r$. Sea $V = V_1 \cup V_2$ el conjunto de vértices de $K_{r,s}$ con V_1 y V_2 dos conjuntos disjuntos de r y s elementos respectivamente, donde $E = \{\{v_1, v_2\} \,|\, v_1 \in V_1, v_2 \in V_2\}$ es su conjunto de aristas. Se observa que V_1 es independiente y, por tanto, $\alpha(K_{r,s}) \geq |V_1| = r$. Además, si $V' \subset V$ tiene más de r vértices, entonces $V' \cap V_1 \neq \emptyset$ y $V' \cap V_2 \neq \emptyset$, concluyendo que no puede ser independiente. De aquí se deduce que $\alpha(K_{r,s}) \leq r$.

Ahora contamos con todos los ingredientes necesarios para poder definir la sensibilidad de un grafo.

Definición 1.8. *La sensibilidad de un grafo $G = (V, E)$ es el menor valor entre los grados máximos de todos los grafos inducidos con más de $\alpha(G)$ vértices, es decir:*

$$\sigma(G) = \text{mín}\,\{\Delta([V']) \mid V' \subset V \text{ y } |V'| > \alpha(G)\}.$$

En general, el cálculo de $\sigma(G)$ es una tarea complicada, de hecho, como veremos más adelante, la Conjetura de Sensibilidad versa sobre el valor de este parámetro para una familia de grafos. En el Ejemplo 1.2, podemos observar el único subgrafo que no es independiente y además tiene más vértices que $\alpha(S_8) = 8$ es S_8, el cual tiene $\Delta(S_8) = 8$ y por tanto $\sigma(S_8) = 8$. Para cualquier grafo de esta familia S_k se deduce de forma análoga que $\sigma(S_k) = k$.

De la propia definición de la sensibilidad de un grafo $G = (V, E)$, podemos afirmar que $\sigma(G) \geq 1$ ya que todo grafo con más de $\alpha(G)$ vértices cuenta al menos con una arista concluyendo entonces que $\sigma(G) \geq 1$.

Proposición 1.9. *Sean $r \geq s \geq 1$ entonces:*

$$\sigma(K_{r,s}) = \text{máx}\left\{r - s + 1, \left\lceil \frac{r+1}{2} \right\rceil\right\}.$$

Demostración. Sea el grafo bipartito completo $K_{r,s}$ con vértices $V_1 \sqcup V_2 = V$ donde $|V_1| = r \geq s = |V_2|$.

Por la Proposición 1.7, sabemos que $\alpha(K_{r,s}) = r$ y sea $V' \subseteq V$ con $|V'| > r$ entonces $V' \cap V_1 \neq \emptyset$, $V' \cap V_2 \neq \emptyset$; además $\Delta([V']) = \text{máx}\{|V' \cap V_1|, |V' \cap V_2|\}$.

Como $r + 1 \leq |V'| = |V' \cap V_1| + |V' \cap V_2|$ se tiene que:

- $|V' \cap V_1| \geq \lceil \frac{r+1}{2} \rceil$ ó $|V' \cap V_2| \geq \lceil \frac{r+1}{2} \rceil$.
- $|V' \cap V_1| = |V'| - |V' \cap V_2| \geq |V'| - |V_2| \geq r - s + 1$.

Deducimos entonces que $\sigma(K_{r,s}) \geq \text{máx}\{r - s + 1, \lceil \frac{r+1}{2} \rceil\}$.

Ahora separamos los casos teniendo $V' = V_1' \cup V_2'$ donde $V_1' \subseteq V_1$ y $V_2' \subseteq V_2$:

1. Si $r - s + 1 \leq \lceil \frac{r+1}{2} \rceil$, entonces $s \geq r + 1 - \lceil \frac{r+1}{2} \rceil$ y tomando $V' = V_1' \cup V_2'$ con $|V_2'| = r + 1 - \lceil \frac{r+1}{2} \rceil \leq s$ y $|V_1'| = \lceil \frac{r+1}{2} \rceil \leq r$.
   Por tanto $\sigma(K_{r,s}) \leq \text{máx}\{|V_1'|, |V_2'|\} = |V_1'| = \lceil \frac{r+1}{2} \rceil$.
2. Si $r - s + 1 \geq \lceil \frac{r+1}{2} \rceil$ entonces tomando $V' = V_1' \cup V_2'$ con $|V_2'| = r - s + 1$ vemos que $\sigma(K_{r,s}) \leq \text{máx}\{r, r - s + 1\} = r - s + 1$.

1.2. Independientes máximos en grafos bipartitos y regulares

Si bien es cierto que para todos los grafos no existe una fórmula que nos facilite este parámetro, existen grafos en los que podemos obtener una fórmula para $\alpha(G)$, siendo un ejemplo de estos los grafos bipartitos y regulares. Más concretamente demostraremos que todo grafo bipartito regular tiene $\alpha(G) = \frac{n}{2}$. Para llegar a probar esto, antes demostraremos el Teorema 1.22 que afirma que todo grafo bipartito regular tiene un emparejamiento perfecto (ver Definición 1.16).

Definición 1.10. *Sea un grafo $G = (V, E)$, decimos que G es bipartito si existe una partición de V en dos independientes A y B, lo denotaremos:*

$$G = (A \sqcup B, E).$$

Veamos el siguiente ejemplo, en el que si colocamos los vértices de una manera más visual podemos ver claramente qué es un grafo bipartito:

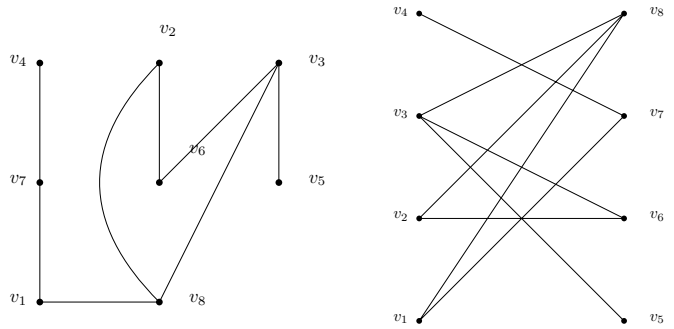

Figura 1.4: Dos dibujos de un mismo grafo bipartito.

En la Figura 1.4, podemos establecer una partición de los vértices del grafo en los conjuntos independientes $A = \{v_1, v_2, v_3, v_4\}$ y $B = \{v_5, v_6, v_7, v_8\}$. A lo largo de este proyecto, desarrollaremos diversas propiedades asociadas a estos grafos, que serán el principal objeto de estudio.

Definición 1.11. *Sea $d \in \mathbb{Z}^+$, se dice que un grafo es $d-$regular si todos sus vértices tienen el mismo grado d, es decir, si para todo vértice $v \in V$ tenemos que* $\deg(v) = d$.

Proposición 1.12. *Sea $G = (V, E)$ un grafo bipartito y $d-$regular donde $V = A \sqcup B$ y $|V| = n$, entonces $|A| = |B| = \frac{n}{2}$.*

Demostración. Dado $S \subset V$, denotamos por E_S al conjunto de aristas adyacentes a S, es decir, $E_S = \{\{v, u\} \in E \mid v \in S \text{ y } u \in V\}$.

Como G es un grafo bipartito, sabemos que el número de aristas que hay en el grafo están únicamente entre A y B, por tanto $|E_A| = |E_B| = |E|$ al ser un grafo regular donde todos los vértices tienen el mismo grado. Es por ello que podemos contar el número de aristas que llegan a cada conjunto, siendo entonces $|E_A| = |E_B| = d \cdot |A| = d \cdot |B|$. Si despejamos obtenemos que $|A| = |B|$, además al tratarse de un grafo bipartito, $A \sqcup B$ es una partición de V y podemos concluir que $|A| = |B| = \frac{n}{2}$.

Vamos a introducir algunas propiedades de los grafos bipartitos, pero para ello primero necesitamos definir los conceptos de camino y ciclo.

Definición 1.13. *En un grafo $G = (V, E)$, llamamos camino de longitud ℓ a una sucesión de vértices de la forma $p = (v_0, \dots, v_\ell)$, donde $\{v_0, \dots, v_\ell\} \subset V$ y $\{v_{i-1}, v_i\}$ es una arista para todo $1 \leq i \leq \ell$.*

Diremos que p es un camino cerrado si $v_0 = v_\ell$, y llamamos ciclo a todo camino cerrado que no pasa dos veces por un mismo vértice exceptuando el primero.

Proposición 1.14. *Sea un grafo bipartito $G = (A \sqcup B, E)$ y sea $p = (v_0, \dots, v_\ell)$ un camino en G. Si $v_0 \in A$, entonces $v_\ell \in A$ si y solo si ℓ es par. En particular, G no tiene caminos cerrados de longitud impar.*

Demostración. Dado que el grafo es bipartito, cualquier camino debe alternar entre vértices de A y B, de aquí se seduce directamente el resultado.

Como consecuencia, en un grafo bipartito $G = (A \sqcup B, E)$ podemos afirmar que todos los caminos cerrados y en particular los ciclos serán de longitud par, ya que empiezan y terminan en un mismo vértice.

Definición 1.15. *Un grafo conexo es aquel en el que entre cualquier par de vértices existe al menos un camino que los une. Sea un grafo $G = (V, E)$, llamamos componente conexa a los subgrafos conexos maximales, es decir, aquellos subgrafos conexos que no están estrictamente contenidos en ningún otro subgrafo conexo. Las componentes conexas forman una partición del mismo.*

Definición 1.16. *Sea un grafo $G = (V, E)$, llamamos emparejamiento a un conjunto de aristas $M \subset E$ sin vértices adyacentes entre si. Es decir, si $m, m' \in M$, y $m \neq m'$ entonces $m \cap m' = \emptyset$.*
Si todos los vértices del grafo pertenecen a una arista del emparejamiento, entonces se dice que es un emparejamiento perfecto. Es decir, para cualquier $v \in V$ existe $m \in M$ tal que $v \in m$.

Definición 1.17. *Sea un grafo $G = (V, E)$ y un emparejamiento $M \subset E$, llamamos $M-$camino alternado a todo camino que alterna entre aristas de M y de $\overline{M} = E - M$ (ver Figura 1.5). Denotaremos como $u - M-$camino alternado al que inicia en el vértice u. Diremos además que $p = (v_0, \dots, v_\ell)$ es un $M-$camino aumentado, si es un $M-$camino alternado tal que $v_0, v_\ell \notin V(M)$.*

Lema 1.18. *Sea un grafo conexo $G = (V, E)$ y $M \subset E$, todo $M-$camino aumentado es de longitud impar.*

Demostración. En un camino aumentado, tanto la primera como la última arista del camino pertenecen a $\overline{M}$ y, ya que es un camino alternado, debe tener longitud impar.

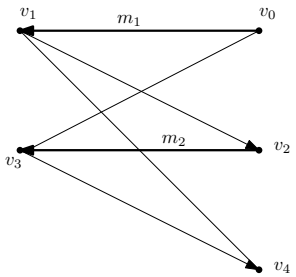

Figura 1.5: Ejemplo de camino $M-$alternado $p = (v_0, v_1, \ldots, v_4)$ para $M = \{m_1, m_2\}$, donde $m_1 = \{v_0, v_1\}$ y $m_2 = \{v_2, v_3\}$.

Definición 1.19. *Sean M y M' dos emparejamientos sobre un grafo $G = (V, E)$, llamamos diferencia simétrica de dos emparejamientos al subgrafo de G que tiene todos los vértices de G y sus aristas son las de la diferencia simétrica de M y M', es decir:*

$$M \Delta M' = (M - M') \cup (M' - M).$$

Lema 1.20. *Cualquier componente conexa de una diferencia simétrica de dos emparejamientos es un camino o un ciclo par.*

Demostración. Sean M y M' dos emparejamientos, y sea G' el grafo diferencia simétrica. Como M y M' son emparejamientos cualquier vértice de G' tiene como mucho dos aristas incidentes, en consecuencia $\Delta(G') \leq 2$. Consideramos C una componente conexa de G', entonces C debe ser un camino $M-$alternado (al tratarse G' de un grafo diferencia simétrica ya que de tener un vértice dos aristas adyacentes estas deben ser de diferente emparejamiento) si este camino es cerrado, debe ser un ciclo de longitud par ya que en este caso los vértices no pueden tener más de dos aristas adyacentes y, por tanto, no podemos pasar dos veces por un mismo vértice exceptuando el inicial, si no es cerrado, debe ser un camino $M-$alternado. En resumen, cualquier componente conexa es un camino $M-$alternado o un ciclo par.

Definición 1.21. *Un emparejamiento M es máximo si tiene el mayor número de aristas posibles. Es decir, es máximo si y solo si para cualquier emparejamiento M' de G resulta que $|M'| \leq |M|$.*

Teorema 1.22. *(Teorema de Berge) Sea un grafo $G = (V, E)$ y un emparejamiento $M \subset E$. Entonces M es un emparejamiento máximo de G si y solo si G no tiene M-caminos aumentados.*

Demostración. ($\Rightarrow$) Procederemos por contrarrecíproco, suponemos que G tiene un M-camino aumentado y vamos a demostrar que existe un emparejamiento M' tal que $|M'| > |M|$. Supongamos que G tiene un M-camino aumentado

$p = (v_0, v_1, \ldots, v_\ell)$ donde $e_i = \{v_{i-1}, v_i\}$ para todo $i \in \{1, \ldots, \ell\}$ y p pasa por todas las aristas de M.

Por un lado tenemos que $v_0, v_\ell \notin \cup_{e \in M} e$ ya que p es un camino aumentado, vemos que $e_i \notin M$ para todo $i \in \{1, \ldots, \ell\}$ impar y $e_i \in M$ para todo $i \in \{1, \ldots, \ell\}$ par.

Por el Lema 1.18, sabemos que para el M-camino aumentado $p = (v_0, v_1, \ldots, v_\ell)$ ℓ es impar, y por tanto si tomamos $M' = M - \{e_i \mid i\ par,\ 1 \leq i \leq \ell\} \cup \{e_i \mid i\ impar,\ 1 \leq i \leq \ell\}$, se observa que $|M'| = |M| + 1$, finalmente se observa que M' es un emparejamiento y $V(M') = V(M) \cup \{v_0, v_\ell\}$.

($\Leftarrow$) Por contrarrecíproco, sea M' un emparejamiento con $|M'| > |M|$, veamos que G tiene un $M-$camino aumentado. Consideramos G' el grafo diferencia simétrica de M y M', es decir, aquel con $V(G') = V(G)$ y $E(G') = M \Delta M' = E_1 \cup E_2$ y siendo $E_1 = M - M'$ y $E_2 = M' - M$, observamos que $|E_2| > |E_1|$ porque $|M'| > |M|$. Como $|E_2| > |E_1|$, entonces hay una componente conexa de G' donde hay más aristas de E_2 que de E_1, por tanto esta componente conexa no puede ser un ciclo par y por el Lema 1.20, es un camino. Podemos afirmar que podemos tomar $M-$camino aumentado, siendo la primera y la ultima aristas elementos de M'.

Definición 1.23. *Sea un grafo $G = (V, E)$ y un emparejamiento $M \subset E$, diremos que el vértice $v \in V$ es saturado por M si existe una arista $e \in M$ tal que $v \in e$. Además consideramos que un conjunto $V' \subset V$ será saturado por M si para cualquier vértice $u \in V'$ existe una arista $e \in M$ tal que $u \in e$.*

Teorema 1.24. *(Teorema de Hall) Sea un grafo bipartito $G = (A \sqcup B, E)$ y sea $X \subset V(G)$, entonces, existe un emparejamiento M tal que $X \subset V(M)$ si y solo si $|N(S)| \geq |S|$, $\forall S \subseteq X$.*

Demostración.

($\Rightarrow$) Sea un emparejamiento M tal que $X \subset V(M)$, para cualquier vértice $v \in X$ existe al menos una arista que lo una a otro vértice, por tanto $|N(S)| \geq |S|$ para cualquier $S \subseteq X$.

($\Leftarrow$) Veamos que si $|N(S)| \geq |S|$ para cualquier $S \subseteq X$, entonces para todo emparejamiento máximo M se tiene que $X \subset V(M)$.

Procedemos por contrarecíproco, sea M' un emparejamiento máximo tal que $X \not\subset V(M')$ veamos que existe $S \subseteq X$ tal que $|N(S)| < |S|$. Como $X \not\subset V(M')$ tomamos $\mu \in V(M') - X$. Todos los vértices alcanzables por $\mu - M'$*caminos alternos* en G, los dividimos en S y T siendo los pertenecientes a A y B respectivamente.

Incluimos el grafo de la Figura 1.6 como ejemplo ilustrado de la demostración:

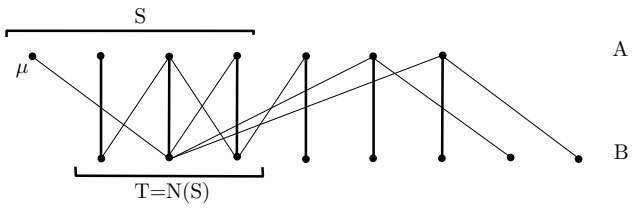

Figura 1.6: Grafo con un emparejamiento entre los vértices de $S - \{\mu\}$ y T, donde T es el conjunto de vértices vecinos de S.

M' empareja T con $S - \{\mu\}$ vértices. Cualquier $\mu - \ M'-$ camino alterno alcanza Y por aristas no pertenecientes a M' y vuelven a X por aristas de M' al ser el primer vértice μ no saturado y tratarse de un grafo bipartito.

Veamos que $|N(S)| < |S|$ para ello vemos que se cumplen:

$$i)|T| = |S - \{\mu\}| = |S| - 1.$$
$$ii)T = N(S).$$

$i)$ Para estimar $|T|$, vamos a establecer una biyección entre T y $S - \{\mu\}$ mediante la existencia de un emparejamiento perfecto para así poder afirmar que tienen el mismo número de elementos. Por hipótesis sabemos que cualquier vértice de $S - \{\mu\}$ es alcanzable por una arista perteneciente a M' pero para la existencia de un emparejamiento perfecto debemos demostrar que T también es alcanzable por una arista de M'.

De ser T únicamente alcanzable por una arista no perteneciente a M' entonces sería mediante un $\mu - M'$ camino aumentado, gracias al Teorema 1.22 como el emparejamiento es máximo entonces no hay caminos aumentados y por tanto el emparejamiento entre T y $S - \{\mu\}$ es perfecto.

Podemos entonces afirmar que T y $S - \{\mu\}$ tienen el mismo número de elementos estableciendo una biyección mediante las aristas del emparejamiento y concluyendo que $|T| = |S - \mu| = |S| - 1$.

$ii)$ Al ser un grafo bipartito sabemos que $T \subseteq N(S)$, como $|N(S)| \geq |T|$ queremos entonces ver que $T = N(S)$ para concluir que $|T| = |N(S)|$.

Sea $y \in Y - T$, veamos si existe $v \in S$ tal que $\{v, y\} \in E$, primero $\{v, y\} \notin M$ porque $S - \{\mu\}$ está emparejado con T y μ es no saturado, además $\{v, y\} \notin \overline{M}$ debido a que no existe un $\mu - M'$- camino alternado al no poder alcanzar y desde v, ya que $y \notin T$.

Como $T = N(S)$ y $T = |S| - 1$ entonces $|N(S)| = |S| - 1 < |S|$ quedando demostrado.

Proposición 1.25. *Sea $G = (A \sqcup B, E)$ un grafo bipartito y d-regular entonces $|N(S)| \geq |S|$ para cualquier $S \subset A$.*

Demostración. Sean los conjuntos de aristas $E_S = \{\{x,u\} \in E \mid x \in S\} \subseteq E_{N(S)} = \{\{u,v\} \mid u \in N(S)\}$. Por tanto $|E_{N(S)}| \geq |E_S|$, como G es un grafo bipartito y $d-$ regular, podemos decir que $|E_S| = d \cdot |S|$ y $|E_{N(S)}| = d \cdot |N(S)|$, siendo entonces $d \cdot |N(S)| \geq d \cdot |S|$ y concluyendo que $|N(S)| \geq |S|$ para cualquier $S \subset A$.

Teorema 1.26. *(Teorema del matrimonio) Sea $G = (A \sqcup B, E)$ un grafo bipartito y regular, entonces existe un emparejamiento perfecto M.*

Demostración. Como G es un grafo bipartito y regular, entonces para cualquier $S \subset A$ tenemos que $|N(S)| \geq |S|$ por la Proposición 1.25. Por el Teorema de Hall 1.24 existe un emparejamiento M que satura A y como $|A| = |B| = \frac{n}{2}$ por la Proposición 1.12 al ser un grafo bipartito y regular, podemos afirmar que se trata de emparejamiento perfecto.

Corolario 1.27. *Sea $G = (A \sqcup B, E)$ un grafo bipartito y regular, si S es un conjunto de más de $\frac{n}{2}$ vértices, no es un independiente.*

Demostración. Sea $S \subset V$ con $|S| > \frac{n}{2}$ veamos que S no es un independiente. Al tratarse de un grafo bipartito y regular por el Teorema del matrimonio sabemos que existe un emparejamiento perfecto M entre A y B independientes. Además por la Proposición 1.12 afirmamos que $|A| = |B| = \frac{n}{2}$. Finalmente concluimos que si $|S| > \frac{n}{2}$ entonces existiría al menos una arista del emparejamiento M entre dos vértices de S y, por tanto, S no es un independiente.

Corolario 1.28. *Sea $G = (A \sqcup B, E)$ un grafo bipartito y regular tal que $|V| = n$ entonces $\alpha(G) = \frac{n}{2}$.*

Demostración. Por la Proposición 1.12, al tratarse G de un grafo bipartito y regular entonces $|A| = |B| = \frac{n}{2}$. Como A y B son independientes tales que $|A| = |B| = \frac{n}{2}$, entonces $\alpha(G) \geq \frac{n}{2}$. Finalmente, se tiene que $\alpha(G) = \frac{n}{2}$ por el Corolario 1.27.

1.3. Sensibilidad en grafos bipartitos y regulares

1.3.1. Sensibilidad de los grafos bipartitos completos regulares

La sensibilidad de un grafo puede ser estudiada en cualquier grafo, pero para todos ellos no se conoce una fórmula que la describa. En esta subsección, calcularemos este parámetro en los grafos bipartitos completos regulares.

Los únicos grafos bipartitos completos regulares son los $K_{s,s}$ con $s \geq 1$, en los cuales $|V(K_{s,s})| = 2s$ y para cualquier $v \in V(K_{s,s})$ tendremos que $\deg(v) = s$. En estos grafos el tamaño del independiente máximo tendrá s vértices, ya que al ser bipartito y regular $\alpha(G) = \frac{|V|}{2}$ por el Corolario 1.28.

En la Figura 1.7 vemos el grafo bipartito y regular $K_{3,3} = (A \sqcup B, E)$ donde $|A| = |B| = 3$ y para cualquier vértice $v \in V(K_{3,3})$ tenemos que $\deg(v) = 3$.

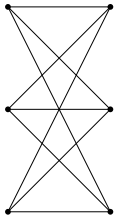

Figura 1.7: Grafo bipartito y regular $K_{3,3}$.

Proposición 1.29. *Sea el grafo bipartito completo y regular $K_{s,s}$, entonces:*

$$\sigma(K_{s,s}) = \left\lceil \frac{s+1}{2} \right\rceil.$$

Demostración. Denotamos $K_{s,s} = (V, E)$ con $V = A \sqcup B$. Antes que nada, al tratarse de un grafo bipartito completo y regular, sabemos que el tamaño del independiente máximo será $\alpha(K_{s,s}) = s$. Ahora, en este caso al ser $K_{s,s}$ un grafo bipartito, tomamos $V' \subseteq V$ y recordemos la definición de sensibilidad:

$$\sigma(K_{s,s}) = \text{mín}\,\{\Delta([V']) \mid V' \subset V \text{ y } |V'| > s\}.$$

Tomamos $V' \subset V$ con $|V'| \geq s+1$, tenemos que $|V' \cap A| + |V' \cap B| = |V'|$. Ahora bien, el grafo inducido $[V']$ se trata de un grafo bipartito completo, donde para todo $v_1 \in V' \cap A$ sabemos que $\deg(v_1) = |V' \cap B|$ y análogamente para todo $v_2 \in V' \cap B$ tendremos que $\deg(v_2) = |V' \cap A|$, deduciendo entonces que $\Delta([V']) = \text{máx}\{\ |V' \cap A|\ ,\ |V' \cap B|\ \}$.

Teniendo en cuenta que $|V' \cap A| + |V' \cap B| = |V'|$, si $|V' \cap A| \leq \frac{s+1}{2}$ entonces $|V' \cap B| \geq \frac{s+1}{2}$, ya que $|V' \cap A| + |V' \cap B| = |V'|$ y $|V'| \geq m+1$. Por tanto, $\Delta([V']) = |V' \cap B| \geq \frac{s+1}{2}$.

Si $|V' \cap B| \leq \frac{s+1}{2}$ siguiendo un razonamiento análogo se deduce que $\Delta([V']) = |V' \cap A| \geq \frac{s+1}{2}$. Veamos que $\Delta([V']) \geq \frac{s+1}{2}$ y por definición de sensibilidad:

$$\sigma(K_{s,s}) \geq \left\lceil \frac{s+1}{2} \right\rceil.$$

Para demostrar que $\sigma(K_{s,s}) \leq \left\lceil \frac{s+1}{2} \right\rceil$, basta con justificar que existe $V' \subset V$ tal que $|V'| > s$ y $\Delta([V']) = \left\lceil \frac{s+1}{2} \right\rceil$ y, en efecto, si tomamos V' tal que $V' \cap A = \left\lfloor \frac{s+1}{2} \right\rfloor$ y $|V' \cap B| = \left\lceil \frac{s+1}{2} \right\rceil$, entonces $|V'| = \left\lfloor \frac{s+1}{2} \right\rfloor + \left\lceil \frac{s+1}{2} \right\rceil = s+1$ y $\Delta([V']) = \left\lceil \frac{s+1}{2} \right\rceil$.

Por tanto, concluimos que $\sigma(K_{s,s}) = \left\lceil \frac{s+1}{2} \right\rceil$.

Veamos el siguiente ejemplo:

Si queremos calcular la sensibilidad de $K_{3,3}$, veamos los posibles subgrafos inducidos con más vértices que $\alpha(K_{3,3}) = 3$:

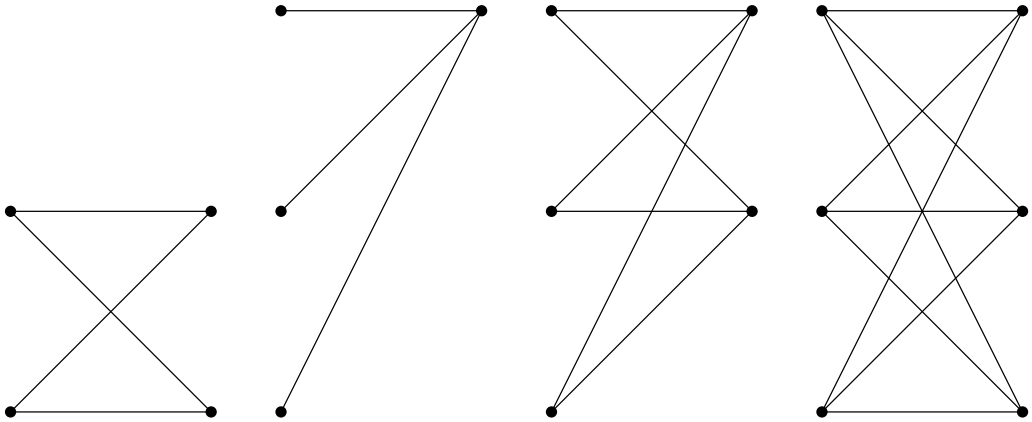

Figura 1.8: Subgrafos inducidos de $K_{3,3}$ con al menos 4 vértices, en el de la izquierda su grado máximo es 2, en los demás es 3.

En la Figura 1.8 se incluyen todos los subgrafos inducidos de 4 vértices y se observa que $\sigma(K_{3,3}) = 2$. La Proposición 1.29 confirma que la sensibilidad del grafo $K_{3,3}$ es $\sigma(K_{3,3}) = 2$.

1.3.2. Enunciado de la conjetura

Para poder enunciar y comprender la conjetura, será necesario definir el grafo del hipercubo ya que la Conjetura de la Sensibilidad nos da una cota inferior de la sensibilidad para este tipo de grafo.

Definición 1.30. *Llamamos hipercubo n-dimensional al grafo bipartito y n-regular Q^n, con conjunto de vértices $V(Q^n) = \{0,1\}^n$ siendo en este grafo dos vértices adyacentes si difieren en una única coordenada.*

En estos grafos para un vértice $v \in V(Q^n)$ denotaremos el peso del vértice como $|v|$ siendo el número de unos con los que cuenta el vértice.

Lema 1.31. *El hipercubo n-dimensional Q^n es un grafo bipartito $n-$regular, con 2^n vértices y $\alpha(Q^n) = 2^{n-1}$.*

Demostración. Para ver que es bipartito basta con considerar $A = \{v \in V(Q^n) \mid |v| \text{ es par}\}$ y $B = \{v \in V(Q^n) \mid |v| \text{ es impar}\}$, y observar que toda arista une un vértice de A con uno de B. Además, si $(x_1, \ldots, x_n) \in V(Q^n)$, sus n vecinos son $(x_1, \ldots, x_{i-1}, 1 - x_i, x_{i+1}, \ldots, x_n)$ con $i \in \{1, \ldots, n\}$ y, por tanto, es $n-$regular. Como $|V(Q^n)| = 2^n$, por el Corolario 1.28 deducimos que $\alpha(Q^n) = 2^{n-1}$.

En la Figura 1.9, vemos la bipartición de Q^3 en los conjuntos $A = \{010, 100, 001, 111\}$ y $B = \{000, 110, 011, 101\}$.

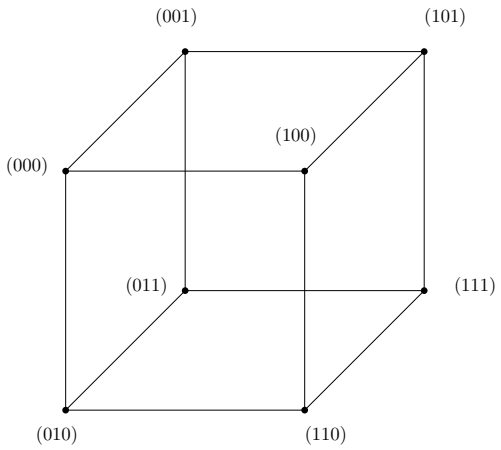

Figura 1.9: Representación de Q^3.

Ahora constamos de los ingredientes necesarios para introducir el enunciado de la conjetura.

