UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
PROGRAMA DE MAESTRÍA Y DOCTORADO EN CIENCIAS MATEMÁTICAS Y DE LA ESPECIALIZACIÓN EN ESTADÍSTICA APLICADA

Resolubilidad del consenso a través de topología combinatoria

T E S I S

QUE PARA OPTAR POR EL GRADO DE:

MAESTRO EN CIENCIAS MATEMÁTICAS

PRESENTA:

JESÚS JORGE ARMENTA SEGURA

Director

DR. SERGIO RAJSBAUM GORODEZKY

INSTITUTO DE MATEMÁTICAS, UNAM

Ciudad Universitaria, Ciudad de México, Junio, 2022.

Universidad Nacional Autónoma de México
UNAM
Biblioteca Central
Dirección General de Bibliotecas de la UNAM

UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

A Jesucristo, testigo único y fidedigno de cómo la calamidad templa mi espíritu para forjar una espada mítica.

Agradecimientos

A Dios, por todas las bendiciones y pruebas de esta vida.

A mis padres y hermanos, por coincidir conmigo en este plano.

Al dr. Sergio Rajsbaum, por ser mi tutor de maestría y por sus comentarios al revisar este trabajo.

Al CONACyT, por su apoyo invaluable mediante la beca nacional de posgrado.

A los taquitos de arrachera sobre Av. Papalotl/eje 10, por ser el único negocio abierto a la una de la mañana cuando necesité proteína con desesperación para seguir haciendo la tesis sin desfallecer (aunque sospecho que me hicieron más mal que bien).[1]

Y hablando de carne para tacos, quiero agradecer al perrito Toby (2018 - ∞), por ser pequeño, cobarde y carecer de utilidad alguna ya que no protege la casa, no ladra cuando se requiere y sólo sabe temblar como menso sin venir a cuento. Pero sobre todo por rellenar el vacío gigantesco que dejó mi querido Winny (2003 - 2018) con su partida.

Y no puede faltar agradecerle a usted, estimado lector, por leer este trabajo.

A todos, ¡muchas gracias!

[1] Tienen de suadero, de *bisté*, al pastor (5x25 de lunes a jueves), tortas, *gringas*, orden de cebollitas a 20 varos (¿o era a 25?) y hasta venden flanecitos por si te *salaste la lengua*. Comprobé empíricamente que no son *fitness*.

Índice general

Introducción.

El problema del consenso consiste en n agentes con valores iniciales dados que quieren decidir uno de ellos. ¿Cómo podrían lograrlo?

Una de las metas más importantes de la computación distribuida es *imitar* el cómputo secuencial con varias computadoras trabajando al mismo tiempo. La finalidad de esto es mejorar el rendimiento (dos cabezas piensan mejor que una) al tiempo que se evita el sobrecalentamiento, fruto del incremento de poder al que las computadoras son sometidas año con año.[2]

Para lograr esta meta, el problema del consenso surge como una tarea fundamental para conseguir que varias computadoras trabajen como una, sin embargo se han hallado casos en los que sencillamente es imposible (por ejemplo cuando las computadoras no se pueden comunicar entre sí), lo que genera el problema lateral de **la resolubilidad del consenso** que consiste en determinar con precisión cuándo es posible alcanzarlo y cuándo no. El objetivo principal de esta tésis es resolver dicho problema, por lo que a continuación se presenta una disertación sobre el estado del arte ya que esta no es la primera vez que se aborda el problema.

[2]Dicho de forma muy burda, en lugar de duplicar el poder de una computadora, *ahora se ejecutan dos al mismo tiempo*. Para una discusión detallada consúltese el prólogo y el capítulo 1 del libro [23], donde se explica la *ley de Amdahl* que formaliza el hecho de que "dos computadoras" no necesariamente equivalen a "una sola con el doble de potencia".

Trabajos relacionados Históricamente, el estudio de la *resolubilidad del consenso* es muy extenso y se puede remontar hasta la década de los años ochenta. Ahí, se puede encontrar el primer resultado relevante conocido en [16], donde los autores Fischer, Lynch y Paterson probaron que cualquier protocolo de consenso en un sistema asíncrono puede no terminar jamás si alguien muere sin que haya forma de saberlo (quizá sólo esté muy lento y le tome un puñado de milenios volver a reaccionar). Posteriormente, Santoro y Widmayer [34] proporcionaron la primera caracterización extensa de la resolubilidad del consenso en sistemas síncronos propensos a fallas en la comunicación, usando los argumentos de bivalencia presentados en [16]. En su artículo, mostraron que el consenso es imposible si algún agente no recibe $n-1$ mensajes en alguna ronda arbitraria y desconocida *a priori* (quizá podría no pasar nunca, quizá pase. No hay forma de saberlo ni cuando). Entonces, Schmid, Weiss y Keidar refinaron esta cota de mensajes al probar en [35] que el consenso aún puede ser resuelto si el número de mensajes perdidos es de orden cuadrático, siempre que nunca aíslen al proceso (es decir que la condición de $n-1$ mensajes perdidos de Santoro y Widmayer). A pesar de que se habían obtenido tantos resultados y tan fructíferos, para principios del siglo XXI todavía había una entendimiento más bien vago sobre la **resolubilidad del consenso**. En el año 2002, Moses y Rajsbaum presentaron en el artículo [29] la *herramienta de las capas* la cual permite analizar ejecuciones con un *buen comportamiento* en términos de resolución del consenso. Además, gracias a esta herramienta, fueron capaces de hacer un análisis independiente del modelo (es decir, que no depende de ser síncrono, asíncrono, que los mensajes se distribuyan a través de un *buffer* de mensajes o por señales de humo, etc.), lo que significó un gran avance rumbo a un entendimiento unificado del problema. Unos de los resultados más recientes sobre resolubilidad del consenso pueden encontrarse en [39, 31], donde se caracteriza para adversarios de mensajes cerrados y generales (ver [1]). En el año 2020, Armenta-Segura, Ledent y Rajsbaum presentaron en el artículo [4] una caracterización para la resolubilidad del problema del acuerdo aproximado[3] para dos agentes utilizando lógica epistémica, y también presentaron un algoritmo basado en mismo resultado. En

[3]En el problema del acuerdo aproximado, los agentes deben elegir valores que estén a distancia a lo más ε entre sí, dada una $\varepsilon > 0$ fija.

mismo trabajo, los autores formalizaron la noción topológica del *conocimiento grupal* en términos de vecindades, sobre la que se basa su algoritmo.

Perspectivas múltiples Este estudio tan extenso en el tiempo y en los enfoques ha conllevado a que se utilicen muchas herramientas matemáticas de índoles muy diversas, desde un acercamiento combinatorio [10, 34], hasta topología de punto fijo [31, 2], pasando por herramientas raras pero útiles como topología combinatoria [22] y lógica epistémica [32]. Entonces uno puede verse tentado a preguntarse sobre puentes. Por ejemplo en el artículo [31] se descubrió un puente entre topología de punto fijo y los argumentos de bivalencia de [16] en términos de límites, mientras que en [10, 34] se esbozó una relación entre combinatoria y lógica epistémica a través de topología combinatoria (relación mucho más explotada y desarrollada en [18, 22]). Finalmente, en el presente trabajo se propone un modelo de topología combinatoria basado en lógica epistémica [22, 18], donde los resultados principales de [34, 39, 31] son interpretados y confrontados entre sí. Además, se proporciona una caracterización de la resolubilidad del consenso en cualquier sistema distribuido basada en la relación entre el **conocimiento común** y alcanzar acuerdos.

El punto de vista epistémico se remonta a principios de los ochentas [32, 28], donde se mostró que el *conocimiento común* (definido por primera vez, al menos hasta donde mejor sabemos, en [25]) es necesario para alcanzar acuerdos, y a veces suficiente en algunos casos (ver capítulo 6 del libro [32]). Posteriormente, en [27] se presentó un protocolo óptimo basado en conocimiento común para el *consenso continuo*, el cual es una variación del consenso en el que los valores iniciales cambian con el tiempo (por ejemplo la base de datos de la página web de un periódico). Por último, los modelos de topología combinatoria para problemas de cómputo distribuído ya han sido propuestos en diversos trabajos, como por ejemplo en el artículo [19] donde Goubault, Lazic, Ledent y Rajsbaum analizaron el problema del *equality negation* bajo esta perspectiva, y también en la tesis de licenciatura [3], donde Armenta-Segura propuso un modelo de topología combinatoria para el problema criptográfico de las Cartas Rusas y aprovechó el poder

del modelo para generalizarlo.

Organización Esta tesis de maestría se divide en cuatro capítulos:

- En el Capítulo 1 se expone la teoría topológica-epistémica sobre la que se cimentan los resultados de esta tesis. Dado que esta área no es muy famosa, se proveen ejemplos y discusiones intuitivas y filosóficas para explicar con claridad sus conceptos.
- En el Capítulo 2 se extiende lo expuesto en el capítulo anterior para el caso de lógica epistémica dinámica, la cual estudia los cambios de conocimiento en los sistemas distribuidos.
- En el Capítulo 3 se aplica la teoría topológica-epistémica para estudiar el problema del consenso. También se proporcionan varios teoremas y lemas importantes para comprender la forma de los modelos simpliciales del consenso (por ejemplo que el consenso binario induce esferas, Teorema 3.2.2), así como de su tarea y la naturaleza topológica subyacente en su resolubilidad.
- En el Capítulo 4 se presenta el resultado más importante de la tesis: el Teorema 4.1.1 que caracteriza la resolución del consenso. Se discuten algunas consecuencias del mismo, y se discuten los resultados de [39, 31] donde se proporcionan caracterizaciones del consenso para casos muy particulares.
- Finalmente, en el Capítulo 5 están las conclusiones.

La escritura de este trabajo pretende ser *jovial* para ser accesible al mayor público posible y que no se requieran conocimientos previos de nivel posgrado para su comprensión. Sin embargo, sí que es conveniente tener los siguientes conocimientos previos de nivel licenciatura para facilitar su comprensión:

- Un conocimiento elemental de lógica matemática y cierta familiaridad con sistemas de primer orden (en particular el sistema con implicación material que describe la lógica clásica).

- Cierta experiencia leyendo/escribiendo pruebas, al menos la que se adquiere al final de un primer año de licenciatura.[4]

  Es menester advertir que existen muchas pruebas densas como las del Capítulo 3.

- Nociones básicas de álgebra abstracta y matemáticas discretas. Concretamente álgebra de conjuntos, particiones, relaciones de equivalencias, conjuntos potencia, inducción y recursión matemática y teoría de grafos (los cuales son el primer paso previo a topología combinatoria).

- Alguna experiencia básica en ciencias de la computación (aunque no es necesario saber programar). Más concretamente en lenguajes formales y gramáticas formales (por ejemplo lenguajes libres de contexto y generaciones de la forma de Backus-Naur), así como los conceptos de *sintaxis* y *semántica* (así como la diferencia entre ambos).

- Es bastante conveniente tener experiencia con sistemas distribuidos pero no es indispensable dado el enfoque teórico del trabajo y los ejemplos introducidos.

En caso de que el lector desee rellenar algún hueco que pudiera tener,[5] a continuación se enumeran algunas referencias útiles:

- El libro de Enderton [13] es perfecto para iniciarse en lógicas formales.

- El *poderosísimo Laveaga* [24] es el libro perfecto para iniciarse en álgebra abstracta y matemáticas discretas, aunque el todopoderoso Fraleigh [17] y el buen Rotman [33] no se quedan atrás (pero son menos didácticos).

- El bien conocido Bondy [8] es uno de los libros más estándar para iniciarse en teoría de gráficas.

Finalmente, es posible extender el entendimiento sobre la parte computacional a través del libro de Herlihy y Shavit [23] (para cómputo distribuido), así como los libros [11, 36] (para gramáticas y lenguajes formales, semántica y sintaxis).

[4] En la Facultad de Ciencias de la UNAM en México, alumnos de este nivel son capaces de probar con soltura propiedades básicas de los números reales y hacer construcciones con regla y compás, como en los *elementos de Euclides* [14]

[5] Y reducir su grupo fundamental al trivial. Este fue el mejor chiste que nadie leyó nunca [21]

Capítulo 1

Un modelo simplicial para lógica epistémica

En este capítulo se presenta el marco teórico de lógica epistémica basada en complejos simpliciales cromáticos como en [18, 37]. Además se presenta un ejemplo sobre cómo aplicarlo en la "*vida real*" para obtener cierta familiaridad con los conceptos. Aunque el consenso no es mencionado con frecuencia, toda esta teoría tiene como fin estudiarlo junto al concepto de *conocimiento común* en términos de *conocimiento grupal*, muy importante para la caracterización presentada en el capítulo 4.

1.1. Fundamentos de lógica epistémica

La lógica epistémica es la rama de la lógica modal que estudia el conocimiento desde una perspectiva formal, y analiza problemas del tipo "¿Cómo puede descubrirse *algo* dadas ciertas restricciones?". Como rama de la lógica que es, consta de un lenguaje con sintaxis propia (las reglas con las que los símbolos pueden pegarse entre sí) y semántica (lo que significan las "palabras" determinadas por la sintaxis).

Un problema inicial de la lógica epistémica es determinar lo que puede conocerse o no. Intuitivamente, es posible conocer sujetos ("yo conozco a Sergio") pero también proposiciones ("yo sólo sé que no sé nada") incluyendo el caso particular de las variables proposicionales parametrizadas por un sujeto y un predicado, por ejemplo:

$$\underbrace{\textit{Anita}}_{\textit{sujeto}}\ \underbrace{\textit{lava}}_{\textit{verbo}}\ \underbrace{\text{la tina}}_{\textit{predicado}}$$

El presente trabajo se centra en este último tipo de cuestiones, pues son suficientes para estudiar el problema del consenso (como se muestra en capítulos futuros). El lenguaje especializado en este tipo de proposiciones se conoce como el **lenguaje básico epistémico modal**, que a continuación se explica.

1.1.1. Sintáxis para lenguajes básicos epistémicos modales

A la hora de observar conceptos de la forma **Yo sé que Anita lava la tina**, lo primero que salta a la vista es que tienen las siguientes partes:

- Los agentes que aprenden las proposiciones.
- Las proposiciones que pueden ser aprendidas por ellos, parametrizadas a su vez por otros agentes a través del *sujeto*.

Mientras los agentes pueden ser formalizados como los elementos de un conjunto finito A, las variables proposicionales están definidas en términos del sujeto y su acción. Para ilustrar esto, considérense los siguientes ejemplos:

1. Anita lava la tina.
2. Los Tigres UANL tienen sólo 3 puntos de 21 posibles en el torneo.

En el primer ejemplo, la agente Anita tiene asociada la propiedad "lavar la tina" (su acción). En el segundo ejemplo, Tigres UANL tiene asociado el valor 3 representando sus puntos en el torneo (también se le puede asociar el valor 3/21). En general, el predicado junto con el verbo pueden corresponder a un valor asociado:

1. Si "lavar la tina" corresponde a una propiedad p entonces Anita tiene asociado el valor p.
2. Los Tigres UANL tienen asociado el valor 3/21.

De esta forma, es posible definir un dominio $\mathcal{V}$ de propiedades (como "lavar la tina") o bien valores (como 3 o 3/21), de manera que las **variables proposicionales** se definen como pares del producto cartesiano $A \times \mathcal{V}$ denotadas $(a, v) = p_{a,v}$ tales que $p_{a,v}$ significa que "el agente a tiene asociado el valor v" o "el agente a satisface la proposición v".

Finalmente, estas fórmulas pueden componerse entre sí para obtener fórmulas más grandes utilizando conectivos de la lógica clásica:

1. Si Anita lava la tina entonces los Tigres UANL pierden el clásico regio.
2. Si los Tigres UANL ganan el clásico regio entonces Anita no lava la tina.[1]
3. Juanito viajó a Zacatecas pero Pedrito viajó a Yucatán. *Te digo esto para que sea de tu conocimiento.*

Formalizando lo anterior, se presenta la siguiente gramática en la forma de Backus-Naur, extraída de [18], que define el lenguaje de las fórmulas epistémicas $\mathcal{L}_{\mathcal{K}}(AP)$ con

[1] ¿A qué equipo le va Anita?

$AP \subseteq A \times \mathcal{V}$ siendo un conjunto no vacío de variables proposicionales denominadas ***atómicas***.[2]

$$\varphi ::= p \mid \neg\varphi \mid (\varphi \wedge \varphi) \mid K_a(\varphi) \qquad p \in AP,\ a \in A$$

Este lenguaje también se denota como $\mathcal{L}_\mathcal{K}$ si los conjuntos A y AP están implícitos. A continuación se presenta una explicación sobre los significados de cada uno de los operadores.

1. Cuando φ es $p \in P$, es una variable proposicional. Nótese que estos son los únicos símbolos terminales por lo que todas las fórmulas de $\mathcal{L}_\mathcal{K}$ consisten en combinaciones de variables proposicionales acorde a las otras reglas.

2. El hecho de que φ pueda ser $\neg\varphi$ significa que el lenguaje incluye negación. Por ejemplo, dado $p_{a,0}$ significando que "el agente a tiene valor 0", $\mathcal{L}_\mathcal{K}$ contiene también la fórmula "el agente a no tiene el valor 0", es decir, $\neg p_{a,0}$

3. φ siendo $(\varphi \wedge \varphi)$ permite pegar dos fórmulas con la conjunción. Si se combina con la negación, esto proporciona disyunción y por tanto también implicación material acorde a las reglas de inferencia de la lógica clásica.

4. Finalmente, el operador del conocimiento $K_a(\varphi)$ se lee como "el agente a sabe φ". Nótese que toda la teoría desarrollada hasta ahora es insuficiente para describir una *semántica* de este operador en términos de los otros operadores.

Este lenguaje epistémico vino junto con varios sistemas axiomáticos como el $\mathbf{S5}_n$ (usado implícitamente en este trabajo) o el $\mathbf{KB4}_n$ (empleado en trabajos como [20] donde los agentes involucrados pueden morir eventualmente). El lector interesado en estudiar estos sistemas a profundidad y gran detalle puede remitirse a las fuentes [7] (Capítulo 4) y [12] (Capítulos 7.2 y 7.3).

1.2. Usando el lenguaje básico epistémico modal

A continuación se presenta un ejemplo de cómo esta versión del lenguaje básico epistémico modal es lo suficientemente expresiva para modelar cuestiones de conocimiento:

Ejemplo 1 (El problema de los memes robados) *En un mundo post-apocalíptico donde el Internet es historia antigua, los últimos memes sobre la tierra son hojas impresas pequeñas, muy vulnerables a la lluvia y a las flamas (lo que los hace más valiosos aún). Un grupo de tres amigos: Alice, Bob y Catalina la grande,*[3] *tienen un gran tesoro*

[2]Este es una versión muy centrada en conocimiento y en cosas "que pasan o no pasan", por lo que el único operador modal que incluye es el de conocimiento y no considera al rombo de la posibilidad ni al cuadrado de la necesidad. No obstante sí que es posible hacer lógica epistémica considerando a estos últimos.

[3]La gran zarina (no confundir con la marca de galletas) fue resucitada con magia chachalaca-dentista marxista-bolchevique. En el fin del mundo este tipo de cosas pasan con mucha frecuencia.

de memes para su deleite propio. Sin embargo, un día horrendo desaparecieron misteriosamente, sin mayor explicación.
Dado que no hay animales salvajes, otros humanos, inundaciones o incendios recientes, los memes sólo pudieron ser robados y el ladrón (o ladrones) está entre ellos. ¿Cómo podrían los inocentes encontrar a los culpables?

A continuación se presenta una disertación sobre herramientas útiles para entender este problema en términos de lenguaje básico epistémico modal. Posteriormente, en la Sección 2.3 se plantea lo que es una solución para este problema (y se anticipa su relación tan íntima con el consenso) y finalmente en la Sección 4.2.1 se presenta una solución.[4]

El lenguaje básico epistémico modal útil para este problema es el siguiente. Los agentes son A (Alice), B (Bob) y C (Catalina, también llamada *Cath* para ahorrar espacio [5]), mientras que las proposiciones y valores son los *estados de culpabilidad*: 0 si se es inocente y 1 en otro caso. Las proposiciones atómicas para este $\mathcal{L}_K$ son $p_{X,0}$ para el agente X siendo inocente y $p_{X,1}$ para el agente X siendo culpable. A continuación se presentan algunos ejemplos de fórmulas compuestas:

- $p_{A,0} \wedge p_{C,1}$. Significa que Alice es inocente pero Catalina no lo es. Vale la pena mencionar que, para casos con valores binarios, se suele establecer como axioma que $p_{A,0}$ si y solo si $\neg p_{A,1}$
- $\neg(p_{B,1} \wedge \neg p_{A,0})$. El significado inmediato es "no es cierto que Bob sea culpable pero no Alice". También puede significar"Bob no es el ladrón, o Alice es inocente" (disyunción), o bien "*Si Bob es el culpable entonces Alice es inocente*" (implicación material).
- $K_B(p_{A,1})$. Significa que Bob sabe que Alice es culpable.
- $K_A(p_{C,0})$. Significa que Alice sabe que Catalina es inocente.

El siguiente paso es descubrir una forma de interpretar el operador de conocimiento en términos formales para poder demostrar la culpabilidad/inocencia de un agente desde el punto de vista de otro, en una situación dada. Para lograr esto, va a ser necesario añadir un nuevo factor: *incertidumbre*, representada por la existencia de *mundos posibles* en los que un agente pueda vivir, dado que *conoce lo que conoce*.

[4]Este ejercicio es meramente informativo y su finalidad es servir como un ejemplo de aplicaciones de toda la teoría presentada aquí. Por lo tanto, no se recomienda saltar a la lectura directa de la secciones 2.3 y 4.2.1 sin antes haber leído lo anterior.

[5]Catalina la grande, la más célebre de todas las zarinas de Rusia, detesta que le llamen simplemente "Cath" pero a nadie le importa: ni a Alice, ni a Bob, ni al que escribe la tesis, ni a su tutor, ni a los sinodales que evaluaron la tesis, ni al rector de la UNAM, etc. Pues en el fin del mundo el anarquismo irrespetuoso es algo muy común: no existen dioses, reyes ni héroes, sólo pedazos andantes de carne que buscan sobrevivir (y reír con memes impresos muy frágiles y de combustión fácil).

1.2.1. Hacia un entendimiento concreto del conocimiento

El conocimiento es el dual natural de la incertidumbre: mientras conocer es consciencia, incertidumbre es también *indistinguibilidad*. Un ejemplo bonito y entrañable sería que uno no puede distinguir entre un mundo en el que la abuela cocina rico de un mundo en el que cocina espantoso, si se desconocen las capacidades culinarias de la abuela.

En el Problema 1, todos los mundos posibles pueden caracterizarse como combinaciones de estados de culpa e inocencia, excluyendo los casos triviales donde todos son inocentes (¡alguien robó los memes!) o todos son culpables (¿cuál sería el punto de robar los memes si todos están involucrados?). Así, los mundos posibles serían:

1. Mundos donde Alice, Bob y Catalina no son inocentes simultáneamente.
2. Mundos donde hay dos inocentes.

Es posible desglosarlos al describirlos mediante fórmulas compuestas de $\mathcal{L}_{\mathcal{K}}$:

1. $W_1 = (P_{A,0} \wedge P_{B,1} \wedge P_{C,1})$ (Alice inocente)
2. $W_2 = (P_{A,1} \wedge P_{B,0} \wedge P_{C,1})$ (Bob inocente)
3. $W_3 = (P_{A,1} \wedge P_{B,1} \wedge P_{C,0})$ (Catalina inocente)
4. $W_4 = (P_{A,0} \wedge P_{B,0} \wedge P_{C,1})$ (Alice y Bob inocentes)
5. $W_5 = (P_{A,1} \wedge P_{B,0} \wedge P_{C,0})$ (Bob y Catalina inocentes)
6. $W_6 = (P_{A,0} \wedge P_{B,1} \wedge P_{C,0})$ (Alice y Catalina inocentes)

Gracias a esto, es posible razonar informalmente sobre conocimiento. Por ejemplo supóngase que Alice es inocente, entonces ella debería poder saber que no vive en los mundos W_2, W_3, W_5 (donde es culpable). En otras palabras, Alice puede distinguir entre los mundos W_2, W_3, W_5 (culpable) y los mundos W_1, W_4, W_6 (inocente).

Supongamos ahora que Alice ignora la identidad del ladrón(es), entonces Alice no puede distinguir el mundo W_1 de W_4 o W_6 ya que sólo sabe lo que tienen en común (que ella es inocente). Partiendo de esto, es legítimo pretender que el conocimiento equivale a las cosas comunes que tienen los mundos indistinguibles para el agente.[6] En términos más generales, si una fórmula φ no se cumple en todos los mundos indistinguibles para Alice entonces φ marca una diferencia entre todos estos mundos por lo que Alice, o la ignora, o es capaz de distinguir entre ellos.

Para definir *indistinguibilidad* formalmente (Alice sabe que puede vivir en los mundos W_1, W_4, W_5, ¿cómo es que no puede distinguir entre ellos si de hecho ya los conoce?) es

[6]Por supuesto es posible discutir esto como se hace en [32]. Por tanto deberá ser establecido como un axioma (uno bien justificado intuitivamente), pero no debe olvidarse que existen modelos más allá del que se presenta aquí.

necesario hablar primero sobre qué significa que una fórmula *sea cierta* en un mundo. En la siguiente sección se proporciona una semántica que define todas estas cuestiones en términos de *complejos simpliciales*.

1.3. Fundamentos de topología combinatoria

En esta sección se presenta la forma de representar mundos posibles a través de complejos simpliciales mostrada en [18] junto con una semántica formal para el lenguaje básico epistémico modal presentado en la Sección 1.1.1 que además es lo suficientemente expresiva para definir formalmente **resolubilidad** y representar la *evolución del conocimiento*.

Considérese un mundo s, por ahora indefinido aunque con la propiedad intuitiva de que hay varios agentes viviendo en él (por ejemplo p). En el mundo s, el agente p conoce muchas cosas dado que vive en él (intuitivamente su *visión del mundo*), lo que puede representarse como una fórmula $s_p \in \mathcal{L}_\mathcal{K}$. Así, es posible representar a p y su conocimiento de manera compacta como un par ordenado (p, s_p). Si se toman todos los agentes $p_1, \ldots, p_n$ que viven en s, entonces es posible definir $s = \{(p_1, s_{p_1}), \ldots, (p_n, s_{p_n})\}$.[7] Finalmente, para quitar la recursión en la definición, s puede definirse como un conjunto arbitrario $\{(p_1, \alpha_1), \ldots, (p_n, \alpha_n)\}$ donde $\alpha_i \in \mathcal{L}_\mathcal{K}$.

Recordando que dos mundos s y r son indistinguibles para un agente p si este conoce lo mismo de ambos (es decir, $s_p = r_p$), se tiene que s y r comparten al par ordenado asociado a p (es decir, $(p, s_p) = (p, s_r)$) de manera que la indistinguibilidad se convierte en una propiedad de *intersección de conjuntos*.

Finalmente, es posible visualizar estos conjuntos como figuras en el espacio. A continuación se expone de manera concreta cómo se hace esto exactamente.

1.3.1. Complejos simpliciales

Una muy buena forma de motivar el concepto de *complejo simplicial abstracto* es a través de su caso particular más famoso: el grafo. Un grafo consiste en un conjunto de *vértices* que pueden unirse dos a dos mediante *aristas*. El *complejo simplicial* generaliza esta noción al unir aristas entre sí con planos, luego planos entre sí con volúmenes, luego hipervolúmenes, etc.

Desde un punto de vista abstracto, la única información relevante necesaria para determinar un complejo simplicial es:

1. Sus vértices.

[7] En este trabajo se asume el estatuto filosófico de que la suma de las visiones de todos los involucrados proporciona la suficiente información para determinar un mundo. Vale la pena preguntarse hasta qué punto este estatuto es vigente dada la física cuántica y la teoría de la relatividad, pero ello es material para otro trabajo.

2. Cómo esos vértices se conectan entre sí (a través de aristas, planos, volúmenes, hipervolúmenes, etc.)

La manera más sencilla de representar esto es a través de la pertenencia a conjuntos: si n vértices están conectados entonces deberían pertenecer a un mismo conjunto por lo que es legítimo definir *complejos simpliciales* como familias de conjuntos. Por último, es necesario añadir una propiedad de consistencia: si tres vértices están conectados entre sí entonces también lo están dos a dos, si cuatro vértices están conectados entonces lo están tres a tres, y esas ternas dos a dos, etc. en general, si n vértices están conectados entonces también lo están cualesquiera subconjuntos de vértices.

Definición 1.3.1 (Complejos simpliciales abstractos [18]) *Un complejo simplicial C sobre un conjunto finito de vértices V es una familia de subconjuntos $C \subseteq \mathscr{P}(V)$ tal que:*

- $\forall v \in V$, $\{v\} \in C$.
- $\forall y \in C$, *si* $\emptyset \neq x \subseteq y$ *entonces* $x \in C$.

El conjunto V se denota $V(C)$ (los vértices de C).

Los elementos de un complejo simplicial se llaman *simplejos* y deben ser entendidos como una generalización de la noción de arista en un grafo, como por ejemplo un triángulo para 3-simplejos (cara de poliedro) o un tetraedro para 4-simplejos (volumen de poliedro). En general se desea que un n-simplejo determine una superficie de dimensión $n-1$ acotada (es decir un poliedro[8]), lo que corresponde a una **realización geométrica**. A continuación se presenta la definición de [30], parafraseada y limitada al caso de un sólo simplejo.

Definición 1.3.2 (Realización Geométrica de un simplejo)
*Considérese un n-simplejo S. Una **realización geométrica** de S en el espacio $\mathbb{R}^d$ con $d \geq n-1$ es una función $G : S \to \mathbb{R}^d$ tal que los elementos de $G[V(C)]$ (es decir, las imágenes de los vértices) satisfacen la siguiente propiedad:*

- ***Impenetrabilidad**: G es inyectiva (dos vértices no pueden ocupar el mismo espacio).*
- ***Geométricamente independientes**: Para cualquier $g \in G[V(C)]$ se tiene que el conjunto:*

$$\{g - h | h \in G[V(C)], h \neq g\}$$

Es linealmente independiente o es unitario.

La independencia geométrica es la manera formal de conseguir que los simplejos sean aristas, caras, volúmenes, hipervólumenes, etc. Con la finalidad de que un n-simplejo determine una superficie acotada de dimensión $n-1$ es necesario que dichas cotas sean

[8] O polítopo, como es denominado en dimensiones superiores.

superficies de dimensiones inferiores: una arista (superficie de dimensión 1) está acotada por sus vértices (superficies de dimensión 0), un triángulo (superficie de dimensión 2) está delimitado por sus lados (los cuales son aristas), y un tetraedro (superficie de dimensión 3) está delimitado por sus caras (las cuales son triángulos). De esta forma, la petición de que el conjunto $\{g - h | h \in G[V(C)], h \neq g\}$ sea linealmente independiente conlleva a que estas superficies de dimensiones inferiores no se traslapen unas con otras y por ende bajen la dimensión real del simplejo: en el ejemplo del 3-simplejo, las dos aristas que determinan al triángulo forman un ángulo no nulo y no se sobreponen entre sí (dicho de otras palabras, los tres puntos no son colineales). Para más ejemplos véase la Figura 1.1

Finalmente, el *relleno* de la realización geométrica se obtiene a través de la **envolvente convexa**:

Definición 1.3.3 (Envolvente convexa [30]) *Considérese un conjunto de puntos en el espacio $X = \{x_i \in \mathbb{R}^d | i \in I\}$ con I un conjunto arbitrario de índices. Se define la envolvente convexa de X como:*

$$conv(X) = \left\{ \sum_{i \in I} a_i x_i \mid a_i \geq 0, \sum_{i \in I} a_i = 1 \right\}$$

Esta envolvente consiste en todas las combinaciones lineales entre estos puntos que quedan comprendidas en su "interior", lo que corresponde a la noción de *rellenar*. El lector más interesado puede remitirse al libro [30] para ahondar más al respecto.

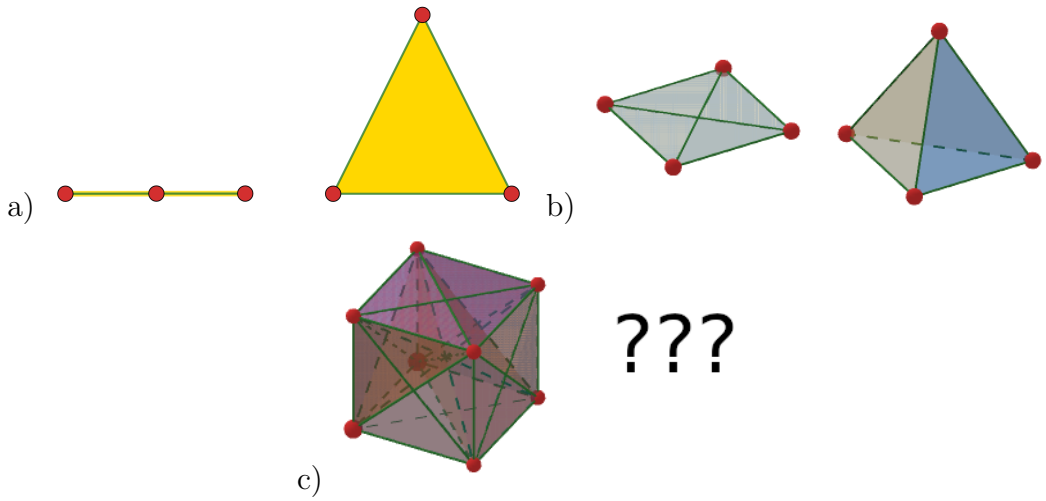


Figura 1.1: (a) Un 3-simplejo es un triángulo pero nunca tres puntos colineales. (b) Un 4-simplejo es un tetraedro pero nunca un cuadrado con sus diagonales. (c) Este maravilloso poliedro de ocho vértices no es un 8-simplejo, ¿pero cómo se vería en realidad uno de esos?

Volviendo a los complejos simpliciales abstractos, dado un simplejo se tiene que todos sus simplejos contenidos se llaman ***caras*** debido a la misma noción geométrica: en

la Figura 1.1(b), el tetraedro tiene cuatro 3-simplejos como caras. Es también posible clasificarlos en ese sentido geométrico:

Definición 1.3.4 (Dimensión [18]) *Sea C un complejo simplicial. $s \in C$ tiene dimensión d si y solo si $|s| - 1 = d$. En este caso, se dice que s es un d-simplejo de C. Finalmente, C tiene dimensión d si y solo si $d = Max\{|s| - 1 | s \in C\}$.*

Definición 1.3.5 (Facetas [18]) *Un simplejo $s \in C$ es una faceta si es $\subseteq$-maximal. Es decir, para todo simplejo $\sigma \in C$ distinto de s es imposible que $s \subseteq \sigma$. El conjunto de facetas de C se denota como $F(C)$.*

Este último concepto es extremadamente importante ya que todos los mundos posibles conformarán las facetas de un complejo simplicial.

Definición 1.3.6 (Pureza [18]) *Un complejo simplicial es* puro *si todas sus facetas tienen la misma dimensión.*

En este trabajo, todos los complejos simpliciales serán puros a menos que se estipule lo contrario.

Antes de empezar a aplicar esta teoría es necesario hablar de la característica más importante de los complejos simpliciales en lo que respecta a este trabajo: la **conexidad**.

Definición 1.3.7 (Conexidad de caminos [8]) *Sea C un complejo simplicial y considérense simplejos s y t. Se dice que s y t están* ***conectados por caminos*** *si y solo si existen vértices $a_0, \ldots, a_n \in V(C)$ tales que:*

1. *$a_0 \in s$ y $a_n \in t$ (o visceversa).*
2. *Para todo $0 \leq i \leq n-1$ se tiene que $\{a_i, a_{i+1}\}$ es un simplejo de C*

Intuitivamente dos simplejos s y t están conectados por caminos si es posible tender una cadena continua de aristas entre ambos. Esta noción se puede abstraer hacia complejos simpliciales:

Definición 1.3.8 (Conexidad [8]) *Sea C un complejo simplicial. Se dice que es* ***conexo*** *si y solo si todos sus simplejos están conectados por caminos. Un subcomplejo $D \subseteq C$ es una* ***componente conexa*** *de C si es $\subseteq$-maximal con la propiedad de ser conectado por caminos.*

Sin embargo es una definición *computacionalmente cara* en el sentido de que no es la forma más eficiente de revisar si un complejo es conexo o no.

Definición 1.3.9 (Conexidad óptima) *Sea C un complejo simplicial. Se dice que es* ***conexo*** *si y solo si todas sus facetas están conectadas por caminos.*

Ambas definiciones son, de hecho, equivalentes. Para probarlo vale la pena probar un lema previo:

Lema 1.3.1 *Sea C un complejo simplicial, entonces todas sus facetas son conexas acorde a la Definición 1.3.8.*[9]

Prueba. Dada una faceta $F \in C$, considérese simplejos $s, t \subseteq F$ y sean $x \in s$, $y \in t$, entonces $\{x, y\} \subseteq F$ por lo que se concluye lo deseado. ■

Teorema 1.3.1 *Las Definiciones 1.3.8 y 1.3.9 son equivalentes.*

Prueba. La ida es trivial: si todos los simplejos de un complejo simplicial C están conectados por caminos entonces en particular lo están sus facetas.
Para la vuelta, considérese simplejos $s, t \in C$ y sean F, G facetas tales que $s \in F$ y $t \in G$. Si $F = G$ entonces por el Lema 1.3.1 se tiene lo deseado. Si $F \neq G$ entonces están conectadas por caminos, sea $a_0, \ldots, a_n$ uno de los posibles y considérese $x \in s$, $y \in t$, entonces $x, a_0, \ldots, a_n, y$ es un camino desde s hasta t (si $x = a_0$ o $y = a_n$ entonces símplemente no se añadan los redundantes). ■

Finalmente, es posible empezar a hablar de complejos simpliciales como las bases de una semántica para el conocimiento.

Indistinguibilidad como una propiedad de conexidad En el Problema 1 de los memes robados, cada uno de los mundos posibles W_i están descritos en términos de fórmulas de $\mathcal{L}_{\mathcal{K}}$. Para representarlos como las facetas de complejos simpliciales, es necesario percatarse de que existen dos tipos de conocimientos iniciales: no saber nada sobre la identidad de los culpables (pues se es inocente), o saber a detalle la identidad de todos los miembros de la conspiración (pues se es culpable). Por tal motivo, sólo puede haber dos tipos de vértices: $(x, \emptyset)$ cuando el agente x es inocente, y $(x, \mathcal{K})$ cuando x conoce a todos los miembros de la conspiración $\mathcal{K} = \{y \in \{A, B, C\} | y \text{ robó los memes}\}$. Formalmente, los vértices son:

$$V(C) = \{(q, \mathcal{K}) | q \in \{A, B, C\}, \mathcal{K} = \emptyset \text{ o } \{q\} \subseteq \mathcal{K} \subsetneq \{A, B, C\}\}$$

De esta forma, los mundos $W_1, \ldots, W_6$ se convierten en las siguientes facetas:

1. $W_1 = (A, \emptyset), (B, \{B, C\})(C, \{B, C\})$
2. $W_2 = (A, \{A, C\}), (B, \emptyset)(C, \{A, C\})$
3. $W_3 = (A, \{A, B\}), (B, \{A, B\})(C, \emptyset)$
4. $W_4 = (A, \emptyset), (B, \emptyset)(C, \{C\})$
5. $W_5 = (A, \{A\}), (B, \emptyset)(C, \emptyset)$
6. $W_6 = (A, \emptyset), (B, \{B\})(C, \emptyset)$

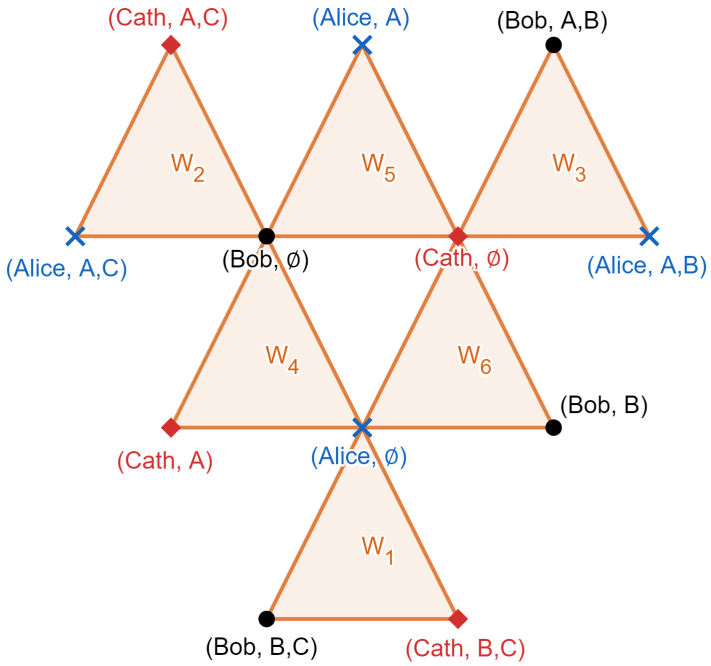


Figura 1.2: Complejo simplicial para el problema de los memes robados. Nótese que los únicos casos con incertidumbre son los casos cuando un agente es inocente. Por ejemplo, si Alice es inocente entonces los ladrones pueden ser Bob (W_6), Cath (W_4) o ambos (W_1).

Por tanto, el complejo simplicial para el problema de los memes robados es el de la Figura 1.2.

A continuación se formaliza la semántica para el conocimiento en complejos simpliciales.

1.3.2. Modelos simpliciales

En el mundo W_4 de la Figura 1.2 se tiene que es cierto $p_{B,0}$ (que Bob es inocente) pero, salvo la representación intuitiva $(B, \emptyset)$ no se tiene una manera formal de comprenderlo en general. Para resolver esto, se puede definir un mapeo que asocie $(B, \emptyset)$ con la fórmula correspondiente $p_{B,0}$. A continuación se presenta todo lo necesario para definir dicho mapeo:

Definición 1.3.10 (Etiquetado [18]) *Sea C complejo simplicial y sea Q un conjunto contable. Un etiquetado es una función $f : V(C) \to Q$ que asigna a cada vértice v una etiqueta $f(v)$ de Q.*

El ejemplo inmediato de etiquetado es cuando $Q = \mathcal{L}_{\mathcal{K}}$, y entonces a cada vértice v se le asigna una fórmula acorde a la regla de correspondencia de f.

[9]Las facetas se toman como complejos simpliciales contenidos en C

Otro ejemplo menos inmediato es la proyección canónica π_1, la cual es un mapeo que lleva cada vértice $(p, p(s))$ a su primera coordenada. En términos de lo ya visto, este mapeo informa a qué agente está asociado cada vértice y cumple con la propiedad de que es inyectivo al restringirse en cada faceta (es decir que los vértices tienen distintos colores) ya que es imposible que un agente se duplique.[10] Esto último es lo que se conoce como **cromatismo**:

Definición 1.3.11 (Cromatismo) *Sea C complejo simplicial y K un conjunto finito de elementos denominados **colores**. Se dice que un etiquetado $\chi : V(C) \to K$ es una K-coloración si es inyectiva restringida a cualquier faceta. C y χ definen una estructura $< C, \chi >$ llamada **complejo simplicial K-cromático** (o sólo **complejo simplicial cromático** si K es evidente por contexto).*

En otros trabajos se suele presentar una definición más estándar como por ejemplo en el libro [22], donde la inyectividad se pide a todos los simplejos y no sólo a las facetas.

Definición 1.3.12 (Cromatismo según [22, 18]) *Sea C complejo simplicial y K un conjunto finito de **colores**. Se dice que un etiquetado $\chi : V(C) \to K$ es una K-coloración si es inyectiva restringida a cualquier simplejo. C y χ definen una estructura $< C, \chi >$ llamada **complejo simplicial K-cromático** (o sólo **complejo simplicial cromático** si K es evidente por contexto).*

Lema 1.3.2 *Ambas definiciones son equivalentes: $\chi : V(C) \to K$ es una K-coloración según [22, 18] si y solo si es inyectiva restringida a cualquier faceta.*

Prueba.
La ida es trivial: si χ es inyectiva en cualquier simplejo entonces en particular lo es restringida a cualquier faceta.
Para la vuelta, sea $s \in C$ un simplejo. Entonces existe una faceta $F \in F(C)$ tal que $s \subseteq F$ (nota: $s = F$ es posible). Supóngase que χ no es inyectiva restringida en s, entonces existen vértices distintos $a, b \in s$ tales que $\chi(a) = \chi(b)$ por lo que existen vértices distintos $a, b \in F$ tales que $\chi(a) = \chi(b)$, lo que es una contradicción. ■

Definición 1.3.13 (Modelo simplicial [18]) *Sea $\mathcal{L}_K$ un lenguaje básico epistémico modal generado por un conjunto de agentes A y proposiciones atómicas AP. Un modelo simplicial $\mathcal{C} =< C, \chi, \ell >$ es una estructura conformada por una estructura A-cromática $< C, \chi >$ y un etiquetado $\ell : V(C) \to \mathcal{P}(AP)$ llamado **valuación** tal que para todo $u \in V(C)$, $p_{i,j} \in \ell(u)$ si y solo si $i = \chi(u)$. Es decir, $\ell(u)$ es un conjunto de proposiciones atómicas que sólo hablan sobre u (como por ejemplo sus valores iniciales o lo que conoce de sí mismo).*

[10] Sin embargo, puede que haya realidades donde este principio no se satisfaga. Por ejemplo, en la serie Padre de Familia hay un *gag* recurrente en el que Peter Griffin es reemplazado por un clon (por ejemplo su gemelo lampiño o su doble de helado), por lo que este modelo es insuficiente para estudiar resolubilidad de problemas distribuidos en Quahog (a menos que los clones se consideren como seres distintos al original).

Ya se tiene lo necesario para definir la semántica para $\mathcal{L}_{\mathcal{K}}$.

Definición 1.3.14 (Estado epistémico) *Sea $\mathcal{C} =< C, \chi, \ell >$ un modelo simplicial. Se definen los estados epistémicos como los elementos del conjunto $Eps = \{\mathcal{C}\} \times F(C)$. Se denotan $(\mathcal{C}, X) = \mathcal{C}, X$*

Para comprender intuitivamente esta definición, un estado epistémico debe leerse como $\mathcal{C}, X =$ "la faceta X considerada en el modelo $\mathcal{C}$ satisface la siguiente fórmula..." (nótese que es el inicio de una oración incompleta).

Definición 1.3.15 (Operador de satisfacción [18]) *Sea $\mathcal{C} =< C, \chi, \ell >$ un modelo simplicial. Se define la **verdad** de una fórmula $\varphi \in \mathcal{L}_{\mathcal{K}}$ en el estado epistémico $\mathcal{C}, X$ como el siguiente operador $\models \subseteq Eps \times \mathcal{L}_{\mathcal{K}}$ tal que:*

$$
\begin{array}{lll}
\mathcal{C}, X \models p & \textit{syss} & p \in \ell[X] \\
\mathcal{C}, X \models \neg\varphi & \textit{syss} & \mathcal{C}, X \not\models \varphi \\
\mathcal{C}, X \models (\varphi \wedge \psi) & \textit{syss} & \mathcal{C}, X \models \varphi \textit{ y } \mathcal{C}, X \models \psi \\
\mathcal{C}, X \models K_q(\varphi) & \textit{syss} & \forall Y \in F(C), q \in \chi(X \cap Y) \textit{ implica que } \mathcal{C}, Y \models \varphi
\end{array}
$$

Donde $\chi(X \cap Y) = \{\chi(v) | v \in X \cap Y\}$ es el conjunto de todos los colores de los vértices compartidos por ambas facetas X y Y

Este operador es definido para cada fórmula posible de $\mathcal{L}_{\mathcal{K}}$ por lo que también es la semántica buscada. A continuación se explica a detalle:

1. $\mathcal{C}, X \models p$ syss $p \in \ell[X]$ significa que las únicas fórmulas atómicas que son ciertas en el mundo X son las de la valuación. Por tanto, ℓ proporciona todo lo que es cierto acerca de los agentes en X en su forma más simple.

2. $\mathcal{C}, X \models \neg\varphi$ syss $\mathcal{C}, X \not\models \varphi$ significa que una fórmula no es cierta en X si este no la satisface. Aunque simple, esta proposición tiene la gran consecuencia de que convierte esta lógica en completa: si una fórmula ψ no se cumple en X entonces $\neg\psi$ sí lo hace.

3. $\mathcal{C}, X \models (\varphi \wedge \psi)$ syss $\mathcal{C}, X \models \varphi \wedge \mathcal{C}, X \models \psi$ significa que la conjunción de dos fórmulas equivale a que estas se cumplan por separado.

4. $\mathcal{C}, X \models K_q(\varphi)$ syss $\forall Y \in F(C), q \in \chi(X \cap Y) \Rightarrow \mathcal{C}, Y \models \varphi$
   Finalmente, la tan esperada semántica para el conocimiento. Esta proposición significa que el agente q conoce φ en el mundo X (es decir, $\mathcal{C}, X \models K_q(\varphi)$) syss φ es cierto en todos los mundos entre los que q no puede distinguir, dado que vive en X (representado por $q \in \chi(X \cap Y)$).

Nótese que el tener una semántica para conjunción y negación permite incorporar también la disyunción y la implicación material.

Definición 1.3.16 (Disyunción e implicación material) *El lenguaje básico epistémico modal se puede expandir a los siguientes dos símbolos: dados $\varphi, \psi \in \mathcal{L}_{\mathcal{K}}$, se define:*

1. ***Disyunción***: $(\varphi \vee \psi) := \neg(\neg\varphi \wedge \neg\psi)$

2. ***Implicación material***: $(\varphi \Rightarrow \psi) := (\neg\varphi \vee \psi)$.

Estas últimas definiciones son de hecho leyes de De Morgan y reglas de inferencia clásicas [13].

Teorema 1.3.2 (Disyunción en modelos simpliciales)
$\mathcal{C}, X \models (\varphi \vee \psi)$ *syss* $\mathcal{C}, X \models \varphi$ *o* $\mathcal{C}, X \models \psi$

Prueba.
Por la Definición 1.3.16 se tiene que $\mathcal{C}, X \models (\varphi \vee \psi)$ syss $\mathcal{C}, X \models \neg(\neg\varphi \wedge \neg\psi)$, luego, por la semántica del operador de satisfacción (Definición 1.3.15) se tiene que $\mathcal{C}, X \models \neg(\neg\varphi \wedge \neg\psi)$ si y solo si $\mathcal{C}, X \not\models \neg\varphi \wedge \neg\psi$ si y solo si no es cierto que $\mathcal{C}, X \models \neg\varphi$ y $\mathcal{C}, X \models \neg\psi$. Finalmente, por leyes de De Morgan se tiene que no es cierto que $\mathcal{C}, X \models \neg\varphi$ y $\mathcal{C}, X \models \neg\psi$ si y solo si $\mathcal{C}, X \not\models \neg\varphi$ o $\mathcal{C}, X \not\models \neg\psi$ si y solo si $\mathcal{C}, X \models \varphi$ o $\mathcal{C}, X \models \psi$ ■

Teorema 1.3.3 (Implicación material en modelos simpliciales) $\mathcal{C}, X \models (\varphi \Rightarrow \psi)$ *syss* $\mathcal{C}, X \models \varphi$ *implica que* $\mathcal{C}, X \models \psi$

Prueba.
Por la Definición 1.3.16 se tiene que $\mathcal{C}, X \models (\varphi \Rightarrow \psi)$ si y solo si $\mathcal{C}, X \models (\neg\varphi \vee \psi)$ y por el Teorema 1.3.2 se tiene que $\mathcal{C}, X \models (\neg\varphi \vee \psi)$ si y solo si $\mathcal{C}, X \not\models \varphi$ o $\mathcal{C}, X \models \psi$. Finalmente, por la regla de inferencia de implicación material, $\mathcal{C}, X \not\models \varphi$ o $\mathcal{C}, X \models \psi$ si y solo si $\mathcal{C}, X \models \varphi$ implica que $\mathcal{C}, X \models \psi$ ■

1.4. Conocimiento como una propiedad de conexidad

En esta sección se aprovecha la semántica del conocimiento para obtener propiedades muy relevantes para el estudio de la resolubilidad del consenso. La primera de estas propiedades es el **conocimiento grupal**: que todos los agentes sepan una fórmula al mismo tiempo.

Definición 1.4.1 (Conocimiento grupal [4])
Considérese $\mathcal{L}_{\mathcal{K}}$ *un lenguaje básico epistémico modal con conjunto de agentes* A*. El* ***operador de conocimiento grupal*** *se define como* $E : \mathcal{L}_{\mathcal{K}} \to \mathcal{L}_{\mathcal{K}}$ *tal que* $E(\varphi) = \bigwedge_{a\in A} K_a(\varphi)$ *donde* $\bigwedge$ *es el operador de conjunción generalizado y su semántica se define como* $\mathcal{C}, X \models \bigwedge_{a\in A} K_a(\varphi)$ *si y solo si para todo* $a \in A$, $\mathcal{C}, X \models K_a(\varphi)$

Nótese que este operador puede ser anidado en sí mismo mediante composición. Por ejemplo, $E^2(\varphi) = \bigwedge_{a\in A} K_a(\bigwedge_{a\in A} K_a(\varphi))$

El conocimiento grupal tiene un significado muy elegante en modelos simpliciales y es que $\mathcal{C}, X \models E(\varphi)$ equivale a que φ es cierta en todos los mundos que intersecan a X.

Luego, el conocimiento grupal doble conlleva a que φ es cierta en todos los mundos que intersecan a los que intersecan a X, e inductivamente $E^n(\varphi)$ conlleva a que φ es cierta en todos los mundos tales que es posible encontrar un camino de longitud n hacia X. Para formalizar esta intuición (usada en [4]) es necesario definir primero el concepto de **vecindad**:

Definición 1.4.2 (n-vecindad) *Sea $\mathcal{C}$ un modelo simplicial y sea $X \in F(C)$. La vecindad de radio n de X se define recursivamente como sigue:*

1. $N^0(X) = \{X\}$
2. $N^1(X) = \{Y \in F(C) | V(X) \cap V(Y) \neq \emptyset\}$ *es el conjunto de todas las facetas Y que comparten al menos un vértice con X (es decir, que lo intersecan).*
3. $N^{n+1}(X) = \bigcup_{Z \in N^n(X)} N^1(Z)$ *es el conjunto de todas las facetas Y que comparten al menos un vértice con alguna faceta de $N^n(X)$.*

Y, finalmente, la semántica para conocimiento grupal. Este lema fue presentado en [4] pero a contiuación se muestra con una prueba extendida original.

Lema 1.4.1 *Sea $\mathcal{C}$ un modelo simplicial, $X \in F(C)$ y $\varphi \in \mathcal{L}_\mathcal{K}$. Entonces para todo $n \geq 1$ se tiene que:*
$\mathcal{C}, X \models E^n(\varphi)$, syss $\mathcal{C}, Y \models E(\varphi)$ para todo $Y \in N^{n-1}(X)$.

Prueba.

La prueba es por inducción aprovechando la definición recursiva de $N^n(X)$.

Para $n = 1$ se tiene que $N^{n-1}(X) = \{X\}$ y $E^n(\varphi) = E(\varphi)$ por lo que $\mathcal{C}, X \models E(\varphi)$, si y solo si $\mathcal{C}, Y \models E(\varphi)$ para todo $Y = X$.

Para $n = 2$ se tiene que $\mathcal{C}, X \models E^2(\varphi)$ si y solo si $\mathcal{C}, X \models E(E(\varphi))$ ya que $E^2(\varphi) = E(E(\varphi))$. Sea $Y \in N^1(X)$, entonces por definición de conocimiento grupal se tiene que $E(E(\varphi)) = \bigwedge_{a \in A} K_a(E(\varphi))$, luego, si $Y \in N^1(X)$ entonces $\mathcal{C}, Y \models E(\varphi)$ debido a que la fórmula $\bigwedge_{a \in A} K_a(E(\varphi))$ equivale a que, para cada $a \in A$, si Y es una faceta que comparte el vértice correspondiente al agente a con X entonces $\mathcal{C}, Y \models E(\varphi)$
Por lo tanto, si $\mathcal{C}, X \models E^2(\varphi)$ entonces $\mathcal{C}, Y \models E(\varphi)$ para todo $Y \in N^1(X)$.
Conversamente, supóngase que $\mathcal{C}, Y \models E(\varphi)$ para todo $Y \in N^1(X)$ y sea $Y \in F(C)$ tal que existe $q \in \chi(X \cap Y)$, entonces $Y \in N^1(X)$ por lo que $\mathcal{C}, Y \models E(\varphi)$ y por tanto $\mathcal{C}, X \models K_a(E(\varphi))$ para todo agente q. Finalmente, $\mathcal{C}, X \models \bigwedge_{a \in A} K_a(E(\varphi)) = E^2(\varphi)$

Para el paso inductivo, sea $n \geq 1$ tal que $\mathcal{C}, X \models E^n(\varphi)$ si y solo si $\mathcal{C}, Y \models E(\varphi)$ para todo $Y \in N^{n-1}(X)$, y supóngase que $\mathcal{C}, X \models E^{n+1}(\varphi)$, entonces anidando el operador de conocimiento grupal se tiene que $\mathcal{C}, X \models E^{n+1}(\varphi)$ si y solo si $\mathcal{C}, X \models E^n(E(\varphi))$, luego, por hipótesis de inducción se tiene que $\mathcal{C}, X \models E^n(E(\varphi))$ si y solo si $\mathcal{C}, Y \models E(E(\varphi))$

para todo $Y \in N^{n-1}(X)$. Nótese ahora que $\mathcal{C}, Y \models E(E(\varphi))$ si y solo si $\mathcal{C}, W \models E(\varphi)$ para todo $W \in N^1(Y)$ y, por definición de n-vecindad, se tiene que $N^n(X) = \{W \in N^1(Y) | Y \in N^{n-1}(X)\} = \bigcup_{Y \in N^{n-1}(X)} N^1(Y)$. Finalmente, se concluye $\mathcal{C}, X \models E^{n+1}(\varphi)$, si y solo si $\mathcal{C}, W \models E(\varphi)$ para todo $W \in N^n(X)$ ■

A continuación se discute un caso muy especial de conocimiento grupal: el **conocimiento común**. Para motivar este concepto, nótese de que, en una faceta aislada, no hay secretos de nadie y para nadie ya que todos los agentes pueden distinguir entre ese mundo y cualquier otro (el que sea). Formalmente esto equivale a que se cumple $\mathcal{C}, X \models \varphi$ si y solo si $\mathcal{C}, X \models E(\varphi)$ para toda fórmula φ, en particular para la fórmula $E^n(\varphi)$ para toda $n \in \mathbb{N}$. En general, cuando esto último sucede se dice que existe **conocimiento común** sobre la fórmula φ

Definición 1.4.3 (Conocimiento común) *Sea $\mathcal{C}$ un modelo simplicial. Se define el conocimiento común de una fórmula φ en un mundo $X \in F(C)$ como el hecho que se cumpla que para todo $n \in \mathbb{N}$, $\mathcal{C}, X \models E^n(\varphi)$. Esto se denota como $\mathcal{C}, X \models E^\infty(\varphi)$.*

En el artículo [18] se puede encontrar otra definición de uso mucho más estándar:

Definición 1.4.4 (Conocimiento común según [18]) *Sea $\mathcal{C}$ un modelo simplicial y añádase el símbolo $C_B(\varphi)$ al lenguaje básico epistémico modal con $\varphi \in \mathcal{L}_\mathcal{K}$ y B un conjunto de agentes.*
Considérese la relación $R_B \subseteq F(C) \times F(C)$ definida como XR_BY si y solo si existe un agente $a \in B$ tal que $a \in \chi(X \cap Y)$, y sea R_B^* su cerradura transitiva, es decir, R_B^* es la $\subseteq$-menor relación que contiene a R_B y que además satisface que si $(X, Y), (Y, Z) \in R_B$ entonces $(X, Z) \in R_B^*$ Entonces la semántica de $C_B(\varphi)$ se define como:

$$\mathcal{C}, X \models C_B(\varphi) \text{ si y solo si } \forall Y \in F(C), \text{ si } XR_B^*Y \text{ entonces } \mathcal{C}, Y \models \varphi.$$

Sin embargo ambas definiciones son equivalentes. Para ello se emplean los siguientes lemas:

Lema 1.4.2 *La relación R_B^* es de equivalencia para todo B conjunto de agentes.*

Prueba. Para probar la **reflexividad**, considérese faceta $X \in F(C)$, entonces $B \subseteq \chi(X \cap X) = \chi(X)$ por lo que XR_B^*X
Para probar la **simetría**, considérense facetas $X, Y \in F(C)$ t.q XR_B^*Y, entonces existe $a \in B \cap \chi(X \cap Y) = B \cap \chi(Y \cap X)$ por lo que YR_B^*X
Finalmente, por definición es **transitiva**. ■

Lema 1.4.3 *Si una cadena de facetas relacionadas bajo R_A es de la forma $X\ R_A\ Z_1\ R_A \cdots R_A\ Z_k\ R_A\ Y$ (se dirá que es de longitud k) entonces $Y \in N^{k+1}(X)$*

Prueba.

La prueba es por iducción sobre la longitud k de la cadena.

Para $k = 0$ (es decir, X, Y comparten al menos un vértice) entonces el resultado se sigue por definición.

Para $k = 1$, supóngase que la cadena es $XR_AZ_1R_AY$. Ahora bien, nótese que $N^2(X) = \bigcup_{Z\in N^1(X)} N^1(Z)$ y $Y \in N^1(Z_1)$ por lo que $Y \in N^2(X)$.

Para el paso inductivo, sea $k \in \mathbb{N}$ tal que si la cadena es de longitud k entonces $Y \in N^{k+1}(X)$, y considérese una cadena de longitud $k+1$, $XR_AZ_1R_A\cdots R_AZ_kR_AZ_{k+1}R_AY$. Nótese que $XR_AZ_1R_A\cdots R_AZ_kR_AZ_{k+1}$ es una cadena de longitud k por lo que $Z_{k+1} \in N^{k+1}(X)$. Ahora bien, como $N^{k+2}(X) = \bigcup_{Z\in N^{k+1}(X)} N^1(Z)$ y $Y \in N^1(Z_{k+1})$, se tiene que $Y \in N^{k+2}(X)$ ■

Lema 1.4.4 *Sea $[X]^*_B$ la R^*_B-clase de equivalencia que contiene a la faceta X, entonces para todo $n \in \mathbb{N}$, $N^n(X) \subseteq [X]^*_A$. Más aún, $[X]^*_A = \bigcup_{n\in\mathbb{N}} N^n(X)$*

Prueba.

Primera parte de la prueba: para todo $n \in \mathbb{N}$, $N^n(X) \subseteq [X]^*_A$

La prueba es por inducción sobre $n \in \mathbb{N}$:

Para $n = 0$ el resultado es trivial, pues $\{X\} \subseteq [X]^*_A$.

Para $n = 1$, como $N^1(X) = \{Y \in F(C) | V(Y) \cap V(X) \neq \emptyset\}$ entonces todo $Y \in N^1(X)$ se relaciona con X a través de R_A ya que existe $a \in \chi(X \cap Y)$ el color de algún elemento de $V(Y) \cap V(X)$ por lo que $N^1(X) \subseteq [X]^*_A$

Para el paso inductivo, sea $n \in \mathbb{N}$ tal que $N^n(X) \subseteq [X]^*_A$. Recuérdese ahora que $N^{n+1}(X) = \bigcup_{Z\in N^n(X)} N^1(Z)$, luego, por hipótesis de inducción, para todo $Z \in N^n(X)$ se tiene que $Z \in [X]^*_A$. Ahora bien, Para todo $W \in N^1(Z)$, $W \in [Z]^*_A$ por lo que, como $Z \in [X]^*_A$, se tiene que $W \in [X]^*_A$, sin embargo W es cualquier elemento de $\bigcup_{Z\in N^n(X)} N^1(Z)$ por lo que $N^{n+1}(X) \subseteq [X]^*_A$

Segunda parte de la prueba: $[X]^*_A \subseteq \bigcup_{n\in\mathbb{N}} N^n(X)$

Sea $Y \in [X]^*_A$, entonces como R^*_A es la cerradura transitiva de R_A se tiene que existen $Z_1, \ldots, Z_k \in F(C)$ tales que $X\ R_A\ Z_1\ R_A \cdots R_A\ Z_k\ R_A\ Y$. Finalmente, por el lema 1.4.3 se tiene de manera inmediata que $Y \in N^{k+1}(X) \subseteq \bigcup_{n\in\mathbb{N}} N^n(X)$ ■

Finalmente, es posible probar de manera sucinta que ambas definiciones de conocimiento común son equivalentes:

Teorema 1.4.1 *$\mathcal{C}, X \models C_A(\varphi)$ si y solo si $\mathcal{C}, X \models E^n(\varphi)$ para todo $n \in \mathbb{N}$*

Prueba.

Para demostrar la ida, supóngase que $\mathcal{C}, X \models C_A(\varphi)$ y sea $n \in \mathbb{N}$. Sea ahora $Y \in N^{n-1}(X)$ y sea $W \in N^1(Y)$, entonces por Lema 1.4.4 se tiene que $Y \in [X]_A^*$ por lo que XR_B^*Y y por tanto $\mathcal{C}, Y \models \varphi$. Análogamente, como también $W \in [X]_A^*$ entonces $\mathcal{C}, W \models \varphi$, y como esto pasa para todo $W \in N^1(Y)$ entonces se concluye que $\mathcal{C}, Y \models E(\varphi)$ y por tanto $\mathcal{C}, X \models E^n(\varphi)$

Para demostrar la vuelta, supóngase que para todo $n \in \mathbb{N}$ se cumple que $\mathcal{C}, X \models E^n(\varphi)$. Sea $Y \in F(C)$ tal que XR_A^*Y, entonces $Y \in \bigcup_{n\in\mathbb{N}} N^n(X)$. Sea $k \in \mathbb{N}$ tal que $Y \in N^k(X)$. Nótese que $\mathcal{C}, X \models E^{k+1}(\varphi)$, por lo que, por el Lema 1.4.1, se tiene que $\mathcal{C}, Y \models E(\varphi)$ ya que $Y \in N^k(X)$. De esta forma, $\mathcal{C}, Y \models \varphi$ por lo que $\mathcal{C}, X \models C_A(\varphi)$ ■

A continuación se presenta otro lema muy útil para comprender aún mejor las clases de equivalencia de R_B^*:

Lema 1.4.5 *Sea $\mathcal{C}$ un modelo simplicial y sea $X \in F(C)$. Sea K_X la componente conexa que contiene la faceta X,*[11] *entonces $K_X = [X]_A^*$*

Prueba.
nótese que:

$$K_X = \{Y \in F(C) | \exists v_0, \ldots, v_k \in V(C) \text{ t.q. } \{v_i, v_{i+1}\} \in C, v_0 \in X, v_k \in Y\}$$

Ahora bien, los vértices de la forma v_i pertenecen a facetas $Z_0, Z_1, \ldots, Z_q, Z_{q+1}$ tales que $Z_0 = X$, $Z_{q+1} = Y$, y además $Z_0R_AZ_1R_A \cdots R_AZ_qR_AZ_{q+1}$ por lo que $K_X \subseteq [X]_A^*$

Finalmente, dado $Y \in [X]_A^*$ con cadena $X = Z_0R_AZ_1R_A \cdots R_AZ_qR_AZ_{q+1}Y$, se escogen vértices $b_i \in V(C)$ tales que $b_i \in V(Z_i) \cap V(Z_{i+1})$, y luego caminos $b_i = i_0, i_1, \ldots, i_{i_p} = b_{i+1}$ dentro de Z_i. De esta forma, se tiene el camino $b_0, i_1, \ldots, i_{p-1}, b_1, \ldots, b_q$ que conecta la faceta X con la faceta Y, por lo que $[X]_A^* \subseteq K_X$

■

En general, hay más propiedades interesantes sobre el conocimiento común que, hasta donde sabemos, no han sido abordadas directamente en otros trabajos (aunque sí han sido usadas implícitamente en [4, 18]). Por ejemplo la siguiente:

Teorema 1.4.2 *Sea $\mathcal{C}$ un modelo simplicial y sea $X \in F(C)$. Entonces $\mathcal{C}, X \models E^\infty(\varphi)$ si y solo si para todo $Y \in K_X$, $\mathcal{C}, Y \models \varphi$*

[11] Las componentes conexas se definieron en la Definición 1.3.8.

Prueba.

Para probar la ida del teorema, supóngase que $\mathcal{C}, X \models E^{\infty}(\varphi)$ y sea $Y \in K_X$. Como $K_X = [X]_A^*$ entonces por Lema 1.4.4 se tiene que existe $n \in \mathbb{N}$ tal que $Y \in N^n(X)$. Además $\mathcal{C}, X \models E^{\infty}(\varphi)$ implica que $\mathcal{C}, X \models E^{n+1}(\varphi)$ por lo que para todo $Z \in N^n(X), \mathcal{C}, Z \models E(\varphi)$ (por Lema 1.4.1), en particular para $Z = Y$ por lo que $\mathcal{C}, Y \models E(\varphi)$ y finalmente $\mathcal{C}, Z \models \varphi$

Finalmente para la vuelta, sea $n \in \mathbb{N}$ y sea $Y \in N^{n-1}(X) \subseteq K_X$, entonces $\mathcal{C}, Y \models E(\varphi)$ ya que para todo $Z \in N(Y) \subseteq \bigcup_{m\in\mathbb{N}} N^m(X)$ se tiene que $\mathcal{C}, Z \models \varphi$ (por hipótesis, pues $\bigcup_{m\in\mathbb{N}} N^m(X) = K_X$). Finalmente, por Lema 1.4.1 se concluye que $\mathcal{C}, X \models E^n(\varphi)$ y por tanto $\mathcal{C}, X \models E^{\infty}(\varphi)$ ■

El siguiente paso es estudiar la forma en la que el conocimiento *evoluciona*: en el problema de los memes robados los inocentes no tienen suficiente conocimiento para determinar a los culpables, por lo que deben idear una forma para revertir ello. En general, cualquier *evento* que altere el conocimiento se denomina *acción*, y estos pueden ser desde un interrogatorio hasta el descubrimiento del arca perdida. En el siguiente capítulo se introduce la formalización de todas estas cuestiones a través de la **lógica epistémica dinámica**.

Capítulo 2

Lógica epistémica dinámica con topología

La lógica epistémica dinámica es la extensión de la lógica epistémica que estudia la evolución del conocimiento a lo largo del tiempo. Por ejemplo, en el Problema de los memes robados 1, alguien inocente puede empezar un interrogatorio con la finalidad de tender trampas a los culpables de manera que se traicionen y acaben revelando su culpabilidad. Este interrogatorio puede visualizarse como una acción de la siguiente manera: las respuestas obtenidas determinan una evolución del conocimiento en un mundo posible. Por ejemplo, si Bob es inocente, le pregunta a Alice y Catalina si también lo son, y ambas confiesan estar coludidas, entonces el conocimiento de Bob habrá cambiado. Eso es una acción.

En esta sección se formaliza con precisión esta cuestión para cualquier problema dentro del marco teórico propuesto en esta tesis.

2.1. Modelos de acción

Como ya se dijo, una acción conlleva a una alteración en los conocimientos (en términos de la conexidad de un complejo simplicial gracias al operador de satisfacción). Para representarlo se puede definir un **modelo de acción** como un complejo simplicial que represente todos los conocimientos finales obtenidos tras el término de la acción.

Definición 2.1.1 (Modelos simpliciales de acción [4]) *Un modelo de acción simplicial $\mathcal{A} =< T, \chi, pre >$ consiste en un complejo simplicial cromático $< T, \chi >$ y un etiquetado $pre : V(T) \to \mathcal{L}_K$ que asigna a cada vértice una **precondición** representada por una fórmula de $\mathcal{L}_\mathcal{K}$. Las precondiciones se extienden a simplejos como sigue: $pre : T \to \mathcal{L}_K$ es tal que $pre(s) = \bigwedge_{u \in s} pre(u)$.*

Cada faceta del modelo $\mathcal{A}$ representa una consecuencia posible de la acción, pues esta no puede ser la misma en todos los mundos posibles (por ejemplo, en el interrogatorio de los memes robados, Alice y Catalina no pueden confesar el crimen de manera fidedigna en un mundo donde Bob es el único culpable). El etiquetado *pre* determina con precisión

qué consecuencia corresponde a qué mundos a través de fórmulas de $\mathcal{L}_{\mathcal{K}}$: una faceta f sólo puede provenir de mundos donde se satisfaga $pre(f)$

El siguiente paso es construir un modelo simplicial que aglutine las acciones junto con los mundos donde se realizan. Ello induce un producto, por lo que antes es necesario definir con presición lo que es esto.

Definición 2.1.2 (Producto cartesiano cromático [18]) *Sean* $< C, \chi >$ *y* $< T, \chi >$ *complejos simpliciales cromáticos (de misma coloración).*
Su ***producto cartesiano cromático*** *se define como el complejo simplicial* $< C \times T, \chi >$ *tal que:*

- ***Vértices:*** $V(C \times T) = \{(u, v) \in V(C) \times V(T) | \chi(u) = \chi(v)\}$.
- ***Simplejos:*** $\{(u_0, v_0), \ldots, (u_k, v_k)\} \in C \times T$ *si y solo si:*

$$\{u_0, \ldots, u_k\} \in C, \{v_0, \ldots, v_k\} \in T \text{ y } \forall 0 \leq i \leq k, \chi(u_i) = \chi(v_i)$$

A veces los simplejos $\{(u_0, v_0), \ldots, (u_k, v_k)\} \in C \times T$ *se denotan como*

$$\{u_0, \ldots, u_k\} \times \{v_0, \ldots, v_k\}$$

Una cuestión curiosa sobre este producto cartesiano es que, a diferencia del producto de espacios vectoriales, la dimensión resultante no es el producto de las dimensiones de los factores. Más aún, puede ser menor como se muestra en la Figura 2.1.

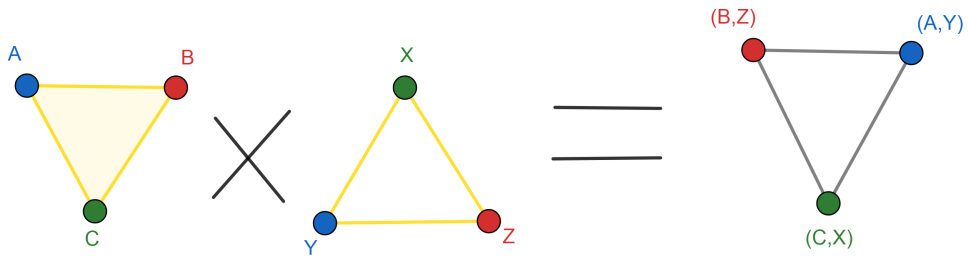


Figura 2.1: El producto de dos complejos simpliciales puros.

Ahora considérense dos modelos simpliciales $\mathcal{C}$ y $\mathcal{D}$. Si sus vértices son de la forma (q, v_C) y (q, v_D) respectivamente entonces los vértices de su producto cartesiano cromático $\mathcal{C} \times \mathcal{D}$ son de la forma (q, v_C, q, v_D). Sin embargo aquí hay redundancia en la primera y tercera coordenada ya que ambas tienen el mismo valor por definición. Por tanto, los vértices del producto cartesiano cromático serán denotados como sigue:

$$(q, v_C, v_D)$$

Lo que también ayuda muchísimo a la intuición, pues (q, v_C, v_D) puede ser leído como: "el agente q empezó con el valor v_C pero, tras la acción $\mathcal{D}$, obtuvo el valor v_D".

Finalmente, es posible formalizar lo previamente discutido sobre el significado de las precondiciones a través del **producto actualizado** (del inglés "product update", de uso muy extendido en trabajos como [18, 20]).

Definición 2.1.3 (Producto actualizado [18]) *Sea $\mathcal{C} =< C, \chi, \ell >$ un modelo simplicial y $\mathcal{A} =< A, \chi, pre >$ un modelo de acción, ambos con la misma coloración. El producto actualizado de $\mathcal{A}$ sobre $\mathcal{C}$ se define como el modelo simplicial*
$\mathcal{C}[\mathcal{A}] =< C[A], \chi[A], \ell[A] >$ tal que:

a) $C[A] \subseteq C \times A$ es tal que $X \times Y \in F(C[A])$ si y solo si $\mathcal{C}, X \models pre(Y)$

b) $\ell[A] : V(C[A]) \to \mathscr{P}(AP)$ se define como $\ell[A]((u, v)) = \ell(u)$

El punto a) proporciona una explicación semántica formal para las precondiciones que coincide con la intuición planteada: si un mundo X en $\mathcal{C}$ satisface la precondición de la acción Y entonces las consecuencias de realizar Y se pueden manifestar en X, representado ello por la faceta $X \times Y$, cuyos vértices son de la forma (q, v, b): "*el agente q empezó con el valor v y, tras realizar Y, terminó con el valor b*".

2.2. Resolución de tareas

Para resolver el Problema de los memes robados 1 es necesario que las personas inocentes descubran las identidades de los ladrones. En el problema del consenso, el objetivo de los agentes es decidir uno de los valores iniciales de alguien. Ambos tienen en común que necesitan decidir estados finales válidos (como coincidir en un mismo valor inicial o conocer a los ladrones de memes), lo que nuevamente puede ser representado con modelos simpliciales: un estado final válido para un sistema distribuido corresponde a un *mundo final válido*, pero estos sólo pueden provenir de mundos iniciales dados. Ello permite modelar **tareas** como modelos de acción.

Un problema de interés es saber si una acción basta para resolver una tarea. Por ejemplo uno querría saber si un interrogatorio realizado por Bob (sea culpable o no) sería suficiente para resolver el problema de los memes robados. Esta cuestión es, de hecho, la **resolubilidad** discutida en la introducción, pero para formalizarla con propiedad es necesario definir un par de conceptos previos que permitirán comparar productos actualizados entre sí.

Definición 2.2.1 (Mapeos simpliciales [18]) *Sean C y D complejos simpliciales arbitrarios. Un **mapeo simplicial** entre ellos se define como la función $f : V(C) \to V(D)$ tal que $\forall s \in C$, $f[s] \in D$.*
Para complejos simpliciales cromáticos $< C, \chi > t < D, \chi >$ con la misma coloración, el mapeo simplicial $f : V(C) \to V(D)$ es también cromático si para todo $u \in V(C)$ se tiene que $\chi(u) = \chi(f(u))$.

Estos mapeos simpliciales pueden extenderse a modelos simpliciales de la siguiente manera:

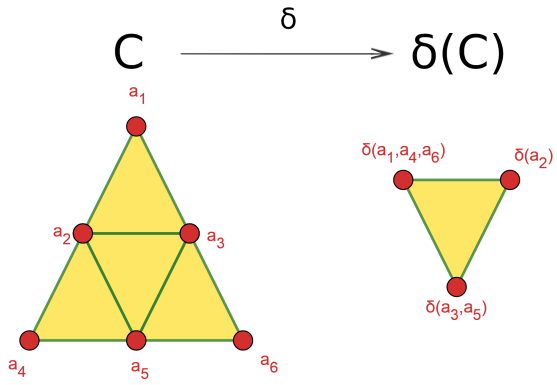


Figura 2.2: Este es un mapeo simplicial δ que lleva cuatro triángulos a uno solo. Claramente no es inyectiva. ¿Existe una coloración que lo haga cromático? Nótese que las preimágenes del vértice inferior de $\delta(C)$ son adyacentes, pero al compartir imagen bajo δ deben ser, por fuerza, del mismo color. Así, δ no puede ser cromático bajo ninguna circunstancia.

Definición 2.2.2 (Morfismo simplicial [18]) *Un **morfismo** f entre modelos simpliciales $\mathcal{C} =< C, \chi, \ell >$ y $\mathcal{D} =< D, \chi, \ell' >$ es un mapeo simplicial cromático $f : C \to D$ que preserva valuaciones. Es decir, $\ell(v) = \ell'(f(v))$ para todo $v \in V(C)$. Se dice que es un **isomorfismo** si además es biyectivo.*

Existen dos propiedades claves que satisfacen estos morfismos: la primera es que preservan conexidad (y por tanto conocimiento) y la segunda es que no incrementan el conocimiento en la imagen: por ejemplo si Bob no sabe que Alice es la ladrona de los memes entonces Bob tampoco puede saberlo en la imagen de un morfismo simplicial.

Lema 2.2.1 *Sea $f : C \to D$ un mapeo simplicial. Si C' es un subcomplejo conexo de C entonces $f(C')$ es un subcomplejo conexo de D.*

Prueba. Considérese $x, y \in f(C')$ y sean $u, v \in V(C')$ tales que $f(u) = x$ y $f(v) = y$. Ya que C' es conexo, existe una secuencia de vértices $u = u_0, \ldots, u_k = v$ en C' tales que $\{u_i, u_{i+1}\} \in C'$ (es decir, que forman un camino) así, $\{f(u_i), f(u_{i+1})\} \in f(C')$ al ser f mapeo simplicial y por tanto $f(u) = x, f(u_1), \ldots, f(u_{k-1}), y = f(v)$ es un camino en $f(C')$ por lo que se tiene la conexidad deseada. ■

A continuación se presenta un caso particular de fórmula de gran interés, con la finalidad de estudiar cómo evoluciona el conocimiento en estos modelos:

Definición 2.2.3 (Fórmulas positivas [18]) *Dado un lenguaje básico epistémico modal $\mathcal{L}_\mathcal{K}$, se dice que $\varphi \in \mathcal{L}_\mathcal{K}$ es una **fórmula positiva** si no contiene negaciones salvo, quizá, en proposiciones atómicas.*

A continuación se reformula esta definición en términos recursivos: el paso base consiste en la parte de la definición que se refiere a las atómicas y negaciones de atómicas, y el paso recursivo está en términos de los demás operadores de $\mathcal{L}_\mathcal{K}$ (conjunción y el operador de conocimiento):

1. Toda atómica es fórmula positiva.
2. Toda atómica negada es fórmula positiva.
3. Sean φ y ψ fórmulas positivas, entonces $\varphi \wedge \psi$ y $K_a(\varphi)$ son fórmulas positivas para todo $a \in A$.
4. No hay más fórmulas positivas que las construidas con este procedimiento.[1]

Lema 2.2.2 (Ganancia de conocimiento [4, 18]) *Considérense modelos simpliciales* $\mathcal{M} =< C, \chi, \ell >$ *y* $\mathcal{M}' =< C', \chi', \ell' >$*, y un morfismo de modelos* $f : \mathcal{M} \to \mathcal{M}'$*. Sea* $X \in \mathcal{F}(C)$ *una faceta de* $\mathcal{M}$*, a un agente (color), y* $\varphi \in \mathcal{L}_{\mathcal{K}}$ *una fórmula positiva. Entonces* $\mathcal{M}', f(X) \models \varphi$ *implica que* $\mathcal{M}, X \models \varphi$*.*

Prueba.
La prueba es por inducción estructural sobre la definición recursiva de las fórmulas positivas. En este caso las bases inductivas son las fórmulas atómicas y sus negaciones, mientras que los pasos inductivos son los demás operadores.

Para las bases inductivas: supóngase que φ es atómica, entonces $\mathcal{M}', f(X) \models \varphi$ si y solo si $\varphi \in \ell(f(X)) = \ell(X)$, por lo que $\mathcal{M}, X \models \varphi$.
Si $\varphi = \neg p$ es la negación de la atómica p entonces $\mathcal{M}', f(X) \not\models p$, por lo que
$p \notin \ell(f(X)) = l(X)$. Por lo tanto $\mathcal{M}, X \not\models p$.

Para los pasos inductivos: supóngase que $\varphi = \psi \wedge \theta$ para fórmulas positivas ψ, θ que satisfacen el teorema (al menos son atómicas o negaciones de atómicas), entonces se tiene que $\mathcal{M}', f(X) \models \psi \wedge \theta$ por lo que $\mathcal{M}', f(X) \models \psi$ y $\mathcal{M}', f(X) \models \theta$ y por tanto $\mathcal{M}', X \models \psi$ y $\mathcal{M}', X \models \theta$. Se concluye entonces que $\mathcal{M}, X \models \psi \wedge \theta$.
Sea $\varphi = K_a(\psi)$ con ψ fórmula positiva que satisface el teorema, y sea $Y \in F(C)$ tal que $a \in \chi(Y \cap X)$, entonces $a \in \chi(f(Y) \cap f(X))$ por lo que $\mathcal{M}', f(Y) \models \psi$ y por lo tanto $\mathcal{M}, Y \models \psi$, implicando esto que $\mathcal{M}, X \models \varphi$.
Finalmente, como toda fórmula positiva se obtiene recursivamente con el procedimiento descrito antes de enunciar el lema, se concluye lo deseado. ■

La restricción de φ siendo *fórmula positiva* cumple con un cometido concreto: limitar a la fórmula de decir cosas sobre lo que un agente no sabe, pues un morfismo simplicial sí permite "ganar" conocimiento sobre este tipo de cuestiones. Para ilustrar mejor esto, considérese el siguiente ejemplo:

Ejemplo 2 *Muchos años antes del episodio desastroso de los ladrones de memes, Alice y Bob no conocían a Catalina por lo que sobrevivían solos en el Apocalipsis. En una ocasión, un demonio oscuro y malévolo les exigió que escogieran un valor del conjunto* $\{0, 1\}$*,*[2] *tras lo cual provocó una anomalía cuántica y provocó el surgimiento de dos universos paralelos:*[3]

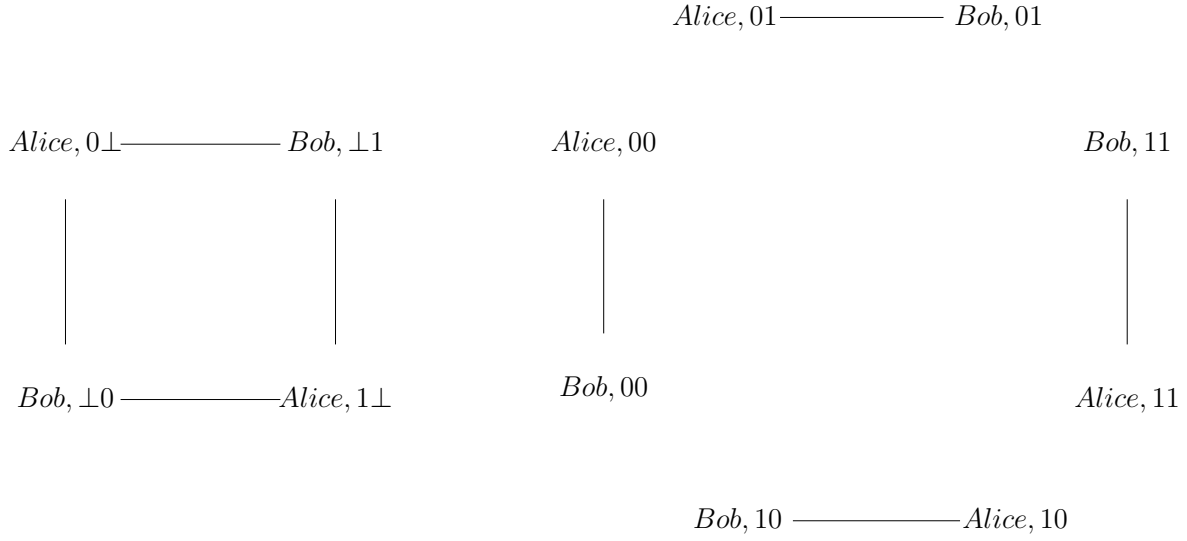
[1] Por tanto no hay disyunciones ni implicaciones materiales positivas.
[2] En el fin del mundo, estas cosas pasan habitualmente.
[3] Leer pie de página anterior.

1. *Universo $Anomalia_1$: donde Alice y Bob obtienen clarividencia sobre el número del otro.*

2. *Universo $Anomalia_2$: donde no obtienen clarividencia alguna.*

El demonio les exigió que hicieran los modelos simpliciales de ambos universos para que descubrieran en cual vivían (les prohibió darse cuenta trivialmente de ello) para así salvar sus almas del castigo eterno (qué demonio tan extraño...)

Dado que poco después conocieron a Catalina y sucedió la catástrofe de los ladrones de memes, queda claro que Alice y Bob pasaron la prueba del demonio. A continuación se muestran los modelos simpliciales que emplearon para salvar sus almas: a la izquierda $Anomalia_2$ y a la derecha $Anomalia_1$



Donde los vértices son de la forma ($Agente$, Valor de Alice, Valor de Bob) utilizando el símbolo $\perp$ para representar ignorancia sobre dