La Columna de Matemática Computacional

Sección a cargo de

Laureano González Vega

La conjetura de la sensibilidad y su resolución vía teoría de grafos

por

Sara Asensio Ferrero

Introducción

Los principales objetivos de esta nota son, por un lado, exponer cómo en 1994 se plantea de forma natural la conjetura de la sensibilidad, un problema enunciado originalmente en el marco de la teoría de la complejidad computacional; y, por otro lado, ver cómo este resultado se demuestra a través de la teoría de grafos casi 30 años después de ser enunciado y de una forma muy breve, clara y sencilla.

En 2010, casi 20 años después de que la conjetura de la sensibilidad fuese enunciada, Scott Aaronson publicaba una entrada en su blog *Shtetl-Optimized* ([1]) animando a la comunidad matemática a estudiar el problema e intentar resolverlo. Ya en aquel entonces, su intuición era que resolver este problema no requeriría del uso de técnicas matemáticas muy profundas, aunque sí de grandes dosis de creatividad. Como veremos, se encontraba en lo cierto. Un par de páginas bastaron a Hao Huang para corroborarlo en 2019 ([9]).

En el momento en el que se consiguió demostrar el resultado, grandes referentes en este campo comenzaron a hacerse eco de la noticia. Nuevamente Scott Aaronson mostraba su admiración en [2], llegando a decir, incluso, que esta demostración «venía directamente del libro», haciendo referencia a ese libro que, según Paul Erdős, Dios había escrito con las demostraciones más bellas de las matemáticas. También Gil Kalai y Terence Tao mostraban en sus blogs (respectivamente, en [11] y [17]) su admiración por esta prueba, al mismo tiempo que daban a conocer fuertes conexiones entre ella y otros conceptos matemáticos.

A pesar de que cada una de las personas que han mostrado su opinión sobre esta demostración lo han hecho desde un punto de vista diferente, todos ellos coinciden en resaltar su increíble belleza. Mi misión con esta nota va a ser, pues, explicar detalladamente el desarrollo de esta historia hasta nuestros días, con el fin de que pronto podáis comprender las opiniones de estos grandes referentes.

La conjetura de la sensibilidad afirma que la sensibilidad por bloques de toda función booleana se puede acotar superiormente por una expresión polinomial que solo depende de su sensibilidad, siendo la sensibilidad y la sensibilidad por bloques dos medidas de complejidad de una función booleana. Para poder comprender bien este resultado, que se enunciará de forma precisa al final de la primera sección de esta nota, previamente expondremos las definiciones y resultados necesarios. A continuación, presentaremos un teorema, conocido como teorema de equivalencia, que permite reformular la conjetura en términos propios de la teoría de grafos. Además, expondremos algunos de los primeros intentos que se llevaron a cabo para demostrar la conjetura debido al interés que presentan las construcciones que en ellos aparecen. Estos primeros intentos condujeron a Hao Huang a la demostración del resultado en 2019. Ofreceremos en este texto la demostración original de Huang, que destaca por su originalidad y por la sencillez de las técnicas empleadas, y detallaremos también una demostración alternativa del resultado, que utiliza técnicas incluso más elementales que la original. Para terminar, comentaremos brevemente algunas de las nuevas líneas de investigación que han surgido en los últimos años gracias a la prueba de la conjetura de la sensibilidad y que se mantienen activas en la actualidad.

La mayor parte de lo que se expone en esta nota se puede encontrar debidamente detallado en [4].

Antes de empezar, me gustaría agradecer a los profesores Ignacio García-Marco y Philippe Gimenez sus sugerencias y correcciones sobre las primeras versiones de esta nota, las cuales he tratado de incorporar de la mejor manera posible.

1. Funciones booleanas

Nuestro objeto principal de estudio en esta nota van a ser las funciones booleanas. Una *función booleana* $f(\mathbf{x}) = f(x_1, \ldots, x_n)$ en n variables no es más que una aplicación $f : \{0,1\}^n \to \{0,1\}$.

Antes de introducir nuestra primera medida de complejidad para funciones booleanas, conviene introducir un nuevo concepto: se dice que un polinomio real multivariante $p : \mathbb{R}^n \to \mathbb{R}$ *representa* a una función booleana f si para cada vector booleano $\mathbf{x} \in \{0,1\}^n$ se tiene que $f(\mathbf{x}) = p(\mathbf{x})$. A partir de esta noción, y teniendo en cuenta que un polinomio multilineal es un polinomio en varias variables donde el exponente de cada variable puede tomar solo los valores 0 o 1, es posible probar el siguiente resultado, cuya demostración incorporamos a nuestro texto aunque se puede encontrar por ejemplo en [12]:

Proposición 1.1. *Para toda función booleana $f : \{0,1\}^n \to \{0,1\}$ existe un único polinomio real multilineal que la representa.*

Observación. Antes de presentar la prueba de este resultado, notemos que la clave de la unicidad está en la multilinealidad.

Se verifica que $x^k = x$ para cada $x \in \{0,1\}$ y para cada número natural k no nulo. Como consecuencia de esto, dado un polinomio real p que represente a una función booleana f, cambiando los exponentes de cualesquiera de las variables que aparecen en p por cualesquiera valores naturales no nulos obtenemos infinitos polinomios que también representan a f, pero que ya no son multilineales.

Demostración de la Proposición 1.1. En primer lugar, vamos a probar que existe una representación polinomial multilineal para toda función booleana f, y lo hacemos por inducción en el número de variables n.

- Si $n = 1$ solo hay 4 funciones booleanas posibles f, y es muy fácil determinar un polinomio real multilineal en una variable que represente a cada una de ellas:
    - Si $f(0) = 0$ y $f(1) = 0$, basta considerar $p(x) = 0$.
    - Si $f(0) = 0$ y $f(1) = 1$, basta considerar $p(x) = x$.
    - Si $f(0) = 1$ y $f(1) = 0$, basta considerar $p(x) = 1 - x$.
    - Si $f(0) = 1$ y $f(1) = 1$, basta considerar $p(x) = 1$.
- Supongamos ahora que el resultado es cierto para funciones booleanas en $n - 1$ variables. Si consideramos las dos funciones booleanas en $n - 1$ variables dadas por $f_1(x_1, \ldots, x_{n-1}) = f(x_1, \ldots, x_{n-1}, 0)$ y $f_2(x_1, \ldots, x_{n-1}) = f(x_1, \ldots, x_{n-1}, 1)$, aplicando la hipótesis de inducción es posible considerar sus representaciones polinomiales multilineales Q y R, respectivamente. Considerando ahora el polinomio

$$P(x_1, \ldots, x_n) = x_n R(x_1, \ldots, x_{n-1}) + (1 - x_n) Q(x_1, \ldots, x_{n-1}),$$

  es claro que P es multilineal y, por la forma en la que se ha definido, que representa a f.

Para terminar, vamos a demostrar que esta representación es, de hecho, única. Para ello, supongamos que P_1 y P_2 son dos representaciones multilineales de f. Entonces se verifica que $(P_1 - P_2)(\mathbf{x}) = 0$ para cada $\mathbf{x} \in \{0, 1\}^n$.