Teorema 2.14. (Conjetura de la Sensibilidad en términos de la Teoría de Grafos) Sea Q^n el grafo del hipercubo $n-$dimensional con $n \geq 1$, y sea H un subgrafo inducido por $2^{n-1}+1$ vértices de Q^n, entonces:

$$\Delta(H) \geq \sqrt{n}.$$

Por el Lema 1.31 sabemos que $\alpha(Q^n) = 2^{n-1}$. Por tanto, teniendo en cuenta la definición de sensibilidad de un grafo (Definición 1.8), el enunciado de la Conjetura de la Sensibilidad es equivalente a:

$$\sigma(Q^n) \geq \sqrt{n}.$$

2

Demostración de la conjetura usando Teoría de Grafos

En este capítulo, vamos a estudiar la demostración de la Conjetura de la Sensibilidad en términos de la Teoría de Grafos obtenida por Huang [8]. Para ello vamos a necesitar varias herramientas del Álgebra Lineal, como el concepto de matriz de adyacencia de un grafo, así como el Teorema del entrelazamiento de Cauchy (mostraremos en esta memoria la demostración de [15]), resultados esenciales en nuestro trabajo.

2.1. Teorema del entrelazamiento

Definición 2.1. *Sea V un $\mathbb{R}$-espacio vectorial, un producto escalar o producto interior es una aplicación $\langle , \rangle : V \times V \to \mathbb{R}$ verificando:*

(i) Es simétrica, es decir, $\langle u, w\rangle = \langle w, u\rangle$ para cualquier $u, w \in V$.

(ii) Es bilineal $\langle u+v, w\rangle = \langle u, w\rangle + \langle v, w\rangle$ y $u, v, w \in V$. Además $\langle \alpha u, w\rangle = \alpha\langle u, w\rangle$ para cualquier $\alpha \in \mathbb{R}$, $u, v, w \in V$.

(iii) Es definida positiva, para cualquier $u \in V$ tal que $\langle u, u\rangle \geq 0$ y además $\langle u, u\rangle = 0$ si y sólo si $u = 0$.

De todos los productos escalares que se pueden definir en $\mathbb{R}^n$, nosotros trabajaremos con el usual, que recordamos a continuación.

Definición 2.2. *Sea el espacio euclideo $\mathbb{R}^n$ y los vectores $u = (u_1, \ldots, u_n)$, $v = (v_1, \ldots, v_n) \in \mathbb{R}^n$, definimos producto escalar usual de u y v como la suma de los productos de las componentes de cada vector, es decir,*

$$\langle u, v\rangle = u \cdot v^T = u_1 \cdot v_1 + u_2 \cdot v_2 + \cdots + u_n \cdot v_n.$$

Para los siguientes resultados, recordamos que $A \in M_{n\times n}$ es una matriz simétrica si, y sólo si, $A = A^T$.

Lema 2.3. *Sean $u, v \in \mathbb{R}^n$ y $A \in M_{n\times n}(\mathbb{R})$ entonces $\langle Au, v\rangle = \langle u, A^T v\rangle$. Por tanto si A es simétrica, entonces $\langle Au, v\rangle = \langle u, A^T v\rangle$.*

Demostración. $\langle Au, v\rangle = (Au)^T \cdot v = (u^T A^T) \cdot v = u^T \cdot (A^T v) = \langle u, A^T v\rangle$.

Proposición 2.4. *Sea A una matriz simétrica y real, entonces todos los valores propios de A son reales, es decir, todas las raíces del polinomio característico de A son reales. Equivalentemente, si $Aw = \lambda w$ donde $\lambda \in \mathbb{C}$, $w \in \mathbb{C}^n$ y $w \neq 0$, entonces $\lambda \in \mathbb{R}$.*

Demostración. Sea $w \in \mathbb{C}^n$ tal que $w \neq 0$ donde $Aw = \lambda w$, tenemos que $w = u + iv$ con $u, v \in \mathbb{R}^n$ además para λ autovalor complejo, sabemos que $\lambda = a + ib$ con $a, b \in \mathbb{R}$. Vamos a demostrar que $b = 0$:
$A(u + iv) = Aw = \lambda w = (a + ib)(u + iv) = (au - bv) + i(av + bu)$ de donde deducimos que $Au = au - bv$ y $Av = av + bu$. Por hipótesis A es simétrica por tanto $\langle Au, v\rangle = \langle u, Av\rangle$. Finalmente:

$$(i)\ \langle Au, v\rangle = \langle au - bv, v\rangle = \langle au, v\rangle - \langle bv, v\rangle = a\langle u, v\rangle - b\langle v, v\rangle.$$
$$(ii)\ \langle u, Av\rangle = \langle u, av + bu\rangle = \langle au, v\rangle + \langle bu, u\rangle = a\langle u, v\rangle + b\langle u, u\rangle.$$

Por tanto, si restamos concluimos que $b(\langle u, u\rangle + \langle v, v\rangle) = 0$. Se tiene $\langle u, u\rangle \geq 0$ y $\langle v, v\rangle \geq 0$ y no son ambos nulos, así que $b = 0$ y $\lambda \in \mathbb{R}$.

Definición 2.5. *Sea U un $\mathbb{R}-$espacio vectorial y $V \subset U$, llamaremos subespacio ortogonal de V a:*

$$V^{\perp} = \{u \in U \mid \langle u, v\rangle = 0,\ \forall v \in V\}.$$

Diremos que dos subespacios vectoriales V_1 y V_2 son ortogonales si $\forall v_1 \in V_1$ y $\forall v_2 \in V_2$ tenemos que $\langle v_1, v_2\rangle = 0$.

Lema 2.6. *Sea A la matriz simétrica y real y $\lambda, \mu \in \mathbb{R}$ autovalores distintos de A, entonces V_λ y V_μ son ortogonales.*

Demostración. Para cualquier $u \in V_\lambda$ y $u \in V_\mu$ si $\langle Au, v\rangle = \langle \lambda u, v\rangle = \langle \lambda u, v\rangle$ y además $\langle u, Av\rangle = \langle u, \mu v\rangle = \langle \mu u, v\rangle$. Como A es simétrica, estos resultados son iguales y como $(\lambda - \mu) \neq 0$, tenemos que:

$$(\lambda - \mu)\langle u, v\rangle = 0 \Rightarrow \langle u, v\rangle = 0.$$

Teorema 2.7. *(Teorema espectral) Toda matriz simétrica real es diagonalizable en $\mathbb{R}$. Además existe una base ortonormal de $\mathbb{R}^n$ formada por autovectores.*

Demostración. Sea la matriz simétrica A. Por la Proposición 2.4 sabemos que todos los autovalores van a ser reales, veamos que $\mathbb{R}^n$ tiene una base formada por autovectores. Sea $U = V_{\lambda_1} \oplus \cdots \oplus V_{\lambda_r} \subset V = \mathbb{R}^n$. Queremos ver que $U = \mathbb{R}^n$ para ello demostraremos que $U^{\perp} = 0$, por reducción al absurdo supongamos que $U \neq \mathbb{R}^n$ siendo $U^{\perp} \neq 0$. Para cualquier $u \in V_{\lambda_i}$ como $Au = \lambda_i u$, si $U^{\perp} \neq 0$ entonces para cualquier $u \in U y\ v \in U^{\perp}$ deducimos que $\langle Av, u\rangle = \langle v, Au\rangle = 0$,

es decir, $AU^{\perp} \subset U^{\perp}$. Como $\dim(U^{\perp}) \geq 1$ para al menos un autovector $v \in U^{\perp}$ tal que $v \neq 0$ tendremos que $Av = \lambda v$ y por tanto $v \in U$ contradiciendo que $U \cap U^{\perp} = \emptyset$, finalmente $U = V_{\lambda_1} \oplus \cdots \oplus V_{\lambda_r} = \mathbb{R}^n$.

Para una matriz simétrica real A por el método de Gram-Schmidt [3], podemos obtener una base ortonormal para cada V_{λ_i} y gracias a el Lema 2.6, su unión será base de $\mathbb{R}^n$, formada por autovectores ortonormales.

El siguiente lema será vital para la demostración del Teorema del entrelazamiento.

Lema 2.8. *(Pricipio de Raylaigh) Sea $A \in M_{n\times n}(\mathbb{R})$ una matriz simétrica y real donde $\lambda_1 \geq \cdots \geq \lambda_n$ son los autovalores de A con $\lambda_i \in \mathbb{R}$ y $\{u_1, \ldots, u_n\}$ una base ortonormal de $\mathbb{R}^n$ tal que $Au_i = \lambda_i u_i$, entonces:*

$$(i)\ \textit{Si } u \in \langle u_1, \ldots, u_i\rangle \textit{ entonces } \tfrac{\langle u, Au\rangle}{\langle u, u\rangle} \geq \lambda_i.$$
$$(ii)\ \textit{Si } u \in \langle u_1, \ldots, u_i\rangle^{\perp} \textit{ entonces } \tfrac{\langle u, Au\rangle}{\langle u, u\rangle} \leq \lambda_i.$$

Demostración. Para la demostración recordemos que al ser $\{u_1, \ldots, u_n\}$ una base ortonormal $u_i \cdot u_j = \begin{cases} 1 \textit{ si } i = j \\ 0 \textit{ si } i \neq j \end{cases}$
(i) Sea $u = \alpha_1 u_1 + \cdots + \alpha_i u_i$ entonces:

$$\begin{aligned} Au &= A(\alpha_1 u_1 + \cdots + \alpha_i u_i) = \\ &= \alpha_1 Au_1 + \cdots + \alpha_i Au_i = \\ &= \alpha_1\lambda_1 u_1 + \cdots + \alpha_i\lambda_i u_i. \end{aligned}$$

Vemos finalmente:

$$\begin{aligned} \langle u, Au\rangle &= \langle(\alpha_1 u_1 + \cdots + \alpha_i u_i), (\alpha_1\lambda_1 u_1 + \cdots + \alpha_i\lambda_i u_i)\rangle = \\ &= {\alpha_1}^2\lambda_1 + \cdots + {\alpha_i}^2\lambda_i \geq {\alpha_1}^2\lambda_i + {\alpha_2}^2\lambda_i + \cdots + {\alpha_i}^2\lambda_i = \\ &= \lambda_i\langle u, u\rangle. \end{aligned}$$

(ii) Sea $u = \alpha_i u_i + \cdots + \alpha_n u_n$ entonces:

$$\begin{aligned} Au &= A(\alpha_i u_i + \cdots + \alpha_i u_i) = \\ &= \alpha_i Au_i + \cdots + \alpha_n Au_n = \\ &= \alpha_i\lambda_i u_i + \cdots + \alpha_n\lambda_n u_n. \end{aligned}$$

Al igual que antes:

$$\begin{aligned} \langle u, Au\rangle &= \langle(\alpha_i u_i + \cdots + \alpha_n u_n), (\alpha_i\lambda_i u_i + \cdots + \alpha_n\lambda_n u_n)\rangle = \\ &= {\alpha_i}^2\lambda_i + \cdots + {\alpha_n}^2\lambda_n \leq {\alpha_1}^2\lambda_i + \cdots + {\alpha_i}^2\lambda_i = \\ &= \lambda_i\langle u, u\rangle. \end{aligned}$$

Definición 2.9. *Sea una matriz cuadrada A, llamamos submatriz principal de A a cualquier matriz resultante de eliminar k filas y las correspondientes k columnas.*

Corolario 2.10. *(Teorema del entrelazamiento) Sea A una matriz simétrica de orden n y B una submatriz principal de A de orden m. Si $\lambda_n \leq \lambda_{n-1} \leq \cdots \leq \lambda_2 \leq \lambda_1$ son los autovalores de A y $\mu_m \leq \cdots \leq \mu_3 \leq \mu_2 \leq \mu_1$ los autovalores de B, entonces para cualquier $i \in \{1, \ldots, n\}$:*

$$\lambda_i \geq \mu_i \geq \lambda_{n-m+i}.$$

Demostración. Observamos que tanto A como B son simétricas reales y, por tanto A como B son diagonalizables en $\mathbb{R}$. Supongamos sin pérdida de generalidad que B está formada por las primeras m filas y columnas de A. Se observa que $B = S^T AS$, siendo:

$$S = \begin{pmatrix} 1\,0 \ldots 0 \\ 0\,1 \ldots 0 \\ \quad \ddots \\ 0\,0 \ldots 1 \\ 0\,0 \ldots 0 \\ 0\,0 \ldots 0 \end{pmatrix} \in \mathbb{M}_{n\times m}(\mathbb{R}).$$

Sean $\{u_1, \ldots, u_n\}$ y $\{v_1, \ldots, v_m\}$ bases ortonormales de $\mathbb{R}^n$ y $\mathbb{R}^m$ con $Au_i = \lambda_i u_i$ y $Bv_j = \mu_j v_i$.

En primer lugar, tomando $W_i = \langle v_1, \ldots, v_i\rangle \cap \langle S^T u_1, \ldots, S^T u_{i-1}\rangle^{\perp} \subseteq \mathbb{R}^m$ para $i \in \{1, \ldots, m\}$ entonces $\dim(\langle v_1, \ldots, v_i\rangle) = i$, y como:

$$\dim(\langle S^T u_1, \ldots, S^T u_{i-1}\rangle) \leq i - 1.$$

Deducimos entonces que:

$$\dim(\langle S^T u_1, \ldots, S^T u_{i-1}\rangle^{\perp}) \geq m - (i-1).$$

Utilizando la fórmula de las dimensiones se tiene que:

$$\begin{aligned} \dim\,(W_i) =& \dim(\langle v_1, \ldots, v_i\rangle) + \dim(\langle S^T u_1, \ldots, S^T u_{i-1}\rangle) - \\ & - \dim(\langle v_1, \ldots, v_i\rangle + \langle S^T u_1, \ldots, S^T u_{i-1}\rangle) \geq \\ & \geq i + m - (i-1) - m = 1. \end{aligned}$$

Podemos concluir que $\dim(W_i) \geq 1$, y finalmente si aplicamos el Principio de Raylaigh 2.8 para $w \in W_i - \{0\}$, tenemos que:

$$(i)\ \frac{\langle w_i, Bw_i\rangle}{\langle w_i, w_i\rangle} \geq u_i.$$

$$(ii)\ \frac{\langle w_i, Bw_i\rangle}{\langle w_i, w_i\rangle} = \frac{w_i^T \cdot S^T ASw_i}{w_i^T \cdot Iw_i} = \frac{w_i^T \cdot S^T ASw_i}{{w_i}^T \cdot S^T Sw_i} = \frac{\langle (Sw_i), A(Sw_i)\rangle}{\langle (Sw_i)^T, (Sw_i)\rangle} \leq \lambda_i.$$

Como consecuencia de (i) y (ii) tenemos que $\lambda_i \geq \mu_i$. Ahora veremos que $\mu_i \geq \lambda_{n-m+i}$ para ello tomaremos en lugar de A y B las matrices $-A$ y $-B$ respectivamente, donde evaluando los autovalores vemos que $-\lambda_1 \leq -\lambda_2 \leq \cdots \leq \lambda_n$ y que $-\mu_1 \leq \cdots \leq -\mu_m$. Recurrimos a un cambio de variable $\lambda'_i = -\lambda_{n-i+1}$ y $\mu'_i = -\mu_{m-i+1}$, concluyendo que como ya hemos visto $\lambda'_i \leq u'_i$ para cualquier $i \in \{1, \ldots, m\}$ y por tanto $\mu_{m-i+1} \geq \lambda_{n-i+1}$ para cualquier $i \in \{1, \ldots, m\}$. Si llamamos a $j = m-i+1$ vemos que $\mu_j \geq \lambda_{n-m+j}$, entonces ya que $i \in \{i, \ldots, m\}$ tenemos $j \in \{1, \ldots, m\}$ y como $\mu_i \geq \lambda_{n-m+i}$, podemos finalmente afirmar que:

$$\lambda_i \geq \mu_i \geq \lambda_{n-m+i}.$$

2.2. Demostración de la Conjetura de la Sensibilidad

En esta sección vamos a desarrollar la prueba de la Conjetura de la Sensibilidad en términos de la Teoría de Grafos de Huang, que nos dice que cualquier subgrafo inducido del hipercubo Q^n con al menos $2^{n-1}+1$ vértices tendrá grado máximo $\sqrt{n}$, es decir, $\Delta(H) \geq \sqrt{n}$, para ello vamos a introducir los últimos resultados necesarios, estos se encuentran en el artículo [8].

