TEMat

Cuestiones existenciales en combinatoria y teoría de números: el método probabilístico

Ismael Morales López
Universidad Autónoma de Madrid
ismael.moralesl@estudiante.uam.es

Resumen: La probabilidad es una rama de las matemáticas indispensable en la formulación de muchos fenómenos físicos y, en general, de procesos que contengan algún tipo de arbitrariedad. Un aspecto menos conocido de esta es el poder que puede llegar a tener en cuestiones de naturaleza discreta.

El método probabilístico es una herramienta que parte de una idea muy limpia y prometedora. Con el fin de demostrar la existencia de un objeto C caracterizado por una determinada propiedad P, se embebe C en un espacio de probabilidad y se demuestra que el suceso correspondiente a tener la propiedad P ocurre con probabilidad positiva.

El objetivo de este artículo es sentar la base teórica tras la cual subyace esta técnica y presentar varias aplicaciones en problemas relacionados con la combinatoria y la teoría de números.

Abstract: Probability is an indispensable branch of mathematics when it comes to formulating many physical phenomena and, in general, processes which contain some arbitrariness. A less-known aspect is the power it can achieve when tackling questions of discrete nature.

The probabilistic method is a tool based on a neat and promising idea. With the aim of proving the existence of an object C characterised by some property P, C is embedded in a probability space and it is proved that the event corresponding to having property P holds with positive probability.

The objective of this paper is to set the theoretical background that rests behind this technique and to present some applications in problems with a combinatorial or number-theoretic flavour.

Palabras clave: espacio y función de probabilidad, independencia entre sucesos, elección aleatoria y uniforme, distribución, variable aleatoria, esperanza, varianza, método probabilístico, propiedad local, comportamiento asintótico.

MSC2010: 05C15, 05D40, 11E99.

Recibido: 6 de mayo de 2019.
Aceptado: 27 de abril de 2020.

Referencia: Morales López, Ismael. «Cuestiones existenciales en combinatoria y teoría de números: el método probabilístico». En: *TEMat*, 4 (2020), págs. 43-65. ISSN: 2530-9633. URL: https://temat.es/articulo/2020-p43.

1. Introducción histórica y motivación

La probabilidad es una de las áreas de las matemáticas que crece a mayor velocidad. Por un lado, ha resultado ser imprescindible en la formulación matemática de nociones como arbitrariedad e incertidumbre en ramas científicas como la informática teórica y la física estadística. También ha sido crucial en el desarrollo de la combinatoria y la teoría de grafos, aunque ciertamente no se puede decir que estos avances fuesen esperados. Al menos no eran parte de las inquietudes reflejadas en el sexto de los 23 problemas que planteó Hilbert para la conferencia de París del *Congreso Internacional de Matemáticos* de 1900, en el que se hablaba de la necesidad de axiomatizar la teoría de la probabilidad.

La influencia de la probabilidad en combinatoria, teoría de grafos y otras ramas como teoría de números, geometría convexa y finita o combinatoria aditiva se debe al método que da nombre al artículo. Comienza siendo un argumento muy concreto pero admite diferentes niveles de sofisticación y generalidad. Vagamente, consiste en demostrar que entre una colección de objetos existe al menos uno, digamos C, con una propiedad P determinada. Para ello, estos objetos pasarán a ser los elementos de un cierto espacio de probabilidad en el cual el suceso correspondiente a tener la propiedad P ocurre con probabilidad positiva, garantizando la existencia de C.

Sin embargo, cuando se consideran versiones más generales y sofisticadas de este argumento, es mucho más difícil entender el fondo, como ocurre con la demostración del teorema de Green-Tao [24], el cual afirma que existen progresiones aritméticas de primos arbitrariamente largas. Habiendo enunciado el resultado anterior, conviene recalcar que la probabilidad parece ser una pieza fundamental en el estudio de los números enteros. Este es un hecho tan sorprendente como el papel que juega el análisis complejo, inevitable en cualquier demostración del teorema de los números primos. Pero no nos perdamos en nuestro afán de conocimiento y remontémonos a mediados del siglo XX para exponer un problema de combinatoria que servirá para explicar el origen del método probabilístico en su versión más simple.

Definición 1. Dados dos enteros positivos n, m, definimos el **número de Ramsey** $R(n, m)$ como el mínimo entero positivo R tal que, para toda coloración de las aristas de un grafo R-completo (véase la definición 11) con los colores azul y rojo, existe un subgrafo n-completo de aristas rojas o un subgrafo m-completo de aristas azules. ◂

Para que lo anterior sea una definición, hay que demostrar que tales números existen. El lector puede encontrar una demostración de este hecho en el libro de Bollobás [6, capítulo 6], donde se prueba que

$$R(n, m) \leq R(n, m-1) + R(n-1, m), \tag{1}$$

que, por las relaciones de recurrencia que satisfacen los coeficientes binomiales, nos lleva a que

$$R(n, m) \leq \binom{n+m-2}{m-1} \quad \text{si } n, m \geq 2. \tag{2}$$

Cuando $n = m = k$, se tienen los números de Ramsey diagonales $R(k, k)$. Se comprueba fácilmente que $R(1, 1) = 1$, $R(2, 2) = 2$ y $R(3, 3) = 6$. Sin embargo, en general no es sencillo calcular explícitamente estos valores. El valor de $R(4, 4) = 18$ también puede hallarse a mano, pero el de $R(5, 5)$ se desconoce por el momento: solo se conoce la estimación $43 \leq R(5, 5) \leq 48$ [44]. Como consecuencia de la ecuación (2) en el caso $n = m = k$, se tiene que

$$R(k, k) < 4^{k-1} \quad \text{si } k \geq 2. \tag{3}$$

La demostración de la ecuación (1) es inductiva y solo hace uso del principio del palomar. De hecho, la misma prueba proporciona incluso un algoritmo para encontrar un subgrafo completo monocromático de manera recursiva. Este argumento aparece en el artículo original de Ramsey [31], donde se introducen versiones más generales del problema que estamos discutiendo con la motivación de encontrar un algoritmo que determine la validez de ciertas fórmulas de una lógica de primer orden. Por otro lado, en este artículo se plantea probar una cota inferior explícita para los números de Ramsey, concretamente que

$$2^{k/2} \leq R(k, k) \quad \text{si } k \geq 2, \tag{4}$$

en el ejercicio 4. Lo interesante es que la demostración es de naturaleza existencial y no produce explícitamente la coloración de un grafo de al menos $2^{k/2}$ vértices sin subgrafos k-completos monocromáticos. En efecto, se colorean las aristas uniformemente al azar y se prueba que el grafo verificará esta propiedad con probabilidad positiva, que corresponde al esquema de demostración que seguiremos en las secciones 3 y 6.

Esta diferencia entre las demostraciones de las ecuaciones (3) y (4) también explica el nombre del artículo, porque las cuestiones que tratamos son únicamente existenciales, en contraposición con las constructivas.

La cota de la ecuación (4) fue descubierta por Erdős en 1947 [16]. Comenzamos hablando de Erdős porque es considerado el pionero de lo llamado posteriormente *método probabilístico*. Bien es cierto que Szele [37] aplicó un argumento probabilístico a un problema de combinatoria en un artículo de 1943 (considerada la primera aplicación del método probabilístico en combinatoria) y que, como analizaremos en la sección 5, Turán [40] también habría empleado técnicas de probabilidad para probar un resultado de teoría analítica de números en 1934, el cual trataremos con detalle en el teorema 21. Sin embargo, es Erdős quien entendió de verdad su potencia y lo aplicó recurrentemente en múltiples resultados. Alon [1] explicó por qué considera que esta es una de las mayores contribuciones de Erdős y añade que él siempre estaba más interesado en discutir nuevos problemas que en evaluar el mérito que tendrían a largo plazo sus resultados. Por ello, resalta que durante la celebración de su 80.º cumpleaños en Keszthely, Hungría, Erdős dijera que creía que esta técnica viviría mucho después de él.

Una objeción de carácter técnico sobre este método puede ser que en algunos casos parece superfluo enfocar el problema desde un punto de vista probabilístico. De hecho, al menos en las demostraciones de las secciones 3 y 4, para probar la existencia de una configuración con una característica determinada, se prueba que la cantidad de configuraciones sin dicha propiedad es menor que el número total de configuraciones posibles, forzando la existencia de al menos una con el requerimiento deseado. Además, en esto se basa la proposición 8, el único ingrediente de dichas secciones. Sin embargo, el lenguaje probabilístico permite simplificar los cálculos y, más importante, resulta inevitable para diseñar un método más potente con condiciones más técnicas de independencia como las del lema local de Lovász, discutido en la sección 6. La justificación para esto último es que la noción de independencia se reconoce fácilmente desde el punto de vista de la combinatoria pero se explota propiamente con las técnicas probabilísticas. Además, aunque no es el caso de este artículo, a veces conviene considerar distribuciones no uniformes, como puede verse en el libro de Alon y Spencer [3, teorema 3.2.1, pág 29, y teorema 1, pág 41].

Por otro lado, aunque por simplicidad restrinjamos nuestra exposición a cuestiones que involucren o permitan reducciones a espacios de probabilidad finitos, no todos los objetos sobre los que podemos aplicar esta técnica son de naturaleza discreta. En efecto, hay espacios mucho más complejos de naturaleza analítica o geométrica que vienen equipados de una medida gracias a la cual pueden recrearse estos argumentos de tipo probabilístico. Hay una rica colección en Wikipedia [41] donde, por ejemplo, se mencionan resultados tan icónicos como el teorema fundamental del álgebra, el teorema de Picard y el teorema de aproximación de Weierstrass. Estos ejemplos de teoremas demostrables con técnicas de probabilidad no fueron probados por primera vez así, sino que estas demostraciones vinieron *a posteriori*. Por el contrario, hay muchos ejemplos de objetos en matemáticas cuya existencia se prueba primero por medio de un argumento de este estilo antes de poder encontrar ejemplos concretos (más discusión en el libro de Alon y Spencer [3, capítulo 9]). Este es el caso de los «*expanders*», un tipo de grafos de gran interés en áreas ligadas a la informática como la teoría de códigos [35], de los cuales no se encontraron construcciones explícitas hasta 1973 [26]. De todas formas, aún en caso de solo haber probado la existencia de un cierto objeto por medio de estos argumentos, en general estos pueden dar lugar a algoritmos probabilísticos efectivos que puedan además desaleatorizarse para construir un tal objeto de manera determinista. Este enfoque práctico, discutido también por Alon y Spencer [3, capítulo 6], solo volverá a mencionarse en contextos más concretos al final de la sección 6.

Habiendo quedado clara la importancia del enfoque probabilístico, hacemos un pequeño resumen de la exposición. En la siguiente sección recordaremos algunas definiciones básicas. Aunque el artículo sea prácticamente autocontenido, es importante tener cierta familiaridad con el cálculo de probabilidades en espacios finitos y, en particular, con el significado de los coeficientes binomiales. Para adquirir o recordar estas técnicas de combinatoria se recomiendan los apuntes de Fernández y Fernández [22], por la selección de ejemplos tratados y su cautivadora redacción. Las distribuciones consideradas son siempre uniformes y, por tanto, los cálculos de probabilidades se harán empleando la regla de Laplace y, a lo largo del artículo, las manipulaciones involucrarán identidades que enunciaremos con antelación, como la proposición 7 o el lema 18. En esta sección 2 también se enuncia el resultado fundamental, recogido en la proposición 8, sobre el cual se apoya la primera versión que desarrollaremos sobre el método probabilístico y que se empleará en las secciones 3 y 4 para resolver problemas relacionados con la teoría de grafos y la combinatoria aditiva.

En la sección 5 se estudiará una aplicación a la teoría de números. Se considera la función ν, donde $\nu(m)$ es la cantidad de divisores primos de m. A través de sus propiedades aritméticas, se estudian la esperanza y la varianza de esta variable aleatoria en segmentos $\{1, \dots, n\}$ de $\mathbb{N}$ para obtener información sobre su distribución cuando $n \to \infty$ por medio de un argumento de Turán. Se cierra la sección con el enunciado del teorema de Erdős-Kac, que describe completamente cómo se distribuye ν, y después se discute en qué consiste el método de momentos en el contexto de la demostración de dicho resultado.

Como adelantamos, en la sección 6 se estudiará el lema local de Lovász. Primero se discutirá la motivación, el significado detrás del lema y se ofrecerá una demostración de la versión general de este lema. Después daremos una versión que es más transparente y fácil de usar, desde el punto de vista de las aplicaciones de este artículo, para aplicarlo en problemas relacionados con la coloración de hipergrafos. Uno de estos corolarios es bastante sorprendente ya que la coloración se considera en $\mathbb{R}$ y se conjetura que el uso de argumentos topológicos es irremplazable. En esta sección también se discute brevemente el aspecto algorítmico tanto del lema local de Lovász como de las estimaciones de los números de Ramsey. Por último, en el apéndice A se resuelven todos los problemas planteados a lo largo de la exposición.

La redacción de este artículo y los temas tratados están profundamente influidos por el estilo y las motivaciones del artículo de Chen [11], los apuntes de Loh [25] y Riordan [32] y, especialmente, por los libros de Alon y Spencer [3] y Tao y Vu [39].

2. Fundamentos del método probabilístico

Comenzamos fijando una notación que se empleará en todo el artículo.

Notación. Se denota por $\mathbb{Z}^+$ el conjunto de enteros positivos. Dado $n \in \mathbb{Z}^+$, denotamos por $[n]$ el conjunto de enteros k tales que $1 \leq k \leq n$. ◂

En esta sección fijaremos nociones fundamentales de probabilidad y daremos la primera herramienta con la que trabajar problemas de combinatoria desde un punto de vista probabilístico en la proposición 8. Las definiciones que se presentan suelen aparecer en libros de probabilidad en un contexto más general, lo cual no es necesario para nuestro propósito. Por lo tanto, haremos un desarrollo *ad hoc* de algunos objetos y nociones asociados a espacios de probabilidad finitos. Se recuerda que, dado un conjunto Ω, se denota por $\mathcal{P}(\Omega)$ a la colección de subconjuntos de Ω, que incluye a $\varnothing$ y Ω.