Razonamos por reducción al absurdo, suponiendo que $P_1 - P_2$ no es idénticamente nulo y que, por tanto, contiene a algún monomio distinto de 0. Sea ahora $S \subseteq \{1, \ldots, n\}$ un conjunto de índices tal que el monomio $\prod_{i \in S} x_i$ aparece en $P_1 - P_2$ con coeficiente no nulo pero los monomios de la forma $\prod_{i \in S'} x_i$, con $S' \subsetneq S$, tienen todos coeficiente nulo. Si denotamos por χ_S al elemento de $\{0, 1\}^n$ cuyas entradas toman valor distinto de 0 solo cuando corresponden a aquellos índices $i \in S$, tenemos que $(P_1 - P_2)(\chi_S) \neq 0$, lo que contradice el hecho de que $(P_1 - P_2)(\mathbf{x}) = 0$ para cada $\mathbf{x} \in \{0, 1\}^n$. Así, podemos concluir que $P_1 - P_2$ es idénticamente nulo y queda por tanto probada la unicidad de nuestra representación. □

Ahora sí, ya podemos definir una primera medida de complejidad para funciones booleanas: vamos a llamar *grado* de una función booleana, y lo representaremos por $\deg(f)$, al grado del único polinomio real multilineal que representa a f.

Otras dos medidas de complejidad importantes en esta historia son la sensibilidad y la sensibilidad por bloques de una función booleana f.

Dado un vector booleano $\mathbf{x}$ y un entero i comprendido entre 1 y n, vamos a denotar por $\mathbf{x}^{\{i\}}$ al vector booleano obtenido a partir de $\mathbf{x}$ cambiando su i-ésima entrada. La *sensibilidad local* de f en $\mathbf{x}$, que denotaremos por $s(f, \mathbf{x})$, se define como el número de índices $i \in \{1, \dots, n\}$ tales que $f(\mathbf{x}) \neq f\big(\mathbf{x}^{\{i\}}\big)$. A partir de este concepto, vamos a definir la *sensibilidad* de una función booleana f, $s(f)$, como el máximo de las sensibilidades locales; es decir, $s(f) = \text{máx}_{\mathbf{x} \in \{0,1\}^n} s(f, \mathbf{x})$. En base a esta definición, se tiene que la sensibilidad de una función booleana mide su comportamiento local con respecto a la distancia de Hamming, siendo la distancia de Hamming entre dos vectores el número de entradas en las que ambos se diferencian. Informalmente, podemos entender también esta medida de complejidad como una medida de la inestabilidad de una función booleana frente a pequeñas perturbaciones en la entrada.

Generalizando la notación anterior, dado un vector booleano $\mathbf{x}$, para cada subconjunto S del conjunto $[n] = \{1, \dots, n\}$ vamos a denotar por $\mathbf{x}^S$ al vector booleano obtenido a partir de $\mathbf{x}$ cambiando todas las entradas x_i tales que $i \in S$. La *sensibilidad local por bloques* de f en $\mathbf{x}$, que denotaremos por $\text{bs}(f, \mathbf{x})$, se define como el máximo número k de subconjuntos $B_1, \dots, B_k$ de $[n]$ disjuntos tales que para cada B_i se verifica que $f(\mathbf{x}) \neq f\big(\mathbf{x}^{B_i}\big)$. A partir de este concepto, definimos la *sensibilidad por bloques* de una función booleana f, $\text{bs}(f)$, como el máximo de las sensibilidades locales por bloques; es decir, $\text{bs}(f) = \text{máx}_{\mathbf{x} \in \{0,1\}^n} \text{bs}(f, \mathbf{x})$.

Para aclarar estos conceptos, vamos a mostrar un ejemplo de cálculo de la sensibilidad y la sensibilidad por bloques, y lo vamos a hacer para la función de conjunción en n variables, esa función booleana que denotamos por AND_n y que asigna a un vector booleano el valor 1 si y solamente si todas las entradas del vector toman también el valor 1. Si consideramos el vector $\mathbf{1} = (1, 1, \dots, 1)$, para cualquier entero $i \in [1, n]$ resulta que $1 = \text{AND}_n(\mathbf{1}) \neq \text{AND}_n\big(\mathbf{1}^{\{i\}}\big) = 0$, de manera que la sensibilidad local en este vector es igual a n. Como la sensibilidad de una función booleana en n variables está acotada superiormente por n en base a la propia definición, concluimos en este caso que $s(\text{AND}_n) = n$. Sin embargo, $s(\text{AND}_n, \mathbf{0}) = 0$ porque $\text{AND}_n(\mathbf{0}) = \text{AND}_n\big(\mathbf{0}^{\{i\}}\big) = 0$ para cada entero $i \in [1, n]$. En cuanto a la sensibilidad por bloques, es claro que $\text{bs}(\text{AND}_n, \mathbf{1}) = n$ porque cambiar una entrada cualquiera del vector $\mathbf{1}$ cambia el valor que le asigna nuestra función de conjunción, lo que hace que $\{1\}, \{2\}, \dots, \{n\}$ sean n bloques disjuntos y sensibles. Como el máximo valor que puede tomar la sensibilidad por bloques es precisamente n, esto nos permite concluir que $\text{bs}(\text{AND}_n) = n$. Sin embargo, $\text{bs}(\text{AND}_n, \mathbf{0}) = 1$ porque el único bloque sensible para este vector es $\{1, \dots, n\}$.

Aunque no vamos a entrar en detalles en esta nota, existen otras medidas de complejidad de funciones booleanas interesantes. Por citar algunas, podemos mencionar el *grado aproximado*, la *complejidad por árbol de decisión* o la *complejidad por certificado*. Se puede encontrar información sobre ellas en [12] o en [13].

Cuando se introducen distintas medidas de complejidad, aparece de manera natural el concepto de equivalencia entre ellas. Vamos a decir que dos medidas de complejidad de funciones booleanas s_1 y s_2 son *equivalentes*, o están *polinómicamente relacionadas*, si existen constantes $C_1, C_2 > 0$ tales que, para toda función booleana f, se cumple que

$$s_2(f)^{C_1} \leq s_1(f) \leq s_2(f)^{C_2},$$

salvo producto de algún término de la cadena de desigualdades anterior por una constante positiva.

En 1994 se conocía ya gran cantidad de relaciones de tipo polinómico entre las distintas medidas de complejidad de funciones booleanas. Por ejemplo, a partir de la definición de la sensibilidad y la sensibilidad por bloques es claro que, para cada función booleana f, $s(f) \leq \mathrm{bs}(f)$ ya que los conjuntos unipuntuales asociados a los índices de las entradas sensibles para un vector booleano constituyen bloques sensibles y disjuntos que intervienen en el cómputo de la sensibilidad local por bloques en ese vector. En cuanto al grado y la sensibilidad por bloques, a través de ciertos resultados intermedios que podemos encontrar en [13], se había conseguido probar que $\sqrt{\mathrm{bs}(f)/2} \leq \deg(f) \leq \mathrm{bs}(f)^4$, que permite concluir la equivalencia de estas dos medidas. De hecho, esta relación entre la sensibilidad por bloques y el grado de una función booleana se consiguió mejorar en 2013 ([16]), obteniendo la siguiente cadena de desigualdades: $\sqrt{\mathrm{bs}(f)} \leq \deg(f) \leq \mathrm{bs}(f)^4$.

Más allá de eso, por aquel entonces Nisan y Szegedy conocían ya relaciones de tipo polinómico entre todas las medidas de complejidad que he citado previamente en esta nota, salvo una: la sensibilidad. Solo faltaba hallar una cota inferior para esta medida en términos de alguna de las otras. Como todas las demás eran equivalentes, era suficiente con relacionar la sensibilidad con cualquiera de ellas. Así, estos dos autores enuncian en [13] la llamada conjetura de la sensibilidad, que afirma lo siguiente:

Conjetura 1.2 (Conjetura de la sensibilidad). *Existe una constante $C > 0$ tal que, para toda función booleana f,*

$$\mathrm{bs}(f) \leq s(f)^C.$$

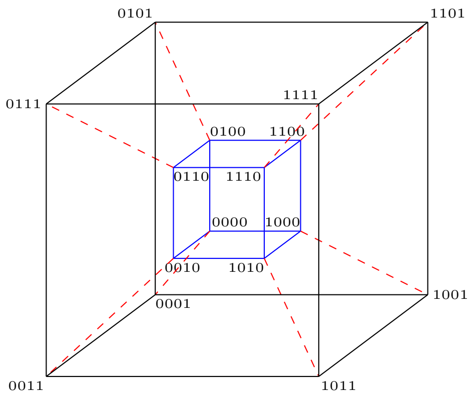
Poco tiempo después de que se enunciara este problema, algo que se había hecho en 1992 aunque no fuese publicado hasta 1994, Gotsman y Linial consiguieron reformular enteramente la conjetura a través de la teoría de grafos. Su forma de hacerlo fue mediante el llamado teorema de equivalencia, enunciado y demostrado en [7] y al que vamos a dedicar un apartado de la siguiente sección.

2. Traducción del problema a teoría de grafos

2.1. Teorema de equivalencia

Como acabamos de comentar, es el teorema de equivalencia el que permite reformular la conjetura de la sensibilidad. A través de él, Gotsman y Linial consiguen establecer, en 1992, una equivalencia entre dos afirmaciones: la primera de ellas se encuadra en el marco de la teoría de la complejidad computacional, a la que pertenece originalmente la conjetura de la sensibilidad; sin embargo, la segunda corresponde a la teoría de grafos y es de naturaleza puramente combinatoria, lo que abre la puerta al uso de gran cantidad de herramientas combinatorias para abordar el problema.

Antes de enunciar este resultado, conviene introducir la notación que vamos a utilizar. Q_n va a denotar el grafo del cubo n-dimensional $C^n = \{0,1\}^n$, en el que dos vértices son adyacentes si y solo si difieren exactamente en una única de sus componentes. Por ejemplo, en el caso $n = 4$, Q_4 sería el grafo siguiente, donde hemos denotado a cada punto de coordenadas (x_1, x_2, x_3, x_4) por $x_1x_2x_3x_4$:



A lo largo de esta nota, todos los grafos con los que vamos a trabajar van a ser no dirigidos, de manera que asumiremos esta condición sin necesidad de especificarla en cada caso. Recordamos ahora que un subgrafo inducido de un grafo H es un grafo cuyos vértices son un subconjunto de los vértices de H y cuyas aristas son todas las aristas de H que unen pares de vértices del subconjunto tomado. Así, siguiendo con cuestiones de notación, para un subgrafo inducido G de Q_n vamos a denotar por $\Delta(G)$ a su grado máximo; es decir, $\Delta(G) = \text{máx}_{\mathbf{x}\in V(G)} \deg_G(\mathbf{x})$, donde $\deg_G(\mathbf{x})$ hace referencia al grado de $\mathbf{x}$ visto como vértice del subgrafo inducido G. Finalmente, vamos a denotar por $\Gamma(G)$ a la siguiente cantidad: $\Gamma(G) = \text{máx}\{\Delta(G), \Delta(Q_n - G)\}$, donde $Q_n - G$ es el subgrafo inducido de Q_n cuyos vértices son aquellos vértices de Q_n que no son vértices de G.

Ahora sí, ya nos encontramos en condiciones de enunciar el teorema de equivalencia, enunciado originalmente en [7].

Teorema 2.1. *Dada una función estrictamente creciente $h : \mathbb{N} \to \mathbb{R}$, las siguientes afirmaciones son equivalentes:*

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

Aunque las dos afirmaciones que relaciona el teorema de equivalencia pueden parecer a priori muy distintas, la idea subyacente en la demostración de este resultado es muy sencilla. La forma de relacionar funciones booleanas y grafos consiste, por un lado, en asociar a cada subgrafo inducido G de Q_n una función booleana g tal que $g(\mathbf{x}) = 1$ si y solo si $\mathbf{x} \in V(G)$. Y viceversa, asociamos a cada función booleana g el subgrafo inducido G de Q_n cuyos vértices son aquellos vectores booleanos $\mathbf{x}$ tales que $g(\mathbf{x}) = 1$. Con esta idea sencilla y unas cuantas manipulaciones, se consigue probar que la primera afirmación del enunciado del teorema es equivalente a

(1′) *Para toda función booleana g, $E(g) \neq \frac{1}{2}$ implica que existe $\mathbf{x} \in C^n$ tal que $s(g, \mathbf{x}) \leq n - h(n)$,*

donde $E(g)$ no es más que el valor medio de la función g en C^n, es decir, $E(g) = \frac{1}{2^n} \sum_{\mathbf{x} \in C^n} g(\mathbf{x})$; y se prueba también que la segunda afirmación del enunciado del teorema es equivalente a

(2′) *Para toda función booleana f, $s(f) < h(n)$ implica que $\deg(f) < n$.*

La demostración del teorema se termina reduciendo, pues, a probar la equivalencia entre (1′) y (2′), que son dos afirmaciones establecidas en términos de medidas de complejidad.

La clave de esta demostración consiste en definir, dada $f : \{0,1\}^n \to \{0,1\}$, la función booleana $\varphi(f) : \{0,1\}^n \to \{0,1\}$ dada por

$$\varphi(f)(\mathbf{x}) = \begin{cases} f(\mathbf{x}), & \text{si } \mathbf{x} \text{ tiene un número par de unos,} \\ 1 - f(\mathbf{x}), & \text{si } \mathbf{x} \text{ tiene un número impar de unos,} \end{cases}$$

para la cual es posible probar lo siguiente:

1. $\varphi \circ \varphi(f) = f$.
2. $\deg(f) = n$ si y solamente si $E(\varphi(f)) \neq \frac{1}{2}$.
3. $s(f, \mathbf{x}) + s(\varphi(f), \mathbf{x}) = n$.

A partir de estos ingredientes, de los cuales el segundo es el único un poco más difícil de probar, es sencillo demostrar que (1′) y (2′) son equivalentes. Veámoslo:

(1′) ⇒ (2′): Para probar esta implicación, comencemos observando que siempre se cumple $\deg(f) \leq n$, luego decir que $\deg(f) < n$ equivale a decir que $\deg(f) \neq n$.

Supongamos que se verifica (1′) y veamos que, para toda función booleana f, $\deg(f) = n$ implica que $s(f) \geq h(n)$.

Si $\deg(f) = n$, entonces $E(\varphi(f)) \neq \frac{1}{2}$; y como estamos suponiendo que se verifica (1′) se tiene que existe $\mathbf{x} \in C^n$ tal que $s(\varphi(f), \mathbf{x}) \leq n - h(n)$.

En consecuencia, para este $\mathbf{x}$ se verifica que $h(n) \leq n - s(\varphi(f), \mathbf{x}) = s(f, \mathbf{x})$ y esto ya nos permite concluir que

$$s(f) = \max_{\mathbf{x} \in C^n} s(f, \mathbf{x}) \geq h(n),$$

que es lo que queríamos probar.

(2′) ⇒ (1′): Para probar esta implicación, supongamos que se verifica (2′) y veamos que, para toda función booleana g, si se cumple que $s(g, \mathbf{x}) > n - h(n)$ para cada $\mathbf{x} \in C^n$, entonces $E(g) = \frac{1}{2}$.

De nuestra hipótesis se deduce que $h(n) > n - s(g, \mathbf{x}) = s(\varphi(g), \mathbf{x})$ para todo $\mathbf{x} \in C^n$. En consecuencia, como C^n tiene una cantidad finita de elementos, se tiene que $s(\varphi(g)) = \max_{\mathbf{x} \in C^n} s(\varphi(g), \mathbf{x}) < h(n)$. Como estamos suponiendo que se verifica (2′), esto implica que $\deg(\varphi(g)) < n$. Por lo tanto, a partir de la segunda de las propiedades de $\varphi(g)$ que hemos enumerado previamente, se tiene que $E(\varphi(\varphi(g)))$ —que coincide con $E(g)$ en virtud de la primera de las propiedades— es igual a $\frac{1}{2}$, que es exactamente lo que queríamos probar.

2.2. PRIMEROS INTENTOS PARA DEMOSTRAR LA CONJETURA DE LA SENSIBILIDAD

Vamos a dedicar este apartado a exponer un resultado publicado en 1988 por Chung, Füredi, Graham y Seymour ([5]) que, combinado con el teorema de equivalencia anterior, nos va a permitir obtener una primera relación entre la sensibilidad y el grado de una función booleana, aunque vamos a ver que no es del tipo deseado.

Antes de introducir el resultado, vamos a comentar una nueva cuestión de notación que va a aparecer con frecuencia a partir de este momento: diremos que $G \in Q_n(N)$ si G es un subgrafo inducido de Q_n con N vértices.

TEOREMA 2.2. *Sea G un subgrafo inducido de Q_n con al menos $2^{n-1}+1$ vértices. Entonces existe un vértice v en G tal que*

$$\deg_G(v) > \frac{1}{2}\log_2 n - \frac{1}{2}\log_2\log_2 n + \frac{1}{2}.$$

Por otra parte, existe un subgrafo $G \in Q_n(2^{n-1}+1)$ tal que $\Delta(G) < \sqrt{n}+1$ y $\Delta(Q_n - G) < \sqrt{n}+1$.

Este teorema consta de dos partes claramente diferenciadas que vamos a analizar por separado.

En cuanto a la primera, lo que nos dice es que, si tenemos un subgrafo inducido G del cubo n-dimensional con al menos $2^{n-1}+1$ vértices, que son la mitad de los vértices más uno, entonces su grado máximo ha de ser al menos $\frac{1}{2}\log_2 n - \frac{1}{2}\log_2\log_2 n + \frac{1}{2}$. Así pues, si tenemos un subgrafo inducido G de Q_n que no tenga exactamente la mitad de los vértices (es decir, tal que $|V(G)|$ sea distinto de 2^{n-1}), entonces o bien él o bien $Q_n - G$ tendrá al menos $2^{n-1}+1$ vértices y en consecuencia su grado máximo estará acotado inferiormente por la cantidad anterior, de manera que tendremos $\Gamma(G) \geq \frac{1}{2}\log_2 n - \frac{1}{2}\log_2\log_2 n + \frac{1}{2}$. Así, por ejemplo, bastaría tomar en el teorema de equivalencia la función h que asigna a cada número natural n el valor $\frac{1}{4}\log_2(n)$, que es estrictamente creciente. Haciendo uso de la implicación (1) $\Rightarrow$ (2) del mencionado teorema, obtenemos una cota superior para el grado de una función booleana en términos de su sensibilidad que es de tipo exponencial, de la forma $\deg(f) \leq 2^{4s(f)} = 16^{s(f)}$. Sin embargo, esto no demuestra la conjetura de la sensibilidad ya que habría que hallar una relación de tipo polinómico entre las dos medidas de complejidad.

En cuanto a la segunda parte del teorema, vamos a dar algunos detalles de la construcción que presentan los autores, la cual ha servido de inspiración para algunos de los resultados que se han publicado en los últimos años, y que Huang utiliza en 2019 para demostrar que su resultado proporciona una relación lo más ajustada posible. La construcción en cuestión consiste en considerar $\mathbf{F} = \{F_1, \ldots, F_k\} \subseteq 2^{[n]}$ una partición del conjunto $\{1, \ldots, n\}$ y definir

$$\begin{aligned}\mathbf{X}(\mathbf{F}) = \{&S \subseteq [n] \text{ tales que } |S| \text{ es par y existe } F \in \mathbf{F} \text{ con } F \subseteq S\}\\ &\cup \{S \subseteq [n] \text{ tales que } |S| \text{ es impar y } F - S \neq \emptyset \text{ para todo } F \in \mathbf{F}\}.\end{aligned}$$

Teniendo en cuenta que la aplicación $\{0,1\}^n \to \mathcal{P}([n])$ que envía a cada $\mathbf{x}$ en $\{i \in [n] : x_i = 1\}$ es una biyección, podemos identificar los conjuntos de vértices de determinados subgrafos de Q_n con familias de subconjuntos finitos de $[n]$. Así, tiene sentido considerar $G(\mathbf{F})$, el subgrafo inducido de Q_n con vértices $\mathbf{X}(\mathbf{F})$, y $G'(\mathbf{F})$, el subgrafo inducido de Q_n con vértices $2^{[n]} - \mathbf{X}(\mathbf{F})$. Estos dos subgrafos inducidos de Q_n son los que permiten probar la cota superior que figura en el enunciado. Lo que se prueba es que $|\mathbf{X}(\mathbf{F})| = 2^{n-1} + (-1)^{n+k+1}$, siendo k el número de conjuntos que forman parte de la familia $\mathbf{F}$, de manera que siempre se va a tener que o bien $G(\mathbf{F})$ o bien $G'(\mathbf{F})$ tiene exactamente la mitad de los vértices de Q_n más uno. Además, sea cual sea de los dos el grafo que tenga exactamente ese número de vértices, se demuestra que el grado máximo de $G(\mathbf{F})$ y $G'(\mathbf{F})$ está acotado superiormente por $\max\{k, \max\{|F_i| : 1 \leq i \leq k\}\}$. Así pues, tomando $\mathbf{F} = \{F_1, \ldots, F_k\}$ una partición del conjunto $\{1, \ldots, n\}$ con $k < \sqrt{n} + 1$ y $|F_i| < \sqrt{n} + 1$ para cada $i \in \{1, \ldots, k\}$, se obtiene un subgrafo inducido G de Q_n tal que $\Delta(G)$ y $\Delta(Q_n - G)$ están acotados superior y estrictamente por $\sqrt{n} + 1$, que es lo que se afirma en la segunda parte del enunciado.

Ahora bien, haciendo uso nuevamente del teorema de equivalencia, es posible extraer otra nueva conclusión de la segunda parte del teorema anterior. Para ello, haremos uso esta vez de la implicación (2) $\Rightarrow$ (1) del teorema de equivalencia. Como hemos construido un subgrafo inducido $G(\mathbf{F})$ del cubo n-dimensional que no tiene exactamente la mitad de sus vértices y tal que tanto su grado como el de $G'(\mathbf{F}) = Q_n - G(\mathbf{F})$ están acotados superior y estrictamente por $\sqrt{n}+1$, resulta que $\Gamma(G(\mathbf{F})) < \sqrt{n} + 1$, con lo cual no se verifica (1) si tomamos $h(n) = \sqrt{n} + 1$, que es una función estrictamente creciente, y en consecuencia existe una función booleana f tal que $s(f) < \sqrt{\deg(f)} + 1$. Esto implica que en general no va a ser cierto que $s(f) \geq \sqrt{\deg(f)} + 1$, aunque vamos a ver que basta cambiar $h(n) = \sqrt{n} + 1$ por $h(n) = \sqrt{n}$ para que el resultado sí sea cierto, y esto es lo que prueba Huang en 2019 para concluir la demostración de la conjetura de la sensibilidad.