Lema 2.11. *Sea $\mu \in \mathbb{N}$ y I_{2^μ} la matriz identidad de dimensión 2^μ, definimos la secuencia de matrices cuadradas y simétricas siguiente:*

$$A_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \ , \ A_{\mu+1} = \begin{bmatrix} A_\mu & I_{2^\mu} \\ I_{2^\mu} & -A_\mu \end{bmatrix}. \tag{2.1}$$

Entonces A_n es una matriz de $2^n \times 2^n$ con autovalores $\sqrt{n}$ y $-\sqrt{n}$ de multiplicidad 2^{n-1}.

Demostración. Por inducción $A_n^2 = nI_{2^n}$. Para $n = 1$ $A_1^2 = I_2$. Suponemos que se cumple para $n-1$ de forma que $A_{n-1}^2 = (n-1)I_{2^{n-1}}$, entonces:

$$A_n^2 = \begin{bmatrix} A_{n-1}^2 + I_{2^{n-1}} & 0 \\ 0 & A_{n-1}^2 + I_{2^{n-1}} \end{bmatrix} = nI_{2^n}. \tag{2.2}$$

Por tanto, los autovalores de A_n son $\sqrt{n}$ o $\sqrt{-n}$. Ya que $\mathrm{Tr}(A_n) = 0$ sabemos que A_n tiene exactamente la mitad de autovalores $\sqrt{n}$ y la otra mitad $-\sqrt{n}$.

Lema 2.12. *Sea $H = (V, E)$ un grafo con $V = \{v_1, \ldots, v_n\}$ y, sea $(A_{i,j}) = A \in \mathbb{M}_{n\times n}(\mathbb{R})$ una matriz simétrica tal que $A_{i,j} = 0$ si $\{v_i, v_j\} \notin E(H)$ y $A_{i,j} = A_{j,i} \in \{1, -1\}$ si $\{v_i, v_j\} \in E$. Si λ_1 es el mayor autovalor de la matriz A, entonces:*

$$\Delta(H) \geq \lambda_1.$$

Demostración. Supongamos que $w = (w_1, \ldots, w_n) \in \mathbb{R}^n$ es un autovector correspondiente a λ_1. Entonces $\lambda_1 w = Aw$. Nuevamente sin perdida de generalidad, asumimos que w_1 es la mayor coordenada en valor absoluto de w. Como:

$$|\lambda_1 w_1| = |\sum_{j=1}^{m} A_{1,j} w_j| \leq \sum_{j=1}^{m} |A_{1,j}||w_j| \leq \Delta(H)|w_j|.$$

Concluimos que $|\lambda_1| \leq \Delta(H)$ ya que $w_1 \neq 0$.

Definición 2.13. *Sea el grafo $G = (V, E)$, llamamos matriz de adyacencia a la matriz cuadrada $A(G) = (Au, v)$ y $u, v \in V$ que representa la relación entre los vértices del grafo, de forma que si para $u, v \in V$ existe $\{u, v\} \in E$, entonces $A_{u,v} = 1$ y en caso contrario $A_{u,v} = 0$.*

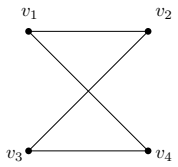

Figura 2.1: Grafo G.

La matriz de adyacencia del grafo G de la Figura 2.1 con $V = \{v_1, v_2, v_3, v_4\}$ es:

$$A(G) = \begin{pmatrix} 0\,1\,0\,1 \\ 1\,0\,1\,0 \\ 0\,1\,0\,1 \\ 1\,0\,1\,0 \end{pmatrix}.$$

Cabe destacar que esta matriz depende de cómo ordenamos los vértices.

Ya estamos dispuestos para presentar la demostración de la Conjetura de la Sensibilidad, enunciada en la Subsección 1.3.2. Veremos que para un subgrafo de dimensión n inducido por $2^{n-1} + 1$ vértices tiene al menos como grado máximo $\sqrt{n}$.

Teorema 2.14. *Sea Q^n, el grafo del hipercubo n-dimensional con $n \geq 1$, sea H un subgrafo inducido por $2^{n-1} + 1$ vértices de Q^n entonces:*

$$\Delta(H) \geq \sqrt{n}.$$

Demostración. Si consideramos la secuencia de matrices A_n como en el Lema 2.11, donde todas las entradas de A_n son $\{1, 0 - 1\}$ de la forma:

$$A_{n+1} = \begin{bmatrix} A_n & I_{2n} \\ I_{2n} & -A_n \end{bmatrix}. \tag{2.3}$$

Podemos observar que si intercambiamos cualquier -1 por 1 en A_n, obtenemos la matriz de adyacencia $A(Q^n)$ del grafo Q^n. Por el Lema 2.11, sabemos que los autovalores de A_n son $\lambda_i = \sqrt{n}$ para todo $i \in \{1, \ldots, 2^{k-1}\}$ y $\lambda_i = -\sqrt{n}$ para todo $i \in \{2^{k-1}+1, \ldots, n\}$. Si consideramos A' submatriz principal de A_n con al menos $2^{k-1}+1$ vértices, podemos obtener de la misma forma una matriz de adyacencia de un subgrafo H de Q^n, de manera general, si aplicamos el Teorema del entrelazamiento 2.10, donde $n = 2^d$ y por hipótesis tomamos $m \geq 2^{d-1}+1$, vemos que:

$$n - m + 1 \leq 2^d - (2^{d-1}+1) + 1 = 2^{d-1}.$$

Concluyendo que $\sqrt{n} = \lambda_1 \geq \mu_1 \geq \lambda_{n-m+1} \geq \lambda_{2^{d-1}} = \sqrt{n}$, entonces $\mu_1 = \sqrt{n}$.

Finalmente por el Lema 2.12 sabemos que $\Delta(H) \geq \sqrt{n}$.

Esta reescritura de la Conjetura de la Sensibilidad en términos de los grafos mejora la primera parte de un resultado previo, publicado por Chung, Füredi, Graham y Seymour en [5].

Teorema 2.15. *(Chung, Füredi, Graham y Seymour) Sea H un grafo inducido por el hipercubo Q^n con al menos $2^{n-1}+1$ vértices, entonces:*

$$\Delta(H) \geq \frac{1}{2}\log(n) - \frac{1}{2}\log\log(n) + \frac{1}{2}.$$

Además existe un subgrafo H inducido de Q^n con $2^{n-1}+1$ vértices y:

$$\Delta(H) < \sqrt{n} + 1.$$

Los autores en el Teorema 2.15 encuentran una cota inferior del grado máximo de un grafo inducido sobre el hipercubo. Además, prueban la existencia de un grafo inducido de Q^n con $2^{n-1}+1$ vértices y $\Delta(H) < \sqrt{n}+1$. Huang mejora notablemente la cota inferior del grado máximo de estos grafos inducidos en el Teorema 2.14, ya que demuestra que para todo subgrafo inducido H del hipercubo Q^n con $2^{n-1}+1$ vértices entonces $\Delta(H) \geq \sqrt{n}$.

Ahora bien, Chung, Füredi, Graham y Seymour probaron en la segunda parte del Teorema 2.15 que existe un grafo inducido H de Q^n con $2^{n-1}+1$ vértices y $\Delta(H) < \sqrt{n}+1$. Este grafo será una cota superior de la sensibilidad en el hipercubo Q^n, de forma que $\sigma(Q^n) < \sqrt{n}+1$. Además por el Teorema 2.14 $\sigma(Q^n) \geq \sqrt{n}$. Juntando los Teoremas 2.14 y 2.15 tenemos el valor exacto de la sensibilidad del hipercubo:

$$\sigma(Q^n) = \lceil \sqrt{n} \rceil.$$

3

Funciones Booleanas

Tras haber probado la reescritura de la Conjetura de la Sensibilidad en términos de la Teoría de Grafos de Hao Huang, podemos ver las consecuencias de esta prueba. Esta demostración nos permite dar respuesta al problema planteado originalmente en el año 1994 [11] por Nisan y Szegedy, el cual estaba abierto hasta el año 2019 y versaba sobre el estudio de las funciones booleanas.

Las funciones booleanas son aplicaciones de $\{0,1\}^n \to \{0,1\}$, y son utilizadas en diversos campos como la lógica, la criptografía, la teoría de juegos y la electrónica digital. Asociada a las funciones booleanas hay varias medidas de complejidad, que buscan cuantificar cuan compleja es una de estas funciones para así poder hacer una estimación de los recursos necesarios por parte de los sistemas computacionales para poder hacer los cálculos que se ven representados a través de estas funciones.

Hay varios resultados (ver [1],[10] o [11]) que afirman que algunas de las medidas de complejidad que veremos en este trabajo son equivalentes, es decir, se puede acotar superiormente una en función de la otra a través de una expresión polinomial y viceversa. En los años 90, se había probado que todas estas medidas de complejidad eran equivalentes entre si excepto la sensibilidad, sobre la cual sólo se sabía que esta estaba acotada superiormente por la sensibilidad por bloques de una función booleana. En [11] Nisan y Szegedy conjeturan que es posible encontrar una cota superior de la sensibilidad en bloques en términos de una expresión polinomial de la sensibilidad, lo cual servirá para concluir que estas dos medidas de complejidad son equivalentes. Esto lo que conocemos como la Conjetura de la Sensibiliad.

En este capítulo buscamos entender la Conjetura de la Sensibilidad original y ver las consecuencias de la prueba de Huang sobre esta.

3.1. Funciones Booleanas

En esta primera sección vamos a dar algunas nociones básicas para la comprensión de las funciones booleanas.

Definición 3.1. *Una función booleana f de n variables es una aplicación:*

$$f: B^n \to B, \text{ donde } B = \{0,1\}.$$

Veamos algunos ejemplos de funciones booleanas interesantes.

Ejemplo 3.2. Sea $x = (\alpha_1, \ldots, \alpha_n) \in \{0,1\}^n$, llamamos función paridad sobre x a la función $\oplus_n(x) = 1 \Leftrightarrow x_1 + \cdots + x_n \equiv 1 \bmod 2$. Es decir, da a cada x el valor de la suma módulo 2 de sus componentes y valdrá 1 si hay un número par de unos entre $x_1, \ldots, x_n$ o 0 en caso contrario.

Ejemplo 3.3. Sea $x = (x_1, \ldots, x_n) \in \{0,1\}^n$, llamaremos función mayoría $Maj_n(x)$ a aquella que da a cada x el valor 1 si y solo si el número de componentes no nulas de x es al menos la mitad, de no ser así valdrá 0, es decir:

$$Maj_n(x) = 1 \Leftrightarrow x_1 + \cdots + x_n \geq \left\lceil \frac{n}{2} \right\rceil.$$

Ejemplo 3.4. Sea $x = (x_1, \ldots, x_n) \in \{0,1\}^n$, llamaremos función umbral $Th_k^n(x)$ a la función que toma el valor 1 si y solo si el número de entradas no nulas es al menos k, es decir, $Th_k^n(x) = 1 \Leftrightarrow x_1 + \cdots + x_n \geq k$.

Podemos darnos cuenta que la función mayoría del Ejemplo 3.3 es un caso de la función umbral, siendo:

$$Maj_n(x) = Th_{\frac{n}{2}}^n(x).$$

Definición 3.5. *Llamaremos polinomio multilineal a todo polinomio $p(x)$ en $\mathbb{R}[x_1, \ldots, x_n]$ en el que el exponente de cada variable sólo puede ser 0 o 1, es decir, un polinomio de la forma $p(x) = \sum_{I \subset [n]} \alpha_I \cdot \prod_{i \in I} x_i$.*

Definición 3.6. *Sea f una función booleana, decimos que un polinomio multilineal $p \in \mathbb{R}[x_1, \ldots, x_n]$ representa a f si para cualquier $x \in \{0,1\}^n$ tenemos que $f(x) = p(x)$. Llamaremos componente de una variable $x \in \{0,1\}^n$ a cualquier elemento x_i donde $i \in \{1, \ldots, n\}$.*

Ya que en el conjunto $\{0,1\}^n$ hay 2^n elementos y una función booleana puede tomar dos posibles valores en cada uno de esos puntos, hay un total de 2^{2^n} funciones booleanas. Ahora demostraremos que toda función booleana f tiene como representación en Q^n un único polinomio multilineal en $\mathbb{R}[x_1, \ldots, x_n]$.

Proposición 3.7. *Sea una función booleana $f: \{0,1\}^n \to \{0,1\}$ entonces existe un único polinomio $p \in \mathbb{R}[x_1, \ldots, x_n]$ multilineal tal que $p(x_1, \ldots, x_n) = f(x_1, \ldots, x_n)$ para cualquier $(x_1, \ldots, x_n) \in Q^n$.*

Demostración. Para $n = 1$ vamos a ver los polinomios multiplicados que representan todas las posibles funciones booleanas.

- $f(0) = 0$ y $f(1) = 0$ tomamos $p(x) = 0$.
- $f(0) = 0$ y $f(1) = 1$ tomamos $p(x) = x$.
- $f(0) = 0$ y $f(1) = 0$ tomamos $p(x) = 1 - x$.
- $f(0) = 0$ y $f(1) = 1$ tomamos $p(x) = 1$.

Vamos a suponer que para cualquier función booleana en $n-1$ variables existe una representación multilineal, si tenemos en cuenta las dos funciones $G_1(x_1, \ldots, x_{n-1}) = f(x_1, \ldots, x_{n-1}, 0)$, $H_2(x_1, \ldots, x_{n-1}) = f(x_1, \ldots, x_{n-1}, 1)$ y aplicamos inducción, podemos tener en cuenta dos representaciones multilineales g y h respectivamente, de forma que:

$$p(x_1, \ldots, x_n) = x_n g(x_1, \ldots, x_{n-1}) + (1 - x_n)h(x_1, \ldots, x_{n-1}).$$

Siendo un f cualquier función booleana, hemos demostrado que existe una representación multilineal de la misma. Para demostrar que es única, supongamos que p_1 y p_2 son dos representaciones multilineales de f y que $(p_1 - p_2)(x) = 0$ para cualquier $x \in \{0,1\}^n$ y vamos a proceder por reducción al absurdo.

Supongamos que $p_1 - p_2 \neq 0$. Sea entonces $S \subseteq [n]$ un conjunto minimal de índices tal que el monomio $\prod_{i \in S} x_i$ tiene coeficiente distinto de 0 en $p_1 - p_2$ (y los monomios $\prod_{i \in S'} x_i$, con $S' \subsetneq S$ tienen coeficiente 0). Si tomamos $x_S \in \{0,1\}^n$ tal que $x_i \neq 0$, si y solo si $i \in S$, entonces $(p_1 - p_2)(x_S) \neq 0$ lo que contradice que para cualquier $x \in \{0,1\}^n$, $(p_1 - p_2)(x) = 0$.

Definición 3.8. *Sea f una función booleana, denotamos* $\deg(f)$ *como el grado de la función booleana siendo este el grado del polinomio multilineal que la represente. Es decir, si $p(x) = \sum_{I \subset [n]} \alpha_I \cdot \prod_{i \subset I} x_i$ representa a f, entonces:*

$$\deg(f) = \text{máx}_{I \subset [n]}\{|I| \mid \alpha_I \neq 0\}.$$

Por comodidad denotamos $[n] = \{1, \ldots, n\}$, cabe recalcar que el rol del conjunto $B = \{0,1\}$ es simplemente de un conjunto dicotómico, podriamos darle dos valores abstractos no numéricos tales que $B = \{a, b\}$, como por ejemplo $\{YES, NO\}$ o $\{ON, OFF\}$, pero de cara al estudio de las funciones booleanas en las demostraciones nos enriquecemos de la información que nos da el uso de valores numéricos además de la necesidad valores numéricos para la correcta interpretación del cubo.

En esta memoria, utilizaremos dos de las notaciones numéricas más comunes de las funciones booleanas, $B = \{0,1\}$ y $B' = \{-1,1\}$. Podemos movernos entre estas representaciones numéricas a través de aplicaciones lineales, de forma que podemos complicar o simplificar la representación de nuestra función. Por ejemplo, podemos transformar $(x_1, \ldots, x_n) \in \{0,1\}^n$ y $f : \{0,1\}^n \to \{0,1\}$ en $f' : \{-1,1\}^n \to \{-1,1\}$ tomando $f'(x_1, \ldots, x_n) = 2 \cdot f\left(\frac{x_1+1}{2}, \ldots, \frac{x_n+1}{2}\right) - 1$, se observa que si $p(x_1, \ldots, x_n)$ es un polinomio multilineal que representa a f, entonces $q(x_1, \ldots, x_n) = 2 \cdot p\left(\frac{x_1+1}{2}, \ldots, \frac{x_n+1}{2}\right) - 1$ es también multilineal,

del mismo grado que $p(x_1, \ldots, x_n)$ y coincide con el valor de p' en $\{-1, 1\}^n$. Por tanto, el valor del grado en la Definición 3.8 no varía al considerar las funciones booleanas de B'^n en B'. Volviendo al Ejemplo 3.2, la función paridad de B'^n en B' es $\oplus_n(x_1, \ldots, x_n) = 1$ si hay un número par de entradas $x_i = 1$ y, $\oplus_n(x_1, \ldots, x_n) = -1$ en caso contrario. Se observa que el polinomio $q(x_1, \ldots, x_n) = \prod_{i=1}^{n} x_i$ representa a g y tiene grado igual a n, en consecuencia la función $\oplus_n$ tiene grado n.

3.2. Medidas de complejidad

En esta sección, vamos a introducir algunas medidas de complejidad y algunas de las propiedades que necesitaremos en la siguiente sección. No incluimos una demostración de todos los resultados, para ello remitimos al lector a [11].

Lema 3.9. *(Igualdad de Parserval) Sea* $f : \{0,1\}^n \to \{0,1\}$ *una función booleana y* $X_S = \prod_{i \in S} x_i$ *para cada subconjunto* $S \subset [n]$*, si representamos* f *a través del polinomio multilineal* $p = \sum_S \alpha_S X_S$*, entonces:*

$$\sum_S \alpha_S^2 = 1.$$

Definición 3.10. *Sea* $f : \{0,1\}^n \to \{0,1\}$ *una función booleana para* $x \in \{0,1\}^n$*, tal que* $x = (x_1, \ldots, x_n)$*, definimos para cualquier componente* x_i *de* x *la influencia de* x_i *en* f *como:*

$$\mathrm{Inf}_i(f) = \mathrm{Prob}[f(x_1, \ldots, x_{i-1}, 0, x_{i+1} \ldots, x_n) \neq f(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n)].$$

Siendo $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$ *componentes que se toman de forma aleatoria en* $\{0,1\}$*. Si* $\mathrm{Inf}(f) = 0$ *se dice que* f *es independiente de* x_i*.*

Lema 3.11. *Para cualquier función booleana* $f : \{0,1\}^n \to \{0,1\}$ *y* p *el polinomio que la represente de forma que* $p = \sum_S \alpha_S X_S$*, entonces:*

$$\sum_{i=1}^{n} \mathrm{Inf}_i(f) = \sum_S |S| \alpha_S^2.$$

Lema 3.12. *Sea* $f : \{0,1\}^n \to \{0,1\}$ *una función booleana y* $X_S = \prod_{i \in S} x_i$ *para cada subconjunto* $S \subset [n]$*, si representamos* f *a través del polinomio multilineal* $p = \sum_S \alpha_S X_S$*, entonces:*

$$\sum_{i=1}^{n} \mathrm{Inf}_i(p) = \sum_S |S| \alpha_S^2.$$

Corolario 3.13. *Sea* $f : \{0,1\}^n \to \{0,1\}$ *una función booleana, entonces:*

$$\sum_{i=1}^{n} \mathrm{Inf}_i(f) \leq \deg(f).$$

Demostración. Hemos visto en el Lema 3.12 que $\sum_{i=1}^{n} \mathrm{Inf}_i(p) = \sum_S |S|\alpha_S^2$, teniendo en cuenta que $|S| \leq \deg(f)$ para cualquier $S \subseteq [n]$ tal que $a_S \neq 0$, tenemos que $\sum_S |S|\alpha_S^2 \leq \deg(f) \sum_S \alpha^2$ y si usamos el Lema 3.9 donde $\sum_S \alpha_S^2 = 1$, probamos que $\sum_{i=1}^{n} \mathrm{Inf}_i(p) \leq \deg(f)$.

Para cualquier polinomio mulitilineal p, vamos a definir un Lema que nos acota superiormente el número de 0 de p.

Lema 3.14. *(Schwartz) Para* $p(x) = p(x_1, \ldots, x_n)$ *polinomio multilineal no nulo de grado* d*. Si elegimos las componentes de* x *de forma aleatoria e independiente en* $\{0,1\}$*, entonces:*

$$\mathrm{Prob}[p(x_1, \ldots, x_n) \neq 0] \geq 2^{-d}.$$

Demostración. Para hacer esta demostración vamos a recurrir a una prueba de inducción sobre n, de forma que para $n = 1$ y p polinomio lineal de una única variable será de grado 0 o 1, no nulo. Por tanto p tendrá a lo sumo un 0 por tanto $\mathrm{Prob}[p(x) \neq 0] \geq \frac{1}{2}$, siendo nuestra hipótesis de inducción.

Realizamos ahora la inducción sobre n, tomando:

$$p(x_1 \ldots, x_n) = x_n \cdot g(x_1, \ldots, x_{n-1}) + h(x_1, \ldots, x_{n-1}).$$

Sacando únicamente x_n como factor común, vamos entonces a evaluar los posibles casos:

- $h + g$ nulo, es decir, $h = -g$ siendo $p = (x_n - 1)g$ y $\deg(g) = d - 1$ (porque $\deg(p) = n$).
  Si desarrollamos tenemos que

$$\begin{aligned}\mathrm{Prob}[p(x) \neq 0] =& \mathrm{Prob}[x_n = 1] \cdot \mathrm{Prob}[p(x) \neq 0 \mid x_n = 1] + \\ &+ \mathrm{Prob}[x_n = 0] \cdot \mathrm{Prob}[p(x) \neq 0 \mid x_n = 0] = \\ &= \frac{1}{2} \cdot \mathrm{Prob}[(-1) \cdot g(x_1, \ldots, x_{n-1}) \neq 0] = \\ &= \frac{1}{2} \cdot \mathrm{Prob}[g(x_1, \ldots, x_{n-1}) \neq 0].\end{aligned}$$

  Usando la hipótesis de inducción, además de tomar los valores $x_1, \ldots, x_n$ de forma aleatoria independiente, tenemos que:

$$\mathrm{Prob}[p(x) \neq 0] = \frac{1}{2} \cdot \mathrm{Prob}[g(x_1, \ldots, x_{n-1}) \neq 0] \geq \frac{1}{2} \cdot 2^{-(d-1)} = 2^{-d}.$$

- $h-g$ nulo, es decir, $h=g$ siendo $p=(x_n+1)g$ y $\deg(g)=d-1$. Lo podemos desarrollar como en el caso anterior.
- $h+g$ no nulo y $h-g$ no nulo, donde $\deg(h)=\deg(g)=d$. Usamos nuestra hipótesis de inducción en $h+g$ a los $(x_1,\ldots,x_{n-1},1)$ y $h-g$ a los $(x_1,\ldots,x_{n-1},0)$ de forma que si lo desarrollamos tenemos que:

$$\begin{aligned}\text{Prob}[p(x)\neq 0] &= \text{Prob}[x_n=1]\cdot\text{Prob}[p(x)\neq 0 \mid x_n=1]+\\ &+\text{Prob}[x_n=0]\cdot\text{Prob}[p(x)\neq 0 \mid x_n=0]=\\ &=\frac{1}{2}\cdot\text{Prob}[(h+g)(x_1,\ldots,x_{n-1})\neq 0 \mid x_n=1]+\\ &+\frac{1}{2}\cdot\text{Prob}[(h-g)(x_1,\ldots,x_{n-1})\neq 0 \mid x_n=0]]=\\ &=\frac{1}{2}\cdot\text{Prob}[(h+g)(x_1,\ldots,x_{n-1})\neq 0]+\\ &+\frac{1}{2}\cdot\text{Prob}[(h-g)(x_1,\ldots,x_{n-1})\neq 0].\end{aligned}$$

Usando la hipótesis de inducción, además de tomar los valores $x_1,\ldots,x_n$ de forma aleatoria independiente, tenemos que:

$$\begin{aligned}\text{Prob}[p(x)\neq 0] &= \frac{1}{2}\cdot\text{Prob}[(h+g)(x_1,\ldots,x_{n-1})\neq 0]+\\ &+\frac{1}{2}\cdot\text{Prob}[(h-g)(x_1,\ldots,x_{n-1})\neq 0]\geq\\ &\geq\frac{1}{2}\cdot 2^{-d}+\frac{1}{2}\cdot 2^{-d}=2^{-d}.\end{aligned}$$

.

Ahora contamos con los conocimientos necesarios para demostrar el siguiente teorema.

Teorema 3.15. *Sea* $f:\{0,1\}^n\to\{0,1\}$ *una función booleana, para* $x\in\{0,1\}^n$ *dependiente de* n *componentes, es decir, tal que* $\text{Inf}_i(f)\neq 0$*, se cumple que:*

$$\deg(p)+\log_2(\deg(p))\geq\log_2(n).$$

Demostración. En primer lugar, para $x=(x_1,\ldots,x_n)$ e $i\in[n]$ definimos f^i como:

$$\begin{aligned}f^i(x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_n) &= f(x_1,\ldots,x_{i-1},0,x_{i+1},\ldots,x_n)-\\ &-f(x_1,\ldots,x_{i-1},1,x_{i+1},\ldots,x_n).\end{aligned}$$

Además junto a la Definición 3.10 si tomamos en $\{0,1\}$ de forma aleatoria e independiente las componentes $x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_n$ tenemos que:

$$\mathrm{Inf}_i(f) = \mathrm{Prob}[f^i(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)] \neq 0.$$

Hemos enunciado que f es dependiente de n componentes por tanto para cualquier $i \in [n]$ tenemos que f^i no es nula, además gracias a la Proposición 3.7 podemos afirmar que nuevamente para cualquier $i \in [n]$ existe un único polinomio multilineal p^i de grado d_i que representa f^i, de forma que $d_i = \deg(f^i) \leq \deg(f) = d$ y $f^i = p^i$ para cualquier $x \in \{0,1\}^n$.

Ya que f^i es no nulo podemos afirmar que p^i tampoco, usando el Lema 3.14 tenemos que:

$$\begin{aligned}\mathrm{Inf}_i(p) &= \mathrm{Prob}[f^i(x_1, \ldots, x_{i-1}, xi+1, \ldots, x_n)] = \\ &= \mathrm{Prob}[p^i(x_1, \ldots, x_{i-1}, xi+1, \ldots, x_n)] \geq \\ &\geq 2^{-d_i} \geq 2^{-d}.\end{aligned}$$

Por otro lado, según el Corolario 3.13 vemos que $\sum_{i=1}^{n} \mathrm{Inf}_i(p) \leq \deg(f) = d$, entonces:

$$d \geq \sum_{i=1}^{n} \mathrm{Inf}_i(p) \geq \sum_{i=1}^{n} 2^{-d} = n \cdot 2^{-d} = \frac{n}{2^d}.$$

Deduciendo entonces que $d \geq \frac{n}{2^d}$ y por tanto $d \cdot 2^d \geq n$. Finalmente podemos aplicar logaritmos a ambos lados de la desigualdad ya que es una función creciente, por tanto

$$\log_2(d) + d = \log_2(d) + \log_2(2^d) = \log_2(d \cdot 2^d) \geq \log_2(n).$$

Definición 3.16. *Sea $f : \{0,1\}^n \to \{0,1\}$ una función booleana, diremos que i es una componente sensible para $x = (\alpha_1, \ldots, \alpha_n) \in \{0,1\}^n$, si para $x^{\{i\}} = (\alpha_1, \ldots, 1-\alpha_i, \ldots, \alpha_n)$ tenemos que $f(x) \neq f(x^{\{i\}})$.*

Definimos la sensibilidad de f en x, denotada por $s(f,x)$ como el número componentes i tales que $f(x) \neq f(x^{\{i\}})$. Siendo entonces la sensibilidad de f, $s(f)$ como el máximo de las sensibilidades, es decir, $s(f) = \max_{x \in \{0,1\}^n} s(f,x)$.

Como $\{0,1\}^n$ son los vértices del hipercubo Q^n, las definiciones anteriores se pueden escribir como:

Sea un hipercubo Q^n, podemos decir que para $x \in V(Q^n)$ y una función booleana f, $s(f,x) = |\{y \in N(x) : \ f(y) \neq f(x)\}|$ y $s(f) = \max_{x \in V(G)} |\{y \in N(x) : \ f(y) \neq f(x)\}|$.

Ejemplo 3.17. Si evaluamos la sensibilidad de la función booleana $AND_n : \{0,1\}^n \to \{0,1\}$ que vale 1 si y solo si todas las componentes de $x \in \{0,1\}^n$ valen 1, esta es n. Si tenemos en cuenta $1 = (1, \ldots, 1)$, para cualquier $i \in [n]$ tenemos que $1 = AND_n(1) \neq AND_n(1^{\{i\}}) = 0$. Por otro lado $s(AND_n, 0) = 0$ ya que $AND_n(0) = AND_n(0^{\{i\}}) = 0$ para cualquier $i \in [n]$.

Definición 3.18. *Sea una función booleana* $f : \{0,1\}^n \to \{0,1\}$ *y* $x = (x_1, \ldots, x_n)$*, para cualquier* $S \subset [n]$ *denotamos por* x^S *al vector obtenido intercambiando todas las componentes* x_i *tales que* $i \in S$*.*

Definimos la sensibilidad por bloques de f *en* x*, denotada por* $bs(f, x)$ *como el máximo número* k *de subconjuntos disjuntos* $A_1, \ldots, A_k \subset [n]$ *tales que para cada* A_i *se cumple que* $f(x) \neq f(x^{B_i})$*. Siendo entonces la sensibilidad por bloques* $bs(f)$ *el máximo de las sensibilidades por bloques, es decir,* $bs(f) = \max_{x \in \{0,1\}^n} bs(f, x)$*.*

Ejemplo 3.19. Si evaluamos la sensibilidad por bloques de la función booleana $AND_n : \{0,1\}^n \to \{0,1\}$, tenemos que $bs(AND_n, 1) = n$ ya que cambiar una componente cualquiera del vector 1 cambia el valor de la función. Así como $1, \ldots, \{n\}$ son n bloques disjuntos y sensibles entonces $bs(AND_n, 1) = n$. Por otro lado $bs(AND_n, 0) = 1$ ya que el único bloque sensible será aquel tal que para $x \in \{0,1\}^n$ de forma que $x = (x_1, \ldots, x_n)$ tengan $x_i = 1$ para $n - 1$ componentes y $x_i = 0$ para una única componente de x, ya que de tener que modificar $0 = (0, \ldots, 0)$ tendríamos que cambiarlos todas su componentes para que valga 1.

3.2.1. Árboles de decisión y el grado aproximado.

Habitualmente en el análisis computacional, para evaluar el número de bits variables necesarios para encontrar el valor de una función, vamos a recurrir a los árboles de decisión.

Sea f una función booleana, un árbol de decisión sobre f es un árbol binario en el que los nodos hojas están etiquetados por 0 o 1 y los demás nodos están etiquetados por una variable. Además de cada nodo que no es una hoja, parten dos arcos, uno etiquetado con un 0 y otro con un 1 (ver Figura 3.1 para un ejemplo).

Para evaluar una función booleana dada por un árbol de decisión en el valor $(y_1, \ldots, y_n)$, comenzamos en el nodo raíz, que estará etiquetado con una variable x_i con $1 \leq i \leq n$. Si $y_i = 1$, tomamos el arco etiquetado por 1 y si $y_i = 0$ hacemos lo propio en el arco etiquetado por 0. Repetimos este proceso hasta llegar a un nodo hoja, la etiqueta de este nodo nos da el valor de la función. Así por ejemplo, al evaluar la función dada por el árbol de la Figura 3.1 en la entrada $(y_1, y_2, y_3) = (1, 1, 0)$. Comenzamos en la raíz etiquetada por x_1, como $y_1 = 1$ nos desplazamos al nodo de la derecha. Como este nodo está etiquetado por x_2 y $y_2 = 1$, nos volvemos a desplazar hacia la derecha. Como finalmente hemos llegado a una hoja etiquetada por 1 se tiene que $f(1, 1, 0) = 1$. En este caso, hemos tomado 2 arcos, por eso decimos que el coste de evaluar f en $(1, 1, 0)$ es 2 y lo denotamos $cost(f, (1, 1, 0)) = 2$.

Diremos que, el coste de un árbol t para cierta componente x_i de x será el menor número de bits de x necesarios en el árbol para llegar a una hoja o valor de f, denotándola como $cost(t, x)$.

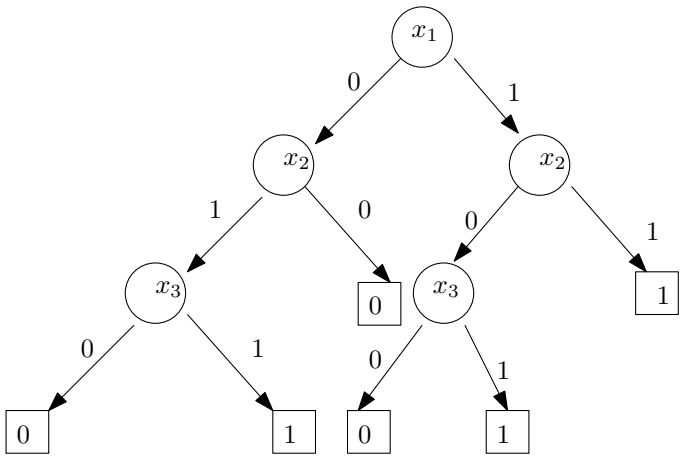

Figura 3.1: Árbol de decisión de la función mayoría en tres variables.

En la Figura 3.1 tenemos un ejemplo de árbol de decisión que podemos encontrar en [13]. En este árbol se representa la función mayoría sobre 3 variables $Maj_3(x)$ (ver Ejemplo 3.3). Es evidente que hay muchos árboles de decisión que calculan la misma función. La complejidad de un árbol de decisión es su profundidad, es decir, el número de consultas realizadas en el peor de los casos. En este ejemplo, la profundidad del árbol es 3 y se alcanza para valores como $x = (0, 1, 1)$.

Definición 3.20. *Definimos la profundidad de un árbol de decisión t como la longitud del camino más largo de t hasta el resultado de alguna de sus hojas, es decir,* $\text{máx}_{x\in\{0,1\}^n} cost(t, x)$.

Introduciremos ahora una medida de complejidad asociada a los árboles de decisión.

Definición 3.21. *Definimos complejidad de un árbol de decisión para una función booleana f como la menor profundidad de todos los árboles de decisión posibles para cualquier valor de f, la denotaremos como $D(f)$. Si tenemos un conjunto T de todos los árboles de decisión que nos pueden hacer llegar a los valores de f, que serán las hojas, tenemos que* $D(f) = \text{mín}_{t\in T}\text{máx}_{x\in\{0,1\}^n} cos(t, x)$.

Para proceder vamos a introducir el concepto de simetrización, usado por Minsky y Papert [10].

Definición 3.22. *Sea $p \in \mathbb{R}[x_1, \ldots, x_n]$ un polinomio en varias variables, definimos la simetrización de p como:*

$$p^{sym}(x_1, \ldots, x_n) = \frac{\sum_{\pi \in S_n} p(x_{\pi(1)}, \ldots, x_{\pi(n)})}{n!}.$$

A continuación, vamos a probar un resultado esencial demostrado en [10] que explica que para $x \in \{0,1\}^n$, p^{sym} depende únicamente de $x_1 + \cdots + x_n$.

Lema 3.23. *Sea $p \in \mathbb{R}[x_1, \ldots, x_n]$ un polinomio en varias variables, entonces existe un polinomio $\widetilde{p} \in \mathbb{R}[x]$ de grado máximo n tal que para cualquier $(x_1, \ldots, x_n) \in \{0,1\}^n$ vemos que:*

$$p^{sym}(x_1, \ldots, x_n) = \widetilde{p}(x_1 + \cdots + x_n).$$

Por otro lado $\deg(\widetilde{p}) \leq \deg(p)$.

Teorema 3.24. *(Markov [4]) Sea $p : \mathbb{R} \to \mathbb{R}$ un polinomio de grado d sobre una variable tal que para cualquier número real $x \in [a_1, a_2]$ se verifica que $b_1 \leq p(x) \leq b_2$. Entonces la derivada de p satisface que:*

$$|p'(x)| \leq d^2 \cdot \tfrac{b_2 - b_1}{a_2 - a_1}, \text{ para todo } x \in [a_1, a_2].$$

En [9] y [16] encontramos el enunciado del siguiente resultado, esencial en nuestro trabajo cuya prueba encontramos en [11].

Teorema 3.25. *(Ehlich, Zeller [9]; Rivlin, Cheney [16]) Sea $p \in \mathbb{R}[x]$ un polinomio que cumple:*

- *Para cualquier entero $i \in [0, n]$ se tiene que $b_1 \leq p(i) \leq b_2$.*
- *Existe un $x \in [0, n]$ tal que la derivada del polinomio p satisface que $|p'(x)| \geq c \geq 0$.*

Entonces $\deg(p) \geq \sqrt{\frac{cn}{c + b_2 - b_1}}$.

Demostración. Sea $c' = \text{máx}_{0 \leq x \leq n} |p'(x)| \geq c$, veamos que para todo número real $x \in [0, n]$, $b_1 - \frac{c'}{2} \leq p(x) \leq b_2 + \frac{c'}{2}$.

En primer lugar, consideramos el mínimo valor de p para un número real $x \in [0, n]$. Sea $y \in \mathbb{N}$ tal que $|y - x| \leq \frac{1}{2}$, por el Teorema del valor intermedio de Lagrange $f(x) - f(y) = f'(\epsilon)(x - y)$, siendo $\epsilon \in \mathbb{R}$ entre x, y. Entonces $f(x) = f(y) + f'(\epsilon)(x - y)$ y como $|f'(\epsilon)| \leq c'$, $|x - y| \leq \frac{1}{2}$ y $b_1 \leq f(y) \leq b_2$ se sigue el resultado.

Si usamos el Teorema 3.24 vemos que para cualquier $x \in [0, n]$:

$$|p'(x)| \leq \deg(p)^2 \cdot \frac{b_2 + \frac{c'}{2} - (b_1 - \frac{c'}{2})}{n - 0} = \deg(p)^2 \cdot \frac{c' + b_2 - b_1}{n}.$$

Además $c' \leq \deg(p)^2 \cdot \frac{c'+b_2-b_1}{n}$, cumpliéndose que $\deg(p)^2 \geq \frac{c'n}{c'+b_2-b_1}$. Si demostramos que $\frac{c'n}{c'+b_2-b_1} \geq \frac{cn}{c+b_2-b_1}$ deducimos que $\deg(p) \geq \sqrt{\frac{cn}{c+b_2-b_1}}$.

Vamos ahora a probar la desigualdad restante.

$$\frac{c'n}{c'+b_2-b_1} - \frac{cn}{c+b_2-b_1} = \frac{cc'n + b_2c'n - b_1c'n - c'cn - b_2cn + b_1cn}{(c'+b_2-b_1)(c+b_2-b_1)} =$$
$$= \frac{b_2n(c'-c) + b_1n(c-c')}{(c'+b_2-b_1)(c+b_2-b_1)} =$$
$$= \frac{n(c'-c)(b_2-b_1)}{(c'+b_2-b_1)(c+b_2-b_1)} \geq 0.$$

Lema 3.26. *Sea $f : \{0,1\}^n$ una función booleana tal que $f(0,\ldots,0) = 0$ y que para cualquier $x = (x_1,\ldots,x_n)$ tal que su peso sea 1, cumple que $f(x) = 1$. Entonces se verifica que:*

$$\deg(f) \geq \sqrt{\frac{n}{2}}.$$

Teniendo en cuenta las siguientes consideraciones:

Sea f nuestra función booleana y p el polinomio que la representa polinómicamente, para un polinomio $\widetilde{p} = p^{sym}$ que aproxima a f tenemos que:

- $\deg(\widetilde{p}) \leq \deg(p)$).
- Para cualquier $x = (x_1,\ldots,x_n)$ tenemos que $p(x) = f(x)$ y, entonces, para un entero $i \in [n]$ se tiene que $p^{sym}(x_1,\ldots,x_n)$, donde $x_1 + \cdots + x_n = i$ vemos lo siguiente:

$$0 \leq \widetilde{p}(i) = p^{sym}(x_1,\ldots,x_n) = \frac{1}{n!}\sum_{\pi\in S_n} p(x_{\pi(1)},\ldots,x_{\pi(n)}) =$$
$$= \frac{1}{n!}\sum_{\pi\in S_n} f(x_{\pi(1)},\ldots,x_{\pi(n)}) \leq \frac{n!\cdot 1}{n!} = 1.$$

Deduciendo que para todo entero $i \in [n]$, $\widetilde{p}(i) \in [0,1]$:

- Se cumple que $p(0) = f(0) = 0$, ya que $\widetilde{p}(0) = p^{sym}(0) = \frac{\sum_{\pi\in S_n} p(0)}{n!} = 0$.
- Para toda permutación $\pi \in S_n$, tenemos que $p(x^{\pi}_{H_1}) = f(x^{\pi}_{H_1}) = 1$. Por tanto, junto a los resultados anteriores vemos que $\widetilde{p}(1) = p^{sym}(x_{H_1}) = \frac{\sum_{\pi\in S_n} p(x^{\pi}_{H_1})}{n!} = 1$.

Si usamos el Teorema de Lagrange deducimos que existe un $z \in (0,1)$ tal que $\widetilde{p}(z) = \widetilde{p}(1) - \widetilde{p}(0) = 1$, y gracias al Teorema 3.25, tomando $c = 1$, $b_1 = 0$ y $b_2 = 1$. Concluimos que $\deg(f) = \deg(p) \geq \deg(\widetilde{p}) \geq \sqrt{\frac{1\cdot n}{1+1}} = \sqrt{\frac{n}{2}}$.

Gracias a estos resultados tenemos cotas inferiores para el grado de unas funciones booleanas en concreto. En el estudio de la acotación del grado buscamos generalizar y encontrar un criterio que podamos llevar a cualquier función booleana.

3.3. Equivalencia entre medidas de complejidad

Existen varias medidas de complejidad, como la profundidad de los arboles de decisión, el certificado o sensibilidad por bloques. La mayor parte de estas medidas están polinómicamente relacionadas como demostraron Nisan y Szegedy [11], a excepción de la sensibilidad. Antes de continuar necesitamos definir qué son dos medidas de complejidad equivalentes o polinómicamente relacionadas.

Definición 3.27. *Sea* $f : \{0,1\}^n \to \{0,1\}$ *una función booleana, con* $s_1(f)$ *y* $s_2(f)$ *dos medidas de complejidad, diremos que están polinómicamente relacionadas si existen dos polinomios* $p_1(x)$ *y* $p_2(x)$ *tales que para cualquier función booleana* f*,* $s_1(f) \leq p_2(s_2(f))$ *y* $s_2(f) \leq p_1(s_1(f))$*. De otra forma diremos que está polinómicamente relacionadas si existen dos constantes* C_1 *y* C_2 *mayores que* 0 *tales que:*

$$s_2(f)^{C_1} \leq s_1(f) \leq s_2(f)^{C2}.$$

Diremos que dos medidas de complejidad son equivalentes si están polinómicamente relacionadas.

Hasta el momento de la prueba de Huang [8], se desconocía si la sensibilidad de una función booleana es equivalente a todas estas medidas de complejidad. Sobre la sensibilidad, lo único que se sabía es que está acotada superiormente en función de la sensiblidad por bloques. Entonces, Nisan y Szegedy [11] sugieren buscar una cota superior de la sensibilidad en función de la sensibilidad por bloques.

Corolario 3.28. *Sea* f *una función booleana,* $s(f)$ *la sensibilidad de la función booleana y* $bs(f)$ *la sensibilidad por bloques de la función booleana, entonces:*

$$bs(f) \geq s(f).$$

Demostración. Si $s(f) = j$ entonces para un $x \in B^n$ existen p valores x^i tales que $f(x^i) \neq f(x)$, por tanto puedo tomar los conjuntos disjuntos $A_1 = \{x_1\}, A_2 = \{x_2\}, \ldots, A_j = \{x_j\}$, concluyendo que $bs(f) \geq s(f)$.

Este resultado acota inferiormente la sensibilidad en términos de la sensibilidad por bloques, para poder afirmar que son equivalentes o, que están polinómicamente relacionadas necesitamos encontrar el caso contrario, una cota inferior de la sensibilidad por bloques en términos de la sensibilidad.

Gracias a la prueba de Huang [8], junto a varios resultados que veremos en este capítulo probaremos la existencia de esta, pero primero vamos a demostrar que el grado de una función booleana es equivalente a la sensibilidad por bloques.

Lema 3.29. *Para cualquier función booleana* f*, se cumple que:*

$$\deg(f) \geq \sqrt{\frac{bs(f)}{2}}.$$

Demostración. Sea f una función booleana, $x \in \{0,1\}^n$ tal que $x = (x_1, \ldots, x_n)$ y $S_1, \ldots, S_t$ los conjuntos para la sensibilidad por bloques de f de la Definición 3.18, de acuerdo a la cota inferior que buscamos tomaremos $S_1, \ldots, S_n$ conjuntos disjuntos, donde para cualquier $i \in [n]$ tenemos que $f(x) \neq f(x^{S_i})$.

Ahora bien, vamos a estudiar sin perdida de generalidad el caso de $f(x) = 0$ ya que de no ser así podemos hacer una transformación $g = 1 - f$, siendo $g(x) = 0, \deg(g) = \deg(f)$ y $f(x) = 1$.

Si tenemos el operador $\oplus$ como la suma de componentes módulo 2 de una variable, definimos $f'(y_1, \ldots, y_t) = f(x \oplus y_1 S_1 \oplus \cdots \oplus y_t S_t)$, donde el j-ésimo componente de f será $x_j \oplus y_i$ si j pertenece a S_i y x_j en caso de que este no pertenezca a ninguno de los conjuntos S_i.

Se cumplen entonces las dos siguientes propiedades:

1. $\deg(f') \leq \deg(f)$, siendo para $t \leq n$ las componentes x_j constantes en f'.
2. f' cumple Lema 3.26.

En primer lugar, consideramos que $f(x) = 0$ y $f'(0, \ldots, 0) = f(x \oplus 0S_1 \oplus \cdots \oplus 0S_t) = f(x)$. A continuación, para y_{H_1} una variable tal que su peso sea 1, es decir $|y_{h_1}| = 1$, todas sus componentes son 0 menos una que valdrá 1.

Ahora queremos ver que $f'(y_{H_1}) = 1$, para ello vamos a suponer que la componente no nula es la i donde $i \in [n]$. Siguiendo que $f'(y_{H_1}) = f(x \oplus 1S_i)$, donde está claro que $x \oplus 1S_i = x^{S_i}$. Deduciendo entonces que $f'(y_{H_1}) = F(x^{S_i}) \neq f(x) = 0$ y, si tenemos en cuenta que $f(x^{S_i}) \in \{0,1\}$, podemos terminar con que $f'(y_{H_1}) = 1$.

Si aplicamos el Lema 3.26 en f' y que $t = bs(f)$, como tenemos $S_1, \ldots, S_t$ bloques disjuntos podemos llegar a $\deg(f) \geq \sqrt{\frac{bs(f)}{2}}$.

Este resultado será muy relevante en nuestro estudio, teniendo en cuenta que nos da una cota superior de la sensibilidad por bloques en términos del grado de una función booleana. Si elevamos al cuadrado y despejamos obtenemos que $b(f) \leq 2\deg(f)^2$, prueba del Teorema siguiente.

Teorema 3.30. *(Nisan [11]) Sea f una función booleana entonces:*

$$bs(f) \leq 2\deg(f)^2.$$

Posteriormente, Tal [1] mejoró esta acotación.

Teorema 3.31. *(Tal) Sea f una función booleana entonces:*

$$bs(f) \leq \deg(f)^2.$$

Hemos probado que existe una relación que acota superiormente la sensibilidad por bloques una función booleana en función del grado, veamos ahora que el grado y la sensibilidad por bloques de una función booleana están polinómicamente relacionadas, probando que existe una relación que acota inferiormente la sensibilidad por bloques de una función booleana en función del grado.

Proposición 3.32. *Sea* $f : \{0,1\}^n \to \{0,1\}$ *una función booleana, se cumple entonces que:*

$$\deg(f) \leq D(f).$$

Demostración. Sea un árbol de decisión T tal que podemos encontrar los valores de F de forma que la profundidad de T sea $D(T)$. Sea L una hoja con valor 1 y $x_1, \ldots, x_n$ las variables que forman parte del camino entre la raíz hasta la hoja L con las componentes $b_1, \ldots, b_r$.

Definimos el polinomio $P_L(x) = \prod_{i:b_i=1} x_i \cdot \prod_{i \cdot b_i=0}(1-x_i)$, tal que $\deg(P_L) \leq D(F)$, donde $P_L(x) = 1$ si x nos lleva a la hoja L y $P_L(x) = 0$ en caso contrario.

Sea $P = \sum_{L \in A} D(P_L)$ la suma de los polinomio P_L, donde L cambia en el conjunto A de las hojas que nos dan los 1 como valor, entonces $\deg(P) = \text{máx}_{L \in A}(\deg(P_L)) \leq D(F)$.

Ya que $P(x) = 1$ si y solo si x nos hace llegar a una hoja con valor 1, deduciendo entonces que P representa polinómicamente a F y por tanto $\deg(F) = \deg(P)$.

Lema 3.33. *Sea* $f : \{0,1\}^n \to \{0,1\}$ *una función booleana, se cumple entonces que:*

$$bs(f) \leq D(f) \leq bs^4(f).$$

La prueba de este resultado la podemos encontrar en [12]. No la añadimos debido a la extensión de este capítulo además de los conceptos necesarios para su prueba.

Gracias al Lema 3.29, como $\sqrt{\frac{bs(f)}{2}} \leq \deg(f)$ y por la Proposición 3.32, sabemos que $\deg(\text{f}) \leq D(f)$. Además, por el Lema 3.33 deducimos que la sensibilidad por bloques acota superiormente al grado de una función booleana, ya que $\deg(f) \leq D(f) \leq bs(f)^4$.

Con todo esto, hemos probando que la sensibilidad por bloques y el grado de una función booleana son equivalentes o están polinómicamente relacionadas, es decir:

$$\sqrt{\frac{bs(f)}{2}} \leq \deg(f) \leq bs(f)^4.$$

En particular, aquí se demuestra que $\deg(f)$ y $bs(f)$ están polinómicamente relacionados.

3.4. La Conjetura de la Sensibilidad

Gracias al Corolario 3.28 sabemos que $s(f) \leq bs(f)$, pero ¿existe un polinomio $p(x)$ tal que $bs(f) \leq p(s(f))$? O, equivalentemente ¿están $s(f)$ y $bs(f)$ polinómicamente relacionados? Es aquí donde nace la Conjetura de la Sensibilidad enunciada por Nisan y Szegedy [11], que afirma que existe una constante $C > 0$ tal que $bs(f) \leq s(f)^C$.

Hemos visto en la sección anterior que, el grado y la sensibilidad por bloques son medidas de complejidad equivalentes. La motivación de este trabajo es responder a la pregunta de si la sensibilidad y la sensibilidad por bloques lo son también. Esto es lo que conocemos como la Conjetura de la Sensibilidad [8].

Vamos a dar el último resultado necesario para la prueba de la conjetura, el Teorema de equivalencia de Gotsman y Linial 3.37, que nos permite trasladar el trabajo de Huang en grafos a las funciónes booleanas donde fue planteada inicialmente esta conjetura por Nisan y Szegedy en [11].

Definición 3.34. *Sea un hipercubo Q^n, y un subgrafo inducido H del mismo, llamamos función gamma a $\Gamma(H) = \max\{\Delta(H), \Delta(Q^n - H)\}$, donde $\Delta(Q^n - H)$ es el subgrafo inducido por el conjunto de los vértices $V(Q^n)\backslash V(H)$.*

Lema 3.35. *Sea una función booleana $f := \{1,-1\}^n \to \{1,-1\}$ y $P(\alpha_1,\ldots,\alpha_n) = \sum_{I\subset[n]} a_I \prod_{i\in I} \alpha_i$ el único polinomio multilineal tal que:*

$$a_\emptyset = \frac{\sum_{(\alpha_1,\ldots,\alpha_n)\in\{-1,1\}^n} f(\alpha_1,\ldots,\alpha_n)}{2^n} = E(f).$$

Donde $E(f)$ es el valor medio de f.

Demostración. Por la Proposición 3.7, hemos visto que existe un único polinomio multilineal p tal que $p(\alpha_1,\ldots,\alpha_n) = f(\alpha_1,\ldots,\alpha_n)$ para cualquier $(\alpha_1,\ldots,\alpha_n) \in \{-1,1\}^n$.

Sea $J \in P([n])$ para evaluar cualquier $(\alpha_1,\ldots;\alpha_n) \in \{-1,1\}^n$ partimos de la biyección:

$$\begin{aligned} W: \quad \{-1,1\}^n &\to P([n]) \\ (\alpha_1,\ldots,\alpha_n) &\to W(\alpha_1,\ldots,\alpha_n) = \{i \mid \alpha_i = 1\}. \end{aligned}$$

Ahora si $J = \{i \mid \alpha_i = 1\}$, tenemos que:

$$f(\alpha_1,\ldots,\alpha_n) = p(\alpha_1,\ldots,\alpha_n) = \sum_{I\subset[n]} a_I \prod_{i\in I} \alpha_i = \sum_{I\subset[n]} (-1)^{|I-J|} a_I.$$

Si desarrollamos:

$$\begin{aligned} \sum_{(\alpha_1,\ldots,\alpha_n)\in Q^n} f(\alpha_1,\ldots,\alpha_n) &= \sum_{J\subset[n]} \Big(\sum_{I\subset[n]} (-1)^{|I-J|}\Big) a_I = \\ &= \sum_{I\subset[n]} \Big(\sum_{J\subset[n]} (-1)^{|I-J|}\Big) a_I. \end{aligned}$$

Como $I \neq \emptyset$, podemos suponer sin pérdida de generalidad que $1 \in I$, entonces si tomamos $I' = I - \{1\}$ vemos que:

$$\begin{aligned}\sum_{J\subset[n]}(-1)^{|I-J|} &= \sum_{J\subseteq\{2,\ldots,n\}}(-1)^{|I'-J|} + \sum_{J\subseteq\{2,\ldots,n\}}(-1)^{|(I'-J)\cup\{1\}|} = \\ &= \sum_{J\subset\{2,\ldots,n\}}(-1)^{|I'-J|} + (-1)^{|I'-J|+1} = \\ &= \sum_{J\subset\{2,\ldots,n\}}(-1)^{|I'-J|}\cdot(1-1) = \\ &= 0.\end{aligned}$$

Para concluir, podemos deducir entonces:

$$\sum_{(\alpha_1,\ldots,\alpha_n)\in Q^n} f(\alpha_1,\ldots,\alpha_n) = (\sum_{J\subset[n]}(-1)^{|\emptyset-J|})a_\emptyset = 2^n a_\emptyset.$$

Quedando entonces demostrado que:

$$a_\emptyset = \frac{\sum_{(\alpha_1,\ldots,\alpha_n)\in Q^n} f(\alpha_1,\ldots,\alpha_n)}{2^n}.$$

Lema 3.36. *Sean $f : \{-1,1\}^n \to \{-1,1\}$ una función booleana y p la función paridad:*

$$\begin{aligned}p :&\{-1,1\}^n \to \{-1,1\}\\ &(x_1,\ldots,x_n) \to x_1\cdots x_n\end{aligned}$$

Si $F = \sum_{I\subset[n]} \alpha_I \cdot \prod_{i\in I} x_i$ es el polinomio que representa a f, y g la siguiente función booleana:

$$\begin{aligned}g :&\{-1,1\}^n \to \{-1,1\}\\ &(x_1,\ldots,x_n) \to g(x_1,\ldots,x_n) = f(x_1,\ldots,x_n)p(x_1,\ldots,x_n)\end{aligned}$$

Entonces el único polinomio multilineal G que represente a g es:

$$G = \sum_{I\subset[n]} \alpha_I \cdot \prod_{i\notin I} x_i.$$

Demostración. Por el Corolario 3.7, sabemos que para g debe haber un único polinomio multilineal G que la represente. Ahora, bien para nuestra demostración, basta con observar que para cualquier $(\alpha_1,\ldots,\alpha_n) \in \{-1,1\}^n$ tendremos que:

$$\begin{aligned} g(\alpha_1,\ldots,\alpha_n) &= f(\alpha_1\ldots\alpha_n)\cdot p(\alpha_1\cdots\alpha_n) = \\ &= F(\alpha_1\ldots\alpha_n)\cdot\alpha_1\cdots\alpha_n = \\ &= \sum_{I\subset[n]} a_I \prod_{i\in I}\alpha_i \prod_{i=1}^{n}\alpha_i = \\ &= \sum_{I\subset[n]} a_I \prod_{i\in I}\alpha_i^2 \cdot \prod_{i\notin I}\alpha_i = \\ &=^{(*)} \sum_{I\subset[n]} a_I \prod_{i\notin I}\alpha_i = G(\alpha_1,\ldots,\alpha_n). \end{aligned}$$

Teniendo en cuenta $(*)$ como $\alpha_i \in \{-1,1\}$, entonces $\alpha_i^2 = 1$.

Teorema 3.37. *(Teorema de equivalencia de Gotsman y Linial) Sea una función $h:\mathbb{N}\to\mathbb{R}$ creciente, las siguientes afirmaciones son equivalentes:*

1. *Para cualquier subgrafo inducido G de Q^n tal que $|V(G)| \neq 2^{n-1}$, $\Gamma(G) \geq h(n)$.*
2. *Para cualquier función booleana f, $\deg(f) < h^{-1}(s(f))$.*

Demostración. Sea $G \subseteq V(Q)^n$ tomamos una función booleana g tal que $g(x) = 1$ si $x \in V(G)$ y $g(x) = -1$ en caso contrario, ahora tomaremos la función booleana $f(x) = g(x)\cdot p(x)$ siendo p la función paridad $p(x) = \prod_{i=1}^{n} x_i$. Es importante recalcar que por como hemos definido $g(x)$ para $x \in \{-1,1\}^n$, tenemos que para $y \in N(x)$ la función paridad cumple que $p(y) = -p(x)$.

Necesitamos dos resultados vitales para la demostración:

$$\begin{aligned} &(i) \quad Si\ x \in V(G),\ \deg_G(x) = n - s(g,x). \\ &(ii) \quad Si\ x \in V(Q^n),\ s(g,x) + s(f,x) = n. \end{aligned}$$

Por una parte, en (i) se puede comprobar rápidamente que $\deg_G(x) = n - s(g,x)$ para todo $x \in V(G)$, ya que por definición $g(x) = 1$ si $x \in V(G)$ y $s(g,x) = |\{y \in N(x) \mid g(y) \neq g(x)\}| = |\{y \in N(x) \mid y \notin V(G)\}| = n - \deg_G(x)$.

Por otro lado, para demostrar (ii) tomaremos $x \in C^n$ y al ser el hipercubo un grafo bipartito y regular sabemos que $|N(x)| = n$, entonces por cómo hemos definido $g(x)$:

$$|N(x)| = n = |\{y \in N(x) :\ g(y) = -g(x)\}| + |\{y \in N(x) :\ g(y) = g(x)\}|.$$

Por definición, sabemos que $s(g,x) = |\{y \in N(x) : g(y) = -g(x)\}|$, pero a continuación demostraremos que $|\{y \in N(x) :\ g(y) = g(x)\}| = |\{y \in N(x) : f(y) = -f(x)\}| = s(f,x)$. Evaluamos $p(x)$ que sólo puede valer 1 o -1. Supongamos que $p(x) = 1$, deduciendo que $g(x) = f(x)$ y por tanto $g(y) = -g(y)$ para $y \in N(x)$ ya que $p(y) = -1$, concluyendo que si $g(x) = g(y)$ entonces $g(y) = f(x) = -f(y)$. Si $p = -1$ es un caso análogo.

Por tanto, para cualquier $x \in C^n$, $\{y \in N(y) : \ g(y) = g(x)\} = \{y \in N(y) : f(y) = -f(x)\}$, como $|\{y \in N(y) : \ f(y) = -f(x)\}| = s(F, x)$ demostramos entonces que $s(g, x) + s(f, x) = n$.

Además de cómo definimos g en función del grafo G se tiene que:

$$E(g) = 0 \Leftrightarrow |V(G)| = 2^{n-1}, \text{ donde } E(g) \text{ es el valor medio de } g.$$

($\Rightarrow$) Vamos a realizar esta prueba por contrarrecíproco, como hemos definido nuestra g se verifica que $g(x) = 1 \Leftrightarrow x \in V(G)$, por tanto $E(g) \neq 0$ ya que de no ser así:

$$\frac{1}{2^n} \sum_{x \in C^n} g(x) = \frac{1}{2^n} \cdot \left[\sum_{x \in V(G)} g(x) + \sum_{x \notin V(G)} g(x) \right] = 0.$$

Deduciendo entonces que

$$|V(G)| = \sum_{x \in V(G)} g(x) = - \sum_{x \notin V(G)} g(x) = -(-1) \cdot |V(Q^n) - V(G)|.$$

Finalizando entonces con que $|V(G)| = |V(Q^n) - V(G)|$. Como tenemos que $|V(G)| + |V(Q^n) - V(G)| = |V(Q^n)| = 2^n$, usando lo anterior concluimos que $|V(G)| = 2^{n-1}$, en contra de nuestra hipótesis.

($\Leftarrow$) Realizaremos esta prueba también por contrarrecíproco, si suponemos que $E(g) \neq 0$ entonces $V(G) = \{x \in C^n \mid g(x) = 1\}$, verificando que $|V(G)| \neq 2^{n-1}$, ya que de no ser así:

$$\begin{aligned} E(g) = \frac{1}{2^n} \sum_{x \in C^n} g(x) = \frac{1}{2^n} \cdot \left[\sum_{x \in V(G)} g(x) + \sum_{x \notin V(G)} g(x) \right] = \\ = \frac{1}{2^n} \cdot [2^{n-1} \cdot 1 + 2^{n-1} \cdot (-1)]. \end{aligned}$$

Yendo en contra de nuestra hipótesis.

Ahora bien, para demostrar que 1 y 2 son equivalentes vamos a reescribir sendos enunciados en términos de funciones booleanas de forma que las originales sean equivalentes a estas:

1'. Sea una función booleana g con $E(g) \neq 0$ entonces existe un $x \in V(Q^n)$ tal que $s(g, x) \leq n - h(n)$.
2'. Sea una función booleana F tal que $s(F) < h(n)$ entonces $\deg(F) < n$.

Comprobamos que las implicaciones originales y estas son equivalentes, es decir, $1 \Leftrightarrow 1'$ y $2 \Leftrightarrow 2'$.

- $1 \Rightarrow 1'$ Sea g una función booleana tal que $E(g) \neq 0$, entonces $|V(G)| \neq 2^{n-1}$ gracias al resultado que acabamos de demostrar. Al cumplirse **1** tenemos que $\Gamma(G) \geq h(n)$, y por la definición 3.34 deducimos que existe al menos un $x \in C^n$ tal que $\deg(x) \geq h(n)$. Como antes razonamos que $\deg(x) = n - s(g,x)$, entonces $n - s(g,x) \geq h(n)$.
  Terminamos con que existe al menos un $x \in C^n$ tal que $s(g,x) \leq n - h(n)$, verificándose **1'**.
- $1' \Rightarrow 1$ Sea G el grafo inducido de Q^n tal que $|V(G)| \neq 2^{n-1}$, como tenemos por g a la función booleana tal que $g(x) = 1$ si y solo si $x \in V(G)$, entonces por lo que hemos visto se verifica que $E(g) \neq 0$. Suponiendo que se cumple **1'**, sabemos que existe al menos un $x \in C^n$ tal que $s(g,x) \leq n - h(n)$, deduciendo que si $\deg(x) = d$ para un x perteneciente a G o $Q^n - G$, entonces $d = n - s(g,x) \geq h(n)$. Concluyendo que $\Gamma(G) \geq h(n)$, verificándose **1**.
- $2 \Rightarrow 2'$ Para cualquier función booleana f tal que $s(f) < h(n)$, si se cumple **2**, tenemos que $\deg(f) \leq h^{-1}(s(f))$. Entonces $\deg(f) \leq h^{-1}(s(f)) < h^{-1}(h(n)) = n$, verificándose **2'**.
- $2' \Rightarrow 2$ Si para cualquier función booleana F tal que $s(F) < h(n)$ se cumple que $\deg(F) < n$ con $h : \mathbb{N} \to \mathbb{R}$ monótona. Entonces, para cualquier función booleana F se cumple que $\deg(F) < h^{-1}(s(F))$, verificándose **2**.

Ahora demostraremos el Teorema comprobando que $1' \Leftrightarrow 2'$. Por el Lema 3.35 podemos afirmar que $E(g) = a_\emptyset$. Además, gracias al Lema 3.36 sabemos que para $x \in V(Q^n)$ si tomamos la función booleana $g(x) = f(x) \cdot p(x)$, donde $p(x)$ es la función pariedad y $g(x) = f(x) \prod_{i=1}^{n} x_i$, entonces existe un único polinomio multilineal g' que la represente de forma que $g'(x) = \sum_{I \subset [n]} \alpha_I \cdot \prod_{i \notin I} x_i$.

$1' \Rightarrow 2'$ Por reducción al absurdo, supongamos que $\deg(f) = n$ y por tanto $E(g) = a_\emptyset \neq 0$, por **1'** sabemos que existe un x tal que $s(g,x) \leq n - h(n)$, como $s(g,x) = n - s(f,x)$ deducimos entonces que existe un x tal que $s(f,x) \geq h(n)$ contradiciendo **1'**.

$2' \Rightarrow 1'$ Nuevamente por reducción al absurdo, supongamos que para cualquier $x \in V(Q^n)$, $s(g,x) > n - h(n)$, lo que implica que $s(f) < h(n)$, ya que para cualquier $x \in V(Q^n)$, $s(g,x) > n - h(n)$ y como $s(g,x) = n - s(f,x)$ se cumple que $n - s(f,x) > n - h(n)$ por tanto $s(f) > h(n)$. Ahora si aplicamos **2'** tenemos que $\deg(f) < n$ y que $a_\emptyset = E(g) = 0$ contradiciendo **1'**.

Finalmente, demostraremos la Conjetura de la Sensibilidad planteada por Nisan y Szegedy [11], gracias a los resultados anteriores.

Teorema 3.38. *(Conjetura de la Sensibilidad) Sea f una función booleana, entonces existe una constante $C > 0$ tal que:*

$$bs(f) \leq s(f)^C.$$

Demostración. Si tomamos $h(n) = \sqrt{n}$ y $G \subseteq Q^n$ subgrafo inducido tal que $|V(G)| \neq 2^{n-1}$, entonces, o bien G o $Q^n - G$ tiene al menos $2^{n-1} + 1$ vértices y, aplicando el Teorema de Huang 2.14 se tiene que $\Gamma(G) \geq \sqrt{n} = h(n)$. En consecuencia, aplicando el Teorema de equivalencia de Gotsman y Linial 3.37 se tiene que $\deg(f) \leq h^{-1}(s(f)) = s(f)^2$. Como Tal demostró 3.31 que $bs(f) \leq \deg(f)^2$, podemos relacionar la sensibilidad por bloques con la sensiblidad, obteniendo que para cualquier función booleana f:

$$bs(f) \leq s(f)^4.$$

Demostrando así la Conjetura de la Sensibilidad.

Bibliografía

[1] A. Tal, Properties and applications of boolean function composition, Proceedings of the 4th conference on Innovations in Theoretical Computer Science, pp. 441-454.

[2] C. Gotsman, N. Linial, The equivalence of two problems on the cube. J. Combin. Theory Ser. A, 61 (1) (1992), pp. 142-146.

[3] L. M. Merino, E. Santos, Álgebra lineal con métodos elementales (1995).

[4] E. W. Cheney, Introduction to approximation theory. McGraw-Hill Book Co (1966).

[5] F. Chung, Z. Füredi, R. Graham, P. Seymour, On induced subgraphs of the cube, J. Comb. Theory, Ser. A, 49 (1) (1988), pp. 180-187.

[6] G. Boole, An Investigation of the Laws of Thought on Which are Founded the Mathematical Theories of Logic and Probabilities, (1854).

[7] M. R. Garey, S. J. David Computers and intractability. A guide to the theory of NP-completeness. A Series of Books in the Mathematical Sciences. W. H. Freeman and Co., San Francisco, Calif (1979).

[8] H. Huang, Induced subgraphs of hypercubes and a proof of the sensitivity conjecture, Annals of Mathematics 190(3) (2019), pp. 949-955.

[9] H. Ehlich y K. Zeller, Schwankung von Polynomen zwischen Git-terpunkten, Mathematische Zeitschrift 86 (1964),pp. 41-44.

[10] M. Minsky y S. Papert, Perceptrons, expanded edition: An introduction to Computational Geometry. The MIT press, (1969).

[11] N. Nisan, M. Szegedy, On the degree of Boolean functions as real polynomials, Comput. Complexity, 4 (1992), pp. 462-467.

[12] N. Nisan, CREW PRAM's and decision trees, STOC' 89, Proceedings of the twenty-first annual ACM symposium on Theory of computing (1989), pp. 327-335.

[13] N. Saurabh, Boolean function complexity, Meeting:5, (22/05/2019). https://nitinsau.github.io/teaching/BFC19-mpii/lecture5.pdf

[14] C. E. Shannon, A mathematical theory of communication. Bell System Technical Journal, 27 (1948).

[15] S. Fisk, A very short proof of Cauchy's interlace theorem for eigenvalues of Hermitian matrices, Amer. Math. Monthly 112 (2005), pp. 118.

[16] T. J. Rivlin y E. W. Cheney, A comparison of Uniform Approximations on an interval and a finite subset thereof, SIAM Journal on Numerical Analysis 3(2) (1966), pp. 311-320.

The Sensitivity Conjecture and its proof via Spectral Graph Theory

Sección de Matemáticas
Universidad de La Laguna

César Martín Ferrer

Facultad de Ciencias · Sección de Matemáticas
Universidad de La Laguna
alu0101036427@ull.edu.es

Abstract

The Sensitivity Conjecture was one of the most important open problems in computational complexity. After 30 years of uncertainty, Hao Huang (Emory, Atlanta, USA) has succeeded in proving it in just over one page [3].
This conjecture states that two measures of boolean complexity: sensitivity and block sensitivity are equivalent, or, formally speaking, are polynomially related. Huang's proof makes creative use of basic tools of Linear Algebra, as well as a rewriting of the conjecture in terms of the hypercube graph by Gotsman and Linial [1].
The goal of this memory is to present the context of the conjecture as well as its proof and implications.

1. Graph Theory: Independence and Sensitivity

Let $G = (V, E)$ be a graph $G = (V, E)$ and $V' \subset V$ be a nonempty set, we call V' independent if for all $v_1, v_2 \in V'$, $\{v_1, v_2\} \notin E$. In other words, V' is an independent set if and only if the subgraph induced by V' has no edges. We denote by $\alpha(G)$ the size of the maximal independent, i.e:

$$\alpha(G) = \max\{|V'| \mid V' \subset V \ independent\}.$$

The sensitivity of a graph $G = (V, E)$ is the smallest value among the maximum degrees of all induced graphs with more than $\alpha(G)$ vertices, that is:

$\sigma(G) = \min\{\Delta([V']) \mid V' \subset V \ y \ |V'| > \alpha(G)\}$, where $\Delta(G)$ denotes the maximum degree of a graph G.

Proposition. Let the graph $G = (V, E)$ where $V \neq \emptyset$, be a complete regular bipartite graph $K_{s,s}$, where $V = A \sqcup B$, we have that:

$$\sigma(K_{s,s}) = \left\lceil \frac{s+1}{2} \right\rceil.$$

2. Proof of the conjecture using Graph Theory

The proof of this result relies on a very smart way of using a classical result in Linear Algebra due to Cauchy and called interlacing theorem.
We call n-dimensional hypercube the bipartite and n-regular graph $Q^n = \{0, 1\}^n$, being in this graph two adjacent vertices if they differ in only one coordinate.

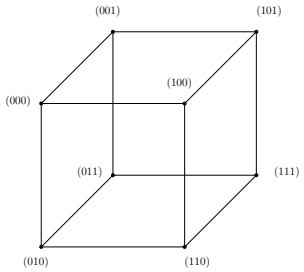

Figure 1: *Representation of Q^3.*

In Figure 1 we have the bipartition of Q^3 on sets $A = \{010, 100, 001, 111\}$ and $B = \{000, 110, 011, 101\}$.

Theorem 1. Sensitivity Conjecture in terms of graph theory [3]. Let Q^n, the graph of the n-dimensional hypercube with $n \geq 1$.

$$\sigma(Q^n) \geq \sqrt{n}.$$

.

Theorem 2. Chung, Füredi, Graham y Seymour. There is an induced subgraph H of Q^n on $2^{n-1} + 1$ vertex such that $\Delta(H) < \sqrt{n} + 1$.
As a consequence of these two theorem we deduce that:

$$\sigma(Q^n) = \lceil \sqrt{n} \rceil.$$

3. Boolean functions

A Boolean function is a map $f : \{0, 1\}^n \to \{0, 1\}$. Given $x = (\alpha_1, \ldots, \alpha_n) \in \{0, 1\}^n$ we say that i is a sensitive component for x if for $x^{\{i\}} = (\alpha_1, \ldots, 1 - \alpha_i, \ldots, \alpha_n)$ we have that $f(x) \neq f(x^{\{i\}})$.
We define the sensitivity of f at x denoted by $s(f, x)$ as the number of components i such that $f(x) \neq f(x^{\{i\}})$. Being then the sensitivity of f, $s(f)$ as the maximum of the sensitivities, i.e,

$$s(f) = \max_{x \in \{0,1\}^n} s(f, x).$$

For any $S \subset [n]$ we denote by x^S to the vector obtained by interchanging all the components x_i such that $i \in S$. We define the block sensitivity of f in x denoted by $bs(f, x)$ as the maximum number k of disjoint subsets. $A_1, \ldots, A_k \subset [n]$ such that for each A_i it is satisfied that $f(x) \neq f(x^{B_i})$. The block sensitivity $bs(f)$ being then the maximum of the block sensitivities, that is,

$$bs(f) = \max_{x \in \{0,1\}^n} bs(f, x).$$

Theorem 3. Sensitivity Conjecture. Let f be a Boolean function, then there exist a constant $C > 0$ such that:

$$b(f) \leq s(f)^C.$$

As a consequence of Theorem 1, one can prove that:

$$bs(f) \leq s(f)^4.$$

A crucial step in this proof is an equivalence Theorem by Gotsman and Linial [1].

References

[1] C. Gotsman, N. Linial, The equivalence of two problems on the cube. J. Combin. Theory Ser. A, 61 (1) (1992), pp. 142-146.

[2] F. Chung, Z. Füredi, R. Graham, P. Seymour, On induced subgraphs of the cube, J. Comb. Theory, Ser. A, 49 (1) (1988), pp. 180-187.

[3] H. Huang, Induced subgraphs of hypercubes and a proof of the sensitivity conjecture, Annals of Mathematics 190(3) (2019), pp. 949-955.

[4] N. Nisan, M. Szegedy, On the degree of Boolean functions as real polynomials, Comput. Complexity, 4 (1992), pp. 462-467.