

MONOGRAFÍA

Presentada el 28 de febrero de 2014 en la

Universidad de La República, UdelaR

para obtener el título de

LICENCIADO
Mención MATEMÁTICA

para

Pablo Gabriel ROMERO RODRÍGUEZ

Título de la monografía :

Diámetro Confiable de una Red

Orientador: Dr. Eduardo Canale

Comité de examinadores:

Dr. Ernesto MORDECKI
Dr. Gonzalo PERERA
Dr. Gonzalo TORNARÍA

Agradecimientos

Este texto merece claridad de contexto.

Las poquitas contribuciones que el lector podrá apreciar en esta lectura fueron realizadas en equipo. Mi agradecimiento especial a los Doctores Pablo Sartor y Franco Robledo por invitarme a explorar el problema de esta monografía con ellos. La tesis doctoral de Pablo Sartor mereció aprobación y fue condecorada con mención especial. Vale destacar que esa tesis trata el mismo tema que la monografía actual (escrita con posterioridad), y aquí se verá apenas una nueva mirada al problema. No por reducir mi mérito pero sí por ser realistas, deseo puntualizar que el uso de interpolación para estimar el polinomio que es objeto de estudio ya estaba en mente del Dr. Gerardo Rubino, quien no había explorado tal posibilidad por cuestiones de tiempo.

Mis gracias a los Doctores Héctor Cancela y Gerardo Rubino, que no solamente dieron forma al estudio de modelos coherentes de confiabilidad en redes, sino que también han desplegado generosidad brindando su tiempo para crear equipos de investigación. Mi tutor, el Doctor Eduardo Canale, es admirado por su estudiante primeramente por su notable experticia en grafos y combinatoria, y segundo por haber aceptado en forma completamente altruista la revisión, supervisión y crítica de esta monografía.

Doy las gracias al selecto Tribunal conformado por los Doctores Ernesto Mordecki, Gonzalo Perera y Gonzalo Tornarúa. Ellos tienen un amplio espectro en Matemática y sus diversas aplicaciones a Economía, Telecomunicaciones, Computación e Ingeniería en general. Este elemento sumado a la seriedad que los caracteriza en torno a la investigación hace que su lectura crítica favorezca no solamente a señalar mis errores, sino también para construir nuevos enfoques en el estudio de la confiabilidad de redes de telecomunicaciones.

Renuevo mi agradecimiento permanente a mi madre, que me ha criado con cariño y dedicación, y mi abuela, una maestra y psicóloga muy comunicativa, que me ha enseñado a sumar y restar, tarea hasta el momento imposible para mi maestra de primaria. Mi merecido agradecimiento a Ana Luisa Álvarez, quien desde su sonrisa y amor me presentó el camino del encuentro.

Es una suerte que los humanos somos imperfectos...

Advierto desde ya que los errores son todos míos, y agradezco aviso de ellos, para repararlos. Los aciertos, si los hay, son producto de un equipo humano de investigadores que respalda.

Índice general

| | |
|---|-----------|
| Índice de Contenidos | 1 |
| I INTRODUCCIÓN | 3 |
| II NOCIONES PRELIMINARES | 11 |
| 1 Nociones Preliminares | 13 |
| 1.1 Terminología de Teoría de Grafos | 13 |
| 1.2 Complejidad de un grafo | 15 |
| 1.3 Flujos en Redes | 21 |
| 1.4 Complejidad Computacional | 29 |
| III DIÁMETRO-CONFIABILIDAD DE UNA RED | 33 |
| 2 Trabajo Relacionado | 35 |
| 2.1 Métodos Exactos en el Problema Clásico | 35 |
| 2.2 Complejidad del Problema Clásico | 37 |
| 2.2.1 Confiabilidad con dos terminales | 39 |
| 2.2.2 Confiabilidad con múltiples terminales | 40 |
| 2.2.3 Confiabilidad con todos los terminales | 40 |
| 2.3 Métodos Aproximados en el Problema Clásico | 40 |
| 2.4 Diámetro Confiabilidad de una Red | 45 |
| 2.4.1 Subproblemas y Complejidad | 45 |
| 2.4.1.1 Red con dos terminales | 47 |
| 2.4.1.2 Red con más de dos terminales | 49 |
| 2.4.2 Cálculo exacto en casos especiales | 54 |
| 2.4.3 Análisis Asintótico | 58 |
| 3 Contribuciones | 63 |
| 3.1 Interpolación para el cálculo de la Confiabilidad clásica | 63 |
| 3.2 Interpolación y Conteo | 68 |

| | | |
|----------|---|-----------|
| 3.3 | Interpolación basada en conocimiento previo de la red | 69 |
| 3.4 | Resultados Numéricos | 72 |
| 4 | Conclusiones | 81 |
| 4.1 | Conclusiones Generales | 81 |
| 4.2 | Problemas Abiertos | 83 |
| | Bibliografía | 90 |
| | Índice de Contenidos | 90 |
| | Lista de Figuras | 91 |

Parte I

INTRODUCCIÓN

RESUMEN

El objeto de estudio de esta monografía es la confiabilidad clásica de una red, y una variante, denominada diámetro confiabilidad de una red. El modelo clásico homogéneo se corresponde con el de un grafo cuyos nodos son perfectos, pero sus enlaces pueden fallar, con idénticas probabilidades $q = 1 - p$ independientes. Se desea hallar la probabilidad de que el subgrafo aleatorio sea conexo. Diversas aplicaciones sugieren una medida alternativa de confiabilidad, donde se exige que un subconjunto de nodos distinguidos (terminales) deben comunicarse por caminos de largo d o inferior. La probabilidad de este evento se denomina diámetro confiabilidad de una red (DCR). La evaluación de la DCR se puede abordar por diversos enfoques: teoría de grafos, complejidad computacional, estadística, combinatoria enumerativa, entre otras. Ello, sumado a sus célebres aplicaciones en telecomunicaciones y sistemas de transporte, motiva el presente estudio.

Partimos de una revisión de conceptos preliminares de teoría de grafos y complejidad computacional. Se incluye terminología relativa al problema, el Teorema de Ford-Fulkerson para el cálculo del corte mínimo de una red y el número de árboles recubridores de un grafo conexo, que resultan ser bloques constructores de la solución propuesta. Luego, veremos métodos exactos y aproximados para la evaluación de la confiabilidad clásica y diámetro acotada, en un capítulo de trabajo relacionado.

En esta monografía se introducen métodos aproximados para la evaluación de ambas medidas de confiabilidad basadas en Métodos de Monte Carlo e interpolación polinómica. Se brinda un listado de problemas abiertos al final de este documento, conclusiones y pistas para trabajo futuro.

Palabras Clave: Teoría de grafos, complejidad computacional, confiabilidad.

INTRODUCCIÓN

Guía Para el lector

La intención de esta monografía es lograr una familiaridad, como también incentivar a la investigación de la confiabilidad de redes de telecomunicaciones.

Si bien el público objetivo es esencialmente estudiantes de Licenciatura en Matemática e Ingeniería, se desea la lectura de estudiantes curiosos pertenecientes a otras áreas. El texto procura mantener sencilla legibilidad de todo lector con conocimientos en probabilidad, análisis matemático y álgebra lineal. Se recomienda la consulta de los libros [4, 62] para una puesta a punto, en caso de resultar necesaria.

Para los estudiantes y aficionados que desean familiarizarse con el problema de la diámetro-confiabilidad de redes, una lectura lineal es recomendada, centrada en los Capítulos 1 y 2. El Capítulo 1 expone el cálculo del número de árboles de un grafo mediante técnicas algebraicas (resumen de los Capítulos 4 a 6 del texto clásico de Teoría Algebraica de Grafos de Biggs [9]), el cálculo de un corte de mínimo cardinal en una red (corolario del Teorema de Ford-Fulkerson, que se halla en libros de programación lineal, por ejemplo [51]) y elementos de la Teoría de la Complejidad, habiendo consultado los Capítulos 1 y 2 del libro de Garey y Johnson [41] como fuente principal. Naturalmente, todo lector que conoce estos temas puede directamente omitirlos. El Capítulo 2 contiene el trabajo relacionado con la confiabilidad clásica y diámetro-acotada.

Un experto en el área de confiabilidad de redes puede atender la discusión de complejidad de subproblemas de DCR del Capítulo 2, luego dirigirse a las Contribuciones del Capítulo 3 que en su mayoría no se hallan en prensa científica hasta el momento, y finalmente ver los problemas abiertos listados al final de la monografía.

Se recomienda a todo lector que desea adquirir experticia en el tema de diámetro confiabilidad en redes complementar la presente monografía con la tesis doctoral de Pablo Sartor [72]. Asimismo, una meticolosa lectura de los artículos fundacionales [22, 23, 63] y desarrollo de métodos de evaluación aproximados [19, 26] será de gran ayuda.

Como siempre, el acercamiento de sugerencias y erratas me será cálidamente bienvenido de parte de todo lector, y siempre agradecido¹.

¹Se agradece dirigir a mi correo personal por opiniones, críticas, sugerencias y/o erratas: promero@fing.edu.uy.

Organización del Documento

La siguiente monografía fue escrita procurando la sencilla legibilidad de todo lector con conocimientos en probabilidad, análisis matemático y álgebra lineal, y se organiza de la siguiente manera. En esta misma introducción se motiva el problema de estudio (se invita al lector la revisión de capítulos subsiguientes para su mayor comprensión) y se listan las contribuciones de esta monografía en tres artículos, donde uno ya fue publicado y los restantes permanecen en referato científico. El Capítulo 1 contiene una revisión de la terminología de teoría de grafos y complejidad computacional. Se incluye el cálculo de un corte de mínimo cardinal y conteo de árboles dentro de un grafo conexo, que son elementos constructores de la solución propuesta.

El Capítulo 2 describe el trabajo relacionado sobre el problema clásico de confiabilidad y el cálculo de la diámetro confiabilidad de redes (DCR), con enfoque en la complejidad computacional de ambos problemas, y de subproblemas de la DCR. Asimismo, incluye expresiones exactas para el cálculo de la DCR de grafos especiales (camino, ciclos, bipartitos y escaleras), como también un análisis asintótico de la DCR para el modelo de grafos aleatorios de Gilbert.

El Capítulo 3 sintetiza las contribuciones, centradas en métodos aproximados para calcular ambas medidas de confiabilidad. Finalmente, se resumen problemas abiertos, conclusiones y trabajo futuro en el Capítulo 4.

Motivación

Desde el origen de la telefonía, el foco en el diseño de redes fue la disponibilidad del servicio. La conducta humana ávida de comunicación sumada a las posibilidades tecnológicas brindadas por la electrónica digital y la física destinada a la miniaturización de componentes permitió el advenimiento de nuevos medios de comunicación, entre ellos la fibra al hogar y los sistemas móviles celulares.

Al anterior requisito de disponibilidad se suman otros elementos deseables, como la calidad del servicio, calidad de experiencia y seguridad de la red. Naturalmente, la Ingeniería de tráfico, Criptografía y Diseño de Redes se han visto altamente potenciadas y complejizadas.

En todos los casos, existe una noción relacionada con la disponibilidad que trascendió con el tiempo: la *confiabilidad*. En modelos estáticos, la confiabilidad representa la probabilidad de ofrecer el servicio correctamente en un instante dado, mientras que en modelos dinámicos se desea ofrecer el servicio correctamente durante un intervalo de tiempo [30]. En el caso más general, el servicio correcto dependerá del correcto funcionamiento de sus componentes, y en función de los costos de cada componente la redundancia será o no una buena estrategia.

Una medida de confiabilidad de particular interés es la *confiabilidad clásica de una red*, donde se tiene un grafo con nodos distinguidos, denominados *terminales*, y los componentes del sistema son los enlaces, que pueden fallar de forma independiente. El servicio será correctamente ofrecido cuando los terminales permanecen comunicados en la red, y esta es la probabilidad que se desea hallar. Pese a tomar aquí como fuente de inspiración a las telecomunicaciones, su aplicación se extiende a redes de transporte, computación paralela,

redes eléctricas y sistemas de control, entre otros. El cálculo de la confiabilidad de una red es un complemento valioso para su diseño, particularmente cuando se tiene la posibilidad de tender diferentes enlaces entre los terminales.

Una medida alternativa, que se denomina *diámetro confiabilidad de una red*, fue introducida por Petingi y Rodríguez [63], inspirados en diversas aplicaciones reales sensibles a la latencia [22, 24, 25]. Casos concretos de interés son el intercambio de video en vivo sobre la infraestructura de Internet [70], sistemas de distribución basados en inundación [1], transmisión de voz sobre IP [47] y sistemas de difusión con degradación en saltos [33], entre otros.

Diámetro Confiabilidad de una Red

Sea $G = (V, E)$ un grafo simple, donde V es un conjunto de nodos y E de enlaces. Consideremos además un conjunto de nodos distinguidos $K \subseteq V$, llamados *terminales*, y un entero positivo d , llamado *diámetro*. Asumiremos a lo largo de todo el texto que los nodos son perfectos, mientras que los enlaces pueden fallar en forma independiente, con probabilidades $q(xy) = 1 - p(xy)$ para cada $\{x, y\} \in E$, donde $p(xy)$ representa la probabilidad de operación del enlace $\{x, y\}$.

En la presente monografía estudiaremos el caso de probabilidades de operación idénticas: $p(xy) = p$. Se desea calcular la probabilidad $R_{K,G}^d(p)$ de que todo par de nodos distinguidos del conjunto K tenga algún camino de largo d o menos en la subred resultante de eliminar los enlaces fallidos. A este número lo denominaremos *diámetro confiabilidad de una red*, que abreviaremos mediante DCR por sus siglas. El objeto de estudio es entonces una función en la variable indeterminada $p \in [0, 1]$, que asigna a cada probabilidad de operación p de los enlaces la diámetro-confiabilidad de la red $R_{K,G}^d(p)$.

Adelantamos desde ya que la función incógnita $R_{K,G}^d(p)$ es un polinomio (ver Capítulo 2), donde sus coeficientes se pueden pensar en términos de problemas de conteo de subgrafos. Veremos allí que la alta complejidad del cálculo exacto nos llevará a aproximar el polinomio objetivo, mediante heurísticas (desarrolladas en el Capítulo 3).

Sin riesgo de confusión, utilizaremos el acrónimo DCR para referirnos tanto a la evaluación del polinomio $R_{K,G}^d(p)$ en un valor concreto de p como a la obtención completa de tal polinomio, valiéndonos del contexto de cada caso. El lector puede comprobar que si fuese posible evaluar el polinomio en cualquier punto luego lo podemos determinar completamente, por lo que ambos problemas tienen la misma dificultad. Asimismo, si bien la palabra *enlace* se reserva especialmente para redes y *aristas* para grafos, utilizaremos ambas indistintamente, mientras que usaremos *arcos* para enfatizar que estamos ante un grafo orientado. Los vértices de un grafo también serán llamados nodos.

Contribuciones

Los artículos [18, 68, 69] se resumen en el Capítulo 3 de esta monografía. El artículo [68] ya ha sido publicado, mientras que los restantes esperan evaluación de referato científico.

A modo de resumen, en [68] se introduce por primera vez una técnica basada en teoría de interpolación polinómica para calcular la confiabilidad clásica de una red. En [18] se discute la complejidad computacional del problema DCR, y se extiende la técnica de interpolación al problema DCR. Si bien la evaluación de la DCR pertenece a la clase computacional de problemas \mathcal{NP} -Difíciles, existen sub-problemas que pertenecen a la clase \mathcal{P} de problemas que admiten solución exacta por un algoritmo con una cantidad polinomial de operaciones elementales en el tamaño de entrada. Asimismo, se desarrolla una técnica de interpolación para DCR, que es esencialmente una extensión natural de aquella propuesta en [68].

Finalmente, en [69] se presentan dos métodos basados en Monte Carlo para el cálculo de la DCR. Al método de interpolación ya desarrollado se le incorpora un estimador puntual que explota conocimiento de la red. Este último es contrastado con otro método elemental, que se basa en conteo de subgrafos mediante Monte Carlo. Se señalan dificultades relativas a inestabilidad numérica del primero, mientras que el segundo, pese a su simplicidad, posee un desempeño superior ante todas las instancias de estudio.

Parte II

NOCIONES PRELIMINARES

Capítulo 1

Nociones Preliminares

1.1 Terminología de Teoría de Grafos

Un grafo G es un par $G = (V, E)$, siendo V un conjunto no vacío y $E \subseteq V \times V$ una relación binaria en V , siendo V el conjunto de *vértices* (o nodos) y E el conjunto de *aristas* (o enlaces). Decimos que un grafo $G = (V, E)$ es *no dirigido* cuando E es una relación simétrica ($(a, b) \in E \rightarrow (b, a) \in E$), y que no posee lazos cuando E es irreflexiva ($(a, a) \notin E$). Un grafo *simple* es un grafo no dirigido sin lazos. Un grafo G es *finito* si $|V|$ es finito.

En un grafo simple, dos vértices v_1 y v_2 son *adyacentes* cuando $(v_1, v_2) \in E$ y $(v_2, v_1) \in E$, que denotaremos $\{v_1, v_2\} \in E$ valiéndonos de la simetría. El *grado* de un vértice v , denotado mediante $gr(v)$, es la cantidad de aristas incidentes a v . Un vértice es *colgante* si tiene grado 1. Un *subgrafo* de G es un grafo $H = (V', E')$ tal que $V' \subseteq V$ y $E' \subseteq E[V']$, siendo $E(V')$ la relación E restringida a los vértices de V' . Tal subgrafo es *recubridor* si $V' = V$. Si $V' \subseteq V$, el grafo inducido por los vértices V' es $G[V'] = (V', E(V'))$. Si $E' \subseteq E$, el grafo sustracción de aristas E' de G es $G - E' = (V, E - E')$. Si $e = \{v_1, v_2\} \in E$, el grafo obtenido de identificar los vértices v_1 y v_2 tiene a $V^* = V - \{v_1, v_2\} \cup v^*$ como conjunto de vértices, y $E^* = E[V^*] \cup \{(v^*, x) : (v_1, x) \in E\} \cup \{(v^*, y), (v_2, y) \in E\}$ como conjunto de aristas; lo denotamos G_e . El grafo complemento \overline{G} de $G = (V, E)$ es $\overline{G} = (V, \overline{E})$, donde $\overline{E} = V \times V - E$ es el complemento de E . Un grafo es completo cuando todo par de vértices distintos posee una arista que los conecta. Denotamos al grafo completo de n vértices (o n -clique) mediante K_n .

Un *camino* sobre un grafo $G = (V, E)$ es una secuencia de vértices v_1, \dots, v_m de G , tales que $\{v_i, v_{i+1}\} \in E, \forall i \in \{1, \dots, m-1\}$. Tal camino es *cerrado* si $v_1 = v_m$, o *abierto* en caso contrario. Un camino es *simple* cuando no repite vértices. El *largo de un camino* es la cantidad de aristas que lo componen (contando posibles repeticiones). La *distancia* entre dos nodos $v, w \in V$ es el largo del camino más corto que conecta a v y w en sus extremos. El *diámetro* de un grafo G es la mayor distancia entre un par de nodos en G . Un *ciclo* de un grafo G es un camino cerrado de largo 3 o mayor, que repite únicamente el primer (último) vértice. Un grafo es un ciclo si todo él es un ciclo. Denotamos mediante C_n al ciclo de n vértices (o de n aristas), y P_n es el grafo que todo él es un camino simple de n vértices (con $n-1$ aristas). Decimos que un nodo v *alcanza* a w si existe un camino de v hacia w , o bien $v = w$. En grafos no dirigidos, la relación de *alcanzabilidad* es de equivalencia. Cada miembro de la clase de

alcanzabilidad es una *componente conexa* del grafo. Un grafo es *conexo* si tiene solamente una componente conexa. Equivalentemente, si es no vacío y existe un camino entre cada par de vértices cualesquiera. Un grafo es *acíclico* si no tiene ciclos. Un *árbol* es un grafo conexo y acíclico.

Sobreentenderemos que un grafo es simple y finito, a menos que se indique que lo contrario, y reservaremos las letras $m = |E|$ y $n = |V|$ para denotar la cantidad de aristas y vértices respectivamente. Las siguientes afirmaciones relativas a árboles permiten tomar dominio de los conceptos anteriores, y sus demostraciones son elementales. Asimismo, estos resultados nos serán un preliminar para contar árboles recubridores de un grafo, en la Sección 1.2.

Definimos el árbol trivial T_0 como el grafo compuesto por un solo nodo y cero enlaces. Los nodos colgantes de un árbol se llaman *hojas*.

Proposición 1.1.1 *Todo árbol no trivial tiene al menos dos hojas.*

Prueba. Sea T un árbol no trivial, y P un camino simple en T cuyo largo coincide con el diámetro. Los extremos de P son hojas, pues P es camino simple maximal.

QED

Corolario 1.1.2 *Todo árbol T de n nodos tiene exactamente $n - 1$ enlaces.*

Prueba. Por inducción sobre $n \geq 1$ natural. El árbol trivial cumple con el enunciado. Sea T_{h+1} un árbol arbitrario con $h+1$ nodos, y supongamos que el resultado es cierto para todo árbol con h nodos. Por la Proposición 1.1.1, T_{h+1} tiene alguna hoja x , y por lo tanto $T_{h+1} - x$ es acíclico, conexo (un árbol), y tiene un nodo menos y una hoja menos que T_{h+1} . Luego, $T_{h+1} - x$ es un nuevo árbol con h nodos, y por hipótesis inductiva tiene $h - 1$ enlaces. Entonces, T_{h+1} tiene h enlaces, como se quería probar.

QED

Proposición 1.1.3 *Si $G = (V, E)$ es un grafo conexo entonces $|E| \geq |V| - 1$*

Prueba. Romper ciclos mediante la eliminación de algunas aristas preservando conexidad, hasta tener un árbol.

QED

Vale un resultado análogo para los grafos acíclicos:

Proposición 1.1.4 *Si $G = (V, E)$ es un grafo acíclico entonces $|E| \leq |V| - 1$*

Prueba. Conectar sus componentes conexas mediante aristas, hasta tener un árbol.

QED

Una lectura de las Proposiciones 1.1.3 y 1.1.4 nos brinda el siguiente

Corolario 1.1.5 *Un árbol es un grafo conexo minimal, o equivalentemente, acíclico maximal.*

En un grafo conexo $G = (V, E)$, toda partición no trivial de nodos $V = S \cup S^C$ define un *corte*, que es el conjunto de aristas $(S, S^C) = \{e \in E : e = (u, v), u \in S, v \in S^C\}$. Todo corte separa un grafo conexo en dos o más componentes. El siguiente lema nos será de utilidad para contar árboles recubridores dentro de un árbol.

Lema 1.1.6 *Sea G un grafo conexo y T un árbol recubridor de G . Entonces:*

- *Toda arista e fuera de T forma un ciclo junto con algunos enlaces de T .*
- *Toda arista e dentro de T determina un corte junto con algunos enlaces fuera de T .*

Prueba. Todo árbol T es acíclico maximal, y se genera un ciclo al agregar e . Como T es conexo minimal $T - e$ ahora tiene dos componentes, y el conjunto de vértices admite una bipartición $V = V_1 \cup V_2$, donde un nodo incidente a e se halla en V_1 y el otro en V_2 . Luego e determina el corte (V_1, V_2) en G .

QED

Llamaremos $c(T, e)$ al corte determinado por $e \in T$, y $C(T, e)$ al ciclo determinado por $e \notin T$. Por la Proposición 1.1.2 hay exactamente $n - 1$ cortes así formados (uno por cada arista de T), y $m - n + 1$ ciclos (uno por cada arista de G fuera de T).

1.2 Complejidad de un grafo

La *complejidad* de un grafo G es la cantidad de árboles recubridores de G , y se denota $\kappa(G)$. Es claro que si G no es conexo, $\kappa(G) = 0$. Supongamos a lo largo de esta sección que $G = (V, E)$ un grafo simple conexo, y sin pérdida de generalidad denotemos $V = \{v_1, \dots, v_n\}$ y $E = \{e_1, \dots, e_m\}$. El cálculo de la complejidad de un árbol fue desarrollado por Gustav Kirchhoff, uno de los matemáticos fundadores de la ingeniería eléctrica, que ha resuelto no solamente este problema de conteo, sino también ha calculado la corriente eléctrica de circuitos lineales e invariantes en el tiempo. En esta sección veremos que $\kappa(G)$ se puede hallar directamente mediante el cálculo de un determinante. A tales efectos, utilizaremos artillería de álgebra lineal, resumiendo el camino de la tesis monográfica de Biggs en sus capítulos 4 a 6 [9]. Aquí se tomarán atajos para evitar el tratamiento general allí expuesto, que aplica también para grafos no conexos.

Definición 1.2.1 *En un grafo simple $G = (V, E)$, su matriz de adyacencias A_G es una matriz binaria de tamaño $|V| \times |V|$, tal que $A_G(i, j) = 1$ si y solo si $(v_i, v_j) \in E$.*

La matriz de adyacencias almacena toda la información necesaria de un grafo simple. Sean \mathbb{C}^E y \mathbb{C}^V el espacio vectorial de funciones a valores complejos con respectivos dominios V y E , llamados *espacio de vértices* y *espacio de aristas*. Tienen respectivas dimensiones $|V| = n$ y $|E| = m$. De hecho, la base canónica de funciones $a_i : V \rightarrow \mathbb{C}$ tal que $a_i(v_j) = \delta_{i,j}$ se corresponde con la base canónica de \mathbb{C}^n (y la situación es análoga para el espacio de aristas). A cada arista $e = \{x, y\} \in E$ le vamos a elegir un nodo positivo y otro negativo, arbitrariamente, y diremos que tal asignación es una *orientación*, mientras que G es un *grafo orientado*.

Definición 1.2.2 La matriz de incidencia $D_G = (d_{ij})$ de un grafo orientado G es una matriz de tamaño $n \times m$ con entradas en $\{-1, 0, 1\}$, tal que $d_{ij} = 1$ si el vértice v_i es positivo para e_j , $d_{ij} = -1$ si v_i es negativo para e_j y $d_{ij} = 0$ si v_i no es adyacente a e_j .

Lema 1.2.3 Sea G un grafo conexo. Luego, el rango de D_G es $r(D_G) = n - 1$.

Prueba. Cada columna de D_G suma 0, por lo que las filas son linealmente dependientes, y $r(D_G) \leq n - 1$. Sea ahora $\sum_{i=1}^n \alpha_i d_i = 0$ una combinación lineal no trivial de las filas d_i de D_G , y tomemos cierto j tal que $\alpha_j \neq 0$. Luego, como G es conexo el vector d_j no es nulo (pues alguna arista incide en v_j). Si la h -ésima entrada de d_j no es nula, existe exactamente una sola fila d_k con valor opuesto, es decir que $d_k(h) = -d_j(h)$, por lo que necesariamente $\alpha_k = \alpha_j$. Este razonamiento se propaga a todas las filas (vértices), porque el grafo es conexo. Luego la única manera de tener $\sum_{i=1}^n \alpha_i d_i = 0$ es que todos los coeficientes sean iguales, y $r(D_G) = n - 1$.

QED

Si G tiene algún ciclo C , recorramos el ciclo en uno de los dos sentidos posibles, y consideremos la siguiente función del espacio de aristas $f_C : E \rightarrow \mathbb{C}$, tal que $f(e) = 1$ si el sentido elegido para $e \in C$ es compatible con la orientación de G , $f_C(e) = -1$ si $e \in C$ pero no es compatible el sentido y $f_C(e) = 0$ si $e \notin C$. Denotemos $x_C = [x_1, \dots, x_m]^t$ a las coordenadas de esta función en la base canónica asociada con el orden $E = \{e_1, \dots, e_m\}$

Lema 1.2.4 El vector de ciclo x_C pertenece al núcleo de la matriz de incidencia.

Prueba. La i -ésima entrada del vector $y = Dx_C$ toma en cuenta la fila d_i asociada al vértice v_i y sus adyacencias con el ciclo C . Si v_i no pertenece a C , el producto interno $\langle d_i, x_C \rangle$ es claramente nulo. Si no, hay exactamente dos entradas no nulas del producto interno $\langle d_i, x_C \rangle$, y toman valores opuestos por construcción de f_C .

QED

Estudiemos ahora el rango de la matriz de incidencia, y veamos que se vincula con los cortes del grafo G . De hecho, asociemos a cada corte (S, S^C) una orientación asignando signo positivo a todos los vértices del conjunto S (o equivalentemente a los vértices de S^C). Ahora definimos una *función de corte*, g_S , tal que $g_S(e) = 1$ si $e \in (S, S^C)$ y la orientación de e coincide con la del corte, $g_S(e) = -1$ si $e \in (S, S^C)$ pero su orientación no coincide con la del corte, o $g_S(e) = 0$ en caso contrario (es decir, si no pertenece al corte).

Definición 1.2.5 El subespacio de ciclos de \mathbb{C}^E es el núcleo de la matriz de incidencia. El subespacio de cortes de \mathbb{C}^E es su complemento ortogonal.

Observación 1.2.6

- El subespacio de cortes de un grafo G conexo tiene dimensión $r(D_G) = n - 1$.
- Por el Teorema de las dimensiones, el subespacio de ciclos tiene dimensión $\ker(D_G) = m - r(D_G) = m - n + 1$.

- De la Proposición 1.1.6, si tomamos un árbol recubridor T de G se deducen exactamente $n - 1$ cortes (uno por cada enlace del árbol), y $m - n + 1$ ciclos (uno por cada arista que no está en el árbol recubridor). Esto sugiere una manera de construir una base de ambos subespacios.

La definición de subespacio de cortes se fundamenta mediante la siguiente:

Proposición 1.2.7 En todo corte orientado (S, S^C) de un grafo G , la función de corte g_S pertenece al subespacio de cortes.

Prueba. Si y es el vector que representa a las coordenadas de g_S en la base canónica del conjunto de aristas, entonces $y = \frac{1}{2} \sum_{i \in S} d_i - \sum_{j \in S^C} d_j$, siendo d_i la i -ésima fila de la matriz de incidencias. Sea ahora z tal que $Dz = 0$, es decir, $\langle d_i, z \rangle = 0$ para todo i . Es claro que $\langle z, y \rangle = 0$. Luego, y pertenece al complemento ortogonal del subespacio de ciclos, como se quería demostrar.

QED

Consideremos un árbol recubridor T para G . Sin pérdida de generalidad, enumeremos las aristas $E = \{e_1, \dots, e_m\}$ de modo que $\{e_1, \dots, e_{n-1}\}$ son precisamente las aristas de T . Sea $f_i, i \in \{1, \dots, n-1\}$ las funciones de corte correspondientes a los cortes $c(T, e_i)$, y $f_j, j \in \{n, n+1, \dots, m\}$ los respectivos ciclos obtenidos por $C(T, e_j)$.

Lema 1.2.8 El conjunto $\{f_i\}_{i=1, \dots, n-1}$ es base del subespacio de cortes de G , mientras que $\{f_j\}_{j=n, \dots, m}$ es base del subespacio de ciclos de G .

Prueba. El conjunto $\{f_j\}_{j=n, \dots, m}$ es independiente porque el ciclo correspondiente a la arista e_j es el único que contiene a e_j . Análogamente, $\{f_i\}_{i=1, \dots, n-1}$ es independiente porque el corte correspondiente a e_i es el único de todos los definidos que contiene a la arista e_i .

QED

Definición 1.2.9 Una matriz es totalmente unimodular si todo menor vale 0, 1 o -1 .

El siguiente resultado se le atribuye a Poincaré.

Teorema 1.2.10 La matriz de incidencia D_G de un grafo G es totalmente unimodular.

Prueba. Sea D' una submatriz de D_G . Por definición de D_G , cada columna de la submatriz D' no puede tener más de dos entradas no nulas. Si cada columna tiene exactamente dos entradas no nulas, la suma de todas las filas es nula, y el determinante de D_G es cero. Si alguna de las columnas de D' es nula, D' también es singular. Por último, si alguna de las entradas tiene exactamente una entrada no nula, un desarrollo de Laplace por tal columna agrega un factor de 1 o -1 , y a las siguientes submatrices se les puede reiterar el proceso de desarrollo de Laplace hasta obtener una matriz en las primeras dos condiciones (suma de filas nula o columna nula), o bien terminar el proceso en una matriz escalar que vale 0, 1 o -1 .

QED

Veamos ahora las condiciones para las cuales una submatriz de D_G resulta ser no singular.

Proposición 1.2.11 *Sea U un conjunto con $n - 1$ aristas del grafo conexo G , y tomemos las correspondientes $n - 1$ columnas de D_G junto con $n - 1$ filas de G elegidas arbitrariamente, y llamemos D_U a la submatriz obtenida. Sea $\langle U \rangle$ el grafo inducido por tales aristas (que posee las aristas de U y todos sus vértices terminales).*

Entonces: D_U es no singular si y solo si $\langle U \rangle$ es un árbol recubridor de G

Prueba. Si $\langle U \rangle$ es un árbol recubridor para G , como $\langle U \rangle$ es conexo la matriz D_G tiene rango $n - 1$, y al tomar $n - 1$ filas arbitrarias resulta que D_U es una matriz no singular. Recíprocamente, si D_U es no singular la matriz de incidencia $D_{\langle U \rangle}$ tiene rango $n - 1$. Como $\langle U \rangle$ es conexo, su subespacio de ciclos tiene dimensión 0, por lo que $\langle U \rangle$ es conexo y acíclico: es un árbol, y por conteo de nodos es recubridor de G .

QED

Nos dirigimos ahora al resultado principal de esta sección. La complejidad de un grafo se vincula con un determinante de una submatriz, que no es precisamente de la matriz de incidencia, sino que de la matriz laplaciana de un grafo.

Definición 1.2.12 *El laplaciano de un grafo G es la matriz $L_G = D_G D_G^t$.*

Observación 1.2.13 *La matriz L_G almacena en la entrada (i, j) el producto interno de las filas d_i y d_j de D_G . Si $i = j$ tenemos que $\|d_i\|^2 = gr(v_i)$, el grado del nodo v_i . En otro caso, el producto $\langle d_i, d_j \rangle$ será no nulo solamente si la arista $\{v_i, v_j\}$ pertenece al grafo G , y como su orientación es positiva para un nodo y negativa para el otro se tiene que $\langle d_i, d_j \rangle = -1$. Entonces: $L_G = \Delta_G - A_G$, siendo Δ_G la matriz diagonal que almacena los grados del grafo G , y A_G la matriz de adyacencias.*

Sabemos que el determinante del producto de matrices cuadradas es el producto de los determinantes de cada matriz. Sin embargo, ese resultado no da pistas de cómo vincular el determinante del laplaciano con la matriz de incidencia, pues D_G no es cuadrada en general. El vínculo es una generalización del determinante de producto de matrices cuando figuran traspuestas y no son necesariamente cuadradas. El siguiente teorema técnico se atribuye a Binet y Cauchy, y nos permitirá calcular el determinante del laplaciano mediante determinantes de submatrices de D_G . Denotemos $[n] = \{1, \dots, n\}$ el conjunto con los primeros n enteros positivos y $\binom{[m]}{n}$ al conjunto formado por todos los subconjuntos de $[m]$ con exactamente n elementos.

Teorema 1.2.14 (Binet-Cauchy) *Sean A y B matrices con respectivos tamaños $n \times m$ y $m \times n$. Entonces:*

$$\det(AB) = \sum_{S \in \binom{[m]}{n}} \det(A_{([n], S)}) \det(B_{(S, [n])}), \quad (1.1)$$

siendo $A_{(S_1, S_2)}$ la submatriz de A formada por las filas dadas por S_1 y columnas dadas por S_2 .

En el texto de Biggs se cita al libro de Teoría de Matrices de Lancaster por una demostración [55]. No obstante, la prueba ofrecida en el libro de J. van Lint y R. Wilson titulado “A course in Combinatorics” es más general, siendo a la vez simple y elemental [77]:

Lema 1.2.15 *En las condiciones del Teorema de Binet Cauchy, si además Δ es una matriz diagonal de tamaño $m \times m$ con respectivas entradas e_1, \dots, e_m , entonces:*

$$\det(A\Delta B) = \sum_{S \in \binom{[m]}{n}} \det(A_{([n],S)}) \det(B_{(S,[n])}) \prod_{i \in S} e_i, \quad (1.2)$$

Prueba. La entrada (i, k) de $A\Delta B$ vale $\sum_{j=1}^m a_{ij} e_j b_{jk}$, y como $A\Delta B$ es de tamaño $n \times n$, la función $\det(A\Delta B)$ es un polinomio de grado n en las variables indeterminadas e_1, \dots, e_m . Calculemos los coeficientes de sus monomios. Tomemos primero un monomio de la forma $e_{i_1}^{t_1} \dots e_{i_s}^{t_s}$, con $s < m$, es decir que hay $s < m$ variables indeterminadas distintas que figuran en el monomio, y existe cierta variable e_r que no figura en tal monomio. Si tomamos $e_r = 0$ en la matriz diagonal Δ reducimos el rango de Δ en una unidad, por lo que el polinomio $\det(A\Delta B)$ al evaluar en $e_r = 0$ es idénticamente nulo. Esto implica todo monomio que no contiene a todas las variables indeterminadas debe tener coeficiente nulo. Por último, sea $S \in \binom{[m]}{n}$ un conjunto arbitrario de n elementos dentro de $[m] = \{1, \dots, m\}$, y consideremos el monomio $\prod_{i \in S} e_i$. El coeficiente de tal monomio correspondiente a la función $\det(A\Delta B)$ se puede hallar tomando $e_i = 1$ para todo $i \in S$, y $e_i = 0$ en caso contrario. Al formar tal matriz Δ y multiplicar tenemos que $A\Delta B = A_{([n],S)} B_{(S,[n])}$, que es un producto de matrices cuadradas, y entonces el coeficiente de $\prod_{i \in S} e_i$ vale $\det(A_{([n],S)}) \det(B_{(S,[n])})$.

QED

Prueba. [Teorema de Binet-Cauchy]. Tómesese $\Delta = I$ en el Lema 1.2.15.

QED

Recordemos que en una matriz cuadrada A , su matriz de cofactores $\text{cof}(A)$ toma en la entrada (i, j) el valor $\text{cof}(A)_{i,j} = (-1)^{i+j} \det(A_{([n]-i, [n]-j)})$. La adjunta es la matriz de cofactores transpuesta: $\text{adj}(A) = (\text{cof}(A))^t$. La utilidad de la matriz adjunta es que $A \text{adj}(A) = \det(A) I_n$, siendo I_n la matriz identidad de tamaño n . Entonces, si A es no singular su inversa se obtiene mediante $A^{-1} = (\det(A))^{-1} \text{adj}(A)$. Denotemos mediante J_n a la matriz de tamaño $n \times n$ que vale 1 en todas sus entradas, 0_n que vale 0 en todas sus entradas, y u_n el vector columna de tamaño n con todas sus entradas iguales a 1. El último ingrediente previo al resultado principal es una propiedad elemental del determinante de la matriz laplaciana.

Lema 1.2.16 *Si $G = (V, E)$ es conexo, la adjunta de su laplaciano cumple $\text{adj}(L_G) = \alpha J_n$ para algún real α .*

Prueba. Calculemos primeramente el núcleo de la matriz laplaciana. Sea $x = (x_1, \dots, x_n)^t$ tal que $L_G x = 0_n$. Entonces $x^t L_G x = 0$, y desarrollando el producto tenemos que

$$\begin{aligned} x^t L_G x &= \sum_{i,j} x_i l_{i,j} x_j = \sum_i d_i x_i^2 - 2 \sum_{i < j} x_i x_j 1_{\{i,j\} \in E} \\ &= \sum_{\{v_i, v_j\} \in E} (x_i - x_j)^2, \end{aligned}$$

siendo $V = \{v_1, \dots, v_n\}$, y d_i el grado de v_i . Como G es conexo tenemos que todo par de nodos tienen al menos un camino que los une, y $x^t L_G x = 0$ si y solo si $x = \alpha u_n$ para cierta constante real α . Esto significa que el núcleo de L_G tiene dimensión uno, y

$$L_G \text{adj}(L_G) = \det(L_G)I = 0_n.$$

Luego, toda columna de la matriz $\text{adj}(L_G)$ se halla en el núcleo de L_G , y $\text{adj}(L_G)$ tiene un múltiplo de u_n en cada columna. Como además L_G es simétrica, $\text{adj}(L_G)$ también debe serlo, y la única posibilidad es que todas las columnas de $\text{adj}(L_G)$ sean iguales, es decir que $\text{adj}(L_G) = \alpha J_n$.

QED

Ahora tenemos todas las herramientas para demostrar el teorema principal, que asegura que el anterior coeficiente α es precisamente $\kappa(G)$, la cantidad de árboles recubridores del grafo conexo G . El enunciado completo es el siguiente [9]:

Teorema 1.2.17 *Sea G un grafo simple conexo, $L_G = D_G D_G^t$ la matriz laplaciana de G y $\kappa(G)$ la complejidad de G . Entonces todo cofactor de L_G coincide con $\kappa(G)$:*

$$\text{adj}(L_G) = \kappa(G)J_n \quad (1.3)$$

Prueba. Por el Lema 1.2.16, es suficiente probar que un cofactor de L_G es igual a $\kappa(G)$. El cofactor correspondiente a la entrada (n, n) de L_G se puede calcular como $\det(D_0 D_0^t)$, siendo D_0 la matriz obtenida eliminando a D_G la última fila. Por el Teorema de Binet y Cauchy :

$$\det(D_0 D_0^t) = \sum_{U \in \binom{[m]}{n-1}} \det(D_{([n-1], U)}) \det(D_{(U, [n-1])}^t), \quad (1.4)$$

Por la Proposición 1.2.11, todos los determinantes de la sumatoria se anulan, salvo aquellas selecciones de aristas $U \in [m]$ tales que $\langle U \rangle$ es árbol recubridor para G . Por el Teorema 1.2.10 de Poincaré, D_G es totalmente unimodular, y para cada árbol recubridor $\langle U \rangle$ se tiene que $\det(D_{([n-1], U)}) = \det(D_{(U, [n-1])}^t) \in \{-1, 1\}$. Luego, todos los sumandos no nulos de la sumatoria valen 1, y hay exactamente un sumando no nulo por cada árbol recubridor de G . Esto significa que todos los cofactores de la matriz laplaciana valen lo mismo (Lema 1.2.16), y además son iguales a la cantidad de árboles recubridores, $\kappa(G)$, como se quería demostrar.

QED

Ejemplos: 1.2.18

- Para el grafo completo K_n tenemos que $L_{K_n} = nI - J_n$, y el cofactor de la entrada $(1, 1)$ es $\kappa(K_n) = \det(nI_{n-1} - J_{n-1})$. Observemos que la matriz J_{n-1} tiene rango 1, por lo que tiene el valor propio 0 con multiplicidad $n - 2$, y el valor propio $n - 1$ con multiplicidad 1 (y vector propio u_{n-1}). Luego, el polinomio característico de J_{n-1} es $p(\lambda) = \det(J_{n-1} - \lambda I_{n-1}) = c\lambda^{n-2}(n - 1 - \lambda)$, y su coeficiente principal vale $(-1)^{n-1}$, por lo que $c = (-1)^n$. Tenemos así que:

$$\det(nI_{n-1} - J_{n-1}) = (-1)^{n-1} p(n) = n^{n-2}. \quad (1.5)$$

La cantidad de árboles recubridores del grafo completo K_n es $\kappa(K_n) = n^{n-2}$, y por lo tanto todo grafo con n nodos tendrá a lo sumo n^{n-2} árboles recubridores. Esta es la llamada Fórmula de Cayley.

- Los grafos bipartitos se caracterizan por su espectro (es decir, por los valores propios de la matriz de adyacencias, y sus respectivas multiplicidades), y es posible hallar una fórmula para su complejidad en términos de sus valores propios.

El lector interesado puede encontrar en [9] métodos de cálculo de $\kappa(G)$ en términos del espectro del grafo G y otros basados en el desarrollo de determinantes.

1.3 Flujos en Redes

El problema de flujos en redes tiene importantes aplicaciones en ingeniería, donde el flujo puede ser de un líquido, de transporte de vehículos, paquetes sobre la infraestructura de Internet, mensajes u otros. En términos coloquiales se tienen dos extremos, uno llamado *fuentes* y otro llamado *sumidero* o pozo, y una cantidad de caminos que comunican a estos extremos. Se desea hallar el flujo máximo posible entre ambos extremos.

En esta sección daremos la definición formal del problema y el algoritmo de Ford-Fulkerson, a quienes se les otorga el mérito por resolver este problema. Esta sección es una síntesis del Capítulo 26 del libro introductorio a Algoritmos [32]. Se sugiere su consulta para acceder a una discusión de algoritmos más eficientes que el original, que se encuentra en [40].

Definición 1.3.1 Una red es un grafo dirigido ponderado $G = (V, E, c)$, donde $c : E \rightarrow \mathbb{R}^+$ es una función que asocia a cada enlace una capacidad.

Una red $s - t$ es una red donde además se identifican dos terminales distinguidos: la fuente, que indicaremos mediante s , y el pozo o sumidero, denotado mediante t (esta notación se adopta del inglés *source-terminal*). Sea $I^+(x)$ el conjunto de enlaces salientes desde el nodo x , e $I^-(x)$ el conjunto de enlaces entrantes a x .

Definición 1.3.2 Dada una red $s - t$, un flujo de s a t es una función $\varphi : E \rightarrow \mathbb{R}^+ \cup \{0\}$ tal que:

1. $\varphi(e) \leq c(e)$, $\forall e \in E$,
2. $\sum_{e \in I^-(s)} \varphi(e) = \sum_{e \in I^+(t)} \varphi(e) = 0$,
3. $\sum_{e \in I^-(x)} \varphi(e) = \sum_{e \in I^+(x)} \varphi(e)$, $\forall x \neq s, x \neq t$.

La Condición 1 indica que el flujo no puede superar la capacidad. La Condición 2 es la definición de fuente s y pozo t , y la Condición 3 es la ley de conservación del flujo, o ley de Kirchhoff.

Observemos que la conservación de flujo se puede expresar en un conjunto de nodos que no tenga la fuente ni el pozo. En efecto, si s ni t pertenecen a S , y $(S, S^C) = \{(x, y) \in E : x \in S, y \in S^C\}$ es el corte dado por S , entonces por la ley de Kirchhoff se consigue que:

$$\sum_{x \in S} \sum_{e \in I^-(x)} \varphi(e) = \sum_{x \in S} \sum_{e \in I^+(x)} \varphi(e). \quad (1.6)$$

Observar que hay términos comunes, que se corresponden con “flujo local en S ”, es decir, flujo de arcos cuyos nodos extremos están ambos en S . Si cancelamos tales términos comunes, tendremos únicamente flujos que se hallan en el corte de (S, S^C) o el de (S^C, S) . Entonces:

$$\sum_{x \in (S^C, S)} \varphi(e) = \sum_{x \in (S, S^C)} \varphi(e), \quad (1.7)$$

identidad cierta siempre que S no contenga a la fuente s ni el pozo t .

Vamos a denotar $|\varphi| = \sum_{e \in I^+(s)} \varphi(e)$ a la magnitud de flujo saliente de la fuente s . Como corolario de la Identidad (1.7), veremos que tal magnitud coincide con el flujo que termina en el pozo t .

Corolario 1.3.3 *La magnitud de flujo que sale de la fuente termina toda en el pozo.*

Prueba. Tomemos $S = V - \{s, t\}$ en la identidad (1.7). Por la Regla 2 de la Definición 1.3.2, no puede salir flujo del pozo ni entrar a la fuente. Por lo tanto, el primer miembro de (1.7) al usar $S = V - \{s, t\}$ coincide con el flujo que sale de la fuente, sin incluir posiblemente el flujo dado por el arco directo (s, t) . El segundo miembro coincide con el flujo que entra al pozo, sin incluir posiblemente el flujo dado por el arco directo (s, t) . Si existe arco (s, t) y flujo en él, se agrega en cada miembro. En cualquier caso se consigue que:

$$\sum_{e \in I^+(s)} \varphi(e) = \sum_{e \in I^-(t)} \varphi(e).$$

QED

Dada una red $s - t$, el objetivo es maximizar $|\varphi|$ respetando la definición de flujo. De ahora en más nos concentraremos en el caso que la función capacidad c asigna capacidades naturales a los enlaces, donde veremos el algoritmo de Ford y Fulkerson resuelve el problema del flujo máximo mediante la construcción de flujos con magnitudes naturales. El caso racional se generaliza directamente tomando un denominador común. El caso real lleva un poco más de esfuerzo. Una definición clave para resolver el problema del flujo máximo en el caso natural es introducir la capacidad de un corte, que es un conjunto de enlaces que desconectan la fuente del pozo. Formalmente:

Definición 1.3.4 *Dada un red $s - t$ y un conjunto de nodos $S \subseteq V$ tales que $s \in S, t \notin S$, el corte $(S - S^C)$, es el conjunto de enlaces que tienen un terminal en S y otro en S^C , es decir: $(S, S^C) = \{(x, y) \in E : x \in S, y \in S^C\}$. Notar que el orden importa, pues E es dirigido. La capacidad del corte (S, S^C) es la suma de las capacidades de los enlaces del corte, es decir: $c(S, S^C) = \sum_{e \in (S, S^C)} c(e)$.*

Todo corte determina una cota superior para el flujo máximo. De hecho, el siguiente resultado vale en general:

Proposición 1.3.5 *Dada una red $s - t$ y un corte (S, S^C) , cualquier flujo φ de s a t verifica $|\varphi| \leq c(S, S^C)$.*

Prueba. Sea φ un flujo de s a t . Consideremos una red extendida con una *super-fuente* s^* , y la red compuesta por los nodos $V^* = V \cup \{s^*\}$, $E^* = E \cup \{(s^*, s)\}$ y una extensión c^* de c tal que $c^*(s^*, s) = |\varphi|$. La red extendida se ilustra en la Figura 1.1.

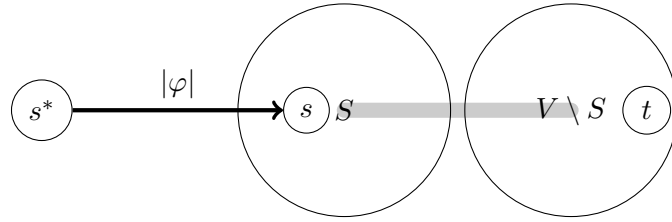


Figura 1.1: Red extendida. Agrega una super-fuente s^* , que incide a la fuente original s con un arco de capacidad $|\varphi|$. El conjunto S no contiene s^* ni t . La línea gris representa posibles arcos para ambos sentidos entre nodos del conjunto S y $V - S$.

El flujo φ también se puede extender a la nueva red definiendo $\varphi^*(s^*, s) = |\varphi|$. Ahora el conjunto S en la red extendida $s^* - t$ no contiene a la superfuente s^* ni tampoco al pozo t . Además, el flujo neto de S^C a S es no menor que $|\varphi|$, pues $s^* \in S^C$. Entonces, la conservación del flujo implica que:

$$\begin{aligned} |\varphi| = \varphi^*(s^*, s) &\leq \sum_{e \in (S^C, S)} \varphi^*(e) \\ &\leq \sum_{e \in (S, S^C)} \varphi^*(e) \leq \sum_{e \in (S, S^C)} \varphi(e) \leq c(S, S^C), \end{aligned} \quad (1.8)$$

donde se ha utilizado que ningún flujo de s^* a t puede incidir en la superfuente s^* , por la Regla 2.

QED

Hasta el momento sabemos que todo flujo φ de s a t cumple que:

$$|\varphi| \leq \min_{S: s \in S, t \notin S} c(S, S^C). \quad (1.9)$$

Sin embargo, no sabemos aún si se alcanza la igualdad. Llamamos *corte mínimo* (S, S^C) al corte que alcanza el valor mínimo del segundo miembro de la Desigualdad (1.9). Para evaluar ese mínimo resulta computacionalmente ineficiente calcular la capacidad de todos los cortes de la red, pues esta cantidad es exponencial con la cantidad de nodos de la red. Veamos ahora un corolario de la Proposición 1.3.5, que permite comprobar si un flujo alcanza el corte mínimo, y en tal caso será evidentemente un flujo máximo:

Corolario 1.3.6 *Dada una red $s - t$, para cualquier flujo $s - t$, φ , y cualquier corte $a - z$, (S, S^C) , se cumple $|\varphi| = c(S, S^C)$ si y solo si se cumplen las dos condiciones simultáneamente:*

1. $\varphi(e) = 0, \forall e \in (S^C, S)$,
2. $\varphi(e) = c(e), \forall e \in (S, S^C)$.

Prueba. Consideremos nuevamente la red extendida definida en la prueba de la Proposición 1.3.5, donde se obtuvo la siguiente cadena de desigualdades:

$$\varphi(s) = |\varphi| \leq \sum_{e \in (S, S^C)} \varphi(e) \leq c(S, S^C),$$

En la red extendida S no contiene a la super-fuente ni al pozo, y usando la ley de Kirchhoff vale la identidad (1.7).

Probemos primero el directo: si $|\varphi| = c(S, S^C)$ debemos tener una cadena de igualdades. Para alcanzar la capacidad del corte se debe cumplir que $\varphi(e) = c(e), \forall e \in (S, S^C)$. Además, la super-fuente $s^* \in S^C$ ya aporta todo el flujo φ de S^C a S , y no puede haber un flujo adicional de S^C a S . Recíprocamente, si las dos condiciones del enunciado son ciertas, se tiene nuevamente la cadena de igualdades, y $|\varphi| = c(S, S^C)$.

QED

La pregunta natural es cómo construir un flujo con capacidad máxima, y si va a conseguir la igualdad del Corolario 1.3.6 o no. Veremos que el Teorema de Ford y Fulkerson da una suerte de respuesta afirmativa a la pregunta. Antes de presentar el algoritmo de construcción del flujo máximo y su corrección, veamos definiciones preliminares. Considérese una red $s - t$ con φ un flujo $s - t$.

Definición 1.3.7 *La holgura de $e \in E$ es la cantidad de flujo que se podría agregar para alcanzar su capacidad: $h(e) = c(e) - \varphi(e)$. Cuando $h(e) = 0$ decimos que el arco e está saturado. Un camino $s - t$ es un camino de s hasta t , y la holgura de un camino $s - t$ es el mínimo de las holguras de los arcos que lo componen.*

Definición 1.3.8 *Una unidad de flujo es un flujo ϕ que asigna una unidad a cada arco de un camino $s - t$, y vale cero en los restantes arcos.*

Una primera aproximación al problema consiste en intentar construir el flujo máximo eligiendo caminos $s - t$ y agregando tantas unidades de flujo en tal camino como lo permite la holgura de tal camino. Sin embargo, esta construcción funcionará solamente si se eligen los caminos adecuados, y en caso de elegir un camino incorrecto es preciso *corregir*. Veremos que el algoritmo de Ford y Fulkerson permite agregar flujo en un camino $s - t$ y posibles correcciones, mediante cadenas.

Definición 1.3.9 *Una cadena $s - t$ es una secuencia de arcos que van desde s hasta t , que posiblemente no respeten el sentido de los arcos. La holgura de una cadena $s - t$ se calcula tomando el cuenta el mínimo de las holguras de los arcos con sentido. Precisamente, si el sentido coincide se toma la holgura habitual. En caso contrario, la holgura es el flujo del arco.*

Definición 1.3.10 Sea C una cadena de s a t con holgura uno o superior. Una unidad de flujo en C es una asignación $\varphi_C : E \rightarrow \{-1, 0, 1\}$ tal que $\varphi_C(e) = 1$ si e es recorrida en sentido correcto del arco, $\varphi_C(e) = -1$ si es recorrida en el sentido contrario y $\varphi_C(e) = 0$ en otro caso.

Cuando se recorre un arco por una cadena $s - t$ en el sentido contrario, el agregado de flujo en tal cadena se corresponde con una “resta de flujo”, que dividirá flujos ya existentes en otros positivos nuevos. Tal resta de flujo brinda una mayor holgura que luego permitirá explorar otros caminos, produciendo así un efecto de corrección.

Ya tenemos todos los ingredientes para presentar el Algoritmo de Ford y Fulkerson, que se esquematiza en la Figura 1.2. El Algoritmo construye reiteradamente cadenas que van de la fuente al pozo, y a ellas les agrega un flujo equivalente a la holgura de tal cadena (en caso de asignar restas se corresponde con una división de flujos positivos). El proceso acaba cuando ya no se puede agregar cadenas, y en base a etiquetados de nodos es posible determinar también los arcos que resultan saturados. Una vez se detectan los arcos saturados, por el Corolario 1.3.6 sabemos que tenemos un flujo máximo. Tenemos también que la magnitud total del flujo construido coincide la capacidad del corte mínimo, y el corte se deduce del etiquetado.

Vamos ahora a detalles del etiquetado y examinación de nodos durante el proceso. El primer nodo a examinar es la fuente s . En la primera etapa se toman todos los nodos antecesores (que inciden) al nodo examinado, que llamemos p para fijar ideas (al inicio es s y luego se van examinando otros nodos). Si el arco (q, p) tiene flujo positivo, se etiqueta al nodo q con $(p^-, D(q))$, donde $D(q)$ es la holgura parcial que se consigue en el camino parcial trazado desde p , y se anota p para tener trazabilidad del camino hacia atrás. Luego, se toman todos los nodos q sucesores al nodo examinado, y si el arco (p, q) tiene holgura positiva el nodo q se marca con una etiqueta $(p^+, D(q))$, donde $D(q)$ es la holgura de la cadena parcial que llega a q desde p . Al terminar se escoge un nodo etiquetado que no haya sido examinado hasta el momento, y se repite el procedimiento que aplica localmente a ese nodo. Cuando se llega a etiquetar el pozo t , el valor $D(t)$ es la holgura del camino que se traza hacia atrás, y se agrega entonces un flujo en la cadena $s - t$ con magnitud $D(t)$. Los flujos y las holguras se recalculan, y el proceso reinicia en la fuente. Si en algún momento no se logra etiquetar al pozo, el conjunto de nodos etiquetados S componen el corte (S, S^C) , y el proceso finaliza.

Teorema 1.3.11 (Ford-Fulkerson [40]) *El flujo máximo de s a t en toda red $s - t$ con capacidades enteras coincide con la capacidad del corte mínimo.*

Prueba. Probemos primeramente la terminación en una cantidad finita de pasos. Puesto que en cada iteración se agrega al menos una magnitud de una unidad a un camino, con certeza la capacidad neta de la red se reduce al menos una unidad. Pero la función de capacidad c asigna valores naturales y $\sum_{e \in E} c(e)$ es finita, por lo que la terminación está asegurada en una cantidad finita de pasos, y tenemos efectivamente un algoritmo. La corrección del algoritmo sigue del Corolario 1.3.6. En efecto, sea S el conjunto final de nodos etiquetados que fueron examinados y tales que el proceso no alcanza el pozo t . Como el primer nodo examinado en cada iteración es la fuente s , tenemos que $s \in S$, y tal conjunto determina un corte $s - t$, que es (S, S^C) . Por la condición de terminación no puede haber un arco del corte (S, S^C) con

Algoritmo 1 $(S, \varphi) = \text{Ford} - \text{Fulkerson}(s, t, V - \{s, t\}, E, c)$

```

1:  $\varphi \leftarrow 0$ 
2:  $p \leftarrow s$ 
3:  $T = \emptyset$  //  $T$  es el conjunto de nodos examinados
4:  $S = \{s\}$  //  $S$  es el conjunto de nodos etiquetados
5: Para todo  $q \notin S : (q, p) \in E$ 
6:   Si  $\varphi(q, p) > 0$  entonces
7:      $S \leftarrow S \cup \{q\}$ 
8:      $D(q) \leftarrow \min\{D(p), \varphi(u)\}$ 
9:      $q \leftarrow (p^-, D(q))$ 
10:     $T \leftarrow T \cup \{q\}$ 
11:   Fin Si
12: Fin Para
13: Para todo  $q \notin S : (p, q) \in E$ 
14:    $s(p, q) \leftarrow c(p, q) - \varphi(p, q) > 0$ 
15:   Si  $s(p, q) > 0$  entonces
16:      $S \leftarrow S \cup \{q\}$ 
17:      $D(q) \leftarrow \min\{D(p), s(p, q)\}$ 
18:      $q \leftarrow (p^+, D(q))$ 
19:   Fin Si
20: Fin Para
21:  $T \leftarrow T \cup \{p\}$  // El nodo  $p$  acaba de ser examinado
22: Si  $t \notin S$  entonces
23:   Si  $T \neq S$  entonces
24:      $p \leftarrow \text{Elegir}(S - T)$  // elegir un nodo de  $S - T$  para examinar
25:     Ir a Línea 5
26:   Si no
27:      $S \leftarrow S \cup \{s\}$ 
28:   Fin Si
29: Si no
30:    $K \leftarrow \text{Retroceder}(D)$  // usar la etiqueta para trazar la cadena  $K$ .
31:    $\varphi \leftarrow \varphi + D(t)\varphi_K$  // agregar tantas unidades de flujo como su holgura permita
32:   Ir a Línea 2
33: Fin Si
34: Retornar  $(S, \varphi)$ 

```

Figura 1.2: Pseudocódigo correspondiente al Algoritmo de Ford y Fulkerson.

holgura positiva, pues en tal caso se debería examinar un elemento de S^C , contradiciendo la definición del conjunto S y la terminación. Esto significa que todos los arcos del corte (S, S^C) están saturados. Además, no existe un antecesor de un nodo de S que se halle en S^C con flujo positivo, pues en caso contrario la etapa de revisar antecesores de un nodo de S hubiera etiquetado algún nodo de S^C . Luego, el flujo del corte (S^C, S) es nulo, y se cumplen las dos condiciones del Corolario 1.3.6, por lo que la magnitud del flujo obtenido coincide con el corte de (S, S^C) , es decir, $|\varphi| = c(S, S^C)$, y el Algoritmo de Ford-Fulkerson es correcto.

QED

El orden computacional del algoritmo de Ford Fulkerson queda acotado por $|E|^2 c_{max}$, siendo c_{max} la capacidad máxima de todos los arcos. En efecto, en el peor de los casos revisamos en cada iteración todas las aristas, y siempre restamos al menos una unidad a la capacidad neta de la red por iteración, siendo $|E|c_{max}$ una cota para la capacidad inicial de la red. Luego del algoritmo propuesto por Ford y Fulkeron, el esfuerzo de investigación entorno al problema clásico de flujo en redes se dirigió a mejorar su eficiencia. Un análisis detallado de la eficiencia computacional de Ford y Fulkerson y sus mejoras se encuentra en [32].

El siguiente corolario del Teorema de Ford-Fulkerson es de gran relevancia en el estudio de confiabilidad de redes de telecomunicaciones, pues brinda una manera eficiente para hallar el corte mínimo de una red. Simplemente se puede variar todos los pares s y t posibles, y aplicar el algoritmo de Ford y Fulkerson a la red con tales terminales y capacidades idénticas e iguales a 1.

Corolario 1.3.12 *Sea $G = (V, E)$ un grafo, s y t dos nodos distintos de V . El cardinal del corte mínimo es $|\varphi|$, el flujo de s a t obtenido al aplicar Ford-Fulkerson en la red (V, E, c) con $c(e) = 1$ para todo $e \in E$.*

Prueba. Por el Teorema 1.3.11, $|\varphi|$ coincide con la capacidad del corte mínimo en tal red. Pero esa capacidad coincide a su vez con el cardinal del corte, puesto que las capacidades valen uno.

QED

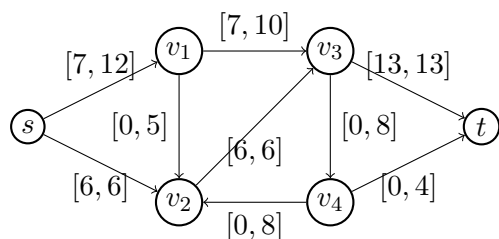
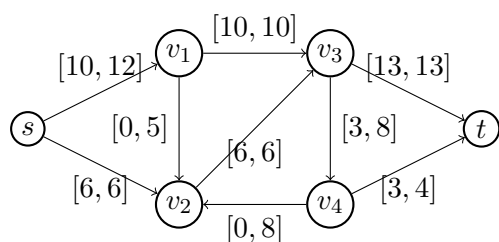
Ejemplo: 1.3.13 *Ilustraremos el algoritmo de Ford y Fulkerson mediante su aplicación a la red de la Figura 1.3, donde se indican las capacidades de cada arco como el valor derecho sobre el mismo arco, mientras que el valor izquierdo representa el flujo. Para acelerar el algoritmo, partimos de un flujo inicial que se consigue a simple vista:*

1. Agregamos 6 unidades de flujo por el camino $\{s, v_2, v_3, t\}$, y
2. Agregamos 7 unidades de flujo por el camino $\{s, v_1, v_3, t\}$.

Si denotamos φ_P a la unidad de flujo por el camino P , entonces hemos tomado el flujo inicial como φ :

$$\varphi = 6\varphi_{\{s, v_2, v_3, t\}} + 7\varphi_{\{s, v_1, v_3, t\}}.$$

Ahora aplicamos una iteración entera del algoritmo de Ford y Fulkerson. Empezamos de la fuente s . Marcamos el nodo v_1 con etiqueta $(s^+, 2)$. Como el arco $\{s, v_2\}$ está saturado, el

Figura 1.3: Red ejemplar con flujo inicial φ .Figura 1.4: Red ejemplar con flujo final φ' .

nodo v_2 no es marcado aún. Luego, el único nodo marcado desde la fuente es v_1 , y es por tanto el siguiente nodo a examinar. Como v_1 no tiene predecesores, vamos a sus sucesores, que son v_2 y v_3 . Marcamos v_2 con posible flujo parcial $2 = \min\{5 - 0, 2\}$, desde v_1 , es decir, con la etiqueta $(v_1^+, 2)$. También marcamos v_3 con $(v_1^+, 2)$. Elegimos a v_3 como el nodo siguiente a examinar (si elegíamos a v_2 inmediatamente pasábamos a v_3 , pues desde v_2 no se extiende camino posible). El único nodo posible a marcar es v_4 , con etiqueta $(v_3, 2)$. Finalmente desde v_4 podemos marcar a t , con etiqueta $(v_4^+, 2)$. Agregamos entonces un flujo de 2 unidades por el camino $\{s, v_1, v_3, v_4, t\}$. Tenemos ahora un nuevo flujo φ' :

$$\varphi' = 6\varphi_{\{s, v_2, v_3, t\}} + 7\varphi_{\{s, v_1, v_3, t\}} + 2\varphi_{\{s, v_1, v_3, v_4, t\}}.$$

La Figura 1.3 ilustra la red con el flujo φ' . Apliquemos una nueva iteración del algoritmo. Desde la fuente es posible marcar únicamente al nodo v_1 , con etiqueta $(s^+, 2)$. Ahora desde v_1 es posible marcar únicamente a v_3 , con etiqueta $(v_1^+, 2)$. Ya no se puede continuar desde v_2 . Luego, el conjunto de nodos $S = \{s, v_1, v_2\}$ determina el corte (S, S^C) de capacidad mínima $c(S, S^C) = 10 + 6 = 16$, y φ' es un flujo máximo con magnitud $\varphi' = 6 + 7 + 2 = 15$, como corresponde.

Se observa que el algoritmo de Ford y Fulkerson se aplica cuando la red tiene capacidades con valores enteros no negativos. De manera análoga resuelve el caso de capacidades racionales, pues basta multiplicar por el común denominador y traducir a una red con capacidades enteras, para luego aplicar el citado algoritmo y finalmente dividir flujos por el común denominador antes hallado. No obstante, el problema de capacidades a valores reales merece mayor profundidad. El algoritmo de Edmonds y Karp se basa en el agregado iterativo de flujos parciales en cadenas s - t , y resuelve el problema de flujo máximo general,

con capacidades reales [35]. Más aún, el nuevo algoritmo mejora la eficiencia de Ford-Fulkerson, pasando a un orden $O(|E|^2|V|)$, que no depende de la capacidad máxima de los arcos (que podría ser enorme, tornando ineficiente el algoritmo de Ford-Fulkerson). La esencia del algoritmo propuesto por Edmonds y Karp es elegir iterativamente la cadena $s-t$ más corta. El camino más corto entre dos nodos se puede hallar empleando el algoritmo de Dijkstra. Nótese al mismo tiempo que el problema de corte de mínimo cardinal en la red se puede hallar empleando el algoritmo de Ford y Fulkerson, que resulta eficiente para nuestros propósitos. El lector interesado en el esfuerzo posterior a la primera solución del problema de flujo máximo en redes puede hallar diversos algoritmos en [32].

1.4 Complejidad Computacional

Dada la creciente familia de nuevos problemas matemáticos pertenecientes a la clase de problemas \mathcal{NP} -Complejos, se torna valioso conocer este concepto de intratabilidad computacional, pues es penetrante a diversas áreas del conocimiento. Garey y Johnson brindan una placentera lectura de la teoría de la complejidad [41], que tiene tanto demostraciones rigurosas como valiosa motivación e intuición de cada tema propuesto. Asimismo, contiene una rica cantidad de ejemplos de problemas, su respectiva clasificación de complejidad y pautas para determinar la dificultad de un problema. Una vez que conocemos que tenemos a mano un problema *intratable* (concepto que se puede formalizar), lo usual es dar baja prioridad a la búsqueda de un algoritmo exacto para toda instancia, por los tiempos que conllevaría ejecutarlo, y como alternativa, desarrollar algoritmos de aproximación, o afrontar relajaciones del problema original.

Una organizada y autorizada fuente de algoritmos de aproximación para diversos problemas, principalmente provenientes de optimización combinatoria, redes y grafos, es el texto de Vazirani [78].

Un *problema* es una pregunta que espera una respuesta, y está ligado a la existencia de diversos parámetros libres, que al fijarlos determinan una *instancia* del problema. Un *algoritmo* es un conjunto finito de pasos que resuelve *toda instancia* de un problema. Consideremos por ejemplo el problema conocido como “Subset sum”, o suma de subconjuntos: dado un subconjunto finito de números naturales, decir si existe un subconjunto cuya suma sea la mitad del primero. Si nos dan una instancia concreta $A = \{1, 2, 8, 14, 12, 3, 5, 9\}$, podemos venir con la solución $B = \{1, 12, 14\}$ obtenida por inspección u otro método útil para ese caso, pero ello no determina a priori un algoritmo válido para cualquier instancia de suma de subconjuntos. Insistimos que un algoritmo debe ser aplicable para resolver *toda* instancia del problema. Un algoritmo válido para el problema de la suma de subconjuntos es ver todos los subconjuntos del conjunto dado A , calcular la suma de cada uno y responder aquél que tenga la mitad de la suma de todos los elementos de A , o que no es posible en caso contrario. Claramente, este algoritmo no es *eficiente*, pues la cantidad de subconjuntos es $2^{|A|}$, exponencial en el cardinal del conjunto de entrada A .

Una vez que tenemos el problema en manos, se desea entonces hallar un algoritmo eficiente. La teoría de la complejidad permite clasificar problemas y frecuentemente reconocer la clase de problemas “equivalentes” a nuestro problema de estudio. La demostración o

hallazgo de la clase que determina la complejidad del problema bajo estudio es en sí mismo un desafío, y las primeras herramientas consisten en conocer problemas anteriores, y notar similitudes en la estructura y los objetos involucrados de nuestro problema con uno anterior. De hecho, existen técnicas basadas en reducción a otro problema, o transformación de otro problema al nuestro, que permiten finalmente decir que nuestro problema es “al menos tan difícil” como el anterior.

Usualmente, la eficiencia de un algoritmo se mide en términos de la cantidad de operaciones realizadas, en relación con el tamaño de la instancia de entrada. Un aspecto técnico que ha merecido intensa investigación de pioneros en teoría de la computación es cómo homogeneizar una medida del tamaño de la instancia, ante diferentes problemas, cuyas entradas pueden ser números, grafos, funciones, programas, entidades lógicas u otras. Alan Turing ha definido una máquina universal incluso antes de la masificación de las computadoras, permitiendo implementar algoritmos para problemas matemáticos. La máquina de Turing es un dispositivo que lee y escribe símbolos contenidos en una cinta discretizada. Cada operación (leer un símbolo, mover la cinta, u otros) agrega una unidad al tiempo de ejecución. La noción de complejidad se basa en la tesis de Church-Turing, que sostiene básicamente que la máquina de Turing es al menos tan eficiente como cualquier otra máquina (esta tesis e intentos por extender la teoría de computación e información al caso cuántico se incluyen en [61]). También en 1936, Turing ha introducido un problema indecidible conocido como “Halting Problem” o problema de parada: dado un programa de computadora arbitrario y una entrada arbitraria a tal programa, Turing probó que es imposible construir un algoritmo que pueda decidir si un programa va a parar o no [75]. Otros problemas matemáticos que se sabe son indecidibles son el décimo problema de Hilbert [56], el problema de la trivialidad de grupos con presentación finita [67], y problema de dominó, relativo a tejar un plano [8], entre otros.

Asumamos que se tiene un esquema de codificación, que permite determinar mediante un conteo de cadena de símbolos el tamaño de la entrada. También debemos asumir un modelo de ordenador para medir tiempos de ejecución de los algoritmos. Afortunadamente, por la tesis de Turing-Church la teoría de la complejidad no depende de estas elecciones. Diremos que $f(n)$ es el orden computacional de un algoritmo si toda instancia de tamaño n se puede ejecutar una cantidad de operaciones que es $f(n)$ en el peor caso. Una función $f(n)$ es de orden $O(g(n))$ si existe alguna constante c tal que $|f(n)| \leq cg(n)$ para todo n natural.

Para comprender la intratabilidad del problema de diámetro-confiabilidad de redes, nos valemos de los siguientes conceptos, que están más detallados y motivados en el libro de Garey y Johnson [41]. Una distinción sencilla pero central en teoría de la complejidad está dada por la siguiente:

Definición 1.4.1 *Un algoritmo A es de tiempo polinomial cuando su función de complejidad es $O(p(n))$ para algún polinomio p . En caso contrario es de tiempo exponencial.*

El desarrollo de un algoritmo de tiempo polinomial de un problema usualmente requiere una profunda comprensión de la estructura de los objetos que componen al problema.

Definición 1.4.2 *Un problema pertenece a la clase \mathcal{P} de problemas resolubles en tiempo polinomial cuando existe un algoritmo A de tiempo polinomial para el problema.*

Un problema es intratable cuando es tan complejo que no admite algoritmo polinomial que lo resuelva. Recién en la década de 1970 se consiguen los primeros problemas decidibles pero intratables, en áreas de lógica matemática [38], teoría de autómatas y lenguajes formales [57].

Los fundamentos de la teoría de \mathcal{NP} -Complejidad fueron introducidos por Stephen Cook en 1971 mediante un breve e importante artículo [31], que incluye tres conceptos esenciales. El primero es la reducción polinomial, que consiste en una transformación de un problema en otro que puede ser ejecutada por un algoritmo en tiempo polinomial. El segundo es la clase \mathcal{NP} de problemas de decisión que se pueden resolver en tiempo polinomial por una máquina de Turing no determinista. En términos más sencillos, un problema de decisión es aquél donde toda instancia admite una respuesta de sí o no, y un problema se halla en la clase \mathcal{NP} cuando se puede verificar si una instancia afirmativa lo es, en tiempo polinomial. Como tercer aporte fundamental, Cook probó que todo problema perteneciente a la clase \mathcal{NP} admite una reducción polinomial a un problema especial, el problema de decisión de satisfactibilidad booleana SATISFACTIBILIDAD: dada una proposición lógica en su forma normal conjuntiva, determinar si existe una asignación de verdad a sus átomos que torne verdadera a la proposición.

Decimos que un problema X es *difícil* para una clase de problemas \mathcal{C} (o \mathcal{C} -Difícil) si todos los problemas dentro de \mathcal{C} pueden ser reducidos en tiempo polinomial a X . Si X es difícil para la clase \mathcal{C} y además X pertenece a \mathcal{C} , entonces decimos que X es *completo* para la clase \mathcal{C} (o \mathcal{C} -completo). Entonces, Cook formalizó el concepto de un problema \mathcal{NP} -Completo, demostrando que SATISFACTIBILIDAD es el primer miembro de esta clase.

Este resultado tiene profundas consecuencias. Una de ellas es que brinda un modo para demostrar si un problema X es \mathcal{NP} -Completo. De hecho, si tenemos un problema X , probamos primero que toda instancia afirmativa admite una verificación en tiempo polinomial, y así X pertenece a la clase \mathcal{NP} . Luego, si conocemos otro problema X' que sea \mathcal{NP} -Completo y admita una reducción polinomial al problema X , entonces X también es \mathcal{NP} -Completo. En efecto, sea Z un problema arbitrario de la clase \mathcal{NP} . Como X' es \mathcal{NP} -Completo, entonces Z admite una reducción polinomial a X' . Por composición tenemos que Z admite entonces una reducción polinomial al problema de estudio X . Luego, X es \mathcal{NP} -Completo.

El artículo de Cook brinda así un método para mostrar que un problema es \mathcal{NP} -Completo, y deja en evidencia la importancia de conocer otros problemas \mathcal{NP} -Completo antes de aventurar un intento de demostración de complejidad de un problema. Karp en 1972 utilizó el resultado de \mathcal{NP} -Complejidad de SATISFACTIBILIDAD y la metodología brindada por Cook para mostrar que otros 20 problemas combinatorios pertenecen a la clase de problemas \mathcal{NP} -Completo [48].

Obsérvese que todo problema de optimización combinatoria X con función objetivo f se puede traducir a un problema de decisión. Basta con tomar un número real arbitrario r y preguntar si existe alguna solución factible S del problema X tal que $f(S) \leq r$, en caso de ser una minimización, o $f(S) \geq r$ para un problema de maximización. Hay una clase de complejidad que aplica en particular a problemas de conteo. Básicamente, un problema X es de conteo si su solución es un entero no negativo (una definición formal basada en máquina de Turing no determinista se halla en el Capítulo 7 de [41]). La versión de conteo de todo problema perteneciente a la clase \mathcal{NP} se conoce como $\#\mathcal{P}$, conjunto definido por primera vez

por Valiant en su estudio de complejidad de problemas de enumeración y confiabilidad [76]. Análogamente, $\#\mathcal{P}$ -completo denota el conjunto de problemas de conteo cuyo correspondiente problema de decisión es \mathcal{NP} -Completo. La familia de problemas $\#\mathcal{P}$ -completos llama la atención de los teóricos en complejidad, puesto que no se sabe hasta el momento si este conjunto está incluido en la clase de problemas \mathcal{NP} .

Puesto que en esta monografía trabajaremos con problemas relativos a redes, los problemas de decisión y de conteo tendrán la siguiente forma:

Definición 1.4.3 (Problema de Decisión en Redes)

1. Entrada: *dado un grafo $G = (V, E)$ y una propiedad P*
2. Salida: *sí, existe un subgrafo de G que cumple la propiedad P , o no existe tal subgrafo.*

Definición 1.4.4 (Problema de Conteo de Redes)

1. Entrada: *dado un grafo $G = (V, E)$ y una propiedad P*
2. Salida: *determinar la cantidad de subgrafos de G que cumplen con la propiedad P .*

Naturalmente, todo problema de conteo es al menos tan difícil como el problema de decisión subyacente, y en consecuencia todo problema $\#\mathcal{P}$ es \mathcal{NP} -Difícil. Un problema de conteo particularmente interesante que está ligado a la Sección 1.3 de Flujos en Redes, pues ya sabemos que la determinación de un corte $s - t$ de cardinal mínimo se halla en \mathcal{P} , mientras que la determinación de la cantidad de cortes de cardinal mínimo es un problema de conteo $\#\mathcal{P}$ -Completo [66].

Para entrenar los conceptos de complejidad definidos, vamos a probar que si un problema \mathcal{NP} -Difícil admite un algoritmo de tiempo polinomial, entonces $\mathcal{P} = \mathcal{NP}$, y en particular podríamos resolver todos los problemas \mathcal{NP} -Completos en tiempo polinomial.

En efecto, supongamos por un momento que encontramos un problema X que es \mathcal{NP} -Difícil (más difícil que todo problema en \mathcal{NP}), que admite un algoritmo A en tiempo polinomial. Primeramente, sabemos que $\mathcal{P} \subseteq \mathcal{NP}$, pues si admite una solución en tiempo polinomial también se puede verificar en tiempo polinomial si una instancia es solución o no. Falta probar la otra inclusión. Sea ahora Z un problema perteneciente a la clase \mathcal{NP} . Como X es \mathcal{NP} -Difícil, existe una reducción polinomial de Z a X , y la aplicación del algoritmo A al problema reducido permite resolver Z en tiempo polinomial. Luego, $Z \in \mathcal{P}$ y tendríamos así que $\mathcal{P} = \mathcal{NP}$.

Actualmente se cree que $\mathcal{P} \neq \mathcal{NP}$. Sin embargo, no existe una prueba de tal aseveración. La pregunta si la familia de problemas \mathcal{NP} -Completos son intratables o no es considerada una de las preguntas abiertas más importantes de matemática moderna y computación.

Se desconoce hasta la fecha si la clase de problemas $\#\mathcal{P}$ -completos pertenece o no a la clase \mathcal{NP} . El problema de la presente monografía es \mathcal{NP} -Difícil, y está estrechamente relacionado con problemas de conteo $\#\mathcal{P}$ -Completos.

Parte III

DIÁMETRO-CONFIABILIDAD DE UNA RED

Capítulo 2

Trabajo Relacionado

En este capítulo se incluye una revisión de literatura relacionada con el problema de confiabilidad clásico y la diámetro-confiabilidad de una red.

2.1 Métodos Exactos en el Problema Clásico

Sea $G = (V, E)$ un grafo simple con enlaces $E = \{e_1, \dots, e_m\}$, que tienen todas probabilidades de operación idéntica $p_e = p$, y funcionan de forma independiente. Denotemos (X_1, \dots, X_m) el respectivo vector aleatorio que representa el estado de cada enlace, donde X_1, \dots, X_m son variables independientes que siguen una ley Bernoulli de parámetro p . Diremos que una configuración operativa es un subgrafo $H = (V, E')$ tal que H es conexo. Sea $\phi : \{0, 1\}^m \rightarrow \{0, 1\}$ la función binaria de estructura, tal que $\phi(x_1, \dots, x_m) = 1$ si y solo si la configuración H que contiene exactamente aquellos enlaces con $x_i = 1$ es operativa. Luego, $\phi(X)$ es una variable aleatoria Bernoulli, con probabilidad de éxito $P(\phi(X) = 1)$. Esta probabilidad se llama *confiabilidad clásica* de G , y se denota $R_{V,G}(p) = P(\phi(X) = 1) = E(\phi(X))$. En definitiva, es la probabilidad de que el subgrafo aleatorio resultante de los sorteos de enlaces resulte conexo.

En esta sección se describen métodos exactos para hallar $R_{V,G}(p)$. Una manera obvia de hallar $R_{V,G}(p)$ es sumar la probabilidad de todas las configuraciones operativas:

$$R_{V,G}(p) = \sum_{x:\phi(x)=1} P(X = x) = \sum_{x:\phi(x)=1} p^{|\{i:x_i=1\}|} (1-p)^{|\{i:x_i=0\}|} \quad (2.1)$$

Una dificultad para utilizar directamente la Expresión 2.1 es que la cantidad de sumandos de la sumatoria es exponencial con el tamaño del grafo, no resultando computacionalmente eficiente para grafos de gran tamaño. Una alternativa posible es atender únicamente las configuraciones operativas minimales, es decir, aquellas que al remover un enlace dejan de ser operativas, y aplicar el principio de inclusión-exclusión. Sea $\mathcal{A} = \{H_1, \dots, H_r\}$ tal conjunto. Si A_i es el evento correspondiente a la operación de todos los enlaces de H_i , se desea calcular la probabilidad de $\cup_{i=1}^r A_i$, que vale:

$$R_{V,G}(p) = \sum_{i=1}^r (-1)^{i-1} \sum_{B \subseteq \{1, \dots, r\}, |B|=i} P(\cap_{j \in B} A_j), \quad (2.2)$$

Nuevamente, la cantidad r de configuraciones operativas minimales puede ser exponencial. Por ejemplo, el Teorema de Cayley asegura que la cantidad de árboles recubridores del grafo completo K_n es $n^{n-2} > 2^{n-2}$, y todos ellos son configuraciones minimales. Existen técnicas duales que utilizan cortes en lugar de configuraciones operativas, que es ventajoso puesto que es usual que los grafos tengan menos cortes minimales que configuraciones operativas minimales. Se sugiere revisar la tesis de Pablo Sartor por referencias que explotan el uso de configuraciones y cortes [72].

Veamos ahora que la función incógnita $p \rightarrow R_{V,G}(p)$ es un polinomio. De hecho, sea F_i la cantidad de configuraciones operativas con exactamente $m - i$ enlaces operativos. Por la homogeneidad de la probabilidad de operación de los enlaces, se tiene que cada una de tales configuraciones tiene la misma probabilidad de ocurrencia, que vale $p^{m-i}(1-p)^i$. La medida de probabilidad aplicada sobre todas las configuraciones disjuntas permite asegurar que:

$$R_{V,G}(p) = \sum_{i=0}^m F_i (1-p)^i p^{m-i}. \quad (2.3)$$

La Expresión (2.3) sugiere que hallar $R_{V,G}(p)$ en forma exacta es equivalente a contar subgrafos. Precisamente, podemos ver nuestro problema de estudio como uno de conteo, y ello será esencial en el capítulo siguiente.

Observaciones 2.1.1

- La confiabilidad clásica $R_{V,G}(p)$ es un polinomio en la variable $p \in [0, 1]$.
- $R_{V,G}(0) = 0$, $R_{V,G}(1) = 1$ y $R_{V,G}(p)$ es monótono creciente en $p \in [0, 1]$.
- El cálculo de la confiabilidad de una red se reduce a hallar el vector $F = (F_0, \dots, F_m)$ de coeficientes enteros.
- Los subgrafos conexos minimales son árboles. Por el Corolario 1.1.2 tienen exactamente $n - 1$ enlaces. Luego, si se remueven más de $m - n + 1$ enlaces, el subgrafo resultante no puede ser conexo: $F_i = 0$, $\forall i > m - n + 1$.
- Por el Teorema 1.2.17, la cantidad de árboles $F_{m-n+1} = \kappa(G)$ se calcula mediante el determinante de un menor del laplaciano.
- Por el Corolario 1.3.12 del Teorema de Ford y Fulkerson, es posible calcular el corte mínimo de $G = (V, E)$ tomando todos los pares de nodos distintos s y t posibles de V y aplicando el algoritmo de Ford y Fulkerson a la red obtenida con capacidades iguales a la unidad. El menor de los flujos así obtenido es $|\varphi| = c$, la menor cantidad de enlaces necesarios para desconectar G . Luego, $F_i = \binom{m}{i}$ si $i < c$.

En suma, hallar el polinomio de confiabilidad se reduce a contar grafos, y algunos de ellos se hallan trivialmente. Vamos a ver que calcular la cantidad de maneras de desconectar G de forma mínima. Precisamente, la determinación del vector $F = (F_0, \dots, F_m)$ es un problema $\#P$ -Completo. Resulta así que los métodos exactos para el cálculo de $R_{V,G}(p)$ conocidos hasta el momento son de tiempo exponencial.

Moskowitz [60] combina reducciones serie-paralelo y eliminación de enlaces irrelevantes, como también el principio de arista sustracción-contracción (o Teorema de Factorización): sea $e = \{x, y\} \in E$ un enlace arbitrario, $G - e = (V, E - e)$ la sustracción del enlace e en G , G_e una arista contracción (donde los nodos $\{x, y\}$ se identifican con uno solo de nombre x , y el grafo G_e tiene posiblemente múltiples enlaces), y K' es el nuevo conjunto de terminales luego de la identificación de los nodos x e y . Entonces:

$$R_{K,G} = (1 - p_e)R_{K,G-e} + p_e R_{K',G_e}. \quad (2.4)$$

Obsérvese que la técnica de arista sustracción-contracción de Moskowitz vale para el problema clásico de K terminales en general, con probabilidades de operación heterogéneas. La arista sustracción-contracción la verifican otros objetos combinatorios, como matroides, polinomios cromáticos y el polinomio de Tutte [43].

Satyanarayana y Chang [73] parten del Teorema de Factorización de Moskowitz, y observan que la cadena de reducciones finalizan en una cantidad de hojas que coincide con la dominancia del grafo original. En base a esta observación optimizan el método de Factorización. Se observa que el grafo G_e deja de ser simple, pues puede tener múltiples aristas compartidas entre dos nodos. No obstante, la probabilidad de tener una conexión directa entre x e y es la probabilidad de operación de alguna de tales aristas, y es simplemente la probabilidad de una unión. Entonces, es posible sustituir estas aristas múltiples por una sola, con mayor probabilidad de operación que todos los caminos individuales.

La fórmula 2.4 sugiere un método recursivo, donde es posible reiterar el proceso a cada subgrafo así obtenido. Puesto que la cantidad de subgrafos de un grafo dado G es exponencial con la cantidad de nodos de G , este método puede resultar lento en grafos de gran tamaño.

2.2 Complejidad del Problema Clásico

Michael Ball ha sintetizado elegantemente los principales resultados de complejidad del problema clásico de confiabilidad en redes [5]. Él enmarca la confiabilidad clásica en un contexto más general, de *sistemas binarios coherentes estocásticos*, que abreviaremos por sus siglas SBCE. Sean $T = \{1, 2, \dots, m\}$ un conjunto ordenado de m componentes que fallan independientemente, y una función binaria $\phi : \{0, 1\}^m \rightarrow \{0, 1\}$, tal que $\phi(x) = 1$ si el sistema está operativo al fallar sus componentes según el vector ordenado x , y $\phi(x) = 0$ en caso contrario. Diremos que el sistema es *coherente* si $\phi(0_n) = 0$, $\phi(u_n) = 1$ y si $x \leq y$ entonces $\phi(x) \leq \phi(y)$, donde dos palabras binarias x e y cumplen que $x \leq y$ si y solo si se verifica $x_i \leq y_i$ para todo bit i . Tenemos así un sistema binario coherente. Tal sistema es además estocástico cuando sus elementos fallan independientemente según ciertas probabilidades p_i . Concretamente, sea $X = (X_1, \dots, X_m)$, donde cada X_i es una variable Bernoulli independiente que representa el estado de la componente i -ésima, tal que $P(X_i = 1) = p_i$, y almacenemos las probabilidades en un vector $p = (p_1, \dots, p_m)$ (observar que $0 \leq p_i \leq 1$, pero p no es necesariamente vector estocástico). Tenemos así un SBCE, donde se denota $r(p) = P(\phi(X) = 1)$ a la confiabilidad del sistema.

Una configuración operativa x es minimal cuando $\phi(x) = 1$ y si alguna entrada de x que vale 1 es reemplazada por 0 el sistema cae, es decir, el nuevo estado x' cumple $\phi(x') = 0$. El

conjunto de todos los estados operativos minimales determina completamente el sistema. En efecto, el retículo dado por el orden binario habitual de crecimiento bit a bit con palabra mínima 0_n y máxima 1_n asigna el estado 1 a toda palabra que es cota superior de algún estado operativo minimal, y 0 en caso contrario. Análogamente, un estado de corte minimal y cumple $\phi(y) = 0$ pero al cambiar cualquier componente de falla a operación el sistema se torna operativo.

Denotemos mediante f_i a la cantidad de estados operativos con i componentes vivas (y $m - i$ en falla) de un sistema estocástico binario coherente, y $f = (f_0, \dots, f_m)$. En su artículo [5], Michael Ball prueba que la complejidad de los tres problemas siguientes es equivalente, es decir, encuentra una reducción polinomial entre cada par de tales problemas:

Definición 2.2.1 (Estimación de la Confiabilidad)

1. Entrada: (T, ϕ, p, ϵ) , siendo ϵ real positivo.
2. Salida: $r' : (1 - \epsilon)r(p) \leq r' \leq r(p)(1 + \epsilon)$.

Definición 2.2.2 (Análisis Racional de la Confiabilidad)

1. Entrada: (T, ϕ, p) , donde ahora p es vector con probabilidades racionales.
2. Salida: $r(p)$.

Definición 2.2.3 (Análisis Funcional de la Confiabilidad)

1. Entrada: (T, ϕ)
2. Salida: f

El nombre del último problema se justifica por el hecho que $r(p) = \sum_{i=0}^m f_i p^i (1 - p)^{m-i}$, y la función de confiabilidad se determina completamente al conocer el vector f . La idea de la triple equivalencia es que si disponemos estimaciones puntuales (o exactas) de la confiabilidad, la evaluación en $m + 1$ puntos permite determinar el vector f , y recíprocamente si tenemos una solución del Análisis Funcional de la Confiabilidad una directa evaluación permite resolver los otros dos problemas.

El nombrado como *problema de confiabilidad clásico* en esta monografía es un SBCE. Concretamente, dado un grafo simple $G = (V, E)$ tenemos que los componentes son las aristas: $T = E$, tenemos un conjunto auxiliar de nodos distinguidos $K \subseteq V$, llamados *terminales*, y al ordenar el conjunto de aristas $E = \{e_1, \dots, e_m\}$, para cada $x \in \{0, 1\}^m$ tendremos que $\phi(x) = 1$ si y solo si el subgrafo $G' = (V, E')$ con $E' = \{e_i \in E : x_i = 1\}$ conecta a todo par de terminales del conjunto K . Una vez que consideramos componentes binarias aleatorias (X_1, \dots, X_m) con operación independiente según el vector p tal que $p_i = P(X_i = 1)$, es posible definir $R_{K,G}(p) = P(\phi(X) = 1)$. Esta medida de confiabilidad se conoce en inglés como *K-terminal reliability*. Dos casos particulares son $K = \{s, t\}$, o *source-terminal reliability* y $K = V$, o *all-terminal reliability*. En nuestro estudio admitimos que p sea vector con probabilidades reales, mientras que en el artículo [5] se considera p como vector con entradas racionales por cuestiones de computabilidad.

Sea c la mínima cantidad de componentes que al fallar asegura el sistema en corte, y n_c la cantidad de estados del sistema en corte con c componentes fallidos. Análogamente, denotemos mediante l a la mínima cantidad de componentes vivos que asegura el sistema en funcionamiento, y n_l a la cantidad de estados en funcionamiento con l componentes vivos.

Vamos a estudiar la Confiabilidad Funcional para el problema clásico y sus casos especiales (dos terminales y todos los terminales). Para ello, vamos a valernos de la siguiente

Proposición 2.2.4 *En todo SBCE, el problema de Confiabilidad Funcional es \mathcal{NP} -Difícil si se cumple alguna de las siguientes condiciones:*

1. *El reconocimiento de un estado de operación de mínimo cardinal es \mathcal{NP} -Completo.*
2. *El reconocimiento de un estado de corte de mínimo cardinal es \mathcal{NP} -Completo.*
3. *El conteo de estados de operación de mínimo cardinal es $\#\mathcal{P}$ -Completo.*
4. *El conteo de estados de corte de mínimo cardinal es $\#\mathcal{P}$ -Completo.*
5. *La determinación del vector f es $\#\mathcal{P}$ -Completo.*

Se observa que la Condición 5 es equivalente al problema de Análisis Funcional de la Confiabilidad en un SBCE, mientras que el cálculo del vector f es al menos tan difícil como los problemas relativos a las otras cuatro condiciones.

A continuación estudiaremos la complejidad computacional de la medida de confiabilidad por casos, considerando K terminales, 2 terminales y todos los nodos terminales. Como guía principal, veremos en orden si alguna de las cinco condiciones anteriores son ciertas.

2.2.1 Confiabilidad con dos terminales

Sea $K = \{s, t\}$ el par de terminales. La Condición 1 se corresponde con hallar un camino P de largo mínimo que conecta s con t . El algoritmo de Dijkstra permite hallar el camino más corto entre dos terminales en tiempo polinomial, existiendo a la vez una amplia gama de algoritmos para resolver eficientemente este problema [59]. La Condición 2 es precisamente un corte $s - t$ de mínimo cardinal. Vimos en la Sección 1.3 de Flujos en Redes que el Algoritmo de Ford y Fulkerson halla en tiempo polinomial este número (el lector puede complementar la Sección 1.3 con el artículo original [40]). La Condición 3 se corresponde con contar la cantidad de caminos que tienen largo mínimo entre s y t . Nuevamente, este problema admite algoritmo polinomial, siendo Michael Ball y James Provan quienes lo concibieron por vez primera, basados en búsqueda en profundidad [6]. La Condición 4 se lee como la cantidad de cortes $s - t$ que tienen mínimo cardinal. Sabemos que el reconocimiento de un corte $s - t$ de cardinal mínimo se puede resolver en tiempo polinomial (Condición 1). Sin embargo, curiosamente, el respectivo problema de conteo es $\#\mathcal{P}$ -Completo [66]. Vale destacar que la Condición 5 también se cumple, como lo ha mostrado Valiant incluso antes que Ball y Provan en su artículo seminal del concepto de la clase $\#\mathcal{P}$ [76].

2.2.2 Confiabilidad con múltiples terminales

La Condición 1 se lee en este caso como encontrar un subconjunto de aristas $E' \subseteq E$ de mínimo cardinal que comunique a todos los nodos terminales. Este es el Problema de Steiner en Grafos, y pertenece a la lista inicial de 21 problemas \mathcal{NP} -Completos de Karp [48]. Luego, la evaluación de la medida clásica de confiabilidad K -terminal es un problema \mathcal{NP} -Difícil.

2.2.3 Confiabilidad con todos los terminales

Cuando todos los nodos son terminales, la Condición 1 consiste en hallar un árbol recubridor de un grafo conexo. Esto se puede hacer, por ejemplo, mediante el algoritmo de Kruskal [53]. La Condición 2 consiste en hallar el corte de cardinal mínimo en el grafo. Observemos que todo corte va a separar al menos a dos nodos, por lo que variando en todos los pares de nodos posibles $\{s, t\}$ y aplicando el Algoritmo de Ford y Fulkerson podemos encontrar los separadores de mínimo cardinal entre cada par de nodos. Luego, tomando el mínimo es posible tener el corte mínimo. El lector puede hallar un algoritmo más eficiente, también utilizando técnicas basadas en flujos en redes, en [37]. La Condición 3 admite un algoritmo de tiempo polinomial, y es el célebre resultado de Kirchhoff relativo al conteo del número de árboles de un grafo conexo [9, 50], que hemos desarrollado en la Sección 1.2. Allí hemos visto que el número de árboles se puede calcular mediante un menor principal cualquiera de la matriz laplaciana, que se puede hallar en tiempo polinomial (usando por ejemplo el algoritmo de escalerización de Gauss para llevarlo al determinante de una matriz triangular). La Condición 4 consiste en determinar el corte de cardinal mínimo, que se puede hacer mediante técnicas similares a la de dos terminales, con técnicas basadas en flujos en redes [37]. Por último, la Condición 5 es la evidencia que la confiabilidad con todos los terminales también es un problema \mathcal{NP} -Difícil. En efecto, Michael Ball y James Provan demostraron que el conteo de cortes $s-t$ en una red de dos terminales admite una reducción al problema de hallar el vector f en el caso de todos los terminales [66]. Puesto que esta es la Condición 5, tenemos que el problema de confiabilidad de todos los terminales también es \mathcal{NP} -Difícil.

2.3 Métodos Aproximados en el Problema Clásico

Una vez que se ha determinado que el problema clásico de confiabilidad es \mathcal{NP} -Difícil, la comunidad científica ha profundizado en el desarrollo de algoritmos exactos en tiempo exponencial, métodos aproximados y subclases de grafos que admiten soluciones eficientes. La literatura especializada es vasta, y nos vemos forzados a seleccionar los artículos inspiradores y más citados.

Hay una amplia familia de métodos aproximados, que apuntan a evaluar el polinomio $R_{V,G}(p)$ eficientemente para cierta probabilidad de operación $p \in [0, 1]$ fija. Diversos estimadores fueron propuestos basados en el Método de Monte Carlo. Si bien este método es ampliamente utilizado para la generación de una muestra i.i.d. de una distribución, a nivel macroscópico, este método permite simular sistemas complejos, y también ha sido utilizado tanto para problemas de conteo como de medición de volúmenes y simulación de eventos raros [39].

Fijemos $p \in [0, 1]$. El método de Monte Carlo Crudo, abreviado CMC por sus siglas inglés, toma una réplica de grafos aleatorios G_1, \dots, G_N que respetan la ley Bernoulli independiente de operación de los enlaces, es decir, $G_i = (V, (X_1^i, \dots, X_m^i))$, y se definen las variables Y^1, \dots, Y^n tales que $Y^i = \Phi(X^i)$. Puesto que Φ es una función medible y la muestra vectorial X^1, X^2, \dots, X^N es i.i.d. tenemos que Y^1, \dots, Y^N es una muestra i.i.d. Además, $P(Y^j = 1) = R_{V,G}(p)$. Por la Ley Fuerte de los grandes números, la variable aleatoria promedio \bar{Y}_N converge casi seguramente a $E(Y^j) = P(Y^j = 1) = R_{V,G}(p)$. Además, el estimador al ser un promedio muestral resulta ser insesgado. Su varianza coincide entonces con el error cuadrático medio, y vale:

$$\text{Var}(\bar{Y}_N) = \frac{\text{Var}(Y^1)}{N} = \frac{R_{V,G}(p)(1 - R_{V,G}(p))}{N}. \quad (2.5)$$

Tomando N suficientemente grande y aplicando el Teorema Central del Límite, el intervalo de confianza a nivel α para $R_{V,G}(p)$ centrado en \bar{Y}_N tiene radio ϵ aproximadamente igual a:

$$\epsilon_\alpha = \frac{z_{\alpha/2} \sqrt{R_{V,G}(p)(1 - R_{V,G}(p))}}{\sqrt{N}}, \quad (2.6)$$

siendo $z_{\alpha/2}$ la abscisa que deja área igual a $\alpha/2$ a la derecha en una densidad normal estándar Z , es decir: $P(Z > z_{\alpha/2}) = \alpha/2$. Es interesante destacar que si $R_{V,G}(p)$ es próxima a 0, entonces el error relativo E_r , que se define como el cociente entre el radio de confianza y el valor correcto, vale:

$$E_r(N, p) = \frac{z_{\alpha/2} \sqrt{(1 - R_{V,G}(p))}}{\sqrt{R_{V,G}(p)} \sqrt{N}} \approx \frac{z_{\alpha/2}}{\sqrt{R_{V,G}(p)} \sqrt{N}}. \quad (2.7)$$

Si deseamos conseguir un error relativo $E_r < u$ para cierta tolerancia u , entonces:

$$N > \frac{z_{\alpha/2}^2}{u^2} \frac{1}{R_{V,G}(p)} \quad (2.8)$$

La reducción lineal en la varianza dada por el método CMC repercute directamente en el tamaño de muestra N necesario para asegurar un error relativo debajo de cierto umbral, con nivel de confianza α . De hecho, si se desea un error relativo menor que el 1%, es decir, $u = 0,01$, y $R_{V,G}(p) = 10^{-9}$ a nivel $\alpha = 0,01$, entonces se requiere $N > 3,84 \times 10^{13}$. Este es el llamado *problema central de simulación de eventos raros*, y el pobre desempeño de CMC en este contexto motiva el desarrollo del área de simulación de eventos raros. Un enfoque se basa en definir un cambio de medida óptimo que torna más probable al evento raro, lo denominado *muestreo por importancia*. Otra técnica usual para lidiar con el evento raro utiliza la descomposición de sucesos, donde a partir de una cadena de sucesos anidados nuevamente se busca recuperar el evento raro que se halla dentro de todos los sucesos, y es por tanto más probable en las medidas condicionales. La obra de los doctores Gerardo Rubino y Bruno Tuffin [71] es un excelente tratado monográfico del problema de simulación de eventos raros basados en el método de Monte Carlo.

A efectos de comparar el rendimiento de dos estimadores insesgados para la confiabilidad, se define la *eficiencia* de un estimador de la confiabilidad mediante el inverso del producto de su varianza y el tiempo computacional necesario para la estimación:

$$ef(\hat{R}) = \frac{1}{Var(\hat{R})t_{\hat{R}}}. \quad (2.9)$$

Evidentemente, a menor varianza tendremos menor error cuadrático medio en la estimación, hecho deseable. Puesto que en la práctica el tiempo de cómputo juega un rol central, debe tenerse presente, y también se desea que sea reducido. Este tiempo dependerá del ordenador elegido, por lo que las comparaciones entre distintos estimadores deben realizarse en el mismo ordenador.

Un destacado método aproximado fue desarrollado por el Dr. Mohammed el Khadiri y Héctor Cancela, y se denomina Reducción Recursiva de la Varianza, abreviado RVR por sus siglas en inglés [20, 21]. Este método toma un corte del grafo G , asigna un orden a las aristas del corte y separa en casos mutuamente excluyentes y exhaustivos, tomando en cuenta la primera arista que falla del orden preestablecido. Dado su destacado desempeño y para ilustrar que es posible desarrollar métodos aproximados más eficientes y de menor error que Monte Carlo Crudo, describiremos las principales propiedades de RVR, siguiendo el texto original [20].

El método RVR fue originalmente propuesto para probabilidades de operación posiblemente heterogéneas $p_l, l \in E$ de un grafo simple $G = (V, E)$, donde se desea comunicar especialmente $K \subseteq V$ nodos distinguidos, denominados terminales. Denotemos $R_{K,G}$ a la probabilidad de comunicación de estos terminales, donde los nodos son perfectos pero los enlaces fallan independientemente con probabilidades $q_l = 1 - p_l$. Sean $m = |E|$, $X = (X_1, \dots, X_m)$ la variable aleatoria m -dimensional de coordenadas binarias correspondiente al estado de operación de los enlaces, y $\phi : \{0, 1\}^m \rightarrow \{0, 1\}$ la función estructura determinística, que para cada estado de enlaces retorna 1 si los terminales están comunicados en el subgrafo resultante de eliminar las aristas faltantes, y 0 en caso contrario. En estas condiciones, se desea estimar la confiabilidad K -terminal, $R_{K,G} = E(\phi(X))$.

Sea $C = \{e_1, e_2, \dots, e_l\}$ un corte de G formado por las aristas ordenadas $e_1 < e_2 < \dots < e_l$. La anticonfiabilidad de G es $Q_{K,G} = 1 - R_{K,G}$. Evidentemente, un estimador para la anticonfiabilidad define automáticamente uno para $R_{K,G}$ (tomando complemento), por lo que no perdemos generalidad si definimos un estimador para $Q_{K,G}$. Sea $Q_C = \prod_{l \in C} q_l$ la probabilidad de ocurrencia del corte C , A_C el evento en el que “ocurre el corte C ”, y B_i el evento “ e_i opera, y todas las aristas anteriores fallan”, cuya probabilidad de ocurrencia es $P(B_i) = p_i \prod_{j < i} q_j$. Observar que el conjunto de eventos $\{A_C, B_1, \dots, B_l\}$ son exhaustivos y mutuamente excluyentes. La idea es condicionar en esos eventos y reconocer subgrafos que respetan la ley de anticonfiabilidad del condicional, en forma recursiva. Si ocurre el evento B_i , entonces el grafo que respeta el condicional es $G_i = G - \{e_1, \dots, e_{i-1}\} * e_i$, es decir, se eliminan las aristas que fallaron e identifican los nodos de e_i , donde los nodos terminales serán los mismos, y el nodo identificado será terminal si y solo si alguno de los extremos de e_i era nodo terminal. Para expresar el estimador para $Q_{K,G}$ es preciso definir variables aleatorias auxiliares. Sea X_i la variable aleatoria a coordenadas binarias cuya medida de probabilidad puntual es $P(X_i = x) = P(X = x | B_i)$, para cada $x \in \{0, 1\}^m$ (es decir, la medida

condicional al evento B_i), y $Y_i = 1 - \phi(X_i)$ la indicatriz de anticonfiabilidad condicionada a B_i . La probabilidad del evento $Y = 1$ es la anticonfiabilidad, que se puede expresar de la siguiente manera: $\{Y = 1\} = A_C \cup \bigcup_{i=1}^l A_C^C \cap B_i \cap \{Y_i = 1\}$. Esta igualdad de eventos sugiere una manera recursiva para estimar $P(Y = 1)$, que va a proceder analizando grafos sucesores G_i siempre que ocurra el evento B_i . Separaremos primeramente en dos casos: si ocurre A_C o no. Para simular las probabilidades de los eventos B_i sabiendo que no ocurre A_C vamos a valernos de una variable aleatoria uniforme, de la siguiente manera. Partimos el intervalo $[0, 1]$ en l intervalos J_1, \dots, J_l , donde J_i precede a J_{i+1} en el orden real habitual y cada J_i tiene longitud igual a $P(B_i)/(1 - Q_C)$. Sea U una variable aleatoria uniforme en $[0, 1]$ que se toma independiente del estado del grafo aleatorio. Consideremos la siguiente variable aleatoria:

$$Z = Q_C + (1 - Q_C) \sum_{i=1}^l 1_{\{U \in J_i\}} Y_i \quad (2.10)$$

Vamos a ver que el valor esperado de Z coincide con $Q_{K,G}$, mientras que su varianza es menor que la varianza de Y , por lo que una técnica basada en promediar muestras independientes de Z tendrá menor error cuadrático medio que CMC. Esta idea a solas aún no permite mejorar CMC, pues es preciso estimar Y_i . Sin embargo, tomando progresivos cortes a los grafos G_i y utilizando promediados de la variable correspondiente Z_i tendremos, tras finalizar en casos triviales, menor varianza global que CMC. Precisamente, sea K_i el conjunto de terminales en el grafo G_i cuando ocurre el evento B_i . Decimos que G_i es K_i -conexo cuando todo par de nodos pertenecientes a K_i están comunicados en el grafo G_i . Se define entonces la nueva variable Y'_i de la siguiente manera:

$$Y'_i = \begin{cases} 1, & \text{si } G_i \text{ no es } K_i\text{-conexo,} \\ 0, & \text{si } G_i \text{ es un solo terminal,} \\ Z_i, & \text{en otro caso,} \end{cases}$$

donde Z_i se construye de la misma manera que para el grafo G . Esto sugiere tomar como estimador el promedio de la siguiente variable aleatoria definida recursivamente:

$$F(G, K) = \begin{cases} 1, & \text{si } G \text{ no es } K\text{-conexo,} \\ 0, & \text{si } G \text{ es un solo terminal,} \\ Q_{C(G,K)} + (1 - Q_{C(G,K)}) \sum_{i=1}^l 1_{\{U \in J_i\}} F(G_i, K_i), & \text{en otro caso,} \end{cases}$$

donde las variables uniformes U siempre se toman independientes de toda variable aleatoria previamente definida. Probemos ahora que RVR tiene menor error que CMC. Antes que nada, veamos que el estimador $\bar{F}(G, K)$ es insesgado para $Q_{G,K}$. Puesto que los eventos $\{A_C, B_1, \dots, B_l\}$ son exhaustivos y mutuamente excluyentes, por el teorema de esperanza total [74] se tiene que:

$$Q_{K,G} = E(Y) = Q_C E(Y|A_C) + \sum_{i=1}^l P(B_i) E(Y|B_i). \quad (2.11)$$

Puesto que $P(Y = 0|A_C) = 0$ y además Y es binaria, tomar valor 1, y $E(Y|A_C) = 1$. Entonces:

$$\begin{aligned} Q_{K,G} = E(Y) &= Q_C + (1 - Q_C) \sum_{i=1}^l P(B_i)/(1 - Q_C)E(Y|B_i) \\ &= Q_C + (1 - Q_C) \sum_{i=1}^l P(U \in J_i)E(Y|B_i) \\ &= Q_C + (1 - Q_C) \sum_{i=1}^l E(1_{\{U \in J_i\}})E(Y|B_i); \end{aligned}$$

Por definición tenemos que $E(Y|B_i) = E(1 - \phi(X)|B_i) = E(1 - \phi(X_i)) = E(Y_i)$. Sustituyendo:

$$\begin{aligned} Q_{K,G} &= Q_C + (1 - Q_C) \sum_{i=1}^l E(1_{\{U \in J_i\}})E(Y_i) \\ &= Q_C + (1 - Q_C) \sum_{i=1}^l E(1_{\{U \in J_i\}}Y_i) \\ &= E(Q_C + (1 - Q_C) \sum_{i=1}^l 1_{\{U \in J_i\}}Y_i) \\ &= E(Z), \end{aligned}$$

donde se ha utilizado que U es independiente de las variables Y_i . Concluimos así que $E(Z) = Q_{K,G}$, por lo que el promedio muestral \bar{F}_N es estimador insesgado, al igual que el estimador \bar{Y}_N sugerido por CMC. Veamos ahora que la varianza de Z es menor que la de Y , asegurando de esta manera que el promedio muestral \bar{F}_N tiene menor varianza que la que se consigue mediante CMC. Para probarlo, la clave es notar que la variable aleatoria $T = \sum_{i=1}^l 1_{\{U \in J_i\}}Y_i$ es Bernoulli, con esperanza $E(T) = (Q_{K,G} - Q_C)/(1 - Q_C)$. Luego:

$$\begin{aligned} Var(Z) &= Var(Q_C + (1 - Q_C)T) = (1 - Q_C)^2 Var(T) \\ &= (1 - Q_C)^2 E(T)(1 - E(T)) \\ &= (1 - Q_C)^2 \frac{Q_{K,G} - Q_C}{1 - Q_C} \frac{1 - Q_{K,G}}{1 - Q_C} \\ &= (1 - Q_{K,G})(Q_{K,G} - Q_C) \\ &\leq (1 - Q_{K,G})Q_{K,G} = Var(Y) \end{aligned}$$

En el artículo [20] se demuestra además que $Var(Z') < Var(Z)$, lo que culmina la prueba que RVR tiene menor varianza que CMC. Más aún, tras una comparación de eficiencia entre CMC y RVR se muestra una notoria ventaja de RVR. Otro elemento a destacar es que la versión de RVR aquí descrita fue ampliamente mejorada por sus autores. Una mejora introducida en [21] considera la variable multinomial que resulta de contar la cantidad de veces que resulta

favorable cada evento B_i o A_C , en cada corte, y tal agrupamiento evita la realización de experimentos en cada grafo G_i . Esencialmente, se evita la repetición de experimentos de cada uno de tales grafos, y los pesos serán tomados respetando la proporción de apariciones de cada grafo, reduciendo así el orden computacional, y por ende mejorando la eficiencia (y preservando la varianza).

Se sugiere revisar los artículos [21] para conocer detalles de la formulación algorítmica y el desempeño de RVR, superado notoriamente a las técnicas de Monte Carlo Crudo y Muestreo con Daga [54]. Otros métodos de aproximación son Entropía Cruzada [45, 52], Variables Antitéticas [34] y cotas uniformes para el polinomio en todo su dominio [15]. Aquí apenas tocamos la superficie. El lector curioso puede encontrar una síntesis de resultados enfocados en el contexto de Eventos Raros en el Capítulo 7 de la monografía [71], un resumen de la medida de confiabilidad clásica en [5] y un libro con más detalles en [29], como también de otras medidas de confiabilidad y su complejidad en [11].

2.4 Diámetro Confiabilidad de una Red

Sea $G = (V, E)$ un grafo simple, donde V es un conjunto de nodos y E de enlaces que los comunican. Consideremos además un conjunto de *terminales* $K \subseteq V$ y un entero positivo d , llamado *diámetro*. Asumiremos a lo largo de todo el texto que los nodos son perfectos, mientras que los enlaces pueden fallar en forma independiente, con probabilidades $q(xy) = 1 - p(xy)$ para cada $\{x, y\} \in E$, donde $p(xy)$ representa la probabilidad de operación del enlace $\{x, y\}$.

En la presente monografía estudiaremos el caso de probabilidades de operación idénticas: $p(xy) = p$. Se desea calcular la probabilidad $R_{K,G}^d(p)$ de que todo par de nodos distinguidos del conjunto K tenga algún camino con largo d o menos en la subred resultante de eliminar los enlaces fallidos. A este número lo denominaremos *diámetro-confiabilidad de una red*, que abreviamos DCR. El objeto de estudio es entonces una función en la variable indeterminada $p \in [0, 1]$, que asigna a cada probabilidad de operación p de los enlaces, la diámetro-confiabilidad de la red $R_{K,G}^d(p)$.

2.4.1 Subproblemas y Complejidad

Puesto que DCR es una extensión de la confiabilidad clásica de una red, la evaluación de la DCR es también un problema \mathcal{NP} -Difícil. Una vez que se conoce que DCR es \mathcal{NP} -Difícil, es natural limitar el estudio a métodos exactos para familias particulares de grafos, sub-problemas especiales de DCR, y métodos aproximados. El lector puede hallar las primeras familias recursivas de grafos que admiten cálculo en tiempo polinomial en la tesis de Pablo Sartor [72]. Además de los allí presentados, apenas se conoce fórmulas eficientes para la DCR de grafos particulares, como ciclos, caminos y pocos casos más [69, 72]. Daremos aquí mismo una discusión de la complejidad de ciertos subproblemas, y en el Capítulo 3 la introducción de nuevos métodos aproximados, basados en teoría clásica de interpolación polinómica y el método de Monte Carlo.

Es posible analizar diversos sub-problemas cuando restringimos ya sea el diámetro d o el número de terminales $|K|$. En esta subsección estudiaremos la complejidad computacional del problema en términos de $|K|$ y d , incluyendo la idea de la prueba de los resultados principales.

Los casos $d = 1$, o $d = 2$ y $|K| = 2$, son triviales [63]. De hecho, si $d = 1$ todos los terminales distinguidos deben estar conectados directamente, y $R_{K,G}^1 = \prod_{x,y \in K} p(xy)$, siendo los enlaces restantes irrelevantes en este caso. Cuando $d = 2$ y $K = \{x_1, x_n\}$, los terminales x_1 y x_n debe estar conectados directamente o bien conectados por un nodo intermedio no terminal. Sin pérdida de generalidad consideremos $V = \{x_1, x_2, \dots, x_n\}$ y el grafo completo, donde la ausencia de enlace se interpreta como probabilidad de operación nula. Entonces:

$$R_{\{x_1, x_n\}, G}^2 = 1 - (1 - p(x_1 x_n)) \prod_{j=2}^{n-1} (1 - p(x_1 x_j) p(x_j x_n)). \quad (2.12)$$

Un fuerte contraste con la simplicidad de la Expresión 2.12 es que la DCR es un problema \mathcal{NP} -Difícil cuando $|K| = 2$ y $d \geq 3$ es fijo [23]. De hecho, este subproblema se halla claramente en el conjunto \mathcal{NP} , y los autores Héctor Cancela y Louis Petingi hallaron una biyección entre los cortes de instancias particulares de la DCR con $|K| = 2$, $d \geq 3$ y el conteo de cubrimiento de vértices en grafos bipartitos, que es un problema $\#\mathcal{P}$ -Completo. La evaluación del polinomio $R_{\{s,t\}, G}^d(p)$ cuando $p = 1/2$ coincide precisamente con el número de d -caminos entre los terminales s y t , dividido entre $2^{|V|}$. De hecho, todos los subgrafos ocurren con igual probabilidad cuando $p = 1/2$. Como consecuencia, $2^{|V|} \times (1 - R_{\{s,t\}, G}^d(p))$ es el número de cortes, y el cómputo de la DCR cuando $|K| = 2$ y $d \geq 3$ es fijo es al menos tan difícil como el conteo de vértices en grafos bipartitos en general.

Una vez que sabemos que la DCR es \mathcal{NP} -Difícil cuando $|K| = 2$ y $d \geq 3$, un corolario inmediato es que la DCR es también \mathcal{NP} -Difícil si agregamos un número fijo de terminales. La clave es conectar los restantes terminales de modo trivial, y así encontrar una reducción al caso de dos terminales. Una prueba completa y rigurosa se puede encontrar en [23].

El siguiente paso natural es determinar la complejidad de DCR cuando $d = 2$. Un valioso resultado hacia tal dirección es que tal problema se halla en la clase \mathcal{P} de problemas que admiten solución polinomial por una máquina universal de Turing, siempre que $|K|$ sea un parámetro fijo. Además, la cantidad de operaciones elementales es lineal en $\min\{|V|, |E|\}$. Hay dos pruebas alternativas de este resultado. Una prueba recursiva se provee en [72]. Alternativamente una fórmula explícita para $R_{K,G}^2(p)$ se obtiene como suma de la probabilidad de todas las configuraciones operativas, tal como se demuestra en [19]. En ambas pruebas la clave es mostrar que la cantidad de tales configuraciones operativas es exponencial con el número de terminales $|K|$, que es fijo, pero lineal en el número total de nodos $|V|$ o enlaces $|E|$, que representa la variable de entrada del problema. Se reconocen las configuraciones operativas en términos de cubrimientos de vértices para K , donde sus terminales son conectados directamente o bien con nodos intermedios. La demostración halla una partición de las configuraciones operativas en base a estas estructuras combinatorias denominadas cubrimientos. El lector puede encontrar detalles en [18, 19, 72].

Es interesante observar que los casos anteriores no consideran la situación en la que $d \geq 2$ y $K = V$, o cuando K es un parámetro libre del problema. Por ejemplo, la complejidad computacional de la DCR cuando $K = V$ y $d = 2$ es aún un problema abierto. Curiosamente, si el polinomio $R_{V,G}^2(p)$ estuviese disponible, entonces $2^{|V|} \times R_{V,G}^2(\frac{1}{2})$ contaría precisamente el número de configuraciones operativas H de G con diámetro $d \leq 2$. En particular, si tomáramos el grafo completo $G = K_n$ estaríamos aptos para contar todos los subgrafos de

K_n con diámetro 2. Esto significa que la evaluación de la DCR cuando $K = V$ y $d = 2$ es al menos tan difícil como contar la cantidad de grafos de diámetro 2 y orden dado.

Como consecuencia, los problemas abiertos de la DCR están estrechamente relacionados con teoría de grafos, y una nueva caracterización de grafos con diámetro 2 daría pistas para determinar la complejidad de la DCR en casos especiales.

En la Figura 2.1 se resume la complejidad computacional de la DCR en términos del diámetro d y la cantidad de terminales $|K|$, indicando asimismo los trabajos donde cada resultado fue probado por primera vez. El lector puede apreciar que la caracterización de la complejidad computacional del problema cuando el número de terminales $|K|$ es un parámetro de entrada libre es un problema abierto. La complejidad del caso en que $K = V$ y $d = 2$ es también un problema abierto.

| | | $ K $ (fijo) | | $ K = n$ o libre |
|--|----------|------------------------------|-------------|-------------------|
| | | 2 | 3... | |
| | 2 | $O(n)$ [23] | $O(n)$ [19] | Desconocida |
| | 3 | \mathcal{NP} -Difícil [23] | | Desconocida |
| | \vdots | | | |
| | d | \mathcal{NP} -Difícil [66] | | Desconocida |
| | \vdots | | | |
| | $n - 2$ | \mathcal{NP} -Difícil [66] | | Desconocida |
| | $n - 1$ | | | |
| | \vdots | | | |

Figura 2.1: Complejidad de la DCR en términos del diámetro d y la cantidad de terminales $|K|$

Para tornar autocontenida esta discusión de complejidad computacional se detallan las pruebas de cada caso, incluyéndose aquí una traducción lo más fiel posible de los textos originales, invitando al lector a las citas correspondientes.

Téngase presente que el problema general es \mathcal{NP} -Difícil [5]. La idea de esta prueba se puede encontrar también en la Subsección 2.2. El lector puede observar de la Tabla 2.1 que los casos en que el parámetro $|K|$ es una entrada libre y $d \leq 2$ es fijo permanecen abiertos, por lo que daremos apartados discutiendo según una cantidad de terminales $|K|$ fija.

2.4.1.1 Red con dos terminales

Ya hemos visto que el subproblema de diámetro $d = 2$ con dos terminales pertenece a la clase \mathcal{P} , y una expresión exacta para la DCR es (2.12). Un fuerte contraste con este resultado lo brinda la siguiente:

Proposición 2.4.1 [23] *La evaluación de la DCR cuando $|K| = 2$ y $d \geq 3$ es un problema \mathcal{NP} -Difícil.*

Prueba. Probaremos primero que el conteo de Cubrimiento de Bipartitos admite una reducción polinomial al conteo de Cortes en una red de dos terminales. Puesto que el reconocimiento de cortes en una red es polinomial, tendremos que el conteo de Cortes en una red de dos terminales es un problema $\#\mathcal{P}$ -Completo.

Sea $d' = d - 3 \geq 0$ y $P = (V(P), E(P))$ un camino con nodos $V(P) = \{s, s_1, \dots, s_{d'}\}$ y aristas $E(P) = \{\{s, s_1\}, \{s_1, s_2\}, \dots, \{s_{d'-1}, s_{d'}\}\}$ (el caso $d' = 0$ es un solo nodo). Dado un grafo bipartito $G = (X \cup Y, E)$ con $E \subseteq X \times Y$, construimos un grafo aleatorio $G' = (X \cup Y \cup V(P) \cup \{t\}, E \cup E(P) \cup \{\{s_{d'}, x\}, x \in X\}) \cup \{\{y, t\}, y \in Y\})$, donde todos sus enlaces operan perfectamente salvo los que pertenecen al conjunto $\{\{s_{d'}, x\}, x \in X\} \cup \{\{y, t\}, y \in Y\}$, que tienen probabilidad de operación igual a $1/2$. Tomemos el par de nodos $K = \{s, t\}$ como terminales que se desean comunicar en G' . El grafo aleatorio G' se ilustra en la Figura 2.2. Esta reducción es polinomial.

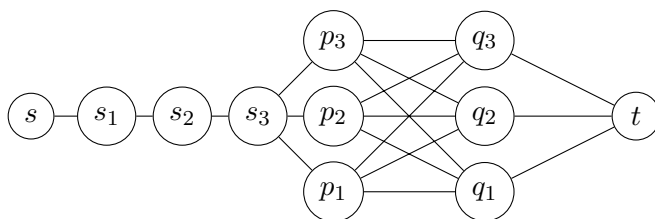


Figura 2.2: Ejemplo concreto de construcción de grafo auxiliar G' , con terminales $\{s, t\}$, $d = 6$ (camino de largo $d' = 3$), seguido de bipartito completo $K_{3,3}$ y terminal t .

A cada cubrimiento $C_X \cup C_Y$ del bipartito G , donde $C_X \subseteq X$ y $C_Y \subseteq Y$, le asignamos el corte $C = \{\{s_{d'}, x\}, x \in C_X\} \cup \{\{y, t\}, y \in C_Y\} = \varphi(C_X \cup C_Y)$. Para cada enlace de la forma $\{x, y\}$ con $x \in X$ e $y \in Y$ debemos tener $x \in C_X$ o $y \in C_Y$, por lo que no hay camino entre s y t . Luego C es efectivamente un corte de G' , por lo que φ está bien definida, y es inyectiva. Veamos que también es sobre: el complemento de todo cubrimiento de vértices es un conjunto de vértices independientes. Luego, si $C = \{\{s_{d'}, x\}, x \in A \subseteq X\} \cup \{\{y, t\}, y \in B \subseteq Y\}$ pertenece al conjunto de cortes \mathcal{C} (que incluye únicamente falla de enlaces con operación imperfecta) tenemos que $A \cup B$ es cubrimiento de vértices, por lo que φ es biyectiva.

Veamos por último que si disponemos de $R_{\{s,t\},G'}(p)$ entonces podemos calcular la cantidad de cortes de G' , resolviendo por ende el problema de conteo de cubrimiento de bipartitos. En efecto, bajo equiprobabilidad en los enlaces imperfectos tenemos que todos los subgrafos factibles son igualmente probables. Luego, $R_{\{s,t\},G'}(1/2) = 1 - \frac{|C|}{2^{|X|+|Y|}}$. En resumen tenemos que la cantidad de cubrimiento de bipartitos coincide con los cortes de la red G' : $|\mathcal{B}| = |\mathcal{C}|$, y además:

$$|\mathcal{B}| = 2^{|X|+|Y|} (1 - R_{\{s,t\},G'}(1/2))$$

Luego, si podemos hallar $R_{\{s,t\},G'}(p)$ entonces es posible hallar la cantidad de cubrimientos de un grafo bipartito G arbitrario mediante una reducción polinomial, y la evaluación de

$R_{\{s,t\},G'}(p)$ es \mathcal{NP} -Difícil, como se quería demostrar.

QED

2.4.1.2 Red con más de dos terminales

Cuando el diámetro es $d \geq 3$, la Proposición 2.4.1 se generaliza al caso de más de dos terminales, y el correspondiente subproblema de DCR es nuevamente \mathcal{NP} -Difícil. La idea es extender una red de dos terminales conectando trivialmente nuevos terminales, y utilizando precisamente la reducción anterior. Precisamente, se conectan a todos los terminales con enlaces perfectos directos salvo el par de terminales s y t , vinculados de la misma manera que con el grafo G' . Un grafo similar al recién expuesto se detalla en la fuente [23].

Falta ahora determinar la complejidad del problema con una cantidad $|K|$ finita de terminales de entrada, con diámetro $d = 2$. Veremos a continuación que el problema pertenece a la clase \mathcal{P} de problemas que admiten algoritmo de evaluación en tiempo polinomial. Sea $G = (V, E)$ un grafo simple, $K \subseteq V$ el conjunto de terminales con cardinal $|K|$ finito, $|V| = n$ y $p(xy)$ la probabilidad de operación del enlace $\{x, y\} \in E$; si $\{x, y\} \notin E$ definimos $p(xy) = 0$. En este contexto las configuraciones operativas son los enlaces $H \subseteq E$ tales que todo par de terminales $x, y \in K$ están conectados directamente o bien admiten un camino de largo 2 en H . Diremos simplemente configuraciones operativas, valiéndonos del contexto. Para demostración utilizaremos la siguiente notación:

- $n' = n - |K|$;
- $\mathcal{O}_K^2(E)$ es el conjunto de configuraciones operativas determinadas por E y K (siguiendo la notación de [64]);
- $X^m = \prod_{i=1}^m X$;
- $X^{\{m\}} = \{Y \subseteq X : |Y| = m\}$;
- $X^{(m)} = \{Y \in X^m : i \neq j \rightarrow Y_i \neq Y_j\}$;
- $(a_1, a_2, \dots, a_n) \otimes (b_1, b_2, \dots, b_n) = \{(a_1, b_1), (a_2, b_2), \dots, (a_n, b_n)\}$;
- $\mathcal{P}(A) = \{B : B \subseteq A\}$.

Diremos que un *requerimiento* $\{x, y\} \in K^{\{2\}}$ es *satisfecho* si hay conexión entre x e y por camino de largo 1 o 2.

La idea de la prueba consiste en hallar primeramente una expresión analítica para $R_{K,G}^2$. Para ello partimos el conjunto $\mathcal{O}_K^2(E)$ en eventos disjuntos. Luego construiremos una función $f : \mathcal{O}_K^2(E) \rightarrow A$ sobre un codominio discreto elegido adecuadamente A para hallar la probabilidad del dominio tomando los eventos que son preimágenes de A :

$$R_{K,G}^2 = P(\mathcal{O}_K^2(E)) = \sum_{a \in A} P(f^{-1}(a)), \quad (2.13)$$

donde el conjunto A se define así:

$$A = \bigcup_{\ell=0}^{n'} \left((V \setminus K)^{(\ell)} \otimes \mathcal{P}(K)^{(\ell)} \right).$$

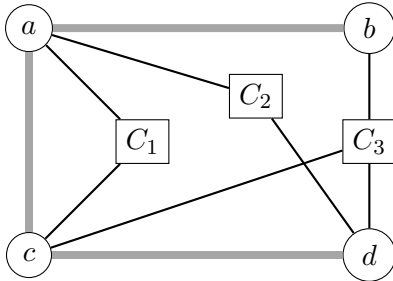
Cada elemento de A es un conjunto $\{\{t_1, C_1\}, \dots, \{t_k, C_k\}\}$ de pares (t_i, C_i) , siendo t_i un nodo de $V \setminus K$ y C_i un subconjunto de K . Cada elemento de A es una colección de conjunto de enlaces entre nodos no terminales y terminales, que pertenecen a alguna configuración operativa (además de enlaces directos entre terminales). Observar que los enlaces que inciden en nodos no terminales son irrelevantes, y los podemos eliminar por completo de nuestro estudio, pues su presencia o ausencia no interviene en las configuraciones operativas (no son parte de ninguna configuración minimal). Definiremos la función f luego por la Expresión (2.14). Mostraremos primero que A se puede construir de modo que la sumatoria de $P(f^{-1}(a))$, $a \in A$ involucre una cantidad de operaciones elementales que es un polinomio en n , para luego concluir con un estudio más fino que es de hecho lineal en n .

Asumamos sin pérdida de generalidad un orden estricto en V . Para partir el conjunto $\mathcal{O}_K^2(E)$ adoptaremos la siguiente:

Definición 2.4.2 Diremos que una familia $\mathcal{C} \subseteq \mathcal{P}(K)$ cubre K para $F \subseteq K^{\{2\}}$, y lo denotaremos con $\mathcal{C} \sqsupseteq_F K$, si en cada requerimiento xy al menos una de las siguientes tres condiciones es cierta:

- i $xy \in F$,
- ii $\exists z \in K : \{xz, zy\} \subseteq F$,
- iii $\exists C \in \mathcal{C} : \{x, y\} \subseteq C$.

La Figura 2.3 ilustra este concepto de cubrimiento. Las líneas gruesas representan los elementos de F . Los nodos conectados por líneas delgadas a los nodos cuadrados representan cada elemento de $\mathcal{C} = \{C_1, C_2, C_3\}$. La Condición 2.4.2.i aplica para los pares ab, ac y cd . La Condición 2.4.2.ii aplica para bc y ad , mientras que la 2.4.2.iii aplica para ac, ad, bc, bd y cd . Como todos los pares satisfacen al menos una de las tres condiciones, tenemos que $\mathcal{C} \sqsupseteq_F K$.



$$\begin{aligned} K &= \{a, b, c, d\} \\ F &= \{ab, ac, cd\} \\ \mathcal{C} &= \{\{a, c\}, \{a, d\}, \{b, c, d\}\} \end{aligned}$$

Figura 2.3: Ejemplo de cubrimiento

Si $E' \in \mathcal{O}_K^2(E)$, entonces la familia $\mathcal{C}_{E'}$ definida por el conjunto

$$\mathcal{C}_{E'} = \{C_{E'}(t) : t \in V \setminus K\} \quad \text{siendo } C_{E'}(t) = \{x \in K : xt \in E'\},$$

cubre K para $F = E' \cap K^{\{2\}}$. Diremos que E' genera $\mathcal{C}_{E'}$.

Recíprocamente, dado un cubrimiento \mathcal{C} de K para F , si $|\mathcal{C}| \leq n - |K|$ entonces existe algún conjunto E' que genera \mathcal{C} ; por ejemplo $E' = \{xy \in E : xy \in F \vee (\exists C \in \mathcal{C} : \{x, y\} \subseteq C)\}$ es una configuración operativa.

Las definiciones precedentes relacionan con los estados operativos de la siguiente manera. Asumamos que los elementos de F corresponden exactamente con los enlaces que inciden directamente en los terminales que operan en cierto momento. Supongamos además que cada elemento $C \in \mathcal{C}$ representa un nodo de $V \setminus K$ cuyos vecinos (ignorando enlaces no operativos), son precisamente los elementos de C (es decir, C_1, C_2, C_3 en la Figura 2.3). Entonces, $\mathcal{C} \sqsupseteq_F K$ implica que cada requerimiento es satisfecho en ese instante. El conjunto de partes de K , $\mathcal{P}(K)$, tiene $2^{|K|}$ elementos. El conjunto de sus partes, $\mathcal{P}(\mathcal{P}(K))$, tiene $2^{(2^{|K|})}$ elementos. Luego, una cota para el número de familias \mathcal{C} para las cuales $\mathcal{C} \sqsupseteq_F K$ es $2^{(2^{|K|})}$, que depende únicamente de $|K|$.

Cuando se considera la familia $\mathcal{C}_{E'}$, si existen dos nodos $t \neq t' \notin K$ con $C_{E'}(t) = C_{E'}(t')$, es posible eliminar t o t' del grafo G , obteniendo aún la misma familia $\mathcal{C}_{E'}$. Por ejemplo, en la Figura 2.3, la adición de un nodo C_4 con vecinos a y c en K no haría la diferencia para producir $\mathcal{C}_{E'}$, puesto que existe un nodo C_1 que tiene exactamente los mismos vecinos en K . En general, dado un camino E' y un elemento C de un cubrimiento $\mathcal{C}_{E'}$, existe uno o más elementos $t \in V \setminus K$ tales que $C_{E'}(t) = C$. Sea $t_{E'}(C)$ el mínimo de ellos al considerar el orden de V , es decir:

$$t_{E'}(C) = \min\{t \in V \setminus K : C_{E'}(t) = C\}.$$

Luego, a cada configuración operativa E' le asignamos exactamente un conjunto $\{t_1, t_2, \dots, t_\ell\}$ y un cubrimiento $\mathcal{C}_{E'} = \{C_1, C_2, \dots, C_\ell\}$ para $F = E' \cap K^{\{2\}}$, tal que $t_i = t_{E'}(C_i) \forall i = 1, \dots, \ell$. Consideremos la función f definida de la siguiente manera:

$$f(E') = \{(t_1, C_1), (t_2, C_2), \dots, (t_\ell, C_\ell)\}. \quad (2.14)$$

Dados $x \in V \setminus K$ y $C \subseteq K$, denotemos mediante $P(x, C)$ al suceso donde los vecinos del nodo x que pertenecen a K y son conectados por enlaces operativos son exactamente los elementos de C . Su probabilidad, denotada $p(x, C)$, vale:

$$p(x, C) = \prod_{y \in C} p(xy) \prod_{y \in K \setminus C} (1 - p(xy)).$$

Estamos en condiciones de definir la siguiente partición para $\mathcal{O}_K^2(E)$, que será clave para la demostración del resultado principal cuando el diámetro es $d = 2$.

Definición 2.4.3 *Dados $C_1, \dots, C_\ell \subseteq K$ y $t_1, \dots, t_\ell \in V \setminus K$ tales que $t_i < t_{i+1} \forall i = 1, \dots, \ell - 1$, se define el suceso $(t_1, \dots, t_\ell, C_1, \dots, C_\ell)$ que cumple las siguientes condiciones:*

- *los nodos t_1, \dots, t_ℓ están conectados directamente a C_1, \dots, C_ℓ de K , respectivamente;*
- *los nodos t con $t < t_1$ no tienen vecinos dentro de K ;*

- los nodos t con $t_i < t < t_{i+1}$ no tienen vecinos dentro de K o bien tienen exactamente como vecinos a uno de C_0, \dots, C_i para $i \in \{0, \dots, \ell - 1\}$;
- los nodos t con $t_\ell < t$ no tienen vecinos dentro de K , o bien tienen exactamente como vecinos a uno de C_1, \dots, C_ℓ .

Por definición tenemos que:

$$\begin{aligned}
 p(t_1, \dots, t_\ell, C_1, \dots, C_\ell) &= \left[\prod_{t < t_1} p(t, \emptyset) \right] p(t_1, C_1) \times \\
 &\quad \left[\prod_{t_1 < t < t_2} [p(t, \emptyset) + p(t, C_1)] \right] p(t_2, C_2) \times \\
 &\quad \left[\prod_{t_2 < t < t_3} [p(t, \emptyset) + p(t, C_1) + p(t, C_2)] \right] p(t_3, C_3) \times \dots \times \\
 &\quad \left[\prod_{t_{\ell-1} < t < t_\ell} [p(t, \emptyset) + p(t, C_1) + \dots + p(t, C_{\ell-1})] \right] p(t_\ell, C_\ell) \times \\
 &\quad \left[\prod_{t_\ell < t} [p(t, \emptyset) + p(t, C_1) + \dots + p(t, C_\ell)] \right]
 \end{aligned}$$

Para dar una expresión más compacta, definamos t_0 y $t_{\ell+1}$ como “nodos virtuales”, tales que $t_0 < t_1$, $t_\ell < t_{\ell+1}$, y $C_0 = \emptyset$. Luego:

$$p(t_1, \dots, t_\ell, C_1, \dots, C_\ell) = \left[\prod_{i=1}^{\ell} p(t_i, C_i) \right] \left[\prod_{i=0}^{\ell} \prod_{t_i < t < t_{i+1}} \sum_{j=0}^i p(t, C_j) \right]. \quad (2.15)$$

Observemos que los términos de $p(t, \emptyset) + p(t, C_1) + \dots + p(t, C_j)$ corresponden con las probabilidades de eventos disjuntos, por la definición de $P(x, C)$ (ver el uso de la palabra “exacta” de la Definición 2.4.3). Luego, la probabilidad de una configuración operativa E' generada por el cubrimiento $\{C_1, C_2, \dots, C_\ell\}$ y las ℓ -uplas $(t_1, t_2, \dots, t_\ell)$ con $t_{E'}(C_i) = t_i \quad \forall i \in 1, \dots, \ell$ es:

$$p(\{E' : \mathcal{C}_{E'} = \{C_1, \dots, C_\ell\} : t_{E'}(C_i) = t_i\}) = p(t_1, \dots, t_\ell, C_1, \dots, C_\ell). \quad (2.16)$$

Finalmente, de las Expresiones (2.13) y (2.16):

$$R_{K,G}^2 = \sum_{F \subset K^{(2)}} \prod_{e \in F} p(e) \prod_{e \in K^{(2)} \setminus F} (1 - p(e)) \sum_{\substack{(C_1, \dots, C_\ell) \in \mathcal{P}(K)^{(\ell)} \\ \{C_1, \dots, C_\ell\} \sqsupseteq_F K}} \sum_{\substack{(t_1, \dots, t_\ell) \in (V \setminus K)^{(\ell)} \\ t_i < t_{i+1}, i=1, \dots, \ell-1}} p(t_1, \dots, t_\ell, C_1, \dots, C_\ell). \quad (2.17)$$

donde la segunda suma varía en todos los cubrimientos de K para F que tienen ℓ elementos entre 0 y $\max(n', 2^{\lfloor 2^{K_1} \rfloor})$ (recordemos que un cubrimiento es un conjunto, y como tal sus elementos son diferentes). Ahora tenemos todos los ingredientes para el siguiente:

Lema 2.4.4 [19] *La evaluación de la DCR cuando $d = 2$ y $|K|$ es fijo pertenece a la clase \mathcal{P} de problemas que admiten algoritmo de tiempo polinomial.*

Prueba. La primera suma de (2.17) tiene $2^{\binom{|K|}{2}}$ términos. La segunda suma no tiene más de $2^{(2^{|K|})}(\ell!)$ términos tales que $\ell \leq 2^{(2^{|K|})}$. La tercera suma tiene $\binom{n'}{\ell}$ términos. Las productorias involucran $\binom{|K|}{2}$ productos. El cálculo de $p(t_1, \dots, t_\ell, C_1, \dots, C_\ell)$ requiere n productos, y una cantidad de sumas acotada por $(\ell + 1)n$. En efecto, si denotamos τ_i a la posición de t'_i con el orden relativo a $V \setminus K$, el número de sumas es igual a $2(\tau_2 - \tau_1 - 1) + 3(\tau_3 - \tau_2 - 1) + \dots + \ell(\tau_\ell - \tau_{\ell-1} - 1) + (\ell + 1)(n - \tau_\ell) = -2 - 3 - \dots - \ell - 2\tau_1 - \tau_2 - \tau_3 - \dots - \tau_\ell + (\ell + 1)n < (\ell + 1)n$. Luego, la cantidad de operaciones elementales (sumas y productos) requeridas para calcular $R_{K,G}^2$ tiene orden

$$2^{\binom{|K|}{2}} \binom{|K|}{2} 2^{(2^{|K|})} 2^{(2^{|K|})!} (n')^{2^{(2^{|K|})}} n(2^{(2^{|K|})} + 2), \quad (2.18)$$

que es un polinomio en n de grado $2^{(2^{|K|})} + 1$.

QED

La enumeración de los conjuntos $\mathcal{P}(K^{(2)})$, $\{\mathcal{C} \sqsubset_F K\}$ y $(V \setminus K)^{(\ell)}$ se puede realizar en una cantidad de pasos lineal en su tamaño. Entonces, el orden de la complejidad computacional de las tres sumas coincide con la cantidad de términos. Ahora veamos que la complejidad de la evaluación de la DCR es, de hecho, lineal en n . Es suficiente mostrar que la última suma de (2.17) se puede realizar en un tiempo lineal en n , dado que las restantes sumatorias y productorias agregan productos que dependen únicamente de $|K|$, que es una constante. Para simplificar notación asumiremos que $V \setminus K = \{1, \dots, n'\}$. Por (2.15), la última suma de la Expresión (2.17) coincide con la sumatoria de todos los productos de la forma

$$p(1, C_{a_1})p(2, C_{a_2}) \dots p(n', C_{a_{n'}})$$

donde $a_t \in \{0, 1, \dots, \ell\}$ (usando que $C_0 = \emptyset$) y hay ℓ enteros t_i con $0 < t_1 < \dots < t_\ell \leq n'$ tales que:

- $a_{t_i} = i \quad \forall i \in \{1, \dots, \ell\}$,
- si $t < t_1$ entonces $a_t = 0$,
- si $t_i < t < t_{i+1}$ con $i \in \{1, \dots, \ell - 1\}$ entonces $a_t \in \{0, \dots, i\}$,
- si $t > t_\ell$, entonces a_t es un entero entre 0 y ℓ .

Estos productos se pueden corresponder con caminos dirigidos en el grafo siguiente:

Definición 2.4.5

$$G = (\{1, \dots, n'\} \times \{0, \dots, \ell\}^2, \vec{E})$$

$$E = \{((t, a, b), (t + 1, a', b')) : t \leq n' - \ell, t \leq b + 1, 0 \leq a' \leq b + 1, b' = \max(a', b)\} \cup$$

$$\{((t, a, b), (t + 1, a', b')) : n' - \ell \leq t \leq n' - \ell + b, \ell - (n' - t) < a' \leq b + 1, b' = \max(a', b)\}$$

que van del vértice $(1, 0, 0)$ al (n', \cdot, ℓ) . Cada vértice (t, a, b) se asocia con la probabilidad $p(t, C_a)$. La variable b acumula la cantidad de nodos de t_1, \dots, t_ℓ ya visitados cuando t va de $t = 1$ a $t = n'$; mientras que a representa a los posibles conjuntos involucrados en el suceso $p(t, C_a)$.

Estamos en condiciones de concluir el resultado principal:

Teorema 2.4.6 [19] *La complejidad computacional de la evaluación de la DCR es lineal en $|V|$ cuando $d = 2$ y $|K|$ es fijo.*

Prueba. Mediante programación dinámica es posible calcular la última suma de la Expresión (2.17), procediendo de los vértices de la forma (n', \cdot, ℓ) hacia atrás, hasta alcanzar $(1, 0, 0)$. En cada paso, se asigna el valor $s(t, a, b)$ al vértice (t, a, b) de la siguiente manera:

$$s(t, a, b) = \begin{cases} p(t, C_a) & \text{si } t = n', \\ p(t, C_a) \sum_{(t,a,b) \rightsquigarrow (t+1,a',b')} s(t+1, a', b') & \text{si } 0 < t < n'. \end{cases}$$

Luego la cantidad de operaciones para computar la última suma de (2.17) no excede la cantidad de enlaces del grafo \vec{G} , y está acotada por $(n' - 1)\ell^2$, multiplicado por el grado máximo posible ℓ^2 , es decir, $(n' - 1)\ell^4$. Esto es lineal en n , completando la demostración.

QED

2.4.2 Cálculo exacto en casos especiales

Es posible efectuar un cálculo exacto y eficiente de familias especiales de subgrafos. Para conseguir familiaridad, realicemos primeramente el cálculo de la DCR para caminos y ciclos. Luego haremos un cálculo más sofisticado de la DCR, para la familia de grafos escalera. En la tesis [72] el lector puede encontrar el cálculo de otra familia de *escaleras generalizadas y abanicos españoles*. Es interesante el estudio de la DCR en otras familias de grafos, pues poco es lo conocido hasta el momento.

Calculemos primero la DCR de un camino simple $P = (V(P), E(P))$, con $V(P) = \{v_0, \dots, v_{n-1}\}$, $K = \{v_0, v_{n-1}\}$, $E(P) = \{\{v_i, v_{i+1}\}, i = 0, \dots, n-2\}$ y respectivas probabilidades de operación $p(v_i v_{i+1})$. Para que se puedan comunicar los terminales es preciso que todos los enlaces de $E(P)$ operen, por lo que $R_{\{v_0, v_{n-1}\}, P}^d \leq \prod_{i=0}^{n-2} p(v_i v_{i+1})$. Si el diámetro es $d < n - 1$, no existe camino entre los terminales de largo d o menor, por lo que $R_{\{v_0, v_{n-1}\}, P}^d = 0$. En otro caso, $R_{\{v_0, v_{n-1}\}, P}^d = \prod_{i=0}^{n-2} p(v_i v_{i+1})$, que coincide con la confiabilidad clásica. El lector puede generalizar a casos de múltiples terminales dentro de un camino, donde va a ser preciso que los caminos que delimita cada par de terminales permanezca en operación, y la expresión se extiende a otras productorias.

Sea ahora C_n un ciclo de n vértices con nodos $\{v_0, \dots, v_{n-1}\}$ conectados en ciclo, siguiendo el orden de escritura junto con $\{v_{n-1}, v_0\} \in E(C_n)$, y probabilidades de operación $p(v_i v_{i+1}), i = 0, \dots, n-1$, tomando el índice con módulo n . Estudiemos el caso de dos terminales $K = \{v_0, v_i\}$, con $i \neq 0$. Notemos que existen exactamente dos caminos entre v_0 y v_i en C_n , y la distancia entre estos nodos vale $d(v_0, v_i) = \min\{i, n - i\}$. Sin pérdida de generalidad asumamos que $d(v_0, v_i) = i$ (si no, cambiamos los subíndices de los nodos

según $i \rightarrow n - i$ en módulo n). Si el diámetro vale $d < i$, claramente $R_{\{v_0, v_i\}, C_n}^d = 0$. Si $i \leq d < n - i$, entonces el camino más corto que une v_0 con v_i debe estar operativo, y $R_{\{v_0, v_i\}, C_n}^d = \prod_{j=0}^{i-1} p(v_j v_{j+1})$. Por último, si $d \geq n - (j - i)$, uno de los dos caminos que unen v_0 con v_i deben operar, y $R_{\{v_0, v_i\}, C_n}^d = 1 - (1 - \prod_{j=0}^{i-1} p(v_j v_{j+1}))(1 - \prod_{j=i}^{n-1} p(v_j v_{j+1}))$, siendo $v_n = v_0$. Es posible generalizar para más terminales de manera análoga.

Otro caso elemental es el grafo bipartito completo, que tiene diámetro 2 y es 2-crítico como también 3-crítico. Esto implica que la DCR del bipartito $G = (X \cup Y, X \times Y)$ en el caso de todos los terminales $K = V$ es $R_{V,G}^2 = R_{V,G}^3 = \prod_{\{x,y\} \in X \times Y} p(xy)$.

Vamos ahora a un cálculo más sofisticado que admite una expresión eficiente del punto de vista computacional de una familia especial de grafos, que aquí llamaremos *grafos escalera* y denotaremos \mathcal{G}_h . Pese a ser una familia arbitraria de topologías, ilustra la existencia de ciertas estructuras de redes que admiten evaluación eficiente de la DCR. Veremos que en el caso DCR de dos terminales puede computarse la DCR de cualquier miembro de \mathcal{G}_h en tiempo polinomial.

Definición 2.4.7 *Dado un entero positivo h , llamaremos \mathcal{G}_h a la familia de grafos no dirigidos $G = (V, E)$ tales que:*

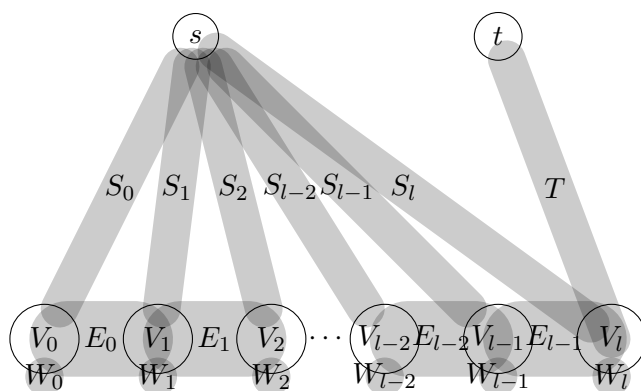
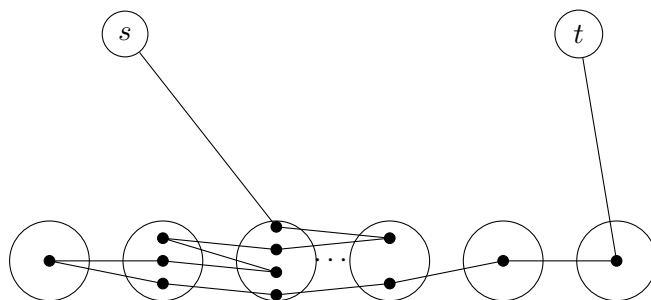
- l es un entero positivo o cero;
- V es una partición $\{s\}, V_0, V_1, \dots, V_l, \{t\}$ con $|V_i| \leq h, i = 0, \dots, l$;
- E es una partición $E_0, \dots, E_{l-1}, S_0, \dots, S_l, W_0, \dots, W_l, T$;
- $E_i \subseteq \{\{x, y\} : x \in V_i, y \in V_{i+1}\} \quad , i = 0, \dots, l - 1$;
- $S_i \subseteq \{\{s, x\} : x \in V_i\} \quad , i = 0, \dots, l$;
- $W_i \subseteq \{\{x, y\} : x, y \in V_i\} \quad , i = 0, \dots, l$;
- $T \subseteq \{\{t, x\} : x \in V_l\}$.

La Figura 2.4 ilustra la estructura de un miembro de la familia \mathcal{G}_h . Las líneas grises representan un conjunto de aristas que unen a diferentes componentes de V . La mínima distancia posible entre s y t es 2, gracias a la existencia de caminos $s - x - t$, siendo $x \in V_l$. Por ejemplo, la Figura 2.5 muestra un camino cuya secuencia de subíndices en V baja dos veces. Esto elimina la posibilidad de hallar las distancias entre s y otro nodo cualquiera de V_i solamente con los subíndices hasta i . Es preciso más información, que será la distancia entre cada par de nodos de V_i , considerando únicamente las aristas con subíndices menores o iguales a i .

Describiremos un algoritmo para calcular la DCR de cualquier red en \mathcal{G}_h , y probaremos que es de tiempo polinomial en el número de nodos. A tales efectos, será preciso probar el siguiente

Lema 2.4.8 [72] *Sea $G = (V, E)$ un grafo simple; u, v, t, w nodos cualesquiera de V con $u \neq v$ y $t \neq w$; $d_{u,v}$ la distancia entre u y v en G . Entonces, la distancia entre t y w en el grafo $G' = (V, E \cup \{u, v\})$ (que se denota $d'_{t,w}$) vale*

$$d'_{t,w} = \min\{d_{t,w}, 1 + d_{t,u} + d_{v,w}, 1 + d_{t,v} + d_{u,w}\}$$

Figura 2.4: La familia de grafos \mathcal{G}_h Figura 2.5: Ejemplo de camino s, t en relación con la secuencia de conjuntos V_i

Prueba. Para cada camino que conecta t y w en G' , exactamente una de las tres siguientes condiciones aplican para la traza correspondiente de t a w :

- (i) no usa la arista $\{u, v\}$;
- (ii) usa la arista $\{u, v\}$ y visita u antes que v ;
- (iii) usa la arista $\{u, v\}$ y visita v antes que u .

Sean d_0 , d_1 y d_2 los largos de caminos más cortos entre caminos $t \rightarrow w$ en G' para las cuales (i), (ii) y (iii) son ciertas, respectivamente (o ∞ si no existe tal camino). Tenemos que

- $d_0 = d_{t,w}$;
- $d_1 = d'_{t,u} + 1 + d'_{v,w} = d_{t,u} + 1 + d_{v,w}$;
- $d_2 = d'_{t,v} + 1 + d'_{u,w} = d_{t,v} + 1 + d_{u,w}$.

Luego, el camino más corto entre t y w en G' tendrá una distancia igual a $\min\{d_0, d_1, d_2\}$.

QED

Lema 2.4.9 Sea $G = (V, E)$ un grafo simple, $H \subseteq V$, $d_{u,v}$ la distancia entre u y v en G para cada $u, v \in H$, y $E' \subseteq \{\{u, v\} : u, v \in H\}$ un conjunto de aristas cuyos nodos pertenecen a H . Entonces, el conjunto de todas las distancias $d'_{u,v} : u, v \in H$ entre nodos de H en $G' = (V, E \cup E')$ pueden hallarse sabiendo solamente $d_{u,v} : u, v \in H$, en una cantidad de operaciones elementales de orden $O(|H|^4)$.

Prueba. Presentaremos un algoritmo que retorna las distancias deseadas con una cantidad de operaciones de orden $O(|H|^4)$. Consideremos el Procedimiento *Nuevas – Distancias*:

Procedimiento *Nuevas – Distancias*

Entradas: (H, d, E')

Salidas: d

- 1: **Para todo** $\{u, v\} \in E'$
- 2: **Para todo** $\{x, y\} \in \{\{t, w\} : t, w \in H\}$
- 3: $d'_{x,y} \leftarrow \min\{d_{x,y}, 1 + d_{x,u} + d_{v,y}, 1 + d_{x,v} + d_{u,y}\}$
- 4: **Fin Para**
- 5: $d \leftarrow d'$
- 6: **Fin Para**
- 7: **Retornar** d

Figura 2.6:

El ciclo interior tiene, a lo sumo, $|H|(|H| - 1)/2$ iteraciones. Cada una incluye cuatro sumas, una comparación de mínimo entre tres elementos y una asignación; es decir, un número constante de operaciones elementales. En virtud del Lema 2.4.8, luego de cada iteración interna, tenemos el conjunto de distancias d para el nuevo grafo obtenido de agregar una arista de E' . Luego de repetir el ciclo externo para cada una de las $|H|(|H| - 1)/2$ aristas de E' , el conjunto d retornado contiene las distancias deseadas, y el número de operaciones elementales es no mayor que $|H|^2(|H| - 1)^2/4$, multiplicado por una constante, de orden $O(|H|^4)$.

QED

Ahora estamos en condiciones de probar el resultado principal relativo a la evaluación de la DCR en la familia de grafos escalera.

Teorema 2.4.10 [72] *La evaluación de la DCR en la familia \mathcal{G}_h es de tiempo polinomial, donde el orden depende de h .*

Prueba. La evidencia es el algoritmo presentado en la Figura 2.7. Este algoritmo recibe como parámetros l , la probabilidad de operación de aristas \vec{p} , el diámetro d_{max} y las particiones que componen el grafo. Emplearemos ternas (x, y, z) para referirnos a que “la distancia entre los nodos x e y es z ”. Dado i , el conjunto de ternas puede verse como el evento donde las distancias (sin considerar aristas que pertenecen a componentes con etiqueta superior a i) están especificadas por ternas. Cada conjunto \mathcal{D}_i es un conjunto de ternas. Usaremos \mathcal{D}_i para almacenar tales eventos. También usaremos funciones μ_i que asignan la probabilidad de cada evento a cada conjunto de ternas. El caso base lo brinda la terna $(s, s, 0)$: la probabilidad

p_0 de tener un elemento de terna simple $\{(s, s, 0)\}$ es siempre 1. El algoritmo realiza un ciclo (Líneas 8 a 30) para considerar secuencialmente i de 0 a l . En cada iteración, se considera un nuevo conjunto F de aristas pertenecientes a componentes con subíndice i . Para cada i , se revisan todas las ternas de conjuntos factibles previamente registradas en \mathcal{D}_i (Líneas 14 a 29). El ciclo interno (Líneas 15 a 28) considera toda terna y todo subconjunto de aristas de F (para armar toda combinación posible de aristas operativas o no dentro de F). La probabilidad de esta combinación de aristas operativas se asigna a ρ . El Procedimiento *Nuevas – Distancias* del Lema 2.4.9 es invocado para calcular las distancias entre los nodos de $V_i \cup V_{i+1} \cup \{s\}$ considerando aristas que pertenecen a componentes con subíndices no mayores que i , y retorna un nuevo conjunto de ternas d' , cuya probabilidades son acumuladas en la función μ_{i+1} para su uso en la iteración externa siguiente. Luego de abandonar las iteraciones anidadas, μ_{l+1} registra la probabilidad de conjunto de ternas, incluyendo todos los escenarios posibles de distancias entre s y t . Finalmente se suma la probabilidad de todos aquellos que respetan la restricción de diámetro d_{max} , y se retorna como $R_{\{s,t\},G}^{d_{max}}$.

Analicemos la complejidad computacional de este algoritmo. El ciclo compuesto por las Líneas 8-30 realiza $l+1 = O(l)$ iteraciones. En cada iteración domina el ciclo de líneas 14-29, que realiza $|\mathcal{D}_i|$ iteraciones. Cada iteración del ciclo 14-29 realiza $2^{|F'|} \leq 2^{h+h^2+h(h-1)/2} \leq 4^{h^2}$ iteraciones. En estas últimas iteraciones, *Nuevas – Distancias* es el procedimiento dominante, que ejecuta en tiempo $O((2h+1)^4) = O(h^4)$. Entonces, el tiempo de ejecución tiene orden $g(h)$:

$$g(h) = \sum_{i=0}^l \left(|\mathcal{D}_i| 4^{h^2} h^4 \right) = f(h) \sum_{i=0}^l |\mathcal{D}_i| \quad (2.19)$$

siendo $f(h)$ una constante que depende del parámetro h . Cada elemento de \mathcal{D}_i especifica distancias de al menos $h+h+1$ nodos, esto es, $(2h+1)(2h+1-1)/2 = (2h+1)h$ pares. Cada par puede tener una distancia que varía entre 2 y $h+hl = h(l+1)$ (dada por el camino cuya traza va hacia atrás y adelante h veces desde V_0 hasta V_i). Entonces, $|\mathcal{D}_i|$ está acotado por $(h(i+1))^{(2h+1)h}$. Reemplazando en (2.19) tenemos que el orden de ejecución es

$$O \left(f(h) \sum_{i=0}^l (h(i+1))^{(2h+1)h} \right) = O \left(g(h) l^{(2h+1)h} \right) \quad (2.20)$$

donde, nuevamente, $g(h)$ es una constante que depende del parámetro h (creciendo incluso más rápido que f con respecto a h). Esto completa la demostración.

QED

2.4.3 Análisis Asintótico

Estudiamos en esta breve sección el valor asintótico de la DCR cuando se considera una sucesión de grafos que crece al infinito siguiendo ciertas reglas probabilísticas. La pregunta básica es determinar si la DCR converge, y su valor, dadas las reglas probabilísticas de una sucesión de grafos. Vamos a derivar resultados directos de la Teoría de Grafos Aleatorios en el modelo de Gilbert. La Teoría de Grafos Aleatorios estudia el comportamiento asintótico

Procedimiento DCR-Polinomial

Entradas: $(l, \vec{p}, d_{max}, V_0, \dots, V_l, S_0, \dots, S_l, W_0, \dots, W_l, E_0, \dots, E_l, T)$

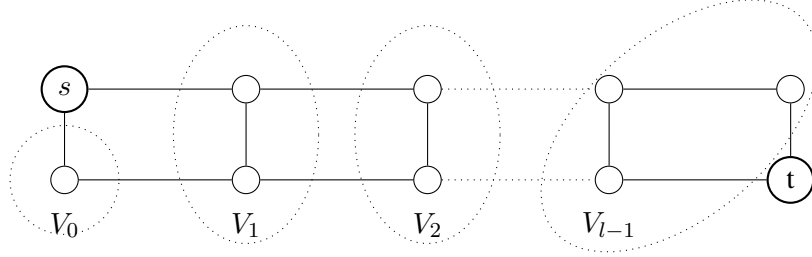
Salidas: r

```

1: Para todo  $i \in 0, \dots, l + 1$ 
2:   inicializar  $\mathcal{D}_i \leftarrow \emptyset$ 
3:   inicializar  $\mu_i(\cdot)$  como vacío
4: Fin Para
5:  $d \leftarrow \{(s, s, 0)\}$ 
6:  $\mathcal{D}_0 \leftarrow \{d\}$ 
7:  $\mu_0(d) \leftarrow 1$ 
8: Para todo  $i \in 0, \dots, l$ 
9:   Si  $i < l$  entonces
10:      $F = S_i \cup W_i \cup E_i$ 
11:   Si no
12:      $F = S_i \cup W_i \cup T$ 
13:   Fin Si
14:   Para todo  $d \in \mathcal{D}_i$ 
15:     Para todo  $F' \subseteq F$ 
16:       Si  $i < l$  entonces
17:          $d' \leftarrow \text{Nuevas-Distancias}(V_i \cup V_{i+1} \cup \{s\}, d, F)$ 
18:       Si no
19:          $d' \leftarrow \text{Nuevas-Distancias}(V_i \cup \{s, t\}, d, F)$ 
20:       Fin Si
21:        $\mathcal{D}_{i+1} \leftarrow \mathcal{D}_{i+1} \cup \{d'\}$ 
22:        $\rho \leftarrow \prod_{x \in F'} p_x \prod_{x \in F \setminus F'} (1 - p_x)$ 
23:       Si  $\mu_{i+1}$  tiene un elemento con índice  $d'$  entonces
24:          $\mu_{i+1}(d') \leftarrow \mu_i(d') + \mu_{i+1}(d) \cdot \rho$ 
25:       Si no
26:          $\mu_{i+1}(d') \leftarrow \mu_i(d) \cdot \rho$ 
27:       Fin Si
28:     Fin Para
29:   Fin Para
30: Fin Para
31:  $r \leftarrow 0$ 
32: Para todo  $d \in \mathcal{D}_{l+1}$ 
33:   Si  $d$  tiene una terna  $(s, t, \delta)$  con  $\delta \leq d_{max}$  entonces
34:      $r \leftarrow r + \mu_{l+1}(d)$ 
35:   Fin Si
36: Fin Para
37: Retornar  $r$ 

```

Figura 2.7: Pseudocódigo para hallar la DCR en grafos \mathcal{G}_h

Figura 2.8: Topología de un miembro de \mathcal{G}_3

(en el número de nodos o aristas) de las propiedades de grafos que crecen siguiendo ciertas reglas. Los primeros grafos aleatorios fueron definidos en [36, 42]. Dos libros valiosos del área son [3, 13]. En el modelo de Gilbert [42], denotado $G(n, p)$, se tiene un grafo con n nodos, donde cada posible arista ocurre con probabilidad p . Erdos y Renyi [36] sugieren un modelo estrechamente relacionado, $G(n, m)$, en el que un grafo es seleccionado al azar y con probabilidad uniforme dentro del conjunto de todos los grafos que tienen n nodos y m aristas. El modelo más aceptado es el de Gilbert, pese a que se lo suele denominar incorrectamente modelo de Erdos-Renyi. Los siguientes modelos apuntaron a mimetizar propiedades y patrones de crecimiento de redes reales, presentes en diferentes disciplinas como Biología, Sociología y Redes Sociales, entre otras. Entre ellos, los modelos más citados son el de Albert-Barabasi [2] para la generación de redes aleatorias libres de escala (conocidas en inglés como redes *scale-free*) y el modelo de Watts-Strogatz [79], que produce grafos con propiedades de mundo pequeño (small-world). El diámetro de un grafo se vincula con la DCR para el caso de todos los terminales. Existen diversos resultados conocidos para el diámetro de grafos aleatorios (ver por ejemplo [12, 14] y en particular la Subsección 5.2 de [28]).

Ilustraremos a continuación cómo algunos resultados relativos al diámetro de grafos aleatorios impactan para determinar el comportamiento asintótico de la DCR, cuando el diámetro vale 2. Sea $G(n, p) = (V, E)$ un grafo de Gilbert. Una simulación directa consiste en sortear de forma independiente una variable uniforme $U_{i,j}$ en el intervalo $[0, 1]$ para cada par de nodos v_i y v_j en el intervalo $[0, 1]$. Si $U_{i,j} < p$ la arista $\{v_i, v_j\}$ está presente; en caso contrario está ausente. Es claro que el valor esperado de $|E|$ es $p \binom{n}{2} = pn(n-1)/2$. Estudiemos el comportamiento asintótico de la DCR cuando $d = 2$ y además $K = \{s, t\}$. La probabilidad de que la distancia entre ambos terminales supere 2 es

$$P(d(s, t) > 2) = (1-p)(1-p^2)^{n-2} \xrightarrow{n} 0,$$

siempre que $p > 0$. Luego, $\lim_n R_{\{s,t\}, G(n,p)}^2 = 1$. Más aún, este límite no depende de los dos terminales elegidos. Este resultado es un corolario inmediato del resultado clásico que el diámetro de un grafo aleatorio de Gilbert tiende a 2 cuando n tiende al infinito, siempre que $p > 0$ (cuya prueba se halla en [17, 58], y un resultado más general en [44]). Luego, vale el siguiente

Lema 2.4.11 *Dados dos reales p y d tales que $0 < p \leq 1$ y $d \geq 2$, la DCR con diámetro d y*

sucesión de terminales $K_n \subseteq \{v_1, \dots, v_n\}$ tiende asintóticamente a uno:

$$\lim_{n \rightarrow \infty} R_{K, G(n, p)}^d = 1 \quad \text{si } p > 0, d \geq 2. \quad (2.21)$$

Prueba. Consideremos las dos sucesiones de eventos:

1. A_n : “todo par de nodos de K_n se comunican por caminos de largo d ”
2. B_n : “el n -ésimo grafo de Gilbert tiene diámetro 1 o 2”

Claramente $B_n \subseteq A_n$ para todo entero positivo n . Como la probabilidad de que el grafo tenga diámetro 2 tiende a 1, tenemos que $\lim_n P(B_n) = 1$, y por lo tanto $\lim_n P(A_n) = 1$. Esto significa que la DCR con diámetro 2 tiende asintóticamente a la unidad, independientemente de la sucesión de terminales considerado.

QED

Un resultado más general se puede deducir de la siguiente propiedad, probada por primera vez en [16]:

Propiedad 2.4.12 *La probabilidad de que un grafo de Gilbert $G(n, p)$ tenga diámetro d tiende a 1 en el infinito si $(pn)^{(d-1)}/n \rightarrow 0$ y $(pn)^d/n \rightarrow \infty$.*

Da la Propiedad 2.4.12 se deduce el siguiente

Corolario 2.4.13 [72] *Dados un real p , un entero d tales que $(pn)^{(d-1)}/n \rightarrow 0$ y $(pn)^d/n \rightarrow \infty$, y cualquier entero $d' \geq d$, la DCR con diámetro d' tiende asintóticamente a uno, independientemente de la evolución del conjunto de terminales K :*

$$\lim_{n \rightarrow \infty} R(G(n, p), K, d') = 1. \quad (2.22)$$

Las hipótesis del Lema 2.4.13 aplicadas al caso $d = 2$ establecen que $p \rightarrow 0$ y que $p\sqrt{n} \rightarrow \infty$. Esto significa que la DCR con $d = 2$ sigue tendiendo a uno, incluso si la probabilidad de operación de las aristas se degrada cuando n crece, siempre que $n^{-1/2}$ sea un infinitesimal de orden mayor que $p(n)$. Dado cualquier entero $d \geq 2$, si tomamos por ejemplo $p(n) = n^\alpha$ con $\alpha < 0$, las condiciones del Lema 2.4.13 son

$$n^{\alpha(d-1)}n^{d-2} \rightarrow 0 \quad \text{y} \quad n^{\alpha d}n^{d-1} \rightarrow \infty$$

y así

$$\alpha < -\frac{d-2}{d-1} \quad \text{y} \quad \alpha > -\frac{d-1}{d}.$$

Luego, para cualquier entero $d' \geq d$, la DCR con diámetro d' tiende a uno siempre que $\alpha \in (-\frac{d-1}{d}, -\frac{d-2}{d-1})$. Observemos que si $\alpha < \alpha' < 0$ entonces $P(G(n, n^\alpha) \text{ sea conexo}) < P(G(n, n^{\alpha'}) \text{ sea conexo})$, por lo que la arista derecha del intervalo puede fijarse en cero. Luego, tenemos el siguiente

Corolario 2.4.14 [72] *Para cada $d \geq 1$, si $p(n) > n^\alpha$ ($\alpha < 0$), entonces la DCR con diámetro d tiende a uno cuando $\alpha > -\frac{d-1}{d}$.*

Resulta atractivo como trabajo futuro explorar el comportamiento asintótico de la DCR para otros modelos de grafos incluidos en [2, 79].

Capítulo 3

Contribuciones

Se sintetizan en este capítulo los artículos [18, 68, 69]. Por razones didácticas, abordamos primeramente el cálculo de la confiabilidad clásica, y luego la diámetro-confiabilidad, cuyas ideas representan en algunos casos una mera extensión o adaptación.

La Sección 3.1 muestra el desarrollo de una técnica de interpolación para el cálculo de la confiabilidad clásica entre todos los terminales de una red, siguiendo lo propuesto en [68]. Una extensión natural de esta técnica de interpolación aplicable al cálculo de la diámetro-confiabilidad de una red (DCR) se describe en [18], y ocupa la Sección 3.2. La Sección 3.3 describe un método de estimación de la DCR basado en Monte Carlo que explota el conocimiento de previos cortes y configuraciones minimales.

Finalmente, se estudia el rendimiento de los distintos métodos desarrollados en la Sección 3.4. Las principales conclusiones de esta monografía y líneas de trabajo futuro se describen en el Capítulo 4.

3.1 Interpolación para el cálculo de la Confiabilidad clásica

Sea $R_{K,G}(p)$ la probabilidad de que los terminales del conjunto K del grafo G permanezcan comunicados bajo rupturas de enlaces independientes con probabilidad de operación p . Del capítulo anterior sabemos que

$$R_{K,G}(p) = \sum_{i=0}^m F_i^K (1-p)^i p^{m-i}, \quad (3.1)$$

siendo F_i^K la cantidad de subgrafos de G con exactamente $m - i$ enlaces que dejan comunicados a los nodos del conjunto K de terminales.

Por otra parte, la diámetro confiabilidad es la probabilidad de que tales nodos permanezcan comunicados por caminos de largo d o menos. Si denotamos $R_{K,G}^d(p)$ a la diámetro confiabilidad, una expresión análoga a (3.1) es válida:

$$R_{K,G}^d(p) = \sum_{i=0}^m F_i^{(K,d)} (1-p)^i p^{m-i}, \quad (3.2)$$

donde ahora $F_i^{(K,d)}$ representa la cantidad de subgrafos de G con exactamente $m - i$ enlaces, tales que todo par de nodos de K admite un camino con d enlaces o menos.

Las Expresiones (3.1) y (3.2) evidencian que ambas medidas de confiabilidad de redes son un polinomio en la variable $p \in [0, 1]$, es decir, un polinomio en la probabilidad de operación de sus enlaces. Obtener el polinomio se reduce a hallar sus coeficientes, y ya hemos visto que existe abundante literatura para hallar los coeficientes en forma exacta (con algoritmos de tiempo exponencial), cotas para cada coeficiente, cotas uniformes para todo el polinomio y métodos aproximados para hallar el polinomio en probabilidades de operación p fijas y selectas dentro del dominio compacto $[0, 1]$.

Curiosamente, la idea de estimar el polinomio en ciertas abscisas y luego interpolar ya era conocida por el Dr. Gerardo Rubino, y posiblemente por otros investigadores. Sin embargo, con el mejor esfuerzo no hemos constatado en la literatura una aproximación al polinomio confiabilidad (ni clásico ni diámetro-acotado) por métodos basados en interpolación. En [68] se desarrolla entonces una técnica basada en interpolación polinómica para hallar la confiabilidad clásica. Es bien sabido que dados $m + 1$ puntos en el plano existe un único polinomio interpolante de grado m o menor (pues el determinante de la matriz de Vandermonde es no nulo). La idea básica es seleccionar $m + 1$ abscisas $\{p_i\}_{i=0,\dots,m}$ dentro del compacto $[0, 1]$ y hallar estimadores y_i de $R_{K,G}(p_i)$. El polinomio interpolante R^* por los puntos (p_i, y_i) usualmente no será precisamente $R_{K,G}$; más aún, no tendrá coeficientes enteros. Se realiza entonces un proceso de corrección, que bien puede consistir en redondear coeficientes. En este caso hemos optado por explotar propiedades de espacios de Hilbert para hallar el polinomio a coeficientes enteros más próximo en $L^2[0, 1]$.

Sin pérdida de generalidad nos vamos a enfocar en el caso que todos los nodos son terminales: $K = V$. En este caso hay coeficientes que son conocidos de antemano, como veremos a continuación (si no se conocen basta con tomar más abscisas en la interpolación). Ya estamos a un paso de reunir todos estos elementos en una misma solución. Nos será de utilidad las siguientes observaciones relativas a los coeficientes del polinomio confiabilidad clásico:

Observación 3.1.1

1. La menor cardinalidad c de un corte se puede hallar utilizando el Teorema de Ford y Fulkerson en forma iterada.
2. La cantidad de cortes de tamaño c se pueden hallar por el Algoritmo de Ball-Provan, por lo que $F_c = n_c$, el número de cortes de mínimo cardinal, se halla en tiempo polinomial.
3. El número F_{m-n+1} coincide con la cantidad de árboles recubridores del grafo. Luego, $F_{m-n+1} = \kappa(G)$, que se puede calcular en tiempo polinomial gracias a trabajos de Kirchhoff de redes eléctricas.
4. Si quitamos menos enlaces que c , todo grafo será conexo. Luego, $F_i = \binom{m}{i}$ siempre que $i < c$.
5. Si dejamos menos enlaces que los que posee un árbol los subgrafos resultantes nunca serán conexos. Luego $F_i = 0$ si $i > m - n + 1$.

A partir de estas observaciones, cuando $K = V$ es posible reescribir (3.1):

$$R_{V,G}(p) = \sum_{i=0}^{c-1} \binom{m}{i} p^{m-i} (1-p)^i + \left(\binom{m}{c} - n_c \right) p^{m-c} (1-p)^c + \sum_{i=c+1}^{m-n} F_i p^{m-i} (1-p)^i + \kappa(G) p^{n-1} (1-p)^{m-n+1}. \quad (3.3)$$

En suma, hay $m - n - c$ coeficientes desconocidos. En lugar de estimar los coeficientes desconocidos, vamos a reescribir el polinomio $R_{V,G}(p)$ para llevarlo a una forma general, y estimarlo con una técnica de interpolación polinómica. La segunda sumatoria de (3.3) se puede llevar a esta forma:

$$f(p) = \sum_{i=c+1}^{m-n} F_i p^{m-i} (1-p)^i = p^m \left(\frac{1-p}{p} \right)^{c+1} \sum_{i=0}^{m-n-c-1} F_{c+1+i} \left(\frac{1-p}{p} \right)^i \quad (3.4)$$

Si realizamos el cambio de variable $x = (1-p)p^{-1}$ y definimos $g(p) = f(p)p^{-m+c+1}(1-p)^{-c-1}$, el polinomio g se halla en su forma general:

$$g(x) = \sum_{i=0}^{m-n-c-1} F_{c+1+i} x^i, \quad (3.5)$$

y los coeficientes son exactamente nuestras incógnitas. Cabe además señalar que mediante cambios de variable es posible obtener las estimaciones $\{f^*(x_1), f^*(x_2), \dots, f^*(x_{m-n-c})\}$ partiendo del conjunto $\{y_i = \overline{\phi_N}(p_i)\}_{i=1, \dots, m-n-c}$.

Reunamos entonces las ideas anteriores coherentemente en un algoritmo, que denominamos *RelInterpol*.

Algoritmo 2 $R' = \text{RelInterpol}(G, x, N)$

- 1: $(c, n_c, \kappa) \leftarrow \text{Hallar}(G)$
 - 2: $y \leftarrow \text{MonteCarlo}(x, N)$
 - 3: $g \leftarrow \text{Newton}(x, y)$
 - 4: $R^* \leftarrow \text{Construir}(g, c, n_c, l, n_l)$
 - 5: $R' \leftarrow \text{Hilbert}(R^*)$
 - 6: **Mientras no** $\text{CriterioFreno}(R') = 1$
 - 7: Incrementar(N)
 - 8: **Ir a Línea 2**
 - 9: **Fin Mientras**
 - 10: **Retornar** R'
-

El Algoritmo *RelInterpol* recibe un grafo G , la cantidad de iteraciones N y un conjunto de abscisas x , y retorna un polinomio R' , que en el mejor de los casos va a coincidir con

$R_{V,G}$. En la Línea 1 se hallan los coeficientes c , n_c y κ haciendo uso de los Algoritmos de Ford-Fulkerson, Teorema de Kirchhoff y Ball-Provan. Se realiza el conjunto de estimaciones puntuales mediante la técnica de Monte Carlo Crudo (detallado en el Capítulo 2), consiguiendo un vector de estimaciones y asociado al vector de entrada x . En la Línea 3 se toma la interpolación polinómica por el método de Newton a la función g de la Expresión 3.5. La Línea 4 permite construir una estimación R^* para el polinomio objetivo, reconstruyéndolo a partir de (3.3) y (3.1). En la Línea 5, el polinomio así obtenido se lleva a coeficientes enteros, utilizando proyecciones en polinomios que conforman una base de Hilbert de $L^2[0, 1]$. Finalmente, si el polinomio R' así obtenido posee varias de las condiciones que comparten todos los polinomios de confiabilidad se retorna como salida, y en caso contrario el proceso se reitera, volviendo a realizar estimaciones puntuales con Monte Carlo Crudo, pero ahora con mayor cantidad de iteraciones. Precisamente, la Función *CriterioFreno* comprueba que los coeficientes F_i satisfagan las propiedades de acotación ya conocidas ¹.

A continuación se detallan los bloques de interpolación y redondeo (precisamente, las Funciones *Newton* y *Hilbert*). Existen diversas maneras de hallar el único polinomio interpolante por ciertos puntos en el plano. El método de Vandermonde es conceptualmente simple, pero se debe afrontar un sistema lineal mal condicionado. Los polinomios de Lagrange son rápidos de escribir, pero no son sencillos de manipular (derivar, integrar, evaluar). El método de interpolación de Newton permite la incorporación de nuevos puntos con facilidad, y es sencillo de evaluar. Además, es posible obtener una cota uniforme para el error mediante la interpolación de Newton. El lector puede encontrar una valiosa exposición de teoría clásica de interpolación en el libro [65].

Por las razones anteriores, hemos seleccionado el método de interpolación de Newton. Este método construye iterativamente la interpolación final incluyendo en cada iteración un nuevo punto (x_i, y_i) . De hecho, si el polinomio g_i interpola los primeros i puntos, entonces $g_{i+1}(x) = g_i(x) + c_{i+1} \prod_{j \leq i} (x - x_j)$ verifica $g_{i+1}(x_k) = g_i(x_k) = y_k$ para todo $k \leq i$, y c_{i+1} se obtiene eligiendo $g_{i+1}(x_{i+1}) = y_{i+1}$.

Además, si g es el polinomio interpolante de cierta función h por los puntos $\{(x_i, h(x_i))\}_{i=1, \dots, m-n-c}$ por medio del método de Newton, el error global se puede hallar *exactamente* para cualquier $x \in [x_1, x_{m-n-c}]$ [46]:

$$h(x) - g(x) = [x_1, x_2, \dots, x_{m-n-c}, x](h) \prod_{i=1}^{m-n-c} (x - x_i), \quad (3.6)$$

donde el operador $[x_1, x_2, \dots, x_n](f)$ se define recursivamente mediante $[x_1]f = f(x_1)$ y

$$[x_1, \dots, x_k]f = \frac{[x_2, \dots, x_k](f) - [x_1, \dots, x_{k-1}](f)}{x_k - x_1}. \quad (3.7)$$

Por lo tanto, podemos hallar el orden de una cota uniforme para el peor error $\{|h(x) - g(x)|\}_{x \in [0,1]}$ en términos de N si despreciamos los errores de redondeo. De hecho, la Ecuación (3.7) asegura que el error de propagación se puede duplicar en el peor caso en cada

¹La función de parada se puede sofisticar comprobando propiedades que poseen todos los polinomios de confiabilidad, incluyendo monotonía, lugar geométrico de sus raíces, desigualdades entre coeficientes, entre otras [10, 49].

paso, por lo que el nuevo radio de confianza es del orden de $\epsilon' = 2^{m-n-c}\epsilon$, siendo ϵ el radio de confianza de una estimación puntual.

Esto sugiere que el tamaño de muestreo N debería crecer exponencialmente con respecto al tamaño del grafo, nuevamente resaltando la dureza del problema que estamos afrontando.

El modo de redondeo de los coeficientes también merece detalles. Mientras que el polinomio R^* obtenido mediante la interpolación de Newton tiene coeficientes reales, todo polinomio de confiabilidad $R_{V,G}$ tiene coeficientes enteros. Más aún: estos coeficientes alternan de signo en su forma general, y respetan ciertas cotas.

Para determinar el modo de redondeo, explotaremos la estructura del espacio de Hilbert $L^2[0, 1]$. Sean R^* una estimación del polinomio $R_{K,G}^d$, y $R'(p) = \sum_{i=0}^m a_i p^i$ el polinomio más cercano a $R^*(p)$ bajo la métrica de $L^2[0, 1]$ con coeficientes enteros a_i :

$$R'(p) = \arg \min_{r(p) = \sum_{i=0}^m a_i p^i, a_i \in \mathbb{Z}} \int_0^1 (R^*(p) - r(p))^2 dp. \quad (3.8)$$

No es cierto que los coeficientes a_i se obtengan por redondeo los de $R^*(p)$. La solución correcta se obtiene usando una base de Hilbert de $L^2[0, 1]$, como lo es la familia de polinomios de Legendre trasladados: $\hat{P}_i(x) = P_i(2x - 1)$, siendo $P_i(x)$ el i -ésimo polinomio de Legendre, que se define recursivamente mediante $P_0(x) = 1$, $P_1(x) = x$ y $(i + 1)P_{i+1}(x) = (2i + 1)xP_i(x) - iP_{i-1}(x)$.

Si $\langle u, v \rangle = \int_0^1 u(x)v(x)dx$ denota el producto interno en $L^2[0, 1]$, entonces $\langle \hat{P}_i, \hat{P}_j \rangle = \delta_{i,j}/(2j + 1)$, siendo $\delta_{i,j}$ la función δ de Kronecker. El conjunto $\{\hat{P}_i\}_{i \geq 0}$ es de hecho una base de Hilbert de $L^2[0, 1]$ ².

Si usamos una base de Hilbert: $R^*(p) = \sum_{i=0}^m b_i \sqrt{2i + 1} \hat{P}_i(p)$ y $R'(p) = \sum_{i=0}^m \hat{b}_i \sqrt{2i + 1} \hat{P}_i(p)$, entonces \hat{b}_i es el redondeo de b_i . En efecto:

$$\begin{aligned} \|R' - R^*\|_2^2 &= \int_0^1 |R' - R^*|^2 dp \\ &= \int_0^1 \left(\sum_{i=0}^m \sqrt{2i + 1} (b_i - \hat{b}_i) \hat{P}_i(p) \right)^2 dp \\ &= \sum_{i=0}^m (b_i - \hat{b}_i)^2, \end{aligned}$$

y la última suma se minimiza exactamente cuando el entero \hat{b}_i es el redondeo de b_i para todo $i = 0, \dots, m$. Como consecuencia, es preferible redondear en la base de Hilbert de polinomios, y no hacerlo en su forma general de monomios (que no es un conjunto ortonormal en $L^2[0, 1]$). La Función *Hilbert* halla los polinomios de Legendre trasladados y luego redondea los coeficientes del polinomio de entrada en tal base.

En la Sección 3.4 veremos el rendimiento de *RelInterpol* para instancias particulares de grafos.

²Los polinomios de Legendre se pueden obtener aplicando el proceso de ortogonalización de Gram-Schmidt al conjunto independiente de monomios $\{x^i\}_{i \geq 0}$, y son densos en $L^2[-1, 1]$ como corolario del Teorema de Stone-Weierstrass.

3.2 Interpolación y Conteo

La diferencia principal entre la confiabilidad clásica y la diámetro acotada es que las configuraciones minimales de la diámetro-confiabilidad ya no son árboles. Por ejemplo, el grafo bipartito completo tiene diámetro 2, pero la eliminación de un enlace cualquiera lo deja con diámetro 3. Esto significa que el grafo bipartito completo tiene un único subgrafo 2-conexo minimal, que es él mismo.

Por otra parte, puesto que no es trivial reconocer configuraciones minimales para la diámetro-confiabilidad, el reconocimiento de cortes de menor cardinalidad tampoco lo es. Esto hace que el cálculo de $\kappa(G)$ y c aplicado a la interpolación clásica para reducir la dimensionalidad del problema clásico deje de ser aplicable ahora.

No obstante, la técnica de interpolación se puede extender naturalmente para la estimación de la diámetro-confiabilidad de una red. Si bien se puede sofisticar estudiando propiedades de sus coeficientes, vamos a plantear la interpolación de la manera más simple posible: hallando $m + 1$ estimaciones puntuales del polinomio de la Expresión (3.2) para su posterior interpolación.

Extendemos entonces el concepto de interpolación para hallar ahora el polinomio objetivo $R_{K,G}^d(p)$, mediante el algoritmo $d - Interpol$:

Algoritmo 3 $R = d - Interpol(G, K, d, N, x)$

- 1: **Para** $i = 0$ a m
 - 2: $y_i \leftarrow MonteCarlo(x_i, N)$
 - 3: **Fin Para**
 - 4: $y \leftarrow (y_1, \dots, y_m)$
 - 5: $g \leftarrow Newton(x, y)$
 - 6: $R \leftarrow Hilbert(g)$
 - 7: **Retornar** R
-

d -Interpol recibe el grafo objetivo G , el conjunto de terminales K , diámetro d , tamaño de muestreo N , y un conjunto de abscisas $x = \{x_0, x_1, \dots, x_m, x_{m+1}\}$ donde $0 \leq x_i \leq x_{i+1} \leq 1$. En el bloque de Líneas 1-3, toma lugar la estimación puntual y_i para $R_{K,G}^d(p)$ en cada abscisa x_i , y la información se almacena en un vector y en la Línea 4. La interpolación se realiza inmediatamente en la Línea 5 (utilizando la regla de agregado de punto de Newton). Si las estimaciones no tuviesen error tendríamos $R = R_{K,G}^d$. Sin embargo, la introducción de la Función *MonteCarlo* en la Línea 6 lleva a desviaciones, y los coeficientes de R usualmente no son enteros. Como consecuencia, toma lugar un proceso de redondeo en la Línea 6, utilizando la misma función que en el caso de confiabilidad clásica.

En [18], esta técnica de interpolación fue contrastada con un método basado en conteo, que procura hallar directamente los coeficientes $F_i^{(K,d)}$ de (3.2). Recordemos que $F_i^{(K,d)}$ es la cantidad de subgrafos del grafo objetivo con exactamente $m - i$ enlaces que conecta a los terminales de K con caminos de largo d o menor. Entonces, si somos capaces de tomar muestras de subgrafos con exactamente $m - i$ enlaces, basta con tomar la proporción de casos favorables para estimar $F_i^{(K,d)}$.

Consideremos entonces subgrafos G_1^i, \dots, G_N^i tomados independientemente y con equiprobabilidad dentro de la familia de subgrafos con $m - i$ enlaces, y sean X_1^i, \dots, X_N^i variables binarias independientes, tales que $X_j^i = 1$ si y solo si el subgrafo G_j^i es d - K conexo (y $X_j^i = 0$ en otro caso). La ley fuerte asegura que la variable promedio \overline{X}_N^i converge casi seguramente a $E(X_j^i)$:

$$E(X^i) = P(X^i = 1) = \frac{F_i^{(d,K)}}{2^{m-i}}, \quad (3.9)$$

donde la última igualdad usa el hecho que los 2^{m-i} subgrafos de G con $m - i$ enlaces son igualmente probables. Combinando las Ecuaciones (3.9) y (3.2), resulta natural proponer la siguiente variable aleatoria como estimador del polinomio:

$$H(p) = \sum_{i=0}^m 2^{m-i} \overline{X}_N^i p^{m-i} (1-p)^i, \quad (3.10)$$

Puesto que $E(2^{m-i} \overline{X}_N^i) = F_i^{(d,K)}$, tenemos que H es un estimador insesgado para $R_{K,G}^d$, uniformemente en la indeterminada p . La Expresión (3.10) sugiere la siguiente heurística:

Algoritmo 4 $R_{K,G}^d = F - MonteCarlo(G, K, d, N)$

- 1: **Para** $j = 0$ a m
 - 2: $Sum_j \leftarrow 0$
 - 3: **Para** $i = 1$ a N
 - 4: $X_i^j \leftarrow MonteCarlo(G, K, d)$
 - 5: $Sum_j \leftarrow Sum_j + X_i^j$
 - 6: **Fin Para**
 - 7: $\overline{X}_N^j \leftarrow Sum_j / N$
 - 8: $F_j^d \leftarrow 2^{m-j} \overline{X}_N^j$
 - 9: **Fin Para**
 - 10: $R_{K,G}^d \leftarrow \sum_{i=0}^m F_i^{(d,K)} p^{m-i} (1-p)^i$
 - 11: **Retornar** $R_{K,G}^d$
-

Un detalle técnico aquí omitido es el muestreo con equiprobabilidad dentro del conjunto de subgrafos con exactamente $m - i$ enlaces. Puesto son en total $\binom{n}{i}$ subgrafos, el sorteo equiprobable es prohibitivo cuando n es grande. Una manera posible de realizarlo es asignar variables uniformes independientes en el intervalo $[0, 1]$ a cada enlace, y considerar operativas las primeras $m - i$ uniformes. Este problema se conoce con el nombre inglés *k out of n*. Una valiosa referencia para profundizar en este tema se encuentra en [7]. En la Sección 3.4 veremos una comparación entre el rendimiento de $F - MonteCarlo$ y $d - Interpol$.

3.3 Interpolación basada en conocimiento previo de la red

Monte-Carlo es una destacada técnica computacional para la simulación. De un punto de vista macroscópico, la idea es simular fielmente un sistema complejo (o parte del mismo),

Algoritmo 5 $R_{K,G}^d = DCR - Interpol(G, K, d, N, x)$

- 1: **Para** $i = 0$ a m
 - 2: $y_i \leftarrow MC - Condicionado(x_i, N)$
 - 3: **Fin Para**
 - 4: $y \leftarrow (y_1, \dots, y_m)$
 - 5: $g \leftarrow Newton(x, y)$
 - 6: $R \leftarrow Hilbert(g)$
 - 7: **Retornar** $R_{K,G}^d = R$
-

y considerar N experimentos independientes de tal simulación, de modo de determinar el rendimiento final del sistema (o sub-sistema) para asistir en la toma de decisiones.

Monte-Carlo ha sido utilizado ampliamente a una gran diversidad de problemas, incluyendo conteo, integración numérica, simulación de eventos discretos (y eventos raros). El lector puede hallar una generosa variedad de aplicaciones en [39], y un análisis exhaustivo de simulación de eventos raros basados en el método de Monte-Carlo en [71]. En el método de Monte-Carlo Crudo (CMC por sus siglas en inglés), se toman N réplicas independientes X_1, \dots, X_N de una variable aleatoria X con media $E(X)$ y varianza $Var(X)$ finitas. La variable promedio \bar{X}_N es insesgada, y por la Ley Fuerte converge casi seguramente a $E(X)$. Su varianza (y por lo tanto su error cuadrático medio) vale $Var(\bar{X}_N) = \frac{Var(X)}{N}$.

Ya hemos visto en la Sección 3.2 un método de Monte-Carlo basado en conteo, que llamamos $F - MonteCarlo$, y un método de interpolación para la DCR que utiliza a Monte Carlo Crudo como maquinaria básica, llamado $d - Interpol$. En esta sección vamos a describir una variante de $d - Interpol$ que explota conocimiento parcial de cortes y configuraciones minimales de la red. Esta técnica fue introducida en [27] para estimaciones puntuales y luego adaptada en [69] para la estimación del polinomio DCR completo.

En la Figura 3.3 se detalla el Algoritmo $DCR - Interpol$, que combina el concepto de interpolación con el Método de Monte-Carlo condicionado a conocimiento previo de la red. La principal diferencia es que se asumirá de antemano el conocimiento de cortes y configuraciones operativas de la red. Veremos que este conocimiento previo permite reducir la varianza de cada estimación puntual. Resulta entonces atractivo contrastar el rendimiento de $d - Interpol$ contra $DCR - Interpol$, para analizar el efecto de mejores estimaciones puntuales sobre el polinomio global. La única función que es novedad y merece detalles es $MC - Condicionado$.

Supongamos que conocemos configuraciones operativas P_1, \dots, P_r y cortes C_1, \dots, C_s . Es posible explotar el hecho que la red funcionará si alguna configuración P_i operativa funciona, o que la red no funcionará si los enlaces operativos son disjuntos con algún corte C_j (es decir, si un corte “ocurre”). Llamemos R_L a la probabilidad de tener alguna configuración $P_j, j \in \{1, \dots, r\}$ en operación, y R_U la probabilidad de que no ocurra un corte. Claramente, la confiabilidad objetivo $R_{K,G}^d$, que abreviamos con R , cumple las desigualdades $R_L \leq R \leq R_U$, pues R es la probabilidad de que alguna configuración operativa funcione, o equivalentemente, la probabilidad de que *ningún* corte ocurra. Sea Γ el conjunto de subgrafos

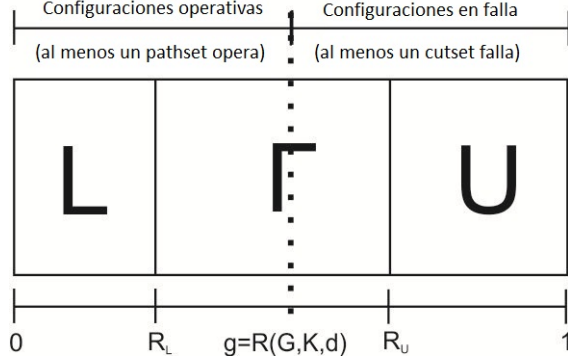


Figura 3.1: Método de Monte Carlo condicionado a cortes y configuraciones minimales

tales que no ocurre ninguna configuración operativa ni corte de los inicialmente conocidos. La esencia del método de Monte Carlo condicionado es reducir el universo de muestreo al conjunto Γ , respetando la medida condicional de no ocurrir ninguno de los cortes ni configuraciones minimales iniciales. El éxito de este plan dependerá de la selección de configuraciones minimales y cortes, pues son los que determinan la dificultad de seleccionar un elemento con equiprobabilidad dentro del conjunto Γ . La Figura 3.1 ilustra esta técnica de acotación y aproximación basada en cortes y configuraciones minimales.

Observar que el universo Γ tiene probabilidad $P(\Gamma) = R_U - R_L$. Utilizando probabilidades condicionadas tenemos que R satisface la siguiente identidad:

$$R = R_L + (R_U - R_L)P(\phi(X) = 1 | X \in \Gamma), \quad (3.11)$$

siendo X el vector aleatorio de estado de los enlaces, y ϕ la función de estructura que retorna 1 si y solo si la configuración comunica a los terminales por caminos de largo d o menor. Por lo tanto, si R_U y R_L son conocidos y somos capaces de muestrear N configuraciones independientes X^1, \dots, X^N dentro del universo Γ respetando las probabilidades condicionales, podremos construir un estimador insesgado para R :

$$\widehat{R}_N = R_L + (R_U - R_L) \sum_{i=1}^N X^{(i)} / N. \quad (3.12)$$

Un análisis detallado de la selección de configuraciones minimales y cortes, como también literatura relacionada, se puede encontrar en la tesis doctoral de Pablo Sartor [72]. Aquí consideraremos una manera simple de producir configuraciones operativas y cortes: sean c_s y p_s el menor cardinal de un corte y configuración operativa, respectivamente. Luego, todos los subgrafos con más de $m - c_s$ enlaces operativos funcionarán; análogamente, todos los subgrafos con menos de p_s enlaces fallarán. El universo Γ es sencillo de muestrear en este caso, pues depende únicamente del número de enlaces de los subgrafos.

El estimador \widehat{R}_N es insesgado, y su varianza vale:

$$\text{Var}(\widehat{R}_N) = (R_U - R_L)^2 \frac{\text{Var}(X)}{N}. \quad (3.13)$$

Como cabe esperar, su varianza es siempre mejor que la que ofrece el método de Monte Carlo Crudo (con igualdad en el caso extremo en el que no hay información condicional, en el que $R_L = 0$ y $R_U = 1$). El cuadrado $(R_U - R_L)^2$ representa la reducción de varianza, y por ende la reducción en el error cuadrático medio de la estimación, para un tamaño muestral N fijo.

3.4 Resultados Numéricos

Hasta el momento hemos desarrollado cuatro estimaciones de las medidas de confiabilidad clásica y diámetro-acotada. A modo de repaso enumeramos estas cuatro estimaciones y sus principales características:

1. *RelInterpol* propone una estimación basada en interpolación polinómica para la confiabilidad clásica cuando el interés radica en comunicar a todos los nodos de la red. Reduce la dimensionalidad mediante el cómputo de $\kappa(G)$ y n_c . Utiliza CMC para la estimación puntual y Newton para la interpolación polinómica. Redondea el polinomio obtenido utilizando una base de Hilbert.
2. *d - Interpol* es la extensión de *RelInterpol* para la DCR. Deja de aplicar la reducción de dimensionalidad, y generaliza a cualquier diámetro y conjunto de nodos terminales.
3. *F - MonteCarlo* estima los coeficientes del polinomio DCR directamente mediante conteo por Monte Carlo.
4. *DCR - Interpol* explota el conocimiento de configuraciones operativas y cortes iniciales para reducir el espacio de muestreo. Reemplaza en *d - Interpol* la estimación puntual por Monte Carlo condicionado, consiguiendo una menor varianza para cada estimación puntual.

En primera instancia ilustraremos el rendimiento de *RelInterpol* para estimar la confiabilidad clásica. A modo de prueba, consideremos el grafo de 7 nodos y 14 aristas que se muestra en la Figura 3.2.

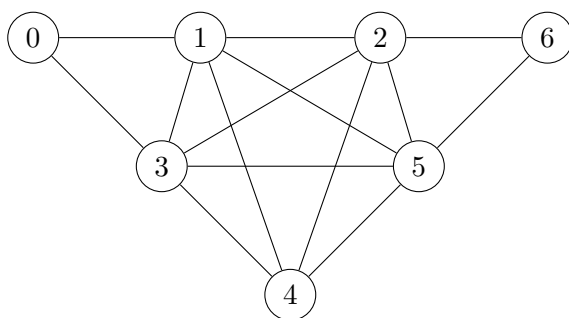


Figura 3.2: Red ejemplar con $n = 7$ nodos y $m = 14$ enlaces.

Gracias a los célebres trabajos de Kirchhoff, Ball y Provan, sabemos que el cardinal del corte mínimo es $c = 2$, el número de tales cortes es $n_c = 2$, y la cantidad de árboles

recubridores es $\kappa(G) = 720$. Puesto que el grafo de muestra tiene exactamente $m = 14$ enlaces y $n = 7$ nodos, precisamos exactamente $m - n - c = 5$ estimaciones puntuales del polinomio confiabilidad. Además, el tamaño de este grafo permite aplicar un algoritmo exacto para obtener la confiabilidad clásica:

$$R_{V,G}(p) = 720p^6 - 4136p^7 + 10741p^8 - 16356p^9 + 15894p^{10} - 10056p^{11} + 4034p^{12} - 936p^{13} + 96p^{14} \quad (3.14)$$

Recordemos que la información del polinomio confiabilidad se almacena en $g(x)$ mediante la Expresión (3.5). Luego, se aplica el método de Newton a $g(x)$ en cinco puntos de $[0, 1]$. Elegimos las abscisas altas (y más interesantes del punto de vista de confiabilidad) $p_k = \frac{5+2k}{14}$, donde $k \in \{0, 1, 2, 3, 4\}$, pues la anti-confiabilidad (su complemento) no es un evento raro en tales casos. La Tabla 3.1 revela los coeficientes estimados tras considerar diferentes tamaños de muestra $N_i \in \{10^i, i = 5, 6, 7, 8\}$.

Tabla 3.1: Rendimiento de *RelInterpol* con diferentes tamaños de muestra.

| Tamaño de muestra (10^i) | P_6 | P_7 | P_8 | P_9 | P_{10} |
|--|----------|----------|----------|----------|----------|
| 5 | 720 | -4020 | 9648 | -12054 | 6674 |
| 6 | 720 | -4047 | 9895 | -12963 | 8477 |
| 7 | 720 | -4113 | 10528 | -15523 | 14110 |
| 8 | 720 | -4125 | 10633 | -15926 | 14957 |
| Exacto: | 720 | -4136 | 10741 | -16356 | 15894 |
| Tamaño de muestra (10^i) | P_{11} | P_{12} | P_{13} | P_{14} | |
| 5 | 1595 | -4669 | 2629 | -523 | |
| 6 | -494 | -3249 | 2103 | -441 | |
| 7 | -7791 | 2328 | -230 | -28 | |
| 8 | -8851 | 3118 | -554 | 29 | |
| Exacto: | -10056 | 4034 | -936 | 96 | |

Se puede apreciar que el error relativo de los coeficientes se reduce consistentemente con respecto al tamaño de muestra, y la estimación es más precisa en los coeficientes dominantes. Es de destacar que el coeficiente dominante fue correctamente estimado incluso con bajo tamaño de muestra. Este hecho evidencia que la técnica de interpolación es prometedora para aplicaciones de eventos raros, donde las fallas ocurren con muy baja probabilidad.

Para evaluar efectos numéricos, aplicamos la interpolación de Newton a los puntos seleccionados del polinomio correcto. El polinomio obtenido fue idéntico al original. Como consecuencia, hemos despreciado los errores de propagación numérica, pues el error que proviene de otras fuentes (principalmente la estimación por Monte Carlo) son dominantes.

A continuación realizamos un estudio comparativo entre *F-MonteCarlo* y *d-Interpol* para la estimación de la DCR, a la luz de los grafos K_5 , Petersen $G(5, 2)$ y Dodecahedro

$G(10, 2)$, que se ilustran en las Figuras 3.3 y 3.4 respectivamente.

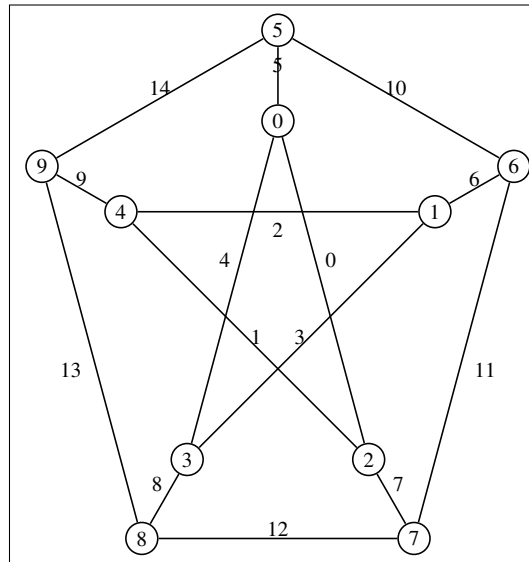


Figura 3.3: Grafo de Petersen

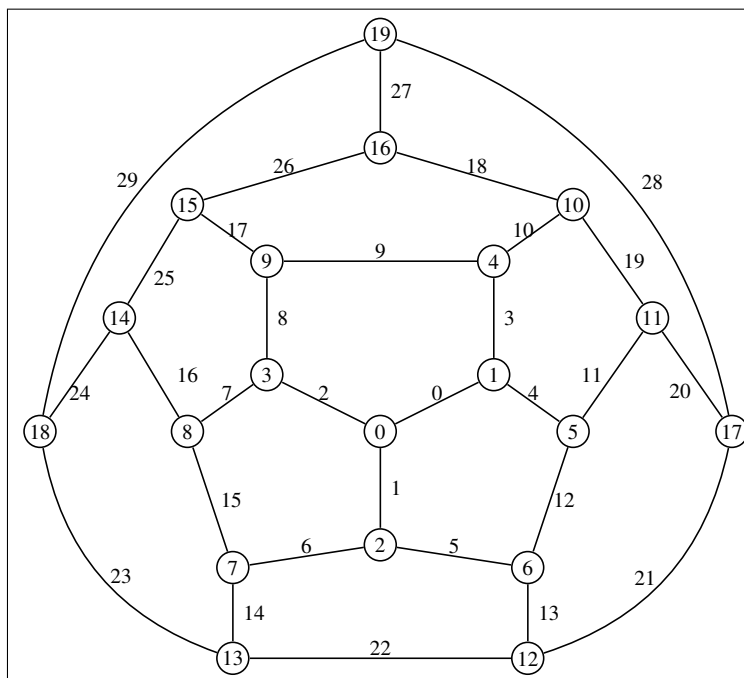


Figura 3.4: Dodecahedro

Consideremos primeramente el caso del grafo completo K_5 con diámetro $d = 2$. Calculemos el polinomio R_{V, K_5}^2 , mediante un conteo de los subgrafos correspondientes F_i^2 ,

para $i \in \{0, \dots, 10\}$. Hay exactamente 5 subgrafos estrella $K_{1,4}$; uno por nodo. Ellos conforman configuraciones operativas con la mínima cantidad de enlaces, por lo que $F_6^2 = 5$ y $F_i^2 = 0$ si $i \geq 6$. Si removemos 3 enlaces o menos tenemos $F_i^2 = \binom{10}{i}$ cuando $i \in \{0, 1, 2, 3\}$. Nos falta contar F_4^2 y F_5^2 . Si eliminamos todos los enlaces que inciden a un terminal cualquiera la subred queda desconectada. Hay 5 maneras posibles de hacerlo (una por nodo). Alternativamente, si se remueven todos los enlaces excepto uno, $\{x, y\}$, incidente a un terminal x , y se remueve otro enlace $\{y, z\}$, los terminales x y z no comparten caminos de largo 1 o 2. Hay 5 maneras de elegir x , 4 maneras de elegir y , y 3 maneras de elegir z : $A_3^5 = 5 \times 4 \times 3 = 60$ configuraciones en este caso. Si todos los nodos de K_5 tienen grado 2 o superior, el subgrafo contiene un ciclo elemental C_5 , que es configuración minimal. Entonces, $F_4^2 = \binom{10}{4} - 5 - 60 = 145$. Finalmente, las únicas configuraciones operativas con exactamente 5 enlaces son isomorfas a C_5 (representando $4!/2 = 12$ casos) y a estrellas $K_{1,4}$ con un enlace adicional (representando $5 \times \binom{4}{2} = 30$ casos), por lo que $F_5^2 = 12 + 30 = 42$. Reemplazando en (3.2) tenemos que la DCR para K_5 con $K = V$ y $d = 2$ es:

$$R_{V,K_5}^2 = p^{10} + 10p(1-p)^9 + 45p^2(1-p)^8 + 120p^3(1-p)^7 + 145p^4(1-p)^6 + 42p^5(1-p)^5 + 5p^6(1-p)^4 \quad (3.15)$$

Es cierto que el cálculo de R_{V,K_5}^2 fue elemental. Un reto para la comunidad científica es extender este razonamiento para calcular R_{V,K_n}^2 , siendo la cantidad de terminales n arbitraria (esto permitiría contar la cantidad de subgrafos de diámetro 2 dentro de un grafo completo).

A efectos de realizar un análisis fiel de rendimiento de $d - Interpol$, es preciso llevar el polinomio R_{V,K_5}^2 a su forma general $R_{V,K_5}^2 = \sum_{i=0}^m P_i^d p^i$, que es aplicación directa del binomio de Newton:

$$R_{V,K_5}^2 = 5p^4 + 12p^5 + 10p^6 - 140p^7 + 210p^8 - 120p^9 + 24p^{10} \quad (3.16)$$

Al aplicar $d - Interpol$ en el caso de K_5 para $K = V$ y $d = 2$ con tamaño de muestra $N = 10^4$, obtenemos el siguiente polinomio:

$$R_{V,K_5}^{2*} = 6p - 170p^2 + 1829p^3 - 10428p^4 + 35489p^5 - 75494p^6 + 101370p^7 - 83537p^8 + 38577p^9 - 7642p^{10} \quad (3.17)$$

A simple vista, los coeficientes de las Expresiones (3.16) y (3.17) sugieren importantes diferencias entre los coeficientes exactos y los obtenidos mediante $d - Interpol$. Este comportamiento no mejora para muestras de tamaño mayor. Hasta el momento sospechamos que esta inestabilidad se relaciona con efectos de eventos raros en los extremos. De hecho, cuando p es próximo a 1, es raro seleccionar un grafo aleatorio que no sea operativo (análogamente, cuando p es cercano a 0 es raro conseguir muestras de grafos operativos). Esta técnica de interpolación es también inestable en el Dodecahedro, y requiere adaptaciones que son parte de trabajo futuro (una discusión de posibles mejoras se incluye en el Capítulo 4).

Nos enfocaremos ahora en el rendimiento de $F - MonteCarlo$. La Tabla 3.2 presenta la evolución de $F - MonteCarlo$ para el grafo completo K_5 en el caso $K = V$ con diámetro

Tabla 3.2: Rendimiento de F – MonteCarlo para el grafo K_5 con $K = V$ y $d = 2$.

| Tamaño de muestra (10^i) | F_0^2 | F_1^2 | F_2^2 | F_3^2 | F_4^2 | F_5^2 | F_6^2 |
|------------------------------|---------|---------|---------|---------|---------|---------|---------|
| 3 | 1 | 10 | 45 | 120 | 147 | 45 | 5 |
| 4 | 1 | 10 | 45 | 120 | 145 | 43 | 5 |
| 5 | 1 | 10 | 45 | 120 | 145 | 42 | 5 |
| 6 | 1 | 10 | 45 | 120 | 145 | 42 | 5 |
| Exacto: | 1 | 10 | 45 | 120 | 145 | 42 | 5 |

$d = 2$: Con muestras de tamaño $N = 10^5$ o mayor el ajuste obtenido por F -MonteCarlo es perfecto, acertando a todos los coeficientes. El lector puede apreciar los pequeños gaps entre los coeficientes exactos y las correspondientes estimaciones para tamaños de muestra menores, al contar F_4^2 y F_5^2 .

Mudémosno ahora a los grafos de Petersen y Dodecahedro, denotados mediante $G(5, 2)$ y $G(10, 2)$ respectivamente (de acuerdo con la terminología de grafos de Petersen generalizados). El diámetro de $G(5, 2)$ es $D(G(5, 2)) = 2$, y el lector puede comprobar que $G(5, 2)$ no es solamente 2-crítico en diámetro, sino que también es 3-crítico (su diámetro crece a $D = 4$ bajo la eliminación de un enlace arbitrario). Concretamente, si eliminamos el enlace $e = \{x, y\}$, los terminales x e y no tienen un camino con menos de 4 saltos. Por otra parte, $D(G(10, 2)) = 5$, y no es 5-crítico.

Mediante conteo es posible obtener los coeficientes $F_i^{(d,K)}$ para ambos grafos. En el grafo de Petersen:

$$R_{V,G(5,2)}^4 = p^{15} + 15p^{14}(1-p) + 105p^{13}(1-p)^2 + 385p^{12}(1-p)^3 + 480p^{11}(1-p)^4 + 72p^{10}(1-p)^5 + 10p^9(1-p)^6,$$

mientras que en Dodecahedro:

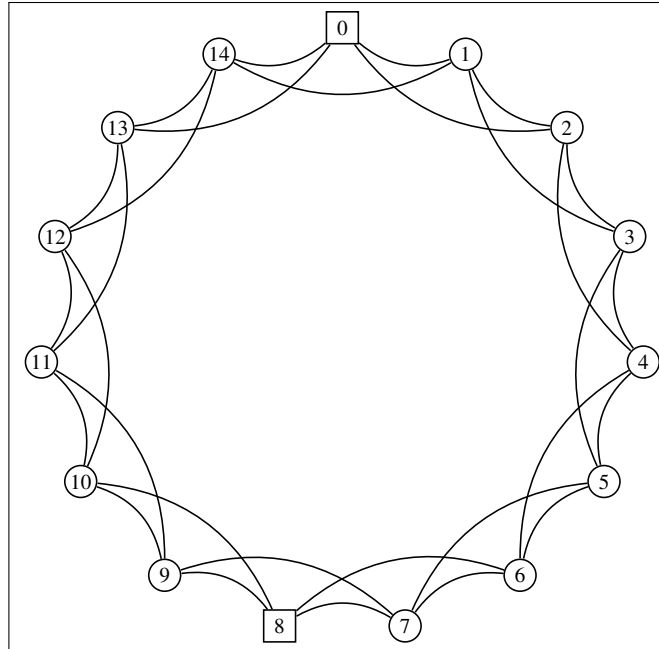
$$R_{V,G(10,2)}^5 = p^{15} + 30p^{14}(1-p) + 375p^{13}(1-p)^2 + 2180p^{12}(1-p)^3 + 5310p^{11}(1-p)^4 + 4152p^{10}(1-p)^5 + 1120p^9(1-p)^6 + 120p^8(1-p)^7.$$

Estudiaremos el rendimiento de F -MonteCarlo a la luz de ambos grafos. Por razones de brevedad, compararemos directamente los coeficientes $F_i^{(d,V)}$ no nulos en este caso (no se muestran los coeficientes nulos). Nuevamente, F -MonteCarlo es capaz de ajustar los

Tabla 3.3: Rendimiento de F -MonteCarlo para el grafo de Petersen $G(5, 2)$.

| Tamaño de muestra (10^i) | F_0^4 | F_1^4 | F_2^4 | F_3^4 | F_4^4 | F_5^4 | F_6^4 |
|------------------------------|---------|---------|---------|---------|---------|---------|---------|
| 3 | 1 | 15 | 105 | 381 | 485 | 54 | 10 |
| 4 | 1 | 15 | 105 | 387 | 489 | 65 | 9 |
| 5 | 1 | 15 | 105 | 384 | 482 | 72 | 10 |
| 6 | 1 | 15 | 105 | 385 | 478 | 71 | 10 |
| Exacto: | 1 | 15 | 105 | 385 | 480 | 72 | 10 |

coeficientes con significativo acierto en el grafo de Petersen, incluso al reducir el tamaño de

Figura 3.5: Grafo de Harary $H_{15,2}$ con 15 nodos y 30 enlaces.

muestra. Cuando $N = 10^6$ todos los coeficientes son correctos salvo dos de ellos con gaps pequeños.

Tabla 3.4: Rendimiento de F -MonteCarlo para el Dodecahedro $G(10, 2)$.

| Tamaño de muestra (10^i) | F_0^5 | F_1^5 | F_2^5 | F_3^5 | F_4^5 | F_5^5 | F_6^5 | F_7^5 |
|------------------------------|---------|---------|---------|---------|---------|---------|---------|---------|
| 3 | 1 | 30 | 370 | 2302 | 5618 | 4703 | 3563 | 0 |
| 4 | 1 | 30 | 377 | 2192 | 5251 | 4133 | 1247 | 204 |
| 5 | 1 | 30 | 375 | 2171 | 5312 | 4185 | 1193 | 61 |
| 6 | 1 | 30 | 375 | 2179 | 5333 | 4167 | 1111 | 145 |
| Exacto: | 1 | 30 | 375 | 2180 | 5310 | 4152 | 1120 | 120 |

F -MonteCarlo es capaz de adivinar los coeficientes menores F_i^5 , $i \in \{1, 2, 3\}$ para el Dodecahedro también, y presenta errores relativos reducidos en los restantes coeficientes.

Por último, realizamos un análisis de sensibilidad de la estimación global del polinomio ante errores locales, comparando Monte Carlo condicionado a configuraciones operativas y cortes contra Monte Carlo Crudo (con $R_L = 0$ y $R_U = 1$) y F -MonteCarlo. Específicamente, ilustraremos la efectividad de F -MonteCarlo y DCR -Interpol con dos casos de prueba, considerando los grafos K_6 y el grafo de Harary $H_{15,2}$ con 15 nodos y 30 enlaces, que se muestra en la Figura 3.5.

En primera instancia, comparamos F -MonteCarlo con DCR -Interpol condicionado y con CMC (es decir, d -Interpol), en un escenario de todos los terminales de K_6 con diámetro $d = 3$ bajo distintos tamaños de muestra $N = 10^i$, $i \in \{3, 4, 5\}$. El polinomio correcto

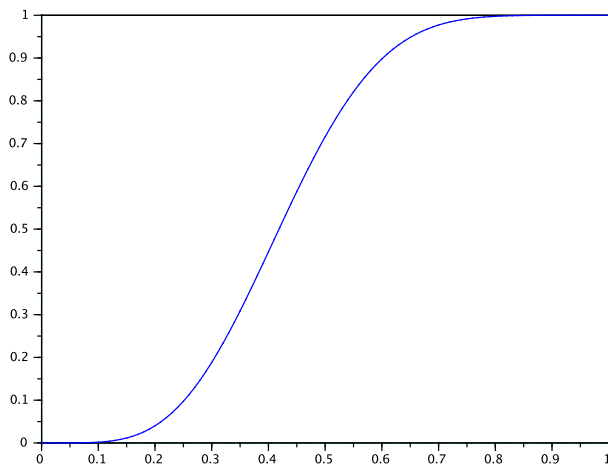


Figura 3.6: Representación gráfica de $R_{V,K_6}^3(p)$ en función de la probabilidad de operación $p \in [0, 1]$.

se muestra en la Figura 3.6, mientras que las Figuras 3.7, 3.8 y 3.9 muestran los respectivos gaps para F -MonteCarlo y $DCR - Interpol$ y $d - Interpol$. Fueron utilizados dos ciclos hamiltonianos disjuntos como configuraciones operativas de K_6 , mientras que los cortes consistieron en todos los enlaces incidentes a uno de los terminales.

F -MonteCarlo es capaz de seguir el polinomio objetivo con éxito en todo el intervalo $[0, 1]$. Sin embargo, el lector puede apreciar de las Figuras 3.8 y 3.9 amplios gaps de las técnicas basadas en interpolación en la proximidad a los bordes del compacto $[0, 1]$. Nuevamente, en los extremos donde p se aproxima a 0 o bien a 1 nos enfrentamos con la simulación de un evento raro. Más experimentos comprueban que estos gaps se tornan aún peor para redes completas K_n con $n > 6$ terminales, lo que evidencia la falta de robustez de técnicas basadas en interpolación ante eventos raros.

Luego consideramos el grafo de Harary $H_{15,2}$ en un escenario de fuente-terminal con diámetro $d = 6$, donde los terminales son los nodos indicados con cuadrados en la Figura 3.5. Hemos corrido F -MonteCarlo para tamaños de muestra $N = 10^i$, $i \in \{3, 4, 5, 6\}$ para determinar la evolución de su rendimiento para seguir el polinomio $R_{V,H_{15,2}}^6$. Ambas técnicas de interpolación evidencian problemas numéricos, pues los coeficientes tienden a desbordamiento al infinito. Como consecuencia, se presentan únicamente los resultados obtenidos mediante $F - MonteCarlo$.

Nuevamente, F -MonteCarlo ha logrado seguir al polinomio objetivo con reducidos niveles de error.

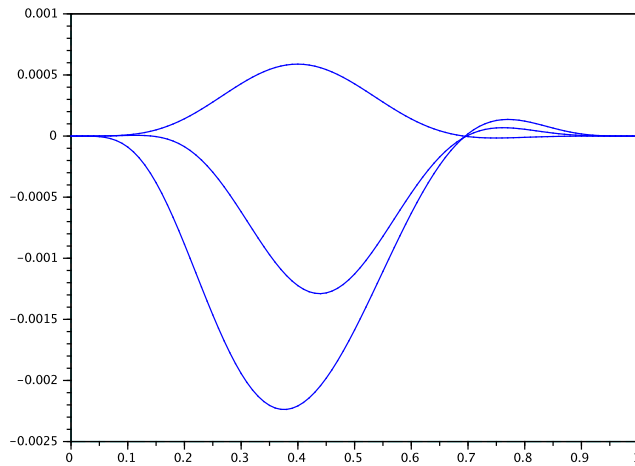


Figura 3.7: Representación gráfica de $R_{V,K_6}^3(p) - R_F(p)$ para $N = 10^i$, $i \in \{3, 4, 5\}$, donde R_F fue obtenido mediante F -MonteCarlo.

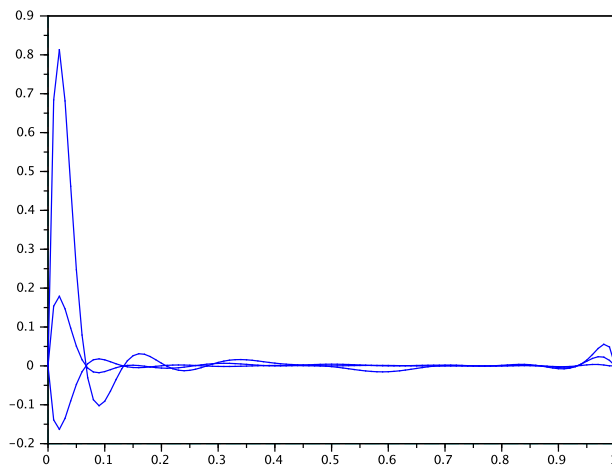


Figura 3.8: Representación gráfica de $R_{V,K_6}^3(p) - R_I(p)$, donde R_I fue obtenido mediante d -Interpol.

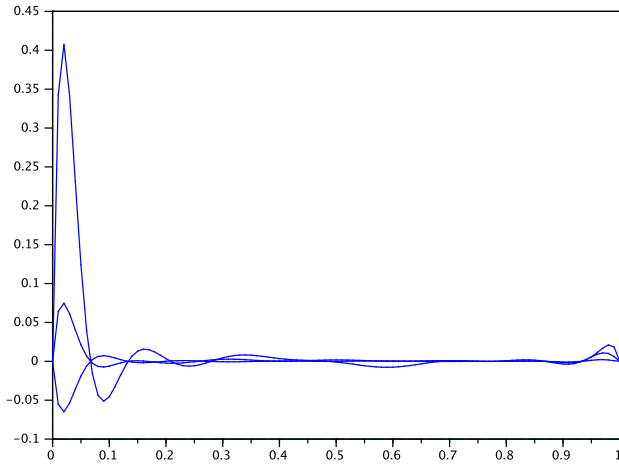


Figura 3.9: Representación gráfica de $R_{V,K_6}^3(p) - R_I(p)$, donde R_I fue obtenido mediante *DCR - Interpol.*

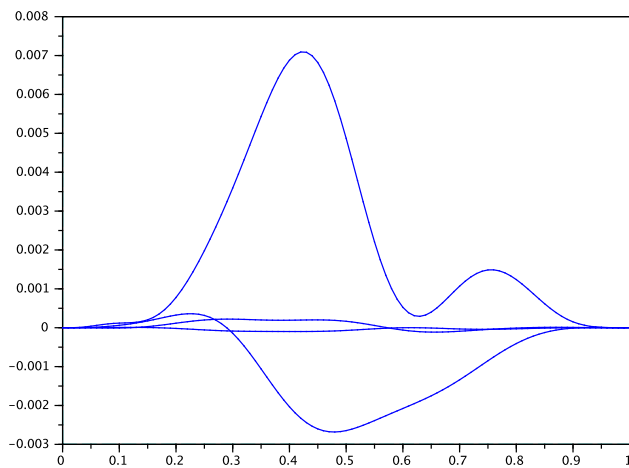


Figura 3.10: Representación gráfica de $R_{V,H_{15,2}}^6(p) - R_F(p)$, donde R_F fue obtenido mediante *F - MonteCarlo.*

Capítulo 4

Conclusiones

4.1 Conclusiones Generales

El problema de estudio de esta monografía, la evaluación de la diámetro-confiabilidad de una red, pertenece a la clase computacional \mathcal{NP} -Difícil, por lo que se halla en el corazón de la teoría de la complejidad. La teoría de confiabilidad de redes tiene como trabajos fundamentales el Teorema de árboles y matrices introducido por el padre de circuitos eléctricos, Kirchhoff, y la resolución del problema de flujo máximo y corte mínimo en redes con dos terminales, debido a Ford y Fulkerson.

La teoría de complejidad computacional nace a mediados del siglo XX , con la introducción de la máquina universal de Turing, y fue formalizada por Cook seguido de Karp, donde se definen la familia de problemas de decisión \mathcal{NP} -Completo, y los primeros 21 miembros de esta clase. La determinación de la complejidad computacional de la confiabilidad clásica debió esperar hasta inicios de la década de los 80, donde Ball y Provan prueban mediante reducciones polinomiales que estos problemas son al menos tan difíciles como los primeros 21 problemas de la lista de Karp. El problema de diámetro-confiabilidad de redes (DCR) generaliza a la confiabilidad clásica, y es por lo tanto al menos tan difícil como este último. Se desconoce un algoritmo polinomial (es decir, eficiente) que permita evaluar la DCR. Más aún, hallar tal algoritmo permitiría hallar algoritmos eficientes a todos los problemas \mathcal{NP} -Completo, resolviendo así uno de los enigmas célebres en matemática moderna y teoría computacional.

Una vez que se conoce la complejidad de la evaluación de la DCR, existen tres ramas para abordar el problema. La primera es estudiar la complejidad computacional de sub-problemas, y enriquecer el conocimiento mediante subproblemas especiales, que admiten solución en tiempo polinomial. La segunda es estudiar familias de grafos particulares que también admiten cómputo eficiente de la DCR. La tercera es desarrollar aproximaciones para calcular la DCR.

En esta monografía se discute la complejidad de sub-problemas para el cálculo de la DCR. Cuando el diámetro vale 1 el problema es trivial, mientras que ya hay problemas abiertos para $d = 2$. De hecho, hasta la fecha se desconoce la complejidad de la DCR en el caso de todos los terminales comunicados con diámetro $d = 2$, y existen conexiones entre este subproblema y el conteo de grafos de diámetro 2 dentro de un grafo arbitrario (y el primer problema es al menos

tan difícil como el segundo).

Asimismo, hemos sintetizado los trabajos [18, 68, 69], que salvo el primero que ya fue publicado, los restantes permanecen bajo evaluación científica. Allí se proponen tres métodos de Monte-Carlo para estimar el polinomio DCR [18, 69], a saber, $F - MonteCarlo$, $d - Interpol$ y $DCR - Interpol$, y uno para hallar la confiabilidad clásica [68], que dimos nombre $RelInterpol$.

El método $F - MonteCarlo$ se basa en el conteo de subgrafos, y se muestra más efectivo a la hora de aproximar el polinomio DCR objetivo. De hecho, en redes pequeñas hemos podido constatar el éxito de $F - MonteCarlo$ para aproximar polinomios DCR. $RelInterpol$ es el primer método basado en interpolación polinómica que figura en la literatura de confiabilidad de redes [68]. Dentro de sus principales características se hallan la utilización de cortes y árboles para minimizar la dimensión del polinomio a interpolar, el agregado recursivo de puntos de Newton y el redondeo de coeficientes en la base de Hilbert de $L^2[0, 1]$ de los polinomios de Legendre trasladados. En [68] se ha señalado su potencial aplicabilidad para abordar el problema principal de eventos raros en redes coherentes, ilustrado con un grafo de tamaño pequeño, y se han discutido diferentes generalizaciones, que fueron concretadas en los siguientes artículos [18, 69].

Pese a su sofisticado diseño, los coeficientes desbordan cuando se toman grafos de gran tamaño, y este inconveniente no lo hemos podido encauzar satisfactoriamente hasta la fecha, limitando el estudio a grafos de tamaño reducido. Su directa extensión al problema DCR fue denominada $d - Interpol$, tomando en consideración que la función a estimar es nuevamente un polinomio [18]. Además, hemos reemplazado la estimación puntual por otra que considera información previa de configuraciones operativas y cortes, apreciando que a partir de un método de estimación puntual con menor varianza conlleva a una estimación global más próxima a la correcta [69]. Es curioso constatar que pese a la lejanía de los coeficientes con el polinomio objetivo, la estimación resulta aproximar satisfactoriamente al polinomio DCR objetivo, dentro de nuestros casos de estudio de grafos de tamaño reducido. La escalabilidad de técnicas basadas en interpolación es un área de trabajo futuro.

Por otra parte, la familia de grafos que admiten evaluación polinomial de la DCR se limita a ciclos, caminos, bipartitos completos, escaleras, abanicos españoles y escaleras generalizadas [72]. El análisis asintótico aquí expuesto de la DCR se ha limitado al modelo de Gilbert, utilizando que los grafos aleatorios de Gilbert tienen casi seguramente diámetro 2, incluso cuando las probabilidades de operación decaen a una tasa no menor que el inverso de la raíz cuadrada del orden del grafo.

Parte de trabajo futuro es ampliar la lista anterior de grafos con cálculo exacto, y considerando modelos de grafos aleatorios complementarios al de Gilbert, enriqueciendo así la comprensión del problema de DCR.

4.2 Problemas Abiertos

A continuación se enumeran problemas abiertos que han surgido de este tratado monográfico, quizás yendo en orden de relevancia:

1. Hallar, si existe, un algoritmo de tiempo polinomial para evaluar la DCR o la confiabilidad clásica en forma exacta ante cualquier instancia de grafo. Resolver este problema abierto implicaría probar que $\mathcal{P} = \mathcal{NP}$.
2. En contraste con el problema anterior, probar que no existe tal algoritmo, y así determinar que $\mathcal{P} \neq \mathcal{NP}$.
3. Completar la clasificación de complejidad computacional de la DCR. Rellenar la Tabla 2.1.
4. Determinar la complejidad computacional del subproblema DCR con $K = V$ y diámetro $d \geq 3$.
5. Calcular la DCR de los grafos completos cuando $K = V$ y $d = 2$.
6. Determinar la complejidad de evaluación de la DCR en subfamilias de grafos cuando $K = V$ y $d = 2$ (por ejemplo, en grafos libres de triángulos).
7. Contar la cantidad de subgrafos de diámetro 2 dentro de K_n .
8. Calcular la DCR eficientemente, en casos distintos de ciclos, caminos, escaleras, escaleras generalizadas y abanicos españoles.
9. Hallar una fórmula de propagación del error en un polinomio, en términos de errores locales en estimaciones puntuales.
10. Analizar la escalabilidad de técnicas basadas en interpolación polinómica.
11. Proponer distancias alternativas entre un polinomio y la familia de polinomios a coeficientes enteros (por ejemplo tomando una subfamilia compacta de la segunda y utilizar la distancia de Hausdorff en $L^2[0, 1]$).
12. Realizar un estudio comparativo entre técnicas basadas en interpolación y conteo, para una cantidad estadísticamente significativa de grafos.
13. Estudiar el comportamiento asintótico de la DCR para grafos aleatorios que no coinciden con el modelo de Gilbert.

Bibliografía

- [1] Eytan Adar and Bernardo A. Huberman. Free riding on gnutella. *First Monday*, 5(10), sep 2000.
- [2] Réka Albert and Albert-László Barabási. Statistical mechanics of complex networks. *Reviews of Modern Physics*, 74:47–97, Jan 2002.
- [3] N. Alon and J. Spencer. *The Probabilistic Method (2nd. ed)*. Wiley-Interscience, 2000.
- [4] T.M. Apostol and F.V. Cantarell. *Calculus. 1, Cálculo con funciones de una variable, con una introducción al álgebra lineal*. Calculus. Reverté, 2005.
- [5] Michael O. Ball. Computational complexity of network reliability analysis: An overview. *IEEE Transactions on Reliability*, 35(3):230–239, aug. 1986.
- [6] Michael O. Ball and J. Scott Provan. Calculating bounds on reachability and connectedness in stochastic networks. *Networks*, 13(2):253–278, 1983.
- [7] R.E. Barlow and K.D. Heidtmann. Computing k-out-of-n system reliability. *IEEE Transactions on Reliability*, 33:58 – 61, oct 1984.
- [8] Robert Berger. *Undecidability of the Domino Problem (Memoirs ; No 1/66)*. American Mathematical Society, 1966.
- [9] N. Biggs. *Algebraic Graph Theory*. Cambridge Mathematical Library. Cambridge University Press, 1993.
- [10] Z.W. Birnbaum, J.D. Esary, S.C. Saunders, Boeing Scientific Research Laboratories. Mathematics Research Laboratory, WASHINGTON UNIV SEATTLE LAB OF STATISTICAL RESEARCH., and United States. Office of Naval Research. *Multi-component Systems and Structures and Their Reliability*. Defense Technical Information Center, 1960.
- [11] F T. Boesch, A. Satyanarayana, and C. L. Suffel. A survey of some network reliability analysis and synthesis results. *Networks*, 54(2):99–107, sep 2009.
- [12] B. Bollobás. The diameter of random graphs. *Transactions of the American Mathematical Society*, 267(1):pp. 41–52, 1981.

- [13] B. Bollobás. *Random Graphs*. Cambridge University Press, 2001.
- [14] B. Bollobás and O. Riordan. The diameter of a scale-free random graph. *Combinatorica*, 24(1):5–34, January 2004.
- [15] Jason I. Brown and Charles J. Colbourn. Non-stanley bounds for network reliability. *Journal of Algebraic Combinatorics*, 5(1):13–36, 1996.
- [16] J. D. Burtin. Extremal metric characteristics of a random graph i. asymptotic estimates. *Teor. Veroyatnost. i Primenen*, 19:740–754, 1974.
- [17] Yu Burtin. Assymptotic estimates of the diameter, independence and domination numbers of a random graph. *Soviet Mat. Doklady*, 14:497–501, 1973.
- [18] Eduardo Canale, Héctor Cancela, Franco Robledo, Pablo Romero, and Pablo Sartor. On the complexity of the diameter-constrained k-reliability problem. *Submitted - International Journal of Metaheuristics*. Available at <http://www2.um.edu.uy/psartor/robromsar2013.pdf>, 2014.
- [19] Eduardo Canale, Héctor Cancela, Franco Robledo, Gerardo Rubino, and Pablo Sartor. On computing the 2-diameter-constrained K-reliability of networks. *International Transactions in Operational Research*, 20(1):49–58, 2013.
- [20] H. Cancela and M. El Khadiri. A recursive variance-reduction algorithm for estimating communication-network reliability. *Reliability, IEEE Transactions on*, 44(4):595–602, 1995.
- [21] Héctor Cancela and Mohamed El Khadiri. The recursive variance-reduction simulation algorithm for network reliability evaluation. *IEEE Transactions on Reliability*, 52(2):207–212, 2003.
- [22] Héctor Cancela and Louis Petingi. Diameter constrained network reliability: exact evaluation by factorization and bounds. In *International Conference on Industrial Logistics (ICIL'2001)*, pages 359–366, 2001.
- [23] Héctor Cancela and Louis Petingi. Reliability of communication networks with delay constraints: computational complexity and complete topologies. *International Journal of Mathematics and Mathematical Sciences*, 2004:1551–1562, 2004.
- [24] Héctor Cancela and Louis Petingi. On the characterization of the domination of a diameter-constrained network reliability model. *Discrete Appl. Math.*, 154:1885–1896, August 2006.
- [25] Héctor Cancela and Louis Petingi. Properties of a generalized source-to-all-terminal network reliability model with diameter constraints. *Omega*, 35(6):659 – 670, 2007. Special Issue on Telecommunications Applications.

- [26] Héctor Cancela, Franco Robledo, Gerardo Rubino, and Pablo Sartor. Monte carlo estimation of diameter-constrained network reliability conditioned by pathsets and cutsets. *Computer Communications*, 36(6):611–620, 2013.
- [27] Héctor Cancela, Franco Robledo, Gerardo Rubino, and Pablo Sartor. Monte Carlo estimation of diameter-constrained network reliability conditioned by pathsets and cutsets. *Computer Communications*, 36(6):611 – 620, 2013.
- [28] Fan Chung and Linyuan Lu. *Complex Graphs and Networks*, volume 107. American Mathematical Society, 2006.
- [29] Charles J. Colbourn. *The Combinatorics of Network Reliability*. Oxford University Press, Inc., New York, NY, USA, 1987.
- [30] Charles J. Colbourn. Reliability issues in telecommunications network planning. In *Telecommunications network planning, chapter 9*, pages 135–146. Kluwer Academic Publishers, 1999.
- [31] Stephen A. Cook. The complexity of theorem-proving procedures. In *Proceedings of the third annual ACM symposium on Theory of computing, STOC '71*, pages 151–158, New York, NY, USA, 1971. ACM.
- [32] Thomas H. Cormen, Clifford Stein, Ronald L. Rivest, and Charles E. Leiserson. *Introduction to Algorithms*. McGraw-Hill Higher Education, 2nd edition, 2001.
- [33] Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory (Wiley Series in Telecommunications and Signal Processing)*. Wiley-Interscience, 2006.
- [34] Institut National de Recherche en Informatique et en Automatique, M.E. Khadiri, G. Rubino, and IRISA (117). *A Monte Carlo Method Based on Antithetic Variates for Network Reliability Computations*. Rapports de recherche. Institut National de Recherche en Informatique et en Automatique, 1992.
- [35] Jack Edmonds and Richard M. Karp. Theoretical improvements in algorithmic efficiency for network flow problems. *J. ACM*, 19(2):248–264, apr 1972.
- [36] P. Erdos and A. Rényi. On random graphs. *Publicationes Mathematicae*, 6:290–297, 1959.
- [37] S. Even and R.E. Tarjan. Network flow and testing graph connectivity. *SIAM J. Computing*, 4:507–518, 1975.
- [38] M. J. Fischer and M. O. Rabin. Super-exponential complexity of Presburger arithmetic. In R. M. Karp, editor, *Complexity of Computation*, pages 27–41, American Mathematical Society, Providence, RI, 1974.
- [39] George Fishman. *Monte Carlo*. Springer Series in Operations Research and Financial Engineering. Springer, 1996.

- [40] L. R. Ford and D. R. Fulkerson. *Flows in Networks*. Princeton University Press, 1962.
- [41] Michael R. Garey and David S. Johnson. *Computers and Intractability: A Guide to the Theory of NP-Completeness*. W. H. Freeman and Company, New York, NY, USA, 1979.
- [42] E. N. Gilbert. Random graphs. *Annals of Mathematical Statistics*, 30:1141–1144, 1959.
- [43] C. Godsil and G.F. Royle. *Algebraic Graph Theory*. Graduate Texts in Mathematics. Springer New York, 2001.
- [44] M. Horváthová. On $(k,1)$ -radius of random graphs. *Acta Mathematica Universitatis Comenianae*, 75(2):149–152, 2006.
- [45] Kin-Ping Hui, Nigel Bean, Miro Kraetzl, and Dirk P. Kroese. The cross-entropy method for network reliability estimation. *Annals of Operations Research*, 134(1):101–118, 2005.
- [46] E. Isaacson and H.B. Keller. *Analysis of numerical methods*. Dover Books on Mathematics Series. Dover Publications, Incorporated, 1994.
- [47] M. Karol, P. Krishnan, and J.J. Li. Using overlay networks to improve voip reliability. In Farn Wang, editor, *Automated Technology for Verification and Analysis*, volume 3299 of *Lecture Notes in Computer Science*, pages 392–401. Springer Berlin Heidelberg, 2004.
- [48] R. M. Karp. Reducibility among combinatorial problems. In R. E. Miller and J. W. Thatcher, editors, *Complexity of Computer Computations*, pages 85–103. Plenum Press, 1972.
- [49] G.O.H. Katona. *A theorem of finite sets*. Akadémia Kiadó, Budapest, 1968.
- [50] G. Kirchoff. Über die auflösung der gleichungen, auf welche man bei der untersuchung der linearen verteilung galvanischer ströme geführt wird. *Ann. Phys. Chem.*, 72:497–508, 1847.
- [51] B. Kolman and R.E. Beck. *Elementary Linear Programming with Applications*. Computer science and scientific computing. Academic Press, 1995.
- [52] Dirk P. Kroese, Kin-Ping Hui, and Sho Nariai. Network reliability optimization via the cross-entropy method. *IEEE Transactions on Reliability*, 56(2):275–287, 2007.
- [53] J. B. Kruskal. On the Shortest Spanning Subtree of a Graph and the Traveling Salesman Problem. In *Proceedings of the American Mathematical Society*, 7, 1956.
- [54] H. Kumamoto, K. Tanaka, K. Inoue, and E. J. Henley. Dagger sampling Monte Carlo for system unavailability evaluation. *IEEE Transactions on Reliability*, 29(2):376–380, 1980.
- [55] P. Lancaster and M. Tismenetsky. *The Theory of Matrices: With Applications*. Computer Science and Scientific Computing Series. Academic Press, 1985.

- [56] I.U.V. Matiyasevich. *Hilbert's Tenth Problem*. Foundations of computing. MIT Press, 1993.
- [57] Albert R. Meyer and Larry J. Stockmeyer. The equivalence problem for regular expressions with squaring requires exponential space. In *SWAT (FOCS)*, pages 125–129, 1972.
- [58] J. Moon and L. Moser. Almost all $(0,1)$ matrices are primitive. *Studia Sci. Math. Hungar.*, 1:153–156, 1966.
- [59] E. Moore. The shortest path through a maze. *Ann. Computational Lab. Harvard University*, 30:285–292, 1959.
- [60] Fred Moskowitz. The analysis of redundancy networks. *American Institute of Electrical Engineers, Part I: Communication and Electronics, Transactions of the*, 77(5):627–632, 1958.
- [61] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information (Cambridge Series on Information and the Natural Sciences)*. Cambridge University Press, 1 edition, jan 2004.
- [62] Gonzalo Perera. *Probabilidad y Estadística*. Fin de Siglo, Montevideo, Uruguay, 2011.
- [63] L. Petingi and J. Rodriguez. Reliability of networks with delay constraints. In *Congressus Numerantium*, volume 152, pages 117–123, 2001.
- [64] Louis Petingi. A diameter-constrained network reliability model to determine the probability that a communication network meets delay constraints. *WTOC*, 7:574–583, June 2008.
- [65] G.M. Phillips. *Interpolation and Approximation by Polynomials*. CMS Books in Mathematics. Springer, 2003.
- [66] Scott J. Provan and Michael O. Ball. The Complexity of Counting Cuts and of Computing the Probability that a Graph is Connected. *SIAM Journal on Computing*, 12(4):777–788, 1983.
- [67] M.O. Rabin. *Recursive Unsolvability of Group Theoretic Problems*. Princeton University, 1957.
- [68] Franco Robledo, Pablo Gabriel Romero, and Pablo Sartor. A novel interpolation technique to address the Edge-Reliability problem. In *RNDM'13 - 5th International Workshop on Reliable Networks Design and Modeling (RNDM'13)*, pages 77–82, Almaty, Kazakhstan, sep 2013.
- [69] Franco Robledo, Pablo Sartor, and Pablo Romero. On the complexity of the diameter-constrained k -reliability problem. *Submitted - Special Issue of Optical Switching and Networking Journal, Elsevier*, 2014.

- [70] Pablo Romero. *Mathematical Analysis of Scheduling Policies in Peer-to-Peer Video Streaming Networks*. PhD thesis, Pedeciba Informática. Universidad de la República, Montevideo, Uruguay, november 2012.
- [71] G. Rubino and B. Tuffin. *Rare event simulation using Monte Carlo methods*. Wiley, 2009.
- [72] Pablo Sartor. *Propriétés et méthodes de calcul de la fiabilité diamètre-bornée des réseaux*. PhD thesis, INRIA/IRISA, Université de Rennes I, Rennes, France, december 2013.
- [73] A. Satyanarayana and Mark K. Chang. Network reliability and the factoring theorem. *Networks*, 13(1):107–120, 1983.
- [74] K.S. Trivedi. *Probability & Statistics With Reliability, Queuing And Computer Science Applications, 2Nd Ed.* Wiley India Pvt. Limited, 2008.
- [75] Alan Turing. On computable numbers with an application to the Entscheidungsproblem. *Proceeding of the London Mathematical Society*, 1936.
- [76] L. Valiant. The complexity of enumeration and reliability problems. *SIAM Journal on Computing*, 8(3):410–421, 1979.
- [77] J.H. van Lint and R.M. Wilson. *A Course in Combinatorics*. Cambridge University Press, 2001.
- [78] Vijay V. Vazirani. *Approximation Algorithms*. Springer-Verlag New York, Inc., New York, NY, USA, 2001.
- [79] D. J. Watts and S. H. Strogatz. Collective dynamics of ‘small-world’ networks. *Nature*, 393:440–442, June 1998.

Lista de Figuras

| | | |
|------|---|----|
| 1.1 | Red extendida. Agrega una super-fuente s^* , que incide a la fuente original s con un arco de capacidad $ \varphi $. El conjunto S no contiene s^* ni t . La línea gris representa posibles arcos para ambos sentidos entre nodos del conjunto S y $V - S$. | 23 |
| 1.2 | Pseudocódigo correspondiente al Algoritmo de Ford y Fulkerson. | 26 |
| 1.3 | Red ejemplar con flujo inicial φ . | 28 |
| 1.4 | Red ejemplar con flujo final φ' . | 28 |
| 2.1 | Complejidad de la DCR en términos del diámetro d y la cantidad de terminales $ K $. | 47 |
| 2.2 | Ejemplo concreto de construcción de grafo auxiliar G' , con terminales $\{s, t\}$, $d = 6$ (camino de largo $d' = 3$), seguido de bipartito completo $K_{3,3}$ y terminal t . | 48 |
| 2.3 | Ejemplo de cubrimiento. | 50 |
| 2.4 | La familia de grafos \mathcal{G}_h . | 56 |
| 2.5 | Ejemplo de camino s, t en relación con la secuencia de conjuntos V_i . | 56 |
| 2.6 | | 57 |
| 2.7 | Pseudocódigo para hallar la DCR en grafos \mathcal{G}_h . | 59 |
| 2.8 | Topología de un miembro de \mathcal{G}_3 . | 60 |
| 3.1 | Método de Monte Carlo condicionado a cortes y configuraciones minimales. | 71 |
| 3.2 | Red ejemplar con $n = 7$ nodos y $m = 14$ enlaces. | 72 |
| 3.3 | Grafo de Petersen. | 74 |
| 3.4 | Dodecahedro. | 74 |
| 3.5 | Grafo de Harary $H_{15,2}$ con 15 nodos y 30 enlaces. | 77 |
| 3.6 | Representación gráfica de $R_{V,K_6}^3(p)$ en función de la probabilidad de operación $p \in [0, 1]$. | 78 |
| 3.7 | Representación gráfica de $R_{V,K_6}^3(p) - R_F(p)$ para $N = 10^i$, $i \in \{3, 4, 5\}$, donde R_F fue obtenido mediante F -MonteCarlo. | 79 |
| 3.8 | Representación gráfica de $R_{V,K_6}^3(p) - R_I(p)$, donde R_I fue obtenido mediante $d - Interpol$. | 79 |
| 3.9 | Representación gráfica de $R_{V,K_6}^3(p) - R_I(p)$, donde R_I fue obtenido mediante $DCR - Interpol$. | 80 |
| 3.10 | Representación gráfica de $R_{V,H_{15,2}}^6(p) - R_F(p)$, donde R_F fue obtenido mediante $F - MonteCarlo$. | 80 |