Definición 2. Un **espacio de probabilidad** es un par $(\Omega, \mathbb{P})$, que consta de un conjunto Ω finito (no vacío) denominado **espacio muestral**, y de una función $\mathbb{P} : \mathcal{P}(\Omega) \to [0,1]$, denominada **función de probabilidad**, que verifica que

- $\mathbb{P}(\Omega) = 1$ y
- dada una colección $\{A_i\}_{i=1}^m$ de subconjuntos de Ω disjuntos entre sí dos a dos, se tiene que

$$\mathbb{P}\left(\bigcup_{k=1}^{n} A_k\right) = \sum_{k=1}^{n} \mathbb{P}(A_k).$$ ◂

Podemos entender cada uno de los elementos del espacio muestral Ω como un posible resultado de un experimento. Por ejemplo, adelantando el primer ejemplo de la siguiente sección, cada $\omega \in \Omega$ puede ser la relación final entre los jugadores de un torneo en el cual se ha determinado al azar el resultado de cada uno de los enfrentamientos. Un suceso S es la colección de resultados ω con una determinada característica, como puede ser la propiedad de tener un jugador que haya ganado a todos. Con el propósito de esta exposición, haremos la siguiente identificación en el lenguaje: diremos que un resultado $\omega \in \Omega$ de un experimento aleatorio tiene las características descritas por el suceso $S \subseteq \Omega$ si $\omega \in S$.

Otro posible ejemplo es el siguiente. Tomamos un número uniformemente al azar en $\{1, \dots, 100\}$ y consideramos el suceso S que viene dado por la propiedad de ser par. Es decir, $S = \{x \in [100] : x \text{ es par}\} = \{2, 4, \dots, 98, 100\}$ y x verifica la propiedad S si y solo si $x \in S$. En casos tan sencillos parece algo innecesariamente confuso, pero, cuando se traten más ejemplos concretos, se podrá comprobar que este abuso de lenguaje resulta ser en realidad una simplificación. Otra justificación para no referirnos a S como un subconjunto de Ω sino como una propiedad es el hecho de que todos los sucesos que nos interesan aparecerán como propiedades y no como una colección explícita de elementos.

En lo que sigue, todas las definiciones y proposiciones parten de un espacio de probabilidad $(\Omega, \mathbb{P})$.

Definición 3. Una **variable aleatoria** es una función $X\colon \Omega \to \mathbb{R}$. ◂

Obedeciendo a la intuición que hemos presentado sobre cada suceso como una colección de resultados ω con una determinada propiedad, vamos a fijar la siguiente notación estándar.

Notación. Sea P una propiedad que pueda adquirir un número real y sea X una variable aleatoria. El suceso $\{\omega \in \Omega : X(\omega) \text{ verifica } P\}$ se escribirá abreviadamente como $\{X \text{ verifica } P\}$. En particular, si $T \subseteq \mathbb{R}$, entonces el suceso $X^{-1}(T) = \{\omega \in \Omega : X(\omega) \in T\}$ se abreviará por $\{X \in T\}$. ◂

Por tanto, lo anterior nos servirá para introducir sucesos en Ω por medio de una variable aleatoria X, ya que una tal propiedad P induce una propiedad en Ω considerando la preimagen por X.

Definición 4. Decimos que n sucesos $S_1, \dots, S_n$ de Ω son **independientes** si, para todo subconjunto $J \subseteq [n]$,

$$\mathbb{P}\left(\bigcap_{j\in J} S_j\right) = \prod_{j\in J} \mathbb{P}(S_j).$$ ◂

Definición 5. Dado $A \subseteq \Omega$, la variable aleatoria **indicatriz** (o indicadora) de A, denotada por X_A, es

$$X_A(\omega) = \begin{cases} 0 & \text{si } \omega \notin A, \\ 1 & \text{si } \omega \in A. \end{cases}$$ ◂

Es oportuno adelantar que las variables aleatorias que consideraremos serán sumas de indicatrices.

Definición 6. Sea X una variable aleatoria que toma los valores $a_1, \dots, a_n$. Entonces, la **esperanza** de X es

$$\mathbb{E}[X] = \sum_{k=1}^{n} a_k \mathbb{P}(X = a_k).$$ ◂

Proposición 7. *En todo espacio de probabilidad $(\Omega, \mathbb{P})$ se verifican estas propiedades:*

1. (Subaditividad de la función de probabilidad) *Dados los sucesos $A_1, \dots, A_n$, se tiene que*

$$\mathbb{P}\left(\bigcup_{k=1}^{n} A_k\right) \leq \sum_{k=1}^{n} \mathbb{P}(A_k),$$

   con igualdad si los sucesos son disjuntos dos a dos.
2. (Linealidad de la esperanza) *Dadas $X_1, \dots, X_k$ variables aleatorias, entonces*

$$\mathbb{E}\left[\sum_{k=1}^{n} X_k\right] = \sum_{k=1}^{n} \mathbb{E}[X_k].$$

Proposición 8 (Resultados de existencia). *En todo espacio de probabilidad $(\Omega, \mathbb{P})$ se verifica lo siguiente:*

1. *Dados los sucesos $A_1, \dots, A_n$, si tenemos que $\sum_{k=1}^{n} \mathbb{P}(A_k) < 1$, entonces se tiene que $\bigcup_{k=1}^{n} A_k \neq \Omega$, o, equivalentemente por las leyes de De Morgan, $\bigcap_{k=1}^{n} A_k^c \neq \emptyset$. De hecho, la probabilidad del suceso anterior es positiva. Por ello, en tal caso se dice que los sucesos $A_1, \dots, A_n$ no cubren todo el espacio de probabilidad.*
2. *Sea X una variable aleatoria. Entonces, existe $\omega \in \Omega$ tal que $X(\omega) \geq \mathbb{E}[X]$.*

Observación 9. Con la notación del primer apartado de la proposición 8, los sucesos $A_1, \dots, A_n$ corresponderían en la práctica a sucesos «malos» que queremos evitar. Así, la proposición 8 nos asegura bajo esa hipótesis que, con probabilidad positiva, ninguno de los sucesos «malos» ocurre. ◂

Observación 10. En el segundo punto de la proposición 8 también puede garantizarse, por razones análogas, la existencia de un elemento $\omega' \in \Omega$ tal que $X(\omega') \leq \mathbb{E}[X]$. ◂

Es conveniente remarcar sobre la proposición 8 que el segundo resultado implica el primero. Aún así, es preferible separarlos en las aplicaciones, ya que el primero refleja un objetivo que volverá a aparecer cuando tratemos el lema local de Lovász en la sección 6 y que consiste en buscar condiciones suficientes bajo las cuales varios sucesos $A_1, A_2, \dots, A_n$ no cubren todo el espacio de probabilidad ambiente. El lema anterior mejora este punto de la proposición 8 complementándolo con ciertas condiciones de independencia entre los sucesos $A_1, A_2, \dots, A_n$ involucrados.

Por otro lado, el segundo resultado permite deducir información sobre la distribución de una variable aleatoria por medio de su esperanza, un método que emplearemos en la sección 4 y que se complementará en la sección 5 con el estudio de la varianza.

Para comprobar que el segundo enunciado de la proposición 8 implica el primero, basta considerar una variable aleatoria contador X que indique cuántos de los sucesos A_i se cumplen para cada uno de los $\omega \in \Omega$ y aplicar la observación 10. Tomando $X = \sum_{k=1}^{n} X_{A_k}$ se observa, por la proposición 7, que la media de X es $\mathbb{E}[X] = \sum_{k=1}^{n} \mathbb{P}(A_k)$ y que un $\omega \in \Omega$ pertenece a $\bigcap_{k=1}^{n} A_k^c$ si y solo $X(\omega) < 1$.

La distinción que hacemos entre estos dos objetos en la proposición 8, una función de probabilidad y una variable aleatoria, también tiene interés desde el punto de vista de la construcción de un espacio de probabilidad. Siempre que hablamos de una elección estamos introduciendo un tal espacio, y cuando añadimos más información sobre nuestra elección (como, por ejemplo, exigir que las elecciones se realicen de manera uniforme o que sean independientes), lo que estamos haciendo es detallar más la información de la función de probabilidad o de las diferentes variables aleatorias de dicho espacio. Por ahora, no es necesario entender este párrafo, pero conviene tenerlo en cuenta cuando veamos ejemplos más concretos, ya que los espacios de probabilidad involucrados no se harán explícitos en el sentido de la definición 2.

3. Demostraciones de existencia directa

Ya tenemos todos los ingredientes para analizar la primera aplicación del método probabilístico, que consistirá en la construcción de un torneo con unas propiedades determinadas. Hay una infinidad de técnicas que se engloban dentro del método probabilístico y aquí pasaremos a analizar la más sencilla de aplicar, que consiste en explotar de manera directa la proposición 8. Aunque es sorprendente la cantidad de problemas que permite resolver, sigue siendo muy primitiva y tiene muchas limitaciones porque se aplica bajo condiciones muy restrictivas. En ese sentido, mejoraremos la técnica en la sección 6 con el lema local de Lovász introduciendo condiciones de independencia.

Recordamos la noción de grafo (simple) porque será útil a lo largo del artículo.

Definición 11. Un **grafo** es un par de conjuntos $G = (V(G), E(G))$, donde $V(G)$ es el conjunto de vértices y $E(G)$ es el conjunto de aristas, tal que $E(G) \subseteq \{\{v_1, v_2\} : v_1 \neq v_2 \in V(G)\}$. Decimos que G es n-completo si $|V(G)| = n$ y el número de aristas es máximo, es decir, $E(G) = \{\{v_1, v_2\} : v_1 \neq v_2 \in V(G)\}$ y $|E(G)| = \binom{n}{2}$. ◂

Un **torneo** de n jugadores consta, primeramente, de un grafo n-completo G. Naturalmente, identificamos los vértices de G con los jugadores del torneo y cada arista $\{i, j\}$ simboliza el enfrentamiento entre los correspondientes jugadores i y j. Para determinar completamente el torneo, se debe apuntar en cada arista $\{i, j\}$ el ganador de ese enfrentamiento (no se admiten empates). Por tanto, para cada $n \geq 1$, es obvio que hay $2^{\binom{n}{2}}$ torneos posibles con n jugadores.

Definición 12. Un torneo de n jugadores cumple la propiedad S_k si $n > k$ y si, para cada colección L de k jugadores, existe otro jugador fuera de L que ha ganado a todos los jugadores de L. ◂

Según cuenta Erdős [17], Schütte le plantea la pregunta de si, para todo k positivo, existen torneos con la propiedad S_k. Finalmente, Erdős consiguió dar una demostración con respuesta afirmativa en 1963 [18], y dicha prueba involucra simples argumentos de probabilidad que ilustran muy bien la filosofía del método probabilístico. Esencialmente, vamos a comprobar que, para valores lo suficientemente grandes de n, será muy probable que un torneo de n jugadores elegido al azar cumpla la propiedad S_k.

Proposición 13. *Si* $\binom{n}{k}(1-2^{-k})^{n-k} < 1$, *entonces existe un torneo de n jugadores con la propiedad* S_k.

Demostración. Para diseñar un torneo de n jugadores solamente hay que asignar un resultado a cada uno de los $\binom{n}{2}$ enfrentamientos. Vamos a construirlo de forma que cada resultado es elegido uniformemente (probabilidad 1/2 para cada sentido) y de manera independiente. Pasaremos después a demostrar que la probabilidad de que un torneo cumpla la propiedad S_k es positiva. Para que el torneo cumpla la propiedad S_k, tiene que cumplir $\binom{n}{k}$ condiciones, a saber, que para cada grupo de k jugadores exista otro jugador en el torneo que gane a todo este grupo. Vamos ahora a introducir los sucesos malos, en el sentido de la observación 9. Ordenamos de 1 a $\binom{n}{k}$ los grupos de k jugadores y al i-ésimo, denotado por L_i, le asignamos el suceso $A_i = \{$No existe un jugador en el torneo que gane a los k jugadores de $L_i\}$. Vamos a comprobar que existe un torneo de n jugadores con la propiedad S_k o, equivalentemente, que los sucesos A_i no cubren todo el espacio de probabilidad descrito. Esto se hará por medio del primer punto de la proposición 8.

Es sencillo realizar el cálculo de $\mathbb{P}(A_i)$ para cada $1 \leq i \leq \binom{n}{k}$. La probabilidad de que un jugador fijo (y fuera de L_i) no gane a todos los jugadores de L_i es igual a $1-2^{-k}$, ya que a cada jugador le gana de manera independiente y con probabilidad 1/2 (véase la definición 4). Para que el suceso A_i se dé, debe darse la condición anterior para cada uno de los $n-k$ jugadores fuera de L_i. Como tales $n-k$ sucesos son independientes y de probabilidad $1-2^{-k}$, se deduce que $\mathbb{P}(A_i) = (1-2^{-k})^{n-k}$. Así que, por la igualdad anterior y la hipótesis del enunciado,

$$\sum_{i=1}^{\binom{n}{k}} \mathbb{P}(A_i) = \binom{n}{k}\left(1-2^{-k}\right)^{n-k} < 1,$$

de modo que $\mathbb{P}(\bigcap_{i=1}^{\binom{n}{k}} A_i^c) > 0$ por el primer punto de la proposición 8. ∎

Esta proposición resuelve la pregunta de Schütte ya que, para k fijo, basta tomar $n > k$ lo suficientemente grande para aplicar este resultado. La existencia de tal n está garantizada porque $\binom{n}{k}(1-2^{-k})^{n-k} \to 0$ cuando $n \to \infty$. De hecho, teniendo en cuenta este límite y la prueba de esta proposición, notamos que la probabilidad de que un torneo aleatorio de n jugadores tenga la propiedad S_k tiende a 1 según n tiende a infinito.

3.1. Ejercicios

Proponemos algunos ejercicios, extraídos del libro de Alon y Spencer [3], el artículo de Chen [11] y las notas de Loh [25], para invitar al lector a familiarizarse con la técnica basada en la proposición 8 antes de analizar otras más avanzadas. Todas las soluciones están en el apéndice A del final del artículo. Se recuerda primero la definición de grafo bipartito para los ejercicios 1 y 3.

Definición 14. Decimos que un grafo G es **bipartito** si $V(G)$ es la unión de dos conjuntos A y B disjuntos y no vacíos tales que $E(G) \subseteq \{\{a,b\} : a \in A, b \in B\}$. Dado $n \in \mathbb{Z}^+$, denotamos por $\mathcal{K}_{n,n}$ el grafo bipartito con $A = \{a_i : i \in [n]\}$, $B = \{b_j : j \in [n]\}$ y aristas $\{\{a_i, b_j\} : i, j \in [n]\}$. ◂

Ejercicio 1. Todo grafo de m aristas contiene un subgrafo bipartito con al menos $m/2$ aristas. ◂

Ejercicio 2. En la Duma hay 1600 delegados, que han formado 16 000 comités de 80 personas cada uno. Prueba que hay dos comités con, al menos, cuatro delegados en común. ◂

Ejercicio 3. Cualquier subgrafo de $2n$ vértices y $n^2 - n + 1$ aristas del grafo bipartito $\mathcal{K}_{n,n}$ admite una partición de sus vértices en n parejas de manera que haya una arista entre cada pareja de vértices. ◂

Ejercicio 4. Se pide probar la ecuación (4), es decir, que el número de Ramsey $R(k,k)$ (definición 1) cumple que $R(k,k) \geq 2^{k/2}$ si $k \geq 2$. ◂

Ejercicio 5. Si en una cuadrícula rectangular de dimensiones $n \times n$ se colocan los números del 1 al n de manera que cada uno de ellos aparezca n veces en la cuadrícula, entonces existe una fila o una columna con al menos $\sqrt{n}$ números distintos. ◂

4. Combinatoria aditiva

Vamos a pasar a analizar un resultado de teoría combinatoria de números. La combinatoria aditiva es un inmenso campo de investigación y motivar una introducción sobre las cuestiones que abarca es una tarea que se escapa de las intenciones de este artículo; se recomienda el libro de Tao y Vu [39]. Expondremos primero un ejemplo que se debe a Erdős [19] y, después de la demostración, discutiremos brevemente la evolución del problema hasta ahora planteado con diferentes parámetros o en otros contextos.

Definición 15. Un conjunto de enteros se dice **libre de sumas** si no existen tres números en dicho conjunto, digamos x, y, z tales que $x + y = z$. ◂

Teorema 16. *Todo conjunto $A = \{a_1, \dots, a_n\} \subseteq \mathbb{Z}$ de enteros no nulos admite un subconjunto libre de sumas con al menos $n/3$ elementos.*

Antes de exponer la demostración, es conveniente adelantar cómo se va a desarrollar. Se va trabajar en la aritmética modular del anillo $\mathbb{Z}/p\mathbb{Z}$, para cierto primo p. Este anillo también es un cuerpo, de modo que los elementos no nulos tienen inverso multiplicativo.

Notación. Para p primo, $z \in \mathbb{Z}/p\mathbb{Z}$ y $W \subseteq \mathbb{Z}/p\mathbb{Z}$, denotamos por zW el subconjunto $\{zw : w \in W\}$. ◂

Para probar el teorema 16, primero se tomará un primo grande para que todos los enteros sean distintos módulo ese primo. Además, consideraremos un subconjunto B de $[p-1]$ libre de sumas de tamaño mayor que un tercio del total. Esto nos da muchos subconjuntos libres de sumas, los que son de la forma cB con c no nulo, y alguno de ellos deberá tener una intersección grande con A, que será libre de sumas.

Demostración del teorema 16. Conservamos la notación de la discusión inmediatamente anterior. Sea p un primo de la forma $3k+2$, para cierto entero k, tal que todos los elementos de A sean distintos módulo p. Por ejemplo, es suficiente que $p > 2\,\mathrm{máx}_{a\in A}|a|$. Consideremos el anillo $\mathbb{Z}/p\mathbb{Z}$ y el siguiente subconjunto libre de sumas con $k+1 > p/3$ elementos:

$$B = \{k+1, \dots, 2k+1\}.$$

Dado que estamos en un cuerpo, para todo elemento a de A, existen exactamente $k+1$ elementos x del conjunto $[p-1]$ tales que $ax \in B$. Ahora, tomando un elemento c de $[p-1]$ uniformemente al azar, se considera la variable aleatoria $X(c) = |A \cap c^{-1}B|$, que es expresable como la suma de indicadores $\sum_{i=1}^{n} X_{a_i^{-1}B}$ (definición 5). Aplicando la linealidad de la esperanza,

$$\mathbb{E}[X] = \sum_{k=1}^{n} \mathbb{E}[X_{a_k^{-1}B}] = \sum_{k=1}^{n} \mathbb{P}(X_{a_k^{-1}B} = 1) = \sum_{k=1}^{n} \mathbb{P}\left(c \in a_k^{-1}B\right) = \sum_{k=1}^{n} \frac{|a_k^{-1}B|}{p-1} = n\frac{k+1}{p-1} > \frac{n}{3},$$

y queda finalizada la demostración por el segundo punto de la proposición 8, ya que para cierto $c \in [p-1]$ se deberá tener que $A \cap c^{-1}B$ es un subconjunto de A libre de sumas con más de $n/3$ elementos. ∎

No se sabe si el resultado anterior es cierto o no reemplazando $n/3$ por $n/3 + 10$ en el enunciado. Sin embargo, sí que podría reemplazarse por $(n+2)/3$, según prueba Bourgain [9] con técnicas de análisis de Fourier. Por otro lado, sí se sabe que $1/3$ es la mayor fracción que se puede poner en el teorema 16 (véase el artículo de Eberhard, Green y Manners [15]).

Nótese que tanto la definición 15 como el teorema 16 pueden reformularse para un grupo G cualquiera, en lugar de $\mathbb{Z}$. Es natural preguntarse qué familias de grupos y qué fracciones pueden considerarse en el teorema 16 de modo que siga siendo cierto. Es decir, queremos entender las familias de grupos $\mathcal{F}$ para las cuales existe una fracción $c > 0$ de forma que para todo grupo G en $\mathcal{F}$ y todo $A \subseteq G$ de n elementos exista un subconjunto de A con al menos nc elementos que sea libre de productos.

Para esta cuestión, tras mirar cuidadosamente la demostración del teorema 16, puede tomarse $\mathcal{F}_1$ compuesta por $\mathbb{Z}$ y los grupos cíclicos $\mathbb{Z}/q\mathbb{Z}$, para q primo, junto con la constante $c = 1/3$. Además, Alon y Kleitman [2] probaron que puede tomarse la familia $\mathcal{F}_2$ de grupos abelianos y la fracción $c = 2/7$ (menor que $1/3$, pero óptima para esta familia más grande).

Sin embargo, Gowers [23] encuentra una familia $\mathcal{F}_3$ para la cual no puede asegurarse tal fracción $c > 0$ absoluta. En efecto, se comprueba para todo primo q que el grupo lineal proyectivo de $\mathbb{F}_q^2$, denotado por $\mathrm{PSL}_2(\mathbb{F}_q)$ y con orden n_q, no tiene subconjuntos libres de productos con más de $2n_q^{8/9}$ elementos. Nótese que, para cada fracción $c > 0$ fija, la cantidad $2n_q^{8/9}$ es menor que cn_q si q es lo suficientemente grande.

El ingrediente principal en la prueba se debe a un resultado de Frobenius de 1897 por el cual, esencialmente, estos grupos $\mathrm{PSL}_2(\mathbb{F}_q)$ no tienen representaciones no triviales de dimensión baja (véase el libro de Davidoff, Sarnak y Valette [13, teorema 3.5.1]). En este sentido, estos grupos están muy lejos de ser conmutativos porque todas las representaciones irreducibles de un grupo abeliano tienen dimensión 1. La moraleja es que las técnicas probabilísticas y el análisis de Fourier en grupos no conmutativos tienen muy distinta naturaleza al caso abeliano.

Por último, planteamos al lector el siguiente ejercicio extraído del libro de Djukić *et al.* [14, sección 3.40.2].

Ejercicio 6. Sea $N \in \mathbb{Z}^+$. Consideramos el grupo $G = \mathbb{Z}/N^2\mathbb{Z}$ junto con un subconjunto $A \subseteq G$ de N elementos. Comprueba que existe una colección B de N elementos de G de manera que $|A+B| \geq |G|/2$. ◂

5. El método del segundo momento en teoría de números

Hemos hablado de la media o esperanza $\mathbb{E}[X]$ de una variable aleatoria X y de cómo su cálculo nos daba una idea primitiva de cómo puede ser X, al menos en un sentido débil reflejado en el segundo punto de la proposición 8. Dando un paso más en el estudio de una variable aleatoria X, estudiaremos tanto $\mathbb{E}[X]$ como su varianza $\mathrm{Var}(X)$, definida por $\mathrm{Var}(X) = \mathbb{E}[(X - \mathbb{E}[X])^2]$. Una posible inquietud es intentar entender cómo estas dos cantidades delimitan las posibles distribuciones de X. Por ejemplo, si $\mathrm{Var}(X) = 0$, entonces X es constante e igual a $\mathbb{E}[X]$. De manera general, $\mathrm{Var}(X)$ restringe las desviaciones en distribución que pueda tener X con respecto a la constante $\mathbb{E}[X]$, como recoge más cuantitativamente la desigualdad de Chebyshov.

Lema 17 (Desigualdad de Chebyshov). *Sea X una variable aleatoria. Se tiene que, para todo c positivo,*

$$\mathbb{P}\left(|X - \mathbb{E}[X]| \geq c\sqrt{\mathrm{Var}(X)}\right) \leq \frac{1}{c^2}.$$

Insistimos en que la naturaleza de las conclusiones obtenidas con el método empleado en esta sección son diferentes a las del resto del artículo. En el caso de la sección 3, solo podía concluirse que $X \geq \mathbb{E}[X]$ con probabilidad positiva apelando al segundo punto de la proposición 8. Aquí se considerará también la varianza y se podrá inferir que X estará en un intervalo centrado en $\mathbb{E}[X]$ con alta probabilidad, obteniendo no solamente resultados de existencia sino también de concentración.

Un hecho conveniente sobre la esperanza es que es lineal en la suma de variables aleatorias (proposición 7), pero la varianza de una suma equivaldrá a la suma de varianzas salvo un término que mide la dependencia entre dichas variables (lema 18). Dicha medida cuantitativa de la dependencia que puede haber entre dos variables aleatorias X, Y viene dada por su covarianza $\mathrm{Cov}(X, Y)$, definida por $\mathbb{E}\left[(X - \mathbb{E}[X])\,(Y - \mathbb{E}[Y])\right]$. Si X e Y son independientes, entonces $\mathrm{Cov}(X, Y) = 0$, pero el recíproco no es cierto.

Lema 18. *Dadas las variables aleatorias $X_1, \ldots, X_n$, se tiene la siguiente identidad:*

$$\mathrm{Var}\left(\sum_{k=1}^{n} X_k\right) = \sum_{k=1}^{n} \mathrm{Var}(X_k) + 2 \sum_{1 \leq i < j \leq n} \mathrm{Cov}(X_i, X_j).$$

El momento de orden k de una variable aleatoria se define por $\mathbb{E}[X^k]$, y el método de momentos consiste, brevemente, en obtener información sobre la distribución de una variable aleatoria a partir del cálculo o estimación de sus momentos. La desigualdad de Chebyshov es un resultado que va en esa dirección y decimos que en esta sección emplearemos el método del segundo momento para adelantar que estudiaremos una variable aleatoria a través de su media $\mathbb{E}[X]$ y su varianza, que puede calcularse como $\mathrm{Var}(X) = \mathbb{E}[X^2] - \mathbb{E}[X]^2$.

Una de las grandes familias de problemas que aparecen en teoría de números es aquella en la que se pretende estudiar cuestiones relacionadas con los números primos. Hay múltiples enfoques al estudio de estos números; en este caso, entenderemos un poco mejor cuáles son su densidad y distribución. Para ello, vamos a necesitar una estimación de Mertens [27], el teorema 20, sobre series asociadas a los números primos, para la cual hay pruebas más directas combinando la sumación de Abel y la fórmula de Stirling. Antes de ello, introducimos una notación asintótica que se usará especialmente en esta sección pero también en alguna estimación de la sección 6. Podrá verse que es muy cómoda y conveniente.

Definición 19. Sean $f\colon \mathbb{Z}^+ \to \mathbb{R}$ y $g\colon \mathbb{Z}^+ \to (0,\infty)$.

- Escribimos $f = \mathcal{O}(g)$ si existe $C > 0$ tal que $|f(n)| \leq Cg(n)$ para todo $n \in \mathbb{Z}^+$.
- Escribimos $f = o(g)$ si $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0$. ◂

Por ejemplo, $10 - n^2 = \mathcal{O}(n^2)$ y $45/n^2 = o(1/n)$. Se recuerda también que el uso del símbolo de igualdad en la definición 19 es un abuso de notación. Por otro lado, se observa que, si $f_1, f_2\colon \mathbb{Z}^+ \to \mathbb{R}$ y $g\colon \mathbb{Z}^+ \to (0,\infty)$ verifican que $f_1 = \mathcal{O}(g)$ y $f_2 = \mathcal{O}(g)$, entonces para todos los reales c_1, c_2 se tiene que $c_1 f_1 + c_2 f_2 = \mathcal{O}(g)$.

Teorema 20 (Mertens). *La suma de los inversos de los primos menores que un cierto entero n cumple lo siguiente:*

$$\sum_{p\leq n} \frac{1}{p} = \log\log n + \mathcal{O}(1).$$

Sea x un entero positivo. Denotamos por $\nu(x)$ el número de primos que dividen a x. El siguiente resultado fue demostrado por primera vez por Hardy y Ramanujan en 1920, pero la prueba que trataremos, ofrecida por Turán en 1934 [40], es menos compleja y tiene un papel crucial en el posterior desarrollo de estas técnicas probabilísticas en teoría de números. Vagamente, viene a decir que la cantidad de factores primos que se espera de un entero positivo en $[n]$ es $\log\log n$.

Teorema 21. *Sea $\omega\colon \mathbb{Z}^+ \to (0,\infty]$ con $\omega(n) \to \infty$. Entonces, la cantidad de valores de x en $[n]$ tales que $|\nu(x) - \log\log n| \geq \omega(n)\sqrt{\log\log n}$ es $o(n)$.*

Demostración. Queremos estudiar los x de un conjunto $[n]$ que verifican una cierta propiedad. Para estudiar la densidad de tales x en $[n]$, se considera una distribución uniforme en este espacio. Es decir, dado $A \subseteq [n]$, se tiene que $\mathbb{P}(A) = |A|/n$. Para cada n, la función $\nu_n\colon [n] \to \mathbb{R}$ definida por $x \mapsto \nu(x)$ es una variable aleatoria en $[n]$. En términos probabilísticos, lo que se pretende probar es lo siguiente:

$$\mathbb{P}\left(\frac{|\nu_n - \log\log n|}{\sqrt{\log\log n}} \geq \omega(n)\right) = o(1). \tag{5}$$

Vamos a denotar la indicatriz de $\{\text{múltiplos de } m\} \cap [n]$ por $X_{m,n}$. Es decir, dado $x \in [n]$, $X_{m,n}(x) = 1$ si m divide x, y $X_{m,n}(x) = 0$ en otro caso.

Es directo ver que $\nu_n = \sum_{p\leq n} X_{p,n}$, donde la suma se toma sobre primos p. Sin embargo, por razones técnicas, no trabajaremos con esta variable aleatoria. El problema que surge al estudiar la suma de indicatrices $X_{p,n}$ es que su varianza no es lo suficientemente estable en n porque la suma de covarianzas que aparece en el lema 18 para realizar el cálculo de $\mathrm{Var}(\nu_n)$ no es negligible. En su lugar, consideraremos la variable aleatoria $\mu_n = \sum_{p\leq n^{1/10}} X_{p,n}$, la cual tiene el mismo comportamiento asintótico que ν_n por un sencillo argumento de conteo que nos lleva al siguiente control entre ambas.

Lema 22. *Para todo $x \in [n]$, $\nu_n(x) - 10 \leq \mu_n(x) \leq \nu_n(x)$.*

Demostración. La segunda desigualdad es inmediata porque $\nu_n(x)$ cuenta los divisores primos de x pero $\mu_n(x)$ solo aquellos divisores primos de x no mayores que $n^{1/10}$. La primera desigualdad se deduce de que ningún $x \leq n$ pueda tener más de diez divisores primos mayores que $n^{1/10}$. ∎

El siguiente objetivo es estimar $\mathbb{E}[\mu_n]$ y $\mathrm{Var}(\mu_n)$ cuando $n \to \infty$. La función $\log\log n$ emergerá en ambos cálculos haciendo uso del teorema 20.

Lema 23. $\mathbb{E}[\mu_n] = \log\log n + \mathcal{O}(1)$.

Demostración. Recuérdese que $r - 1 < \lfloor r \rfloor \leq r$ para todo $r \in \mathbb{R}$. Se observa que $\mathbb{E}[X_{p,n}] = \lfloor n/p \rfloor / n$, ya que la cantidad de múltiplos de p en $[n]$ es $\lfloor n/p \rfloor$. Luego $1/p - 1/n < \mathbb{E}[X_{p,n}] \leq 1/p$ y, por tanto, $\mathbb{E}[X_{p,n}] = 1/p + \mathcal{O}(1/n)$. Aplicando la linealidad de la esperanza y, en la última igualdad, el teorema 20, concluimos que

$$\mathbb{E}[\mu_n] = \sum_{p \leq n^{1/10}} \left(\frac{1}{p} + \mathcal{O}\left(\frac{1}{n}\right)\right) = \sum_{p \leq n^{1/10}} \frac{1}{p} + n^{1/10} \cdot \mathcal{O}\left(\frac{1}{n}\right) = \log\log n + \mathcal{O}(1). \qquad \blacksquare$$

Lema 24. $\mathrm{Var}(\mu_n) = \log\log n + \mathcal{O}(1)$.

Demostración. Tenemos que $\mathrm{Var}(X_{p,n}) = \mathbb{E}[X_{p,n}^2] - \mathbb{E}[X_{p,n}]^2 = (1 - 1/p)/p + \mathcal{O}(1/n)$. Por tanto,

$$\sum_{p \leq n^{1/10}} \mathrm{Var}(X_{p,n}) = \sum_{p \leq n^{1/10}} \frac{1}{p} - \sum_{p \leq n^{1/10}} \frac{1}{p^2} + n^{1/10} \mathcal{O}\left(\frac{1}{n}\right) = \log\log n + \mathcal{O}(1), \tag{6}$$

donde hemos usado, análogamente al lema anterior, el teorema 20 y el hecho de que tenemos que $\sum_{p \leq n} 1/p^2 \leq \sum_{k=1}^{n} 1/k^2 = \mathcal{O}(1)$, ya que esta es una serie convergente. Sobre el cálculo de las covarianzas, tenemos que

$$\begin{aligned}\mathrm{Cov}(X_{p,n}, X_{q,n}) &= \mathbb{E}[X_{p,n}X_{q,n}] - \mathbb{E}[X_p]\,\mathbb{E}[X_q] = \mathbb{E}[X_{pq,n}] - \mathbb{E}[X_p]\,\mathbb{E}[X_q] \\ &= \frac{1}{pq} + \mathcal{O}\left(\frac{1}{n}\right) - \left(\frac{1}{p} + \mathcal{O}\left(\frac{1}{n}\right)\right)\left(\frac{1}{q} + \mathcal{O}\left(\frac{1}{n}\right)\right) = \left(1 + \frac{1}{p} + \frac{1}{q}\right) \cdot \mathcal{O}\left(\frac{1}{n}\right) = \mathcal{O}\left(\frac{1}{n}\right).\end{aligned}$$

Lo siguiente será probar que $\sum_{p \neq q \leq n^{1/10}} \mathrm{Cov}(X_{p,n}, X_{q,n}) = o(1)$. Efectivamente,

$$\sum_{p \neq q \leq n^{1/10}} \mathrm{Cov}(X_{p,n}, X_{q,n}) = \sum_{p \neq q \leq n^{1/10}} \mathcal{O}\left(\frac{1}{n}\right) = n^{2/10} \cdot \mathcal{O}\left(\frac{1}{n}\right) = o(1). \tag{7}$$

Nótese que es en el cálculo anterior donde precisamente se explota el hecho de que el rango de primos considerado está acotado por $n^{1/10}$ y no solo por n. Así, la dependencia entre las variables aleatorias $X_{p,n}$ es muy pequeña y no altera (asintóticamente) la varianza de μ_n. Por el lema 18 y las estimaciones (6) y (7),

$$\mathrm{Var}(\mu_n) = \sum_{p \leq n^{1/10}} \mathrm{Var}(X_{p,n}) + \sum_{p \neq q \leq n^{1/10}} \mathrm{Cov}(X_{p,n}, X_{q,n}) = \log\log n + \mathcal{O}(1). \qquad \blacksquare$$

Ya tenemos todos los ingredientes para demostrar la ecuación (5). De hecho, vamos a comprobar que existe N_0, que solo depende de la función ω, tal que para todo $n \geq N_0$ se cumple que

$$\mathbb{P}\left(\frac{|\nu_n - \log\log n|}{\sqrt{\log\log n}} \geq \omega(n) \right) \leq \frac{32}{\omega(n)^2}, \tag{8}$$

lo cual finaliza la prueba porque $\omega(n) \to \infty$ cuando $n \to \infty$. Teniendo en cuenta los dos lemas anteriores y que $\omega(n) \to \infty$ cuando $n \to \infty$, se sigue que existe N_0 tal que, para todo $n \geq N_0$, las tres siguientes condiciones se dan:

$$\frac{10}{\sqrt{\log\log n}} \leq \frac{\omega(n)}{2}, \quad \frac{|\mathbb{E}[\mu_n] - \log\log n|}{\sqrt{\log\log n}} \leq \frac{\omega(n)}{4}, \quad \frac{\mathrm{Var}(\mu_n)}{\log\log n} \leq 2.$$

Empleando el lema por el cual $|\nu_n - \mu_n| \leq 10$, se deduce que para todo $n \geq N_0$ se cumple lo siguiente:

$$\begin{aligned}\mathbb{P}\left(\frac{|\nu_n - \log\log n|}{\sqrt{\log\log n}} \geq \omega(n) \right) &\leq \mathbb{P}\left(\frac{10 + |\mu_n - \log\log n|}{\sqrt{\log\log n}} \geq \omega(n) \right) \leq \mathbb{P}\left(\frac{|\mu_n - \log\log n|}{\sqrt{\log\log n}} \geq \frac{\omega(n)}{2} \right) \\ &\leq \mathbb{P}\left(\frac{|\mu_n - \mathbb{E}[\mu_n]| + |\mathbb{E}[\mu_n] - \log\log n|}{\sqrt{\log\log n}} \geq \frac{\omega(n)}{2} \right) \\ &\leq \mathbb{P}\left(\frac{|\mu_n - \mathbb{E}[\mu_n]|}{\sqrt{\log\log n}} \geq \frac{\omega(n)}{4} \right) \leq \mathbb{P}\left(\frac{|\mu_n - \mathbb{E}[\mu_n]|}{\sqrt{\mathrm{Var}(\mu_n)}} \geq \frac{\omega(n)}{4\sqrt{2}} \right).\end{aligned}$$

Finalmente, por el lema 17, la última expresión está acotada por $32/\omega(n)^2$, demostrando así (8). $\blacksquare$

Este teorema admite una extensión que da una descripción más precisa de la distribución de ν, la cual se comporta, en el límite, como una normal de media y varianza iguales a $\log\log n$. Este es un teorema de Erdős y Kac, de 1940 [20].

Teorema 25. *Sea $\lambda \in \mathbb{R}$ fijo. Entonces, se tiene que*

$$\lim_{n\to\infty} \frac{1}{n} \left| \left\{ \nu \geq \log\log n + \lambda\sqrt{\log\log n} \right\} \cap [n] \right| = \int_\lambda^\infty \frac{1}{\sqrt{2\pi}} \mathrm{e}^{-x^2/2}\, \mathrm{d}x.$$

Recordemos que una distribución N es normal (o también conocida como gaussiana) de media μ y varianza σ^2 si y solo si es de la forma $N = \mu + \sigma N_0$, donde N_0 sigue una distribución normal estándar, esto es, de media 0 y varianza 1. Equivalentemente, el primer caso se da si $\frac{N-\mu}{\sigma}$ sigue un distribución normal estándar. La función de densidad de N_0 es $f(x) = \frac{1}{\sqrt{2\pi}} e^{-x^2/2}$, así que $\mathbb{P}(N_0 \geq c) = \int_c^\infty f(x)\,\mathrm{d}x$ para todo $c \in [-\infty, \infty]$. Podemos reescribir el límite del teorema de Erdős y Kac de manera más esclarecedora:

$$\lim_{n\to\infty} \mathbb{P}\left(\frac{\nu_n - \log\log n}{\sqrt{\log\log n}} \geq \lambda \right) = \mathbb{P}(N_0 \geq \lambda), \quad \text{para todo } \lambda \in \mathbb{R},$$

en forma de una convergencia en distribución. El hecho más importante en el tipo de argumentos involucrados en la prueba del teorema 25 es que hay variables aleatorias X, como la gaussiana, que están totalmente determinadas por sus momentos en el siguiente sentido: cualquier variable aleatoria Y con momentos $\mathbb{E}[Y^k] = \mathbb{E}[X^k]$ para todo $k \in \mathbb{N}$ cumple que $\mathbb{P}(X = Y) = 1$. El lector puede dirigirse al libro de Billingsley [5, capítulo 30] para ver condiciones suficientes en las que la situación anterior se da, esencialmente cuando la sucesión de momentos crece lo suficientemente despacio para que la función $M_X(t) = \mathbb{E}[\mathrm{e}^{\mathrm{i}XT}]$ pueda estudiarse como la función generatriz que contiene como coeficientes de su desarrollo en serie de potencias a la sucesión $\{\mathbb{E}[X^k]/k!\}_{k\geq 0}$. La importancia de la función $M_X(t)$ radica en que, dadas las variables aleatorias X_n e Y, la convergencia de X_n a Y en distribución puede reducirse a comprobar la convergencia puntual de las funciones $M_{X_n}(t)$ a $M_Y(t)$, lo cual también puede reducirse a probar, para cada $k \geq 1$, la convergencia de $\mathbb{E}[X_n^k]$ a $\mathbb{E}[Y^k]$, una tarea mucho más sencilla. Al igual que en esta sección hemos aplicado el *método del segundo momento*, la sección 3 podría llamarse *método del primer momento* y en la demostración del teorema 25 se aplica el *método de momentos* descrito con más detalle en el libro de Billingsley [5, teorema 30.3]. Otra idea importante en esta demostración, que ya aparece en el teorema 21 y que es muy común en probabilidad, es el método de truncamiento. En ocasiones, una variable aleatoria en su totalidad oscila demasiado, como ocurre con la varianza de ν_n, y por ello es mejor aproximarla, considerando μ_n. Para estimar los momentos de orden $n \geq 3$ de ν_n y probar el teorema 25 se emplean las mismas técnicas que en la prueba del teorema 21, pero el truncamiento sí que resulta ser más sutil y se basa en el teorema 20.

Aprovechando que a esta alturas hemos descrito pruebas probabilísticas de distinta naturaleza, queremos indicar que, entendiendo el método probabilístico en este sentido amplio que se considera en la introducción, la primera aplicación de este método se le atribuye a Emil Borel [8], uno de los padres fundadores de la teoría de la medida y la probabilidad. En el artículo anterior se prueba que casi todos los números reales son normales.

6. Lema local de Lovász

Una de las debilidades del argumento empleado en la proposición 13 es que requiere condiciones muy fuertes para ser aplicado y, en el sentido de la observación 9, las probabilidades de los sucesos malos deben ser muy pequeñas para que se pueda proceder con esta técnica. En efecto, la conclusión del resultado no es solo que exista algún torneo con la propiedad S_k, sino que casi todos la verifican cuando el número de vértices es muy grande. Esto sugiere investigar nuevas formas de asegurar que ciertos sucesos malos no cubran un espacio de probabilidad.

Por otro lado, hay otro fenómeno muy usual en problemas de combinatoria de interés como las coloraciones: la independencia de sucesos. Obsérvese, por la definición 4, que si d sucesos malos tienen probabilidad a lo sumo $p < 1$ y son independientes, entonces, con probabilidad al menos $(1-p)^d > 0$, ninguno de ellos ocurre. Así que ya conocemos dos condiciones extremas bajo las cuales una colección finita de sucesos no cubre un espacio de probabilidad: o bien no lo cubren individualmente y son independientes o bien sus probabilidades son muy pequeñas en el sentido del primer punto de la proposición 8. Ambos casos son demasiado favorables. El lema local de Lovász permite cuantificar y explotar casos intermedios.

Antes de enunciar este lema necesitamos introducir una nueva noción de independencia en la definición 26 diferente de la que aparece en la definición 4, para la cual usaremos la siguiente notación.

Notación. La probabilidad $\mathbb{P}(A \mid B)$ de un suceso A condicionado al suceso B viene dada por $\mathbb{P}(A \cap B)/\mathbb{P}(B)$ y está definida solo cuando $\mathbb{P}(B) > 0$. Nótese que A y B son independientes si y solo $\mathbb{P}(A \mid B) = \mathbb{P}(A)$. Es por esto que la notación de probabilidad condicionada es más cómoda y contiene más significado. Así que escribiremos identidades del estilo de $\mathbb{P}(A \mid B) \geq c_1$ o $\mathbb{P}(A \mid B) = c_2$, que son simplemente una abreviación para $\mathbb{P}(A \cap B) \geq c_1 \mathbb{P}(B)$ y $\mathbb{P}(A \cap B) = c_2 \mathbb{P}(B)$, respectivamente. En el caso degenerado de que $\mathbb{P}(B) = 0$, se tiene que $\mathbb{P}(A \cap B) = 0$ también y ambas desigualdades son trivialmente ciertas. ◂

Definición 26. Decimos que un suceso S es independiente de una colección $\{S_k\}_{k=1}^n$ de sucesos si para todo $I \subseteq [n]$ se tiene que $\mathbb{P}(S \mid \bigcap_{k \in I} S_k) = \mathbb{P}(S)$. ◂

Definición 27. Dados $A_1, \dots, A_n$ sucesos en un espacio de probabilidad, su **grafo de dependencia** es un grafo G (definición 11) cuyo conjunto de vértices es $\{1, \dots, n\}$ (que debemos pensar como $\{A_1, \dots, A_n\}$) y cuyas aristas indican la posible dependencia entre los correspondientes sucesos. De manera precisa, A_k es independiente de la colección $\{A_i\}_{\{k,i\} \notin E(G)}$ para todo $k \in [n]$. ◂

Observación 28. Se remarca que la condición anterior, que A_k sea independiente de la colección $\{A_i\}_{\{k,i\} \notin E(G)}$, es mucho más débil que la de imponer que los sucesos de la colección $\bigcup_{\{k,i\} \notin E(G)} \{A_i\} \cup \{A_k\}$ sean independientes, recuérdese la definición 4. ◂

Observación 29. También se verifica que S es independiente de $\{S_k, S_k^c\}_{k=1}^n$ si lo es de $\{S_k\}_{k=1}^n$. ◂

El siguiente resultado apareció en un artículo de Erdős y Lovász en 1975 [21] y a modo de motivación adelantamos que nos llevará directamente al lema 31, que cuantifica esta intuición: si una colección de sucesos malos tiene probabilidad positiva de no ocurrir y cada uno de ellos tiene una probabilidad pequeña en comparación con el número de sucesos de los que depende, entonces, con probabilidad positiva, ninguno de ellos sucede.

Lema 30 (Versión general del lema local de Lovász). *Sean $A_1, \dots, A_n$ sucesos en un espacio de probabilidad $(\Omega, \mathbb{P})$ con grafo de dependencia G. Supongamos que existen números reales $\{x_i\}_{i=1}^n \subseteq [0,1)$ tales que*

$$\mathbb{P}(A_i) \leq x_i \prod_{\{i,j\} \in E(G)} (1 - x_j), \quad \text{para todo } i \in [n].$$

Entonces, se tiene que

$$\mathbb{P}\left(\bigcap_{i=1}^n A_i^c\right) \geq \prod_{i=1}^n (1 - x_i) > 0.$$

Demostración. Vamos a asumir ahora el siguiente enunciado que probaremos más tarde:

$$\mathbb{P}\left(A_i^c \,\middle|\, \bigcap_{j \in J} A_j^c\right) \geq 1 - x_i, \ \forall J \subseteq [n], \forall i \notin J. \tag{9}$$

De esta forma, es fácil terminar la prueba del lema:

$$\mathbb{P}\left(\bigcap_{k=1}^n A_k^c\right) = \mathbb{P}(A_1^c)\,\mathbb{P}(A_2^c \mid A_1^c)\,\mathbb{P}(A_3^c \mid A_1^c \cap A_2^c) \cdots \mathbb{P}\left(A_n^c \,\middle|\, \bigcap_{j=1}^{n-1} A_j^c\right) \geq (1-x_1)(1-x_2)(1-x_3)\cdots(1-x_n).$$

Procederemos por inducción en $|J|$ para demostrar el siguiente enunciado equivalente a (9):

$$\mathbb{P}\left(A_i \,\middle|\, \bigcap_{j\in J} A_j^c\right) \leq x_i, \ \forall J \subseteq [n], \forall\, i \notin J. \tag{10}$$

El caso base es $|J| = 0$. Se recuerda que la intersección vacía de subconjuntos es el conjunto total. Así,

$$\mathbb{P}\left(A_i \,\middle|\, \bigcap_{j\in J} A_j^c\right) = \mathbb{P}(A_i) \leq x_i \prod_{\{i,j\}\in E(G)} (1 - x_j) \leq x_i \quad \forall\, i \in [n].$$

Para el paso inductivo, vamos a asumir que la propiedad se verifica para todo subconjunto J con $|J| < m$ (hipótesis de inducción fuerte) y vamos a comprobarlo para cualquier subconjunto $J \subseteq [n]$ de tamaño $|J| = m$. Dado $i \notin J$, definimos $J_{i,1} = \{j \in J : \{i, j\} \in E(G)\} = \{u_1, \ldots, u_b\}$, con b elementos, y $J_{i,2} = J - J_{i,1}$, con $m - b$ elementos. También definimos $B_i = \bigcap_{j\in J_{i,1}} A_j^c$ y $C_i = \bigcap_{j\in J_{i,2}} A_j^c$. Reordenando,

$$\mathbb{P}(A_i \mid B_i \cap C_i) = \frac{\mathbb{P}(A_i \cap B_i \cap C_i)}{\mathbb{P}(B_i \cap C_i)} = \frac{\mathbb{P}(A_i \cap B_i \cap C_i)}{\mathbb{P}(C_i)} \frac{\mathbb{P}(C_i)}{\mathbb{P}(B_i \cap C_i)} = \frac{\mathbb{P}(A_i \cap B_i \mid C_i)}{\mathbb{P}(B_i \mid C_i)}. \tag{11}$$

Teniendo en cuenta que A_i es independiente de C_i, por la observación 29 después de la definición 26,

$$\mathbb{P}(A_i \cap B_i \mid C_i) = \frac{\mathbb{P}(A_i \cap B_i \cap C_i)\mathbb{P}(A_i)}{\mathbb{P}(A_i \cap C_i)} \leq \mathbb{P}(A_i) \leq x_i \prod_{\{i,j\}\in E(G)} (1 - x_j), \tag{12}$$

lo cual nos da esta cota superior para el numerador de (11). Ahora pasamos a analizar el denominador,

$$\mathbb{P}(B_i \mid C_i) = \mathbb{P}(A_{u_1}^c \cap A_{u_2}^c \cap \cdots \cap A_{u_b}^c \mid C_i) = \prod_{k=1}^{b} \mathbb{P}\left(A_{u_k}^c \mid C_i \cap A_{u_1}^c \cap \cdots \cap A_{u_{k-1}}^c\right). \tag{13}$$

Teniendo en cuenta que cada uno de los conjuntos $C_i \cap A_{u_1}^c \cap \cdots \cap A_{u_{k-1}}^c$, con $k \in [b]$, es intersección de $(m - b) + k - 1 < m$ conjuntos de la colección inicial $\{A_i\}_{i=1}^n$, podemos aplicar la hipótesis de inducción a cada factor del lado derecho de (13) y la observación de que $\{u_1, \ldots, u_b\} \subseteq \{j : \{i, j\} \in E(G)\}$ para deducir que

$$\mathbb{P}(B_i \mid C_i) = \prod_{k=1}^{b} \mathbb{P}\left(A_{u_k}^c \mid C \cap A_{u_1}^c \cap \cdots \cap A_{u_{k-1}}^c\right) \geq \prod_{k=1}^{b} (1 - x_{u_k}) \geq \prod_{\{i,j\}\in E(G)} (1 - x_j). \tag{14}$$

Finalmente, se observa que (11), (12) y (14) implican que $\mathbb{P}(A_i \mid B_i \cap C_i) \leq x_i$, es decir, (10). ∎

Es necesario plantearse por qué llamamos «lema local» a este resultado. Siguiendo la discusión anterior, es valioso entender el problema general de garantizar que una colección de sucesos en un espacio de probabilidad no cubra todo el espacio. Con la ayuda de este lema no tendríamos que comprobar una condición que involucre a todos los sucesos A_i para concluir que $\mathbb{P}(\bigcap_{k=1}^n A_k^c) > 0$, sino que la condición en cada uno de los A_i es local porque solamente aparecen involucrados aquellos sucesos que puedan depender de A_i. El lema 30 tiene su propio interés pero, a primera vista, parece difícil de usar porque involucra muchos pesos x_i y muchas condiciones a comprobar. Una versión más homogénea y manejable del lema local de Lovász, que será suficiente para las aplicaciones que veremos, es la siguiente.

Lema 31 (Versión simétrica del lema local de Lovász). *Sean $A_1, \ldots, A_n$ sucesos en un espacio de probabilidad $(\Omega, \mathbb{P})$ con grafo de dependencia G. Supongamos que cada vértice de G es extremo de a lo sumo d aristas y que, además, para algún $p \in [0, 1]$ se cumple que $\mathbb{P}(A_k) \leq p$ para todo $k \in [n]$. Si, además, se tiene que $\mathrm{e}p(d + 1) \leq 1$, entonces*

$$\mathbb{P}\left(\bigcap_{k=1}^{n} A_k^c\right) > 0.$$

Por simplicidad, dejamos enunciado el siguiente lema sencillo.

Lema 32. *Sea n un entero distinto de 0 y -1. Entonces, $\left(1 + \frac{1}{n}\right)^n \leq \mathrm{e}$ si y solo si $n > 0$.*

Demostración del lema 31. Es consecuencia de la versión general. Consideramos los pesos $x_i = \frac{1}{d+1}$. De esta forma se comprueba que, para todo $i \in [n]$:

$$x_i \prod_{\{i,j\}\in E(G)} (1 - x_j) = \frac{1}{d+1}\left(\frac{d}{d+1}\right)^d \geq \frac{1}{d+1}\frac{1}{\mathrm{e}} \geq p \geq \mathbb{P}(A_i),$$

donde hemos aplicado el lema 32 con $n = d + 1 > 0$. Por tanto, el resultado se sigue directamente del lema 30. ∎

Como curiosidad, la constante e que aparece en el lema 31 no es arbitraria, y Shearer [34] demostró que es la mejor que puede considerarse, es decir, la más pequeña para que siga siendo cierto el teorema. Conviene analizar ahora una aplicación estándar de este lema antes de proponer algunos ejercicios.

Definición 33. Un hipergrafo H es un par (V, E), donde V y E son conjuntos tales que $E \subseteq \mathcal{P}(V)$. Llamamos a los elementos de V vértices, y a los elementos de E hiperaristas (o simplemente aristas). Decimos que H es finito si V es finito. Decimos que dos aristas $e, e' \in E$ del hipergrafo se cortan si comparten algún vértice, es decir, si $e \cap e' \neq \emptyset$. Una coloración del hipergrafo (V, E) con k colores es una función $c : V \to \{1, \dots, k\}$. Decimos que un hipergrafo es 2-coloreable si admite una coloración con dos colores que no contenga ninguna arista monocromática. ◂

Teorema 34. *Sea (V, E) un hipergrafo finito que verifica las dos siguientes propiedades:*

1. *Toda arista $e \in E$ tiene al menos k vértices.*
2. *Cada arista $e \in E$ interseca a lo sumo a otras d aristas.*

Si se cumple que $\mathrm{e}(d + 1) \leq 2^{k-1}$, entonces el hipergrafo (V, E) es 2-coloreable.

Demostración. Coloreamos al azar cada vértice con probabilidad 1/2 y de manera independiente. Se considera, para cada arista a, el suceso $S_a = \{\text{La arista } a \text{ es monocromática}\}$. Claramente, si la arista a tiene c_a vértices, entonces $\mathbb{P}(S_a) = 2/2^{c_a} \leq 1/2^{k-1}$ porque $c_a \geq k$. Además, S_a es independiente de la colección de sucesos $\{S_b : b \in E, a \cap b = \emptyset\}$, así que S_a es independiente de una colección de sucesos que contiene a todos los de S quitando aquellos a los que interseca, a lo sumo d. Como $\mathrm{e}(d + 1)/2^{k-1} \leq 1$, se sigue por el lema 31 que $\bigcap_{a\in E} S_a^c \neq \emptyset$ y que, por tanto, existe tal coloración. ∎

Una observación importante es que la desigualdad $\mathrm{e}(d + 1) \leq 2^{k-1}$ del teorema 34 no depende del tamaño de V sino del parámetro local d. Si quisiéramos demostrar el teorema 34 con un argumento de existencia directa al estilo de la sección 3, entonces no habría una manera obvia de aprovechar la segunda condición del enunciado de este teorema. Si empleáramos solo la primera condición y buscáramos aplicar la primera parte de la proposición 8 a lo bruto, necesitaríamos que se cumpliera que $|E(V)| < 2^{k-1}$. Esta desigualdad será, generalmente, mucho más fuerte que la anterior.

Para exhibir esta diferencia en un ejemplo concreto, tomamos dos enteros positivos $k \leq n$ y consideramos el hipergrafo de vértices $V = \mathbb{Z}/n\mathbb{Z}$ y aristas $\{i, i + 1, \dots, i + k - 1\}_{i\in[n]}$ (se recuerda que estos enteros se suman módulo n). Para probar que este hipergrafo es 2-coloreable con un argumento de existencia directa necesitamos $n < 2^{k-1}$ y, en particular, $k > \log_2(n)$, lo cual deja muchos casos sin cubrir. Para aplicar el lema local de Lovász, notando que podemos tomar $d + 1 = 2k$, basta con tener $2\mathrm{e}k \leq 2^{k-1}$, lo cual se cumplirá siempre que $k \geq 7$. Esta desigualdad no involucra a n y, además, prueba la 2-coloración de prácticamente toda la familia de hipergrafos descrita, con parámetros $k \leq n$.

Queremos resaltar que el hipergrafo del párrafo anterior es 2-coloreable si $k \geq 3$ o si n es par y $k = 2$ (coloreando de manera alternada los vértices). Pero esta observación depende de la propia estructura global del grafo y lo que se pretende con estos argumentos probabilísticos es probar que sea inevitable la presencia de cierta estructura (ser 2-coloreable) recurriendo únicamente a ciertas condiciones débiles del grafo que aún den mucha libertad para su posible aspecto (como ocurre con las dos condiciones impuestas en el teorema 34).

En el ejemplo anterior es evidente la potencia del lema local de Lovász. La razón por la que funciona mucho mejor que la proposición 8 es que las dependencias entre los correspondientes sucesos malos eran poco comunes (por ejemplo, $1 + d = 2k$ no dependía del tamaño n del grafo). Sin embargo, en la solución

del ejercicio 4, donde se prueba que $R(k,k) \geq 2^{k/2}$ si $k \geq 2$, sí se trabaja con sucesos malos que presentan mucha dependencia mutua. Al final de la solución se comenta que, con el mismo método, el dado por la proposición 8, y solo usando mejores estimaciones de los coeficientes binomiales (por ejemplo, por medio de la fórmula de Stirling), se obtiene que

$$R(k,k) \geq \frac{k \cdot 2^{k/2}}{\sqrt{2}\,\mathrm{e}}(1+o(1)).$$

Lo interesante es que, con el lema local de Lovász (véase el libro de Alon y Spencer [3, teorema 5.3.1], junto con los comentarios posteriores), se llega a que

$$R(k,k) \geq \frac{\sqrt{2}\cdot k \cdot 2^{k/2}}{\mathrm{e}}(1+o(1)),$$

que solo mejora en un factor 2 porque el alto número de dependencias entre los sucesos malos no puede producir una mejora significativa con respecto al método directo. Esta última cota inferior, descubierta por Spencer [36], es la mejor que se conoce hasta el momento.

Planteamos dos ejercicios, extraídos de [33] y Wikipedia [42], para invitar al lector a emplear el lema 31 antes de exponer una última aplicación más elaborada. Las soluciones pueden encontrarse en el apéndice A.

Ejercicio 7. Sean k y n enteros positivos tales que $k \geq 3\sqrt{n}$. Entonces, es posible pintar las aristas del grafo completo $\mathcal{K}_n$ con k colores de manera que no haya ningún triángulo monocromático. ◂

Ejercicio 8. Se consideran $11n$ puntos sobre una circunferencia y se pintan con n colores de forma que haya 11 puntos de cada color. Se pide probar que pueden elegirse n puntos de distinto color y mutuamente no consecutivos en la circunferencia. ◂

Vamos a pasar ahora a analizar un resultado del cual no se conoce ninguna demostración que no involucre consideraciones probabilísticas. Un aspecto interesante añadido a la demostración del siguiente resultado es que emplea el lema local de Lovász para resolver la versión finita del problema y dota al espacio de configuraciones de una topología, según la cual es compacto, para concluir con la versión global.

Teorema 35. *Sean m, k dos enteros positivos tales que*

$$\mathrm{e}\,(m(m-1)+1)\,k\left(1-\frac{1}{k}\right)^m \leq 1. \tag{15}$$

Entonces, para cualquier conjunto de m reales $W = \{x_1, \ldots, x_m\}$, existe una coloración $c : \mathbb{R} \to [k]$ tal que toda traslación $x + W$, con $x \in \mathbb{R}$, contiene los k colores.

Miremos detenidamente el enunciado anterior. Lo sorprendente es que, fijado el número de colores k, siempre podemos tomar m lo suficientemente grande para que se cumpla la conclusión del teorema. Este resultado es el teorema 5.2.2 del libro de Alon y Spencer [3] y, tal y como se observa después en este libro, puede tomarse $m \geq (3+o(1))k\log k$ para asegurar que se cumple la ecuación (15).

Demostración del teorema 35. Observamos que aparecen términos similares a los del teorema 34. Fijemos el conjunto W. Hay que encontrar una coloración del hipergrafo $H = (\mathbb{R}, E)$, donde $E = \{x + W : x \in \mathbb{R}\}$, de manera que cada arista verifique una propiedad. Dicha propiedad no será, como en el teorema 34, no ser monocromática, sino contener todos los k colores. Lo común con la prueba del teorema 34 es que las coloraciones aleatorias las haremos uniformemente al azar y que en este caso también es fácil tener un control de la correspondiente condición local de dependencia.

Fijada una arista $u \in E$, hay a lo sumo otras $m(m-1)$ aristas que intersecan a u. Vamos a probar esto último. Fijamos $y_1 \in \mathbb{R}$. Para que las dos aristas distintas $y_1 + W, y_2 + W$ ($y_2 \in \mathbb{R}$) se corten, deben existir dos elementos $x_i, x_j \in W$ tales que $y_1 + x_i = y_2 + x_j$. Es decir, $y_2 = x_i + y_1 - x_j$ y hay a lo sumo $m(m-1)$ tales y_2, porque hay como mucho uno por cada par ordenado (x_i, x_j) de $W \times W$ con $x_i \neq x_j$. Con el objetivo de aplicar el lema 31, tomamos $d = (m-1)m$.

Ahora introducimos los sucesos malos. Para cada arista $f \in E$ se define $S_f = \{f \text{ no contiene los } k \text{ colores}\}$. Por la proposición 7, la probabilidad de cada suceso S_f admite la siguiente cota sencilla:

$$S_f = \bigcup_{i=1}^{k} \{f \text{ no contiene el color } i\} \implies \mathbb{P}(S_f) \leq \sum_{i=1}^{k} \mathbb{P}\left(f \text{ no contiene el color } i\right) = k\left(1 - \frac{1}{k}\right)^m.$$

Así que, nuevamente con la mirada en el lema 31, definimos $p = k(1-1/k)^m$. Como se cumple que $ep(d+1) \leq 1$, todo apunta a que el teorema 35 sea una aplicación del lema local de Lovász análoga al teorema 34, pero hay una gran diferencia que quizá el lector atento haya notado, y es que el hipergrafo que estamos considerando no es finito, ni tampoco la cantidad de sucesos malos. Recordamos que el resultado 31 es cierto cuando se considera una cantidad finita de sucesos, así que no podemos aplicarlo directamente como antes.

Sin embargo, no está todo perdido porque podemos aproximar el teorema 35 por sus versiones finitas. En lugar de considerar todas las traslaciones de W, tomaremos un subconjunto $A \subseteq \mathbb{R}$ finito y probaremos que existe una coloración de $\mathbb{R}$ de tal manera que todas las traslaciones de W por elementos de A contengan los k colores. Ahora, el hipergrafo H_A tiene aristas $E_A = \{x + W : x \in A\}$, vértices $V_A = \bigcup_{x \in A}(x + W)$ y sucesos malos $\{S_f : f \in E_A\}$. Con la notación del lema 31 y por lo comentado anteriormente, podemos tomar $d = (m-1)m$ y $p = k(1-1/k)^m$, ya que en este nuevo subgrafo finito de H nos encontramos en unas condiciones locales más débiles y cada S_f sigue teniendo la misma probabilidad. Por tanto, ahora sí podemos concluir con la existencia de tal coloración porque la ecuación (15) equivale a la desigualdad dada en el teorema 34.

El espacio de posibles coloraciones de H es $[k]^{\mathbb{R}}$, que corresponde a un producto cartesiano $\prod_{i \in I} Q_i$ de conjuntos idénticos $Q_i = [k]$ con $I = \mathbb{R}$ como conjunto de índices. Para cada $A \subseteq \mathbb{R}$, llamaremos $C_A \subseteq [k]^{\mathbb{R}}$ al conjunto de coloraciones de $\mathbb{R}$ para las cuales todas las traslaciones $a + W$, con $a \in A$, contienen a todos los colores. Hemos demostrado que C_A es no vacío si A es finito, porque basta considerar la coloración de los vértices de H_A dada por el argumento existencial anterior y, después, se puede pintar el resto de $\mathbb{R}$ de cualquier forma. Esto se debe a que los vértices de H_A son exactamente los reales que aparecen en las traslaciones de W por elementos de A.

En definitiva, hemos comprobado que C_A es no vacío para todo $A \subseteq \mathbb{R}$ finito y queremos probar que $C_{\mathbb{R}}$ es no vacío. Para pasar del caso finito al de todo $\mathbb{R}$, recurriremos a un argumento topológico que consiste en entender mejor el espacio $[k]^{\mathbb{R}}$ y los subconjuntos C_A. Con ese objetivo vamos a introducir, sin demostración, un lema básico y un teorema de topología.

Lema 36. *Sea K un espacio topológico compacto. Sea $\{U_i\}_{i \in I}$ una colección de cerrados de K con todas las intersecciones finitas no vacías, es decir, para todo $n \in \mathbb{Z}^+$ y cualesquiera $i_1, \ldots, i_n \in I$, tenemos que $\bigcap_{k=1}^{n} U_{i_k} \neq \emptyset$. Entonces, $\bigcap_{i \in I} U_i \neq \emptyset$.*

Este lema procede reformular la definición usual de espacio compacto tomando el paso al complementario en todos los conjuntos involucrados. De esta forma, reemplazamos abiertos y uniones por cerrados e intersecciones, respectivamente. El siguiente resultado es conocido como el teorema de Tychonoff y es equivalente al axioma de la elección.

Teorema 37. *El producto de una colección arbitraria de espacios topológicos compactos, dotado de la topología producto, es compacto.*

Como consecuencia de este teorema, tenemos que el espacio de coloraciones $[k]^{\mathbb{R}}$ con la topología producto es compacto si consideramos cada espacio $[k]$ equipado de la topología discreta. Además, con esta topología, los conjuntos $C_{\{a\}}$, con $a \in \mathbb{R}$, son cerrados y cumplen las condiciones del lema anterior, ya que cada intersección finita es igual a $C_A \neq \emptyset$ para cierto $A \subseteq \mathbb{R}$ finito. Por tanto, por la compacidad del espacio $[k]^{\mathbb{R}}$, se deduce que $C_{\mathbb{R}} = \bigcap_{a \in \mathbb{R}} C_{\{a\}} \neq \emptyset$, como queríamos. ∎

El argumento topológico empleado al final de la demostración es bastante común en matemáticas, es un argumento de compacidad por el cual podemos tratar a los compactos como conjuntos finitos. La siguiente cita de René Thom, de su libro *Stabilité Structurelle et Morphogenèse*, hace referencia a esta idea: «La topologie est précisément la discipline mathématique qui permet le passage du local au global».

Además de las fuentes de problemas ya mencionadas, muchas más aplicaciones del método probabilístico pueden encontrarse en el libro de Alon y Spencer [3]. Más en particular, se recomienda la colección de problemas de existencia directa de Boppana [7] y el libro de Molloy y Reed [28], con aplicaciones del lema local de Lovász en cuestiones de coloraciones de grafos.

Nótese que las aplicaciones del lema 31 que hemos tratado contienen como conclusión la existencia de un cierto objeto pero, en la práctica, no permiten saber cómo poder encontrarlo de manera eficiente. Esto se debe a que la prueba del lema 30 involucra argumentos puramente probabilísticos. Por ejemplo, en el teorema 35 se prueba la existencia de una coloración pero no aparece ninguna pista sobre cómo podría ser un algoritmo para hallarla explícitamente en un caso concreto. Es cierto que, aún así, estas demostraciones probabilísticas pueden dar, cuando las probabilidades involucradas son lo suficientemente buenas, un algoritmo aleatorio con el objetivo anterior y que puede simplemente consistir en sortear configuraciones con alguna distribución adecuada varias veces y comprobar si alguna cumple lo deseado.

La línea de investigación que plantea este punto de vista algorítmico comenzó en 1991, cuando Beck [4] probó una versión constructiva del lema local de Lovász con condiciones más restrictivas. Posteriormente, Moser [29] dio una demostración constructiva del lema 30 en 2009, que sería mejorada en 2010 por Moser y Tardos [30] para cubrir casi todos los casos que la versión no constructiva del lema resuelve. Puede consultarse en el blog de Tao [38] una breve discusión del argumento de compresión de entropía utilizado en estos dos últimos trabajos aplicado al *Problema de satisfacibilidad booleana* [43], la versión algorítmica de un problema de lógica sintáctica que consiste en encontrar, dadas varias fórmulas de una cierta forma, una asignación de valores de verdad a sus variables proposicionales para que todas las fórmulas se satisfagan.

Para finalizar, resumimos brevemente lo que se conoce sobre la versión algorítmica de otro de los resutados de naturaleza existencial que hemos tratado sobre estimaciones de los números diagonales de Ramsey. En el ejercicio 4 se planteó probar que $R(k,k) \geq 2^{k/2}$ si $k \geq 2$. Antes de explicar el problema algorítmico que plantea esta desigualdad, vamos a cambiar un poco su formulación. Decimos que un grafo es m-Ramsey si no tiene ningún subgrafo completo de m vértices ni tampoco un subgrafo de m vértices sin aristas. Así que $R(k,k)-1$ sería el máximo entero n para el cual existe un grafo k-Ramsey de n vértices. Con esta formulación, la desigualdad anterior refleja el hecho de que, para cada $n \geq 2$, existe un grafo de n vértices que es $2\log n$-Ramsey. Como se remarca en la introducción, la prueba original de Erdős en 1947 [16] (descrita en la solución del ejercicio 4 en el apéndice A) no produce explícitamente tal grafo, aunque es necesario aclarar dicha noción de explicitud porque no es evidente y, de hecho, ha ido evolucionando.

El propio Erdős ofreció cien dólares (desde su muerte, Graham mantiene esta oferta) a quien pudiera dar, para cierta constante C, ejemplos de grafos $C\log n$-Ramsey de n vértices para un n general. Por entonces, lo noción de explicitud era diferente y, tras la era computacional, se relajó considerablemente hasta llegar a la siguiente interpretación. De manera imprecisa, decimos que un grafo G de n vértices es dado de forma explícita si para dos vértices u y v cualesquiera de G se puede determinar eficientemente si existe una arista entre u y v. Dicha eficiencia significa, cuantitativamente, que existe un algoritmo que pueda realizar la correspondiente tarea en una cantidad de tiempo que sea polinomial en $\log n$, ya que $\log n$ es aproximadamente el número de bits necesarios para codificar cada vértice de G.

Con este planteamiento, ha habido bastante progreso en los últimos años y los mejores resultados actualmente se deben a Chattopadhyay y Zuckerman [10] y Cohen [12]. En ambos se dan explícitamente grafos $2^{(\log\log n)^c}$-Ramsey de n vértices, para una constante c absoluta. Con la intención de comparar la cota de este resultado con la propuesta por Erdős, observamos que, para $c=1$, un grafo $C\cdot 2^{(\log\log n)^c}$-Ramsey es también $C\log n$-Ramsey, pero el c que se asegura en los artículos anteriores no es tan pequeño, así que aún nadie ha podido llevarse los cien dólares.

El desarrollo de esta cuestión a lo largo de los años también exhibe el poder de la aleatoriedad. Con un breve argumento probabilístico quedó resuelta esta cuestión sobre los números de Ramsey a nivel existencial. Sin embargo, en su versión constructiva, incluso con una noción de explicitud relajada a nivel computacional, constituye aún un problema abierto.

Referencias

[1] Alon, Noga. «Paul Erdős and the Probabilistic Method». En: *Notices of the American Mathematical Society* 62.3 (2015), págs. 226-230. issn: 0002-9920. https://doi.org/10.1090/noti1223.

[2] Alon, Noga y Kleitman, Daniel J. «Sum-free subsets». En: *A tribute to Paul Erdős*. Ed. por Baker, Alan; Bollobás, Béla, y Hajnal, András. Cambridge: Cambridge University Press, 1990, págs. 13-26. https://doi.org/10.1017/CBO9780511983917.003.

[3] Alon, Noga y Spencer, Joel H. *The probabilistic method*. With an appendix on the life and work of Paul Erdős. 2.ª ed. Wiley-Interscience Series in Discrete Mathematics and Optimization. Nueva York: Wiley-Interscience, 2000. https://doi.org/10.1002/0471722154.

[4] Beck, József. «An algorithmic approach to the Lovász local lemma. I». En: *Random Structures & Algorithms* 2.4 (1991), págs. 343-365. issn: 1042-9832. https://doi.org/10.1002/rsa.3240020402.

[5] Billingsley, Patrick. *Probability and measure*. 3.ª ed. Wiley Series in Probability and Mathematical Statistics. Nueva York: Wiley-Interscience, 1995. isbn: 978-0-471-00710-4.

[6] Bollobás, Béla. *Graph theory. An introductory course*. Vol. 63. Graduate Texts in Mathematics. Nueva York-Berlín: Springer-Verlag, 1979. https://doi.org/10.1007/978-1-4612-9967-7.

[7] Boppana, Ravi. *Unexpected Uses of Probability*. 2005. url: http://www.aops.com/Forum/viewtopic.php?p=1943887#p1943887/.

[8] Borel, Émile. «Les probabilités dénombrables et leurs applications arithmétiques». En: *Rendiconti del Circolo Matematico di Palermo* 27 (1909), págs. 247-271. https://doi.org/10.1007/BF03019651.

[9] Bourgain, Jean. «Estimates related to sumfree subsets of sets of integers». En: *Israel Journal of Mathematics* 97 (1997), págs. 71-92. issn: 0021-2172. https://doi.org/10.1007/BF02774027.

[10] Chattopadhyay, Eshan y Zuckerman, David. «Explicit two-source extractors and resilient functions». En: *Annals of Mathematics. Second Series* 189.3 (2019), págs. 653-705. issn: 0003-486X. https://doi.org/10.4007/annals.2019.189.3.1.

[11] Chen, Evan. «Expected Uses of Probability». En: *Mathematical reflections* 6 (2014). url: https://web.evanchen.cc/handouts/ProbabilisticMethod/ProbabilisticMethod.pdf.

[12] Cohen, Gil. «Two-source dispersers for polylogarithmic entropy and improved Ramsey graphs». En: *STOC'16—Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing*. Nueva York: ACM, 2016, págs. 278-284. https://doi.org/10.1145/2897518.2897530.

[13] Davidoff, Giuliana; Sarnak, Peter, y Valette, Alain. *Elementary number theory, group theory, and Ramanujan graphs*. Vol. 55. London Mathematical Society Student Texts. Cambridge University Press, Cambridge, 2003. https://doi.org/10.1017/CBO9780511615825.

[14] Djukić, Dušan; Janković, Vladimir; Matić, Ivan, y Petrović, Nikola. *The IMO Compendium*. 2.ª ed. Problem Books in Mathematics. Nueva York: Springer-Verlag, 2011. https://doi.org/10.1007/978-1-4419-9854-5.

[15] Eberhard, Sean; Green, Ben, y Manners, Freddie. «Sets of integers with no large sum-free subset». En: *Annals of Mathematics. Second Series* 180.2 (2014), págs. 621-652. issn: 0003-486X. https://doi.org/10.4007/annals.2014.180.2.5.

[16] Erdös, Paul. «Some remarks on the theory of graphs». En: *Bulletin of the American Mathematical Society* 53 (1947), págs. 292-294. issn: 0002-9904. https://doi.org/10.1090/S0002-9904-1947-08785-1.

[17] Erdős, Paul. «Applications of probability to combinatorial problems». En: *Colloquium on Combinatorial Methods in Probability Theory*. 1962, págs. 90-92. url: https://users.renyi.hu/~p_erdos/Erdos.html.

[18] Erdős, Paul. «On a problem in graph theory». En: *The Mathematical Gazette* 47 (1963), págs. 220-223. issn: 0025-5572. https://doi.org/10.2307/3613396.

[19] Erdős, Paul. «Extremal problems in number theory». En: *Proceedings of Symposia in Pure Mathematics*. Vol. VIII. Providence, Rhode Island: American Mathematical Society, 1965, págs. 181-189. https://doi.org/10.1090/pspum/008.

[20] Erdös, Paul y Kac, Mark. «The Gaussian law of errors in the theory of additive number theoretic functions». En: *American Journal of Mathematics* 62 (1940), págs. 738-742. issn: 0002-9327. https://doi.org/10.2307/2371483.

[21] Erdős, Paul y Lovász, László. «Problems and results on 3-chromatic hypergraphs and some related questions». En: *Infinite and finite sets (Colloq., Keszthely, 1973; dedicated to P. Erdős on his 60th birthday)*. Vol. II. Colloquia Mathematica Societatis Janós Bolyai 10. Amsterdam, 1975. url: https://www.renyi.hu/~p_erdos/1975-34.pdf.

[22] Fernández, Pablo y Fernández, José Luis. «El discreto encanto de la matemática». 2018. url: http://verso.mat.uam.es/~pablo.fernandez/.

[23] Gowers, William T. «Quasirandom groups». En: *Combinatorics, Probability and Computing* 17.3 (2008), págs. 363-387. issn: 0963-5483. https://doi.org/10.1017/S0963548307008826.

[24] Green, Ben y Tao, Terence. «The primes contain arbitrarily long arithmetic progressions». En: *Annals of Mathematics. Second Series* 167.2 (2008), págs. 481-547. issn: 0003-486X. https://doi.org/10.4007/annals.2008.167.481.

[25] Loh, Po-Shen. *Probabilistic method in combinatorics*. 2009. url: http://www.math.cmu.edu/~ploh/public_html/olympiad.shtml.

[26] Margulis, Grigori A. «Explicit constructions of expanders». En: *Problemy Peredači Informacii* 9.4 (1973), págs. 71-80. issn: 0555-2923.

[27] Mertens, Franz. «Ein Beitrag zur analytischen Zahlentheorie». En: *Journal für die reine und angewandte Mathematik* 78 (1874), págs. 46-62. issn: 0075-4102. https://doi.org/10.1515/crll.1874.78.46.

[28] Molloy, Michael y Reed, Bruce. *Graph colouring and the probabilistic method*. Vol. 23. Algorithms and Combinatorics. Berlín: Springer-Verlag, 2002. https://doi.org/10.1007/978-3-642-04016-0.

[29] Moser, Robin A. «A constructive proof of the Lovász local lemma». En: *STOC'09—Proceedings of the 2009 ACM International Symposium on Theory of Computing*. Nueva York: ACM, 2009, págs. 343-350. https://doi.org/10.1145/1536414.1536462.

[30] Moser, Robin A. y Tardos, Gábor. «A constructive proof of the general Lovász local lemma». En: *Journal of the ACM* 57.2 (2010). issn: 0004-5411. https://doi.org/10.1145/1667053.1667060.

[31] Ramsey, Frank P. «On a Problem of Formal Logic». En: *Proceedings of the London Mathematical Society. Second Series* 30.4 (1929), págs. 264-286. issn: 0024-6115. https://doi.org/10.1112/plms/s2-30.1.264.

[32] Riordan, Oliver. *Lecture notes on Probabilistic Combinatorics*. 2019. url: https://courses.maths.ox.ac.uk/node/view_material/41048.

[33] Riordan, Oliver. *Oxford materials about the course on Probabilistic Combinatorics*. 2019. url: https://courses.maths.ox.ac.uk/node/view_material/41304.

[34] Shearer, Jean B. «On a problem of Spencer». En: *Combinatorica* 5.3 (1985), págs. 241-245. issn: 0209-9683. https://doi.org/10.1007/BF02579368.

[35] Sipser, Michael y Spielman, Daniel A. «Expander codes». En: *IEEE Transactions on Information Theory* 42.6 (1996). Codes and complexity, págs. 1710-1722. issn: 0018-9448. https://doi.org/10.1109/18.556667.

[36] Spencer, Joel. «Ramsey's Theorem — A New Lower Bound». En: *Journal of Combinatorial Theory. Series A* 18.1 (1975), págs. 108-115. issn: 0097-3165. https://doi.org/10.1016/0097-3165(75)90071-0.

[37] Szele, Tibor. «Kombinatorikai vizsgálatok az irányitott teljes gráffal». En: *Matematikai és Fizikai Lapok* 50 (1943), págs. 223-256.

[38] Tao, Terence. *Moser's entropy compression argument*. 2009. url: https://terrytao.wordpress.com/2009/08/05/mosers-entropy-compression-argument/.

[39] Tao, Terence y Vu, Van. *Additive combinatorics*. Vol. 105. Cambridge Studies in Advanced Mathematics. Cambridge: Cambridge University Press, 2006. https://doi.org/10.1017/CBO9780511755149.

[40] Turán, Paul. «On a Theorem of Hardy and Ramanujan». En: *The Journal of the London Mathematical Society* 9.4 (1934), págs. 274-276. issn: 0024-6107. https://doi.org/10.1112/jlms/s1-9.4.274.

[41] Wikipedia. *List of probabilistic proofs of non-probabilistic theorems*. En: *Wikipedia, The Free Encyclopedia*. 2019. url: https://en.wikipedia.org/w/index.php?title=List_of_probabilistic_proofs_of_non-probabilistic_theorems&oldid=910281376.

[42] Wikipedia. *Lovász local lemma*. En: *Wikipedia, The Free Encyclopedia*. 2019. url: https://en.wikipedia.org/w/index.php?title=Lov%5C%C3%5C%A1sz_local_lemma&oldid=895002723.

[43] Wikipedia. *Problema de satisfacibilidad booleana*. En: *Wikipedia, La enciclopedia libre*. 2019. url: https://es.wikipedia.org/w/index.php?title=Problema_de_satisfacibilidad_booleana&oldid=117829273.

[44] Wikipedia. *Ramsey's theorem*. En: *Wikipedia, The Free Encyclopedia*. 2020. url: https://en.wikipedia.org/w/index.php?title=Ramsey%5C%27s_theorem&oldid=937680845.

A. Anexo: soluciones a los ejercicios planteados

Solución del ejercicio 1. Con el objetivo de construir un subgrafo bipartito de G, consideramos una partición aleatoria de los vértices de G en dos conjuntos A y B. Esta partición se dará a partir de elegir de manera independiente para cada vértice de G el conjunto al que pertenecen, A o B, cada uno con probabilidad $1/2$. Para cada tal partición de $V(G)$ aleatoria, quitamos las aristas de G que unan dos vértices de A o dos vértices de B, dando así lugar a un subgrafo bipartito G_{bip} de G con partición de vértices $V(G_{\text{bip}}) = A \cup B$ (con la notación de la definición 14). Sea X la variable aleatoria correspondiente al número de aristas de este grafo bipartito G_{bip} aleatorio. Probaremos que $\mathbb{E}[X] = m/2$ y la conclusión del ejercicio 1 se seguirá directamente del segundo punto de la proposición 8. Vemos que $X = \sum_{e \in E(G)} X_{e \in E(G_{\text{bip}})}$ y, además, dado $e \in E(G)$, $\mathbb{P}(e \in E(G_{\text{bip}})) = \mathbb{P}(\text{los extremos de } e \text{ están en el mismo conjunto de la partición}) = 1/2$. Por la proposición 7, $\mathbb{E}[X] = m/2$. ∎

Solución del ejercicio 2. Tomaremos al azar un par de comités. Sea X el número de delegados en común que tienen ambos comités, de modo que $X = X_1 + ... + X_{1600}$, donde cada X_i es una indicatriz que toma el valor 1 si y solo si el i-ésimo delegado está en ambos comités seleccionados. Supongamos que el delegado i-ésimo aparece en a_i comités. Entonces, por un argumento de doble conteo, $a_1 + ... + a_{1600} = 16000 \cdot 80$. Para estimar $\mathbb{E}[X]$ también es necesario hacer uso de un caso particular de la desigualdad de Jensen.

Lema 38 (Desigualdad de Jensen). *Dada una función $f : \mathbb{R} \to \mathbb{R}$ convexa, para cualesquiera $x_1, ..., x_n \in \mathbb{R}$ se cumple lo siguiente:*

$$\sum_{k=1}^{n} \frac{f(x_k)}{n} \geq f\left(\sum_{k=1}^{n} \frac{x_k}{n}\right).$$

Vamos a aplicar este lema a la función $f(x) = x(x-1)/2$ que, por tener segunda derivada positiva, es convexa. Notemos que, si $n \geq 0$ es entero, entonces $f(n) = \binom{n}{2}$. Tenemos que

$$\mathbb{E}[X] = \sum_{i=1}^{1600} \mathbb{P}(X_i = 1) = \frac{\sum_{k=1}^{1600} f(a_i)}{\binom{16000}{2}} \geq \frac{1600 \cdot f\left(\frac{16000 \cdot 80}{1600}\right)}{\binom{16000}{2}} \approx 3{,}995 > 3$$

y, por la proposición 8, se garantiza la existencia de un par P de comités tal que $X(P) \geq \mathbb{E}[X] > 3$ y, como X toma valores enteros, $X(P) \geq 4$ como queríamos. ∎

Solución del ejercicio 3. Denotamos por G cualquier subgrafo de $\mathcal{K}_{n,n}$ (véase la definición 14). Una partición de las descritas en el enunciado consiste en elegir una permutación $\sigma \in S_n = \text{Sim}([n])$ tal que $\{a_i, b_{\sigma(i)}\}$ es una arista de G para todo $i \in [n]$. Para probar que existe tal permutación, elegiremos $\sigma \in \text{Sim}([n])$ uniformemente al azar, de entre las $n!$ permutaciones posibles, y probaremos que la variable aleatoria X definida por $X(\sigma) = |\{i \in [n] : \{a_i, b_{\sigma(i)}\} \in E(G)\}|$ tiene esperanza mayor que $n-1$. Notemos que $X = \sum_{e \in E(G)} X_e$, donde cada variable X_e es la indicatriz del suceso $\{\exists\, i \in [n] : e = \{a_i, b_{\sigma(i)}\}\}$. Se calcula fácilmente que $\mathbb{P}(X_e = 1) = (n-1)!/n! = 1/n$ y, por la proposición 7, $\mathbb{E}[X] = (n^2 - n + 1)/n > n - 1$. Por

tanto, por el segundo punto de la proposición 8, para algún emparejamiento σ tendremos que $X(\sigma) > n-1$ y, por tanto, $X(\sigma) = n$, lo cual termina la solución del ejercicio.

Queremos remarcar que el valor de n^2-n+1 es el mejor posible. En efecto, puede considerarse un subgrafo G en el que $\{a_i, b_j\}$ sea una arista si y solo si $j \neq 1$. En este caso, tenemos $n(n-1) = n^2 - n$ aristas y no es posible hacer un emparejamiento de los descritos. Como curiosidad, en este caso la variable aleatoria X sería constante e igual a $n-1$. ∎

Solución del ejercicio 4. Teniendo en cuenta que $R(2,2) = 2$, la desigualdad se cumple para $k = 2$. Vamos a comprobarla para $k \geq 3$ y, para ello, realizaremos la coloración de un grafo n-completo uniformemente al azar y probaremos que, con probabilidad positiva, no tendrá ningún subgrafo k-completo monocromático si $n \leq 2^{k/2}$. Tenemos $\binom{n}{k}$ subgrafos completos de k elementos en el grafo completo $\mathcal{K}_n$. Los enumeramos y, para cada uno de ellos, definimos el suceso malo $A_i = \{$el subgrafo k-completo i-ésimo es monocromático$\}$. Se tiene que $\mathbb{P}(A_i) = 2^{1-\binom{k}{2}}$. Observamos la siguiente cota para los coeficientes binomiales: $\binom{n}{k} \leq n^k/k!$, directo porque $\binom{n}{k} = \frac{1}{k!}\prod_{i=0}^{k-1}(n-i)$. Entonces,

$$\sum_{1\leq i\leq \binom{n}{k}} \mathbb{P}(A_i) = \binom{n}{k}\frac{2}{2^{\binom{k}{2}}} \leq \frac{n^k 2^{k/2+1}}{k! 2^{k^2/2}} \leq \frac{2^{k/2+1}}{k!} < 1,$$

usando que $k \geq 3$ en el último paso. La conclusión se sigue del primer punto de la proposición 8.

Tras el teorema 3.1.1 del libro de Alon y Spencer [3] se observa que puede tomarse $n = (1+o(1))k2^{k/2}/(\mathrm{e}\sqrt{2})$ para que se siga cumpliendo la desigualdad $\binom{n}{k}2^{1-\binom{k}{2}} < 1$. Esto puede hacerse estimando mejor los coeficientes binomiales con la fórmula de Stirling. De este modo, la misma prueba que hemos dado, acompañada de un mejor análisis de los posibles n como acabamos de comentar, nos lleva a concluir que $R(k,k) \geq (1+o(1))k2^{k/2}/(\mathrm{e}\sqrt{2})$, mejorando claramente la anterior desigualdad. ∎

Solución del ejercicio 5. Por la simetría de filas y columnas en el problema anterior, nos referiremos a ellas indistintamente como líneas. Vamos escoger una línea al azar y uniformente para después estudiar la variable aleatoria X, que devuelve, para cada línea L, la cantidad $X(L)$ de números distintos en dicha línea.

Tenemos que X es la suma de n variables indicatrices, $X = X_1 + \ldots + X_n$, donde cada X_k vale 1 en cada línea que contenga a k y 0 en el resto. Para cada k,

$$\mathbb{E}[X_k] = \frac{1}{2n}\left(\sum_{L \text{ línea}} X_k(L)\right) = \frac{|\{L \text{ línea} : L \text{ contiene a } k\}|}{2n}.$$

Digamos que k aparece en a_k filas y en b_k columnas exactamente. Entonces, k aparece en exactamente $a_k + b_k$ líneas. Por otro lado, tenemos que k aparece n veces en la cuadrícula y dichas casillas deben estar en una de las a_k filas y en una de las b_k columnas anteriormente descritas. Así que k puede aparecer en a lo sumo $a_k b_k$ casillas. Por la versión más simple de la desigualdad aritmético-geométrica tenemos que $a_k + b_k \geq 2\sqrt{a_k b_k} \geq 2\sqrt{n}$. Por tanto, para cada $k \in [n]$, $\mathbb{E}[X_k] = (a_k + b_k)/2n \geq 1/\sqrt{n}$. Finalmente, $\mathbb{E}[X] = \sum_{k=1}^n \mathbb{E}[X_k] \geq \sum_{k=1}^n 1/\sqrt{n} = \sqrt{n}$, así que, por el segundo punto de la proposición 8, para alguna línea L tenemos que $X(L) \geq \sqrt{n}$, como queríamos. ∎

Solución del ejercicio 6. El enunciado es trivial para $N = 1$. Estudiemos ahora el caso $N > 1$. Vamos a hacer N elecciones de elementos de G, con posibles repeticiones, y a formar así nuestro conjunto B. Aplicaremos el segundo punto de la proposición 8 a la variable aleatoria $X = |A + B|$, que verifica que $\mathbb{E}[X] \geq N^2/2$. Podemos escribir X como suma de indicadores X_k, con $k \in G$, que toman el valor 1 si y solo si $k \in A + B$. Esto se da precisamente cuando $k - a \in B$ para algún $a \in A$, es decir, si alguno de tales N elementos está en B. Así que $\mathbb{P}(X_k = 1) = 1 - (1 - N/N^2)^N$. Finalmente, $\mathbb{E}[X] = N^2(1 - (1 - 1/N)^N) \geq N^2(1 - 1/\mathrm{e}) \geq N^2/2$, haciendo uso del lema 32 para $n = -N < -1$. ∎

Solución del ejercicio 7. Vamos a proceder de manera estándar. Consideramos una coloración que asocie a cada arista del grafo un color de manera uniforme e independiente al resto. Los malos sucesos que vamos a estudiar, de los cuales queremos probar que su unión no cubre todo el espacio de probabilidad, son precisamente aquellos en los que alguno de los triángulos es monocromático. No necesitamos saber

cuántos sucesos malos hay, aunque sea inmediato de contar. Solamente necesitamos comprobar la condición local. La probabilidad de que un triángulo cualquiera sea monocromático es $p = k/k^3 = 1/k^2$. Además, el suceso que consiste en que un triángulo T sea monocromático es dependiente del suceso que consiste en que el triángulo $T' \neq T$ sea monocromático si y solo si T y T' tienen una arista en común. Fijado T, tenemos $3(n-3)$ tales T', así que $d = 3n-9$ con la notación del lema 31 y $\mathrm{e}p(d+1) \leq \mathrm{e}\frac{1}{9n}(3n) < 1$. ∎

Solución del ejercicio 8. Vamos a optar por elegir, para cada uno de los n colores, uno de los once puntos de dicho color uniformemente al azar. Es fácil darse cuenta de cuáles son los sucesos malos: para cada pareja de puntos consecutivos con distinto color, un suceso malo sería el que corresponda a seleccionar ambos puntos tras realizar la anterior elección aleatoria. Llamaremos pareja especial a una tal pareja de puntos.

Consideramos un conjunto de índices I que enumera las parejas especiales. Para cada $i \in I$, se denota por P_i la pareja especial asociada al índice i, y por S_i el suceso malo correspondiente que describimos antes. Para todo i, se tiene que $p = \mathbb{P}(A_i) = 1/11^2$, ya que cada punto de la pareja P_i tiene probabilidad $1/11$ de ser elegido y cada elección es independiente (porque tienen distintos colores, por asunción).

Además, podemos tener una cota en el número de dependencias. Consideremos una pareja P_i especial, cuyos puntos tienen los colores C_1 y C_2. Ahora afirmamos que A_j va a ser independiente de la familia de sucesos a los que A_i pertenece si y solo si los colores de su pareja P_i son ambos distintos de C_1 y C_2. Esto se debe a que la elección de cada uno de los n puntos se hace para cada color de manera independiente. Ahora vamos a contar cuántas parejas especiales P_k van a tener alguno de sus colores igual a C_1 o C_2. Cada una de esas parejas P_k debe contener un punto D_k de color C_1 o C_2 (hay a lo sumo 22 puntos con estas condiciones) y el otro punto E_k que forme la pareja $P_k = \{D_k, E_k\}$ debe ser consecutivo a D_k. Así que, fijado D_k, hay como máximo dos opciones para E_k, y por ello hay como máximo $22 \times 2 = 44$ tales parejas especiales, de entre las cuales debemos eliminar la propia pareja del suceso A_j fijada inicialmente. Con la notación del lema 31, hemos comprobado que podemos tomar $p = 1/11^2$ y $d+1 = 44$. Se comprueba simplemente que $\mathrm{e}p(d+1) < 1$ y, así, por el lema 31, habrá una posible elección de n puntos tal que ninguno de los sucesos malos se da, que es precisamente la conclusión del enunciado. ∎