Antes de pasar a exponer detalladamente la prueba del resultado de Hao Huang, conviene destacar que hasta 2019, año en que se cierra la demostración de la conjetura de la sensibilidad, todas las relaciones que se habían obtenido entre la sensibilidad y la sensibilidad por bloques de una función booleana eran de tipo exponencial, no polinómico. Sin embargo, algunos autores habían conseguido construir ejemplos de funciones booleanas particulares para las cuales esta relación era polinómica y, de hecho, de orden cuadrático. Entre ellas, destacamos la primera, construida por David Rubinstein en 1995 en [15]. Tras una interpretación posterior del artículo original de Rubinstein que podemos encontrar en una charla impartida por Hao Huang para el *Simons Institute for the Theory of Computing* de la Universidad de California ([10]), dicha función booleana se puede definir de la siguiente manera: el conjunto de partida de la función, a la que vamos a denotar por f, va a ser $\{0,1\}^{n^2}$. Así, nos va a resultar más cómodo representar cada vector booleano como una matriz de la siguiente manera:

$$\mathbf{x} = \begin{pmatrix} x_{11} & x_{12} & \ldots & x_{1n} \\ x_{21} & x_{22} & \ldots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \ldots & x_{nn} \end{pmatrix},$$

donde cada x_{ij} puede tomar solamente los valores 0 o 1. Así, si denotamos por $\bigvee$ a la función OR de disyunción que asigna a un vector booleano el valor 0 si y solo si todas sus entradas toman también el valor 0, vamos a definir la función booleana $f : \{0,1\}^{n^2} \to \{0,1\}$ como

$$f\begin{pmatrix} x_{11} & x_{12} & \dots & x_{1n} \\ x_{21} & x_{22} & \dots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \dots & x_{nn} \end{pmatrix} = \bigvee_{i=1}^{n} g(x_{i1}, \dots, x_{in}),$$

donde $g : \{0,1\}^n \to \{0,1\}$ es una función booleana que toma el valor 1 en $\mathbf{x} = (x_1, \dots, x_n)$ si y solamente si existe un único valor j entre 1 y $n-1$ tal que $x_j = x_{j+1} = 1$ y $x_k = 0$ para todas las demás coordenadas.

En el caso de esta función, es sencillo probar que su sensibilidad por bloques es al menos del orden de n^2. Para ello, vamos a prestar atención al valor de la sensibilidad local por bloques de f en $\mathbf{0} \in \{0,1\}^{n^2}$, teniendo en cuenta que $f(\mathbf{0}) = 0$. En primer lugar, notemos que si en una fila cambiamos el valor de dos coordenadas nulas consecutivas por 1, el valor que toma g en esa fila pasa también a ser 1 y lo mismo ocurre con el valor de f. Así pues, vamos a distinguir ahora dos casos:

- Si n es par, en cada fila es posible tomar un máximo de $\frac{n}{2}$ bloques sensibles y disjuntos. Si nos fijamos en la fila i-ésima, se trata de los bloques correspondientes a los índices (i,j) e $(i,j+1)$, con j impar.

  Como hay un total de n filas, resulta que la sensibilidad local por bloques de f en $\mathbf{0}$ en el caso de n par es $n \cdot \frac{n}{2} = \frac{n^2}{2}$.
- Si n es impar, en cada fila es posible tomar un máximo de $\frac{n-1}{2}$ bloques sensibles y disjuntos. Por ejemplo, si consideramos la fila i-ésima, podemos considerar los bloques correspondientes a los índices (i,j) e $(i,j+1)$, con j impar, de manera que la última entrada de cada fila no pertenezca a ningún bloque.

  Como hay un total de n filas, resulta que la sensibilidad local por bloques de f en $\mathbf{0}$ en el caso de n impar es $n \cdot \frac{n-1}{2} = \frac{n^2-n}{2}$.

Entonces $\mathrm{bs}(f) \geq \mathrm{bs}(f, \mathbf{0})$, siendo esta última del orden de n^2.

Vamos a ver ahora que $s(f) = O(n)$, considerando el valor de la sensibilidad local de f en dos casos distintos.

- En primer lugar, consideramos aquellos $\mathbf{x}$ con $f(\mathbf{x}) = 0$. En este caso, tenemos que el valor de la función g en cada fila de nuestra matriz booleana es 0.

  Si la fila en cuestión tiene todas sus coordenadas nulas, no existe ninguna entrada sensible en ella, ya que cambiar cualquiera de las entradas por 1 no cambia del mismo modo el valor que toma g en la fila.

  Sin embargo, si la fila sí tiene coordenadas no nulas, entonces tendrá como mucho 2 coordenadas sensibles. Esto corresponderá, por ejemplo, al caso en el que la fila sea de la forma $(0 \dots 0\ 1\ 0 \dots 0)$, con una única entrada no nula, y las coordenadas sensibles serán las que se encuentran a la izquierda y a la derecha de esa coordenada no nula.

Así pues, en cada fila tendremos a lo sumo 2 coordenadas sensibles. Como hay un total de n filas, esto nos permite concluir que $s(f, \mathbf{x}) \leq 2n$.

- Si consideramos ahora los $\mathbf{x}$ tales que $f(\mathbf{x}) = 1$, es posible distinguir de nuevo dos posibilidades:
  - Si existen al menos dos filas en las que g toma el valor 1, entonces la sensibilidad local de f en $\mathbf{x}$ es 0, ya que modificando una entrada de una fila solo podríamos cambiar el valor que toma g en esa fila, mientras que en la otra seguiría tomando el valor 1 y en consecuencia f también.
  - Si g toma el valor 1 en una única fila, pongamos la i-ésima, cambiar una entrada de cualquier otra fila no afecta al valor de f. Así pues, todas las coordenadas sensibles se encuentran en la fila i-ésima, que será de la forma $(0 \ldots 0\ 1\ 1\ 0 \ldots 0)$. En consecuencia, todas las entradas de esta fila corresponden a coordenadas sensibles y resulta que $s(f, \mathbf{x}) = n$.

Hemos probado, entonces, que $s(f, \mathbf{x}) \leq 2n$ para cada $\mathbf{x} \in \{0,1\}^{n^2}$ y por tanto $s(f) \leq 2n$, de manera que, como habíamos anunciado, $s(f) = O(n)$.

En resumen, para esta función que hemos definido se cumple que $\mathrm{bs}(f)$ es al menos del orden de n^2, mientras que $s(f) = O(n)$.

La no existencia de ejemplos que evidenciasen una mayor separación entre la sensibilidad y la sensibilidad por bloques hacía sospechar que la conjetura de la sensibilidad iba a ser cierta y que, de hecho, se iba a poder acotar superiormente la sensibilidad por bloques de una función booleana por el cuadrado de su sensibilidad.

Pasemos, ahora sí, a demostrar detalladamente la conjetura de la sensibilidad.

2.3. Demostración de la conjetura de la sensibilidad

En este apartado vamos a exponer en primer lugar, y con todo detalle, el resultado que Hao Huang probó en 2019 en [9]. Además, veremos cómo este resultado permite concluir definitivamente la demostración de la conjetura de la sensibilidad.

Dicho resultado es el siguiente:

Teorema 2.3. *Para todo entero $n \geq 1$, sea H un subgrafo inducido cualquiera de Q_n con $2^{n-1} + 1$ vértices. Entonces*

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

Además, esta cota es la mejor posible.

Antes de pasar a detallar su demostración, conviene hacer una observación e introducir la notación necesaria.

Observación. Como Q_n es un grafo bipartito, sabemos que existe un subgrafo inducido de Q_n con exactamente la mitad de los vértices que tiene grado 0 porque está formado por vértices aislados, sin aristas.

El teorema muestra que el grado máximo de cualquier subgrafo inducido con simplemente un vértice más aumenta repentinamente hasta $\sqrt{n}$.

Notación. Para un grafo G, denotamos por $\lambda_1(G)$ al mayor autovalor de su matriz de adyacencia, siendo la matriz de adyacencia de un grafo aquella matriz simétrica cuyas filas y columnas están indexadas en el conjunto de vértices del grafo, de manera que todos los valores de la diagonal son 0 y la entrada de la fila u y la columna v vale 1 si u y v son vértices adyacentes y 0 en caso contrario. El hecho de que esta matriz sea simétrica implica que es diagonalizable y todos sus autovalores son reales.

En cuanto a la nomenclatura utilizada: dada una matriz A, una submatriz principal de A se obtiene eliminando en A el mismo conjunto de filas y de columnas. Por ejemplo, si eliminamos la segunda y la tercera filas de A, debemos eliminar también la segunda y la tercera columnas. Es fácil observar a partir de esta definición que una submatriz principal de una matriz simétrica también es simétrica.

Abordemos ahora la demostración del Teorema 2.3. Para probarlo, vamos a necesitar una serie de resultados.

El primero de ellos es un resultado clásico, conocido como *teorema del entrelazamiento de Cauchy*, que afirma lo siguiente:

Teorema 2.4 (Teorema del entrelazamiento de Cauchy). *Sea A una matriz simétrica $n\times n$ y sea B una submatriz principal $m\times m$ de A para algún $m < n$. Si los autovalores de A son $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$, y los autovalores de B son $\mu_1 \geq \mu_2 \geq \cdots \geq \mu_m$, entonces para todo i con $1 \leq i \leq m$ se cumple que*

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

Además de este resultado, del que se puede encontrar una prueba sencilla en [8], vamos a hacer uso de otros dos lemas que enunciamos y demostramos a continuación:

Lema 2.5. *Definimos una sucesión de matrices cuadradas simétricas de la forma recursiva siguiente:*

$$A_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad A_n = \begin{pmatrix} A_{n-1} & I \\ I & -A_{n-1} \end{pmatrix}.$$

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

Demostración. Empezamos probando, por inducción, que $A_n^2 = nI$.

- Si $n = 1$,
$$A_1^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I.$$

- Supongamos que el resultado es cierto para $n-1$, es decir, que $A_{n-1}^2 = (n-1)I$, y veamos que entonces también lo es para n:

$$\begin{aligned} A_n^2 = A_n \cdot A_n &= \begin{pmatrix} A_{n-1} & I \\ I & -A_{n-1} \end{pmatrix} \cdot \begin{pmatrix} A_{n-1} & I \\ I & -A_{n-1} \end{pmatrix} \\ &= \begin{pmatrix} A_{n-1}^2 + I & 0 \\ 0 & I + A_{n-1}^2 \end{pmatrix} = \begin{pmatrix} (n-1)I + I & 0 \\ 0 & I + (n-1)I \end{pmatrix} = nI. \end{aligned}$$

Tenemos entonces que $A_n^2 = nI$, de manera que el único autovalor de A_n^2 es n. Ahora bien, es sencillo probar que los autovalores de una matriz B cualquiera se pueden obtener a partir de las raíces cuadradas de los autovalores de B^2.

Así pues, en nuestro caso concreto, los posibles autovalores de A_n son $\sqrt{n}$ y $-\sqrt{n}$.

Como la traza de una matriz es la suma de sus autovalores, la traza de A_n es igual a 0 y los posibles autovalores son $\sqrt{n}$ y $-\sqrt{n}$, tenemos que la mitad de los autovalores corresponden al primer valor y la otra mitad corresponden al segundo; es decir, $\sqrt{n}$ tiene multiplicidad $\frac{2^n}{2} = 2^{n-1}$, y lo mismo ocurre con $-\sqrt{n}$. □

Lema 2.6. *Supongamos que H es un grafo con m vértices y A es una matriz simétrica cuyas entradas pertenecen al conjunto $\{-1, 0, 1\}$ y cuyas filas y columnas están indexadas por $V(H)$, con $A_{u,v} = 0$ si y solo si u y v no son adyacentes en H (a veces se dice que A es una matriz de adyacencia signada o con signo del grafo H). Entonces $\Delta(H) \geq \lambda_1 := \lambda_1(A)$ (el mayor autovalor de A).*

Demostración. Supongamos que $\mathbf{v}$ es un autovector correspondiente al autovalor λ_1. Entonces $A\mathbf{v} = \lambda_1\mathbf{v}$. Si λ_1 fuese igual a 0, entonces el resultado es trivial. Por lo tanto, vamos a trabajar en la demostración con $\lambda_1 \neq 0$, y también con $\mathbf{v} \neq \mathbf{0}$ por ser $\mathbf{v}$ un autovector.

Supongamos sin pérdida de generalidad que v_1 es la coordenada de $\mathbf{v}$ con mayor valor absoluto. Entonces

$$|\lambda_1 v_1| = |(A\mathbf{v})_1| = \left|\sum_{j=1}^{m} A_{1,j} v_j\right| \leq \sum_{j=1}^{m} |A_{1,j}||v_j| \leq |v_1| \sum_{j=1}^{m} |A_{1,j}|.$$

Además, por la forma en la que se ha definido la matriz A, se tiene que la suma de los valores absolutos de las entradas de la primera fila es igual al grado del vértice de H correspondiente a esa fila y, en consecuencia, menor o igual que el grado máximo de H. Por lo tanto,

$$|\lambda_1||v_1| = |\lambda_1 v_1| \leq |v_1|\Delta(H),$$

y como $v_1 \neq 0$ obtenemos que efectivamente $|\lambda_1| \leq \Delta(H)$. □

Y concluimos, ahora sí, la demostración del Teorema 2.3:

Demostración del Teorema 2.3. Sea A_n la n-ésima de las matrices de la sucesión definida en el Lema 2.5, matrices todas ellas cuyas entradas pertenecen al conjunto $\{-1, 0, 1\}$. Gracias a la construcción recursiva de estas matrices, es claro que si cambiamos en A_n aquellas entradas que toman el valor -1 por 1 obtenemos exactamente la matriz de adyacencia del cubo n-dimensional Q_n. En efecto, podemos ver los bloques superior izquierdo e inferior derecho de esta matriz como las matrices de adyacencia de los dos subcubos $(n-1)$-dimensionales de Q_n, y los dos bloques formados por la matriz identidad como los correspondientes a las aristas que conectan estos dos subcubos. En consecuencia, la matriz A_n y el grafo Q_n satisfacen las hipótesis del Lema 2.6. Pero también un subgrafo inducido H de Q_n con $2^{n-1} + 1$ vértices y la submatriz principal A_H de A_n inducida de forma natural por H las satisfacen. Como consecuencia, $\Delta(H) \geq \lambda_1(A_H)$.

Por otra parte, gracias al Lema 2.5, sabemos que los autovalores de A_n son $\sqrt{n}$ y $-\sqrt{n}$, ambos con multiplicidad 2^{n-1}.

Notemos que, como A_H es la submatriz de A_n inducida de forma natural por el subgrafo H de Q_n, que tiene $2^{n-1}+1$ vértices, resulta que A_H es una submatriz de dimensiones $(2^{n-1}+1)\times(2^{n-1}+1)$ de la matriz A_n, que tiene dimensiones $2^n \times 2^n$. En consecuencia, aplicando el teorema del entrelazamiento de Cauchy y teniendo en cuenta que $2^n-(2^{n-1}+1)=2^{n-1}-1$, tenemos que

$$\lambda_1(A_H) \geq \lambda_{1+2^{n-1}-1}(A_n) = \lambda_{2^{n-1}}(A_n) = \sqrt{n}.$$

De esta manera, combinando las dos desigualdades que hemos obtenido gracias a los lemas previos, podemos concluir que

$$\Delta(H) \geq \lambda_1(A_H) \geq \sqrt{n},$$

que es lo que queríamos probar.

Finalmente, para el subgrafo inducido de Q_n con $2^{n-1}+1$ vértices construido por Chung, Füredi, Graham y Seymour cuya construcción hemos presentado en la subsección anterior, la cota se alcanza. Efectivamente, el grado máximo de ese grafo está acotado superior y estrictamente por $\sqrt{n}+1$. Como acabamos de probar que este grado máximo es también mayor o igual que $\sqrt{n}$, ya podemos concluir que la cota proporcionada por este teorema es la mejor posible. $\square$

Observación. Aunque esta demostración destaca por su sencillez, Shalev Ben-David, que es precisamente un antiguo alumno de Scott Aaronson, dejaba un comentario en la entrada [2] del blog de su antiguo profesor proporcionando una nueva demostración del resultado que no requiere hacer uso del teorema del entrelazamiento de Cauchy, sino de otros resultados más elementales y bien conocidos. Vamos a dar los detalles de la misma a continuación, dentro de esta misma observación:

Sea S el espacio de vectores propios asociados al autovalor $\sqrt{n}$ de la matriz A_n, de manera que S tiene dimensión 2^{n-1}.

Consideramos la matriz A_H que aparece en la demostración original de Huang, que recordemos que no es más que la submatriz principal de A_n inducida de forma natural por un subgrafo inducido H de Q_n con $2^{n-1}+1$ vértices. En dicha demostración, el teorema del entrelazamiento de Cauchy se utiliza para proporcionar una cota inferior para el mayor autovalor de esta matriz. Por lo tanto, lo que vamos a hacer ahora es buscar esa cota inferior sin hacer uso del mencionado teorema, y lo hacemos recordando que el mayor autovalor de una matriz real y simétrica coincide con su norma espectral, que viene dada por

$$\|A_H\|_2 = \max_{\|\mathbf{x}\|_2=1} \|A_H\mathbf{x}\|_2.$$

Además, es fácil darse cuenta de que hallar el máximo de las cantidades anteriores en el conjunto de vectores de norma 1 equivale a hallar el máximo de las cantidades $\|A_n\mathbf{x}\|_2$ en el conjunto de vectores de norma 1 cuyas entradas con índices correspondientes a columnas de A_n que no forman parte de A_H son nulas. Si denotamos por L al subespacio formado por todos estos vectores, entonces L tiene dimensión al menos $2^{n-1}+1$, que es el número de columnas de A_H. Ahora bien, teniendo en cuenta que la dimensión del subespacio $L+S$ está acotada superiormente por 2^n, que es la dimensión del espacio total, aplicando la fórmula de las dimensiones resulta que

$$\dim(L \cap S) = \dim(L) + \dim(S) - \dim(L+S) \geq 2^{n-1} + 1 + 2^{n-1} - 2^n = 1.$$

En consecuencia, existe un vector $\mathbf{x}_0$ de norma 1 que pertenece a L y a S; es decir, es un vector propio asociado al autovalor $\sqrt{n}$ de A_n y todas sus entradas con índices correspondientes a las columnas de A_n que no están en A_H son nulas. Así pues, si denotamos por $\mathbf{x}_0^*$ al vector unitario obtenido a partir de $\mathbf{x}_0$ eliminando todas esas entradas nulas con índices correspondientes a las columnas de A_n que no están en A_H, tenemos que

$$\|A_H \mathbf{x}_0^*\|_2 = \|A_n \mathbf{x}_0\|_2 = \|\sqrt{n} \cdot \mathbf{x}_0\|_2 = \sqrt{n}\,\|\mathbf{x}_0\|_2 = \sqrt{n},$$

y de aquí se sigue que el mayor autovalor de A_H está acotado inferiormente por $\sqrt{n}$, que es lo que queríamos probar.

Volvamos, para terminar, al problema de la conjetura de la sensibilidad.

Acabamos de probar que para todo subgrafo inducido H de Q_n con $2^{n-1}+1$ vértices se verifica que $\Delta(H) \geq \sqrt{n}$. Así pues, si consideramos cualquier subgrafo inducido G de Q_n con $|V(G)| \neq 2^{n-1}$, o bien G o bien $Q_n - G$ será un grafo con al menos $2^{n-1}+1$ vértices. Como la función Δ es monótona (en el sentido de que $\Delta(G_1) \leq \Delta(G_2)$ si G_1 es un subgrafo de G_2), el teorema que acabamos de probar nos permite afirmar que $\Gamma(G) = \text{máx}\{\Delta(G), \Delta(Q_n - G)\} \geq \sqrt{n}$, y esto no es más que la primera de las afirmaciones del enunciado del Teorema 2.1 (de equivalencia) tomando como h la función raíz cuadrada, que es estrictamente creciente. En virtud de este teorema, lo que acabamos de probar es equivalente a que toda función booleana f verifica que $s(f) \geq \sqrt{\deg(f)}$, obteniendo de esta manera una cota inferior para la sensibilidad de una función booleana en términos de otra de las medidas de complejidad que hemos considerado en esta nota.

Para poder relacionar la sensibilidad y la sensibilidad por bloques de una función booleana, que es como se había enunciado originalmente la conjetura de la sensibilidad, basta recordar que el grado de una función booleana y su sensibilidad por bloques están polinómicamente relacionados a partir de la cadena de desigualdades $\sqrt{\mathrm{bs}(f)} \leq \deg(f) \leq \mathrm{bs}(f)^4$.

Combinando esto con la desigualdad que acabamos de obtener, resulta que $\mathrm{bs}(f) \leq \deg(f)^2 \leq s(f)^4$, lo que concluye definitivamente la prueba de la conjetura de la sensibilidad, proporcionando una cota superior de grado 4 para la sensibilidad por bloques de una función booleana en términos de su sensibilidad.

La demostración de este resultado tiene varias consecuencias importantes. En primer lugar, como ya habíamos comentado previamente, nos permite concluir que todas las medidas de complejidad de funciones booleanas que he mencionado en este trabajo, e incluso algunas definidas más recientemente y relacionadas con la computación cuántica, están polinómicamente relacionadas. Así, desde el punto de vista computacional, la conjetura de la sensibilidad implica que las funciones booleanas «suaves» (de baja sensibilidad) son fáciles de calcular utilizando algunos de los modelos computacionales más simples, como por ejemplo los árboles de decisión. Algebraicamente, de este resultado se deduce que las funciones booleanas con estas propiedades tienen un grado bajo como polinomios reales.

Además de estas consecuencias inmediatas, la demostración de la conjetura de la sensibilidad ha abierto nuevas líneas de investigación, de las que vamos a hablar brevemente en la siguiente sección.

3. Nuevas líneas de investigación

En primer lugar, y como ya habíamos comentado cuando presentamos la función de Rubinstein, construyendo funciones booleanas particulares se ha conseguido obtener una separación de, al menos, orden cuadrático entre la sensibilidad y la sensibilidad por bloques de ciertas funciones booleanas. Varios autores sugieren que esta es la mayor separación que puede haber entre ambas medidas de complejidad. No obstante, la relación que hemos obtenido entre ellas a partir de la combinación del resultado de Huang con el teorema de equivalencia, que proporciona una relación ajustada entre la sensibilidad y el grado, es de grado cuatro. A día de hoy, todavía no se ha conseguido probar que dicha separación de orden cuadrático sea cierta en general. El autor de la demostración de la conjetura de la sensibilidad sí cree que la sensibilidad por bloques de una función booleana se debe poder acotar superiormente, salvo constante, por el cuadrado de su sensibilidad, y piensa que este resultado podría probarse utilizando técnicas de álgebra lineal y teoría espectral (como en la demostración de su resultado), aunque en estos momentos es un problema abierto.

Otra de las cuestiones que Huang plantea tras su demostración consiste en generalizar los resultados que hemos expuesto para grafos de hipercubos n-dimensionales a otros grafos que tengan «mucha» simetría.

Dado un grafo G, se llama *conjunto independiente de* G a un conjunto de vértices de G tales que no existen entre ellos dos vértices adyacentes, y *número de independencia de* G al cardinal del mayor conjunto independiente. Así, concretamente, las preguntas que plantea Huang son las siguientes: si G es un grafo con «mucha» simetría y denotamos por $\alpha(G)$ su número de independencia, ¿qué podemos decir acerca del mínimo del conjunto de grados máximos de subgrafos inducidos de G con $\alpha(G)+1$ vértices? Si denotamos por $f(G)$ a este valor, ¿en qué condiciones podremos proporcionar una cota inferior para $f(G)$ que se alcance? Es fácil apreciar que esto busca generalizar la situación a la que Huang se enfrenta en su resultado, con el grafo simétrico Q_n y sus subgrafos inducidos con $2^{n-1}+1$ vértices, valor que coincide en este caso con $\alpha(Q_n)+1$.

Gran parte de los trabajos que se han publicado en relación con estas dos preguntas consideran a los grafos de Cayley como grafos con suficiente simetría que permitan generalizar los resultados sobre hipercubos n-dimensionales que hemos comentado. Dado un grupo G y un subconjunto $S \subseteq G$, se define *el grafo de Cayley de* G *con respecto a* S, que denotaremos por $\mathrm{Cay}(G,S)$, como el grafo cuyos vértices son los elementos de G y cuyas aristas son los pares $\{a, a \cdot s\}$, donde $a \in G$ y $s \in S$. De hecho, Q_n no es más que un caso particular de grafo de Cayley; concretamente, $Q_n = \mathrm{Cay}\big(\mathbb{Z}_2^n, \{e_1, \ldots, e_n\}\big)$, donde los e_i son los vectores que forman la base canónica de $\mathbb{Z}_2^n$.

En el caso en el que G es un grupo abeliano y $\mathrm{Cay}(G, S)$ es bipartito, se ha conseguido probar que $f(G) \geq \sqrt{(|S| + t)/2}$, siendo t el número de elementos de orden 2 en S. Esto generaliza el resultado de Huang en este caso particular y fue demostrado en 2020 por Aaron Potechin y Hing Yin Tsang ([14]), los cuales se apoyan en un trabajo de Noga Alon y Kai Zheng publicado el mismo año ([3]).

Además, aunque existen artículos previos en los que se prueba que el valor que hemos denotado por $f(G)$ no puede ser acotado inferiormente por una función del grado para grafos de Cayley en general, vamos a destacar uno de los más recientes: ha sido publicado en 2022 y sus autores son Ignacio García-Marco y Kolja Knauer ([6]), que abordan distintos problemas en relación con este tema. En primer lugar, proporcionan tres familias de grafos de Cayley que tienen grado no acotado pero tales que $f(G) = 1$ para todos sus miembros G. Además, en relación con la pregunta de si se puede dar una cota inferior para $f(G)$ que se alcance, los autores enuncian y demuestran como consecuencia del resultado de Huang que si un grafo de Cayley bipartito G tiene como subgrafo inducido a un hipercubo de dimensión máxima $\kappa(G)$, entonces $f(G) \geq \sqrt{\kappa(G)}$. A continuación, obtienen infinitas familias de grafos de Cayley con el valor κ no acotado para las cuales la cota inferior anterior se alcanza. Para ello, estudian los grupos de Coxeter. Un *sistema finito de Coxeter* es un par (W, S), donde W es un grupo con generadores $S = \{a_1, \ldots, a_n\}$ y presentación $W = \langle a_1, \ldots, a_n : (a_i a_j)^{m_{ij}} = 1\rangle$, donde $m_{ij} > 1$ y $m_{ii} = 2$. Es precisamente W quien recibe el nombre de *grupo de Coxeter*. Dentro de este estudio, los autores conjeturan que para todo grafo de Cayley G de un grupo de Coxeter se verifica que $f(G) = \lceil \sqrt{\kappa(G)} \rceil$.

Más allá de esto, y volviendo al problema del hipercubo, Huang planteó una nueva pregunta. Si $g(n, k)$ es el mínimo valor t tal que todo subgrafo inducido H de Q_n con t vértices tiene grado máximo al menos k, lo que se ha probado ya es que $g(n, \sqrt{n}) = 2^{n-1} + 1$. Huang sugiere que podría resultar interesante hallar el valor de $g(n, k)$ para distintos valores de k.

En cualquier caso, cerrar la demostración de la conjetura de la sensibilidad ha permitido abrir nuevas puertas hacia distintos caminos que poco a poco se van consolidando como un área de trabajo muy prolífica.

REFERENCIAS

[1] S. AARONSON, My philomath project: Sensitivity versus block-sensitivity, *Shtetl-Optimized*, `https://scottaaronson.blog/?p=453`, 2010.

[2] S. AARONSON, Sensitivity Conjecture resolved, *Shtetl-Optimized*, `https://scottaaronson.blog/?p=4229`, 2019.

[3] N. ALON Y K. ZHENG, Unitary signings and induced subgraphs of Cayley graphs of $\mathbb{Z}_2^n$, *Adv. Comb.* 2020, paper no. 11, 12 pp.

[4] S. Asensio Ferrero, *Sobre la conjetura de la sensibilidad y su resolución vía teoría de grafos*, Trabajo de fin de grado, Facultad de Ciencias, Universidad de Valladolid, 2022. Disponible en `https://uvadoc.uva.es/handle/10324/57957`.

[5] F. R. K. Chung, Z. Füredi, R. L. Graham y P. Seymour, On induced subgraphs of the cube, *J. Combin. Theory Ser. A* **49** (1988), 180–187.

[6] I. García-Marco y K. Knauer, On sensitivity in bipartite Cayley graphs, *J. Combin. Theory Ser. B* **154** (2022), 211–238.

[7] C. Gotsman y N. Linial, The equivalence of two problems on the cube, *J. Combin. Theory Ser. A* **61** (1992), no. 1, 142–146.

[8] W. H. Haemers, Interlacing eigenvalues and graphs, *Linear Algebra Appl.* **226-228** (1995), 593–616.

[9] H. Huang, Induced subgraphs of hypercubes and a proof of the sensitivity conjecture, *Ann. of Math. (2)* **190** (2019), no. 3, 949–955.

[10] H. Huang, Sensitivity Conjecture and Its Applications, *Simons Institute for the Theory of Computing*, YouTube, 2020. Disponible en `https://www.youtube.com/watch?v=EJoe4qH6kLs`.

[11] G. Kalai, Amazing: Hao Huang Proved the Sensitivity Conjecture!, *Combinatorics and more*, `https://gilkalai.wordpress.com/2019/07/02/amazing-hao-huang-proved-the-sensitivity-conjecture/`, 2019.

[12] S. Kopparty, E. Cai y Z. Langley, Lecture 3: Boolean Function Complexity Measures, *Advanced Topics in Algorithms and Complexity*, Rutgers University, 2020. Disponible en `https://sites.math.rutgers.edu/~sk1233/courses/topics-S20/lec3.pdf`.

[13] N. Nisan y M. Szegedy, On the degree of Boolean functions as real polynomials, *Comput. Complexity* **4** (1994), 301–313.

[14] A. Potechin y H. Y. Tsang, A conjecture on induced subgraphs of Cayley graphs, `https://arxiv.org/abs/2003.13166`, 2020.

[15] D. Rubinstein, Sensitivity vs. block sensitivity of Boolean functions, *Combinatorica* **15** (1995), 297–299.

[16] A. Tal, Properties and applications of Boolean function composition, *Proc. 4th Conf. on Innov. Theor. Comput. Sci.*, 441–454, ACM Digital Library, 2013.

[17] T. Tao, Twisted convolution and the sensitivity conjecture, *What's new*, `https://terrytao.wordpress.com/2019/07/26/twisted-convolution-and-the-sensitivity-conjecture/`, 2019.

Sara Asensio Ferrero, Universidad de Valladolid
Correo electrónico: `saraasensioferrero@gmail.com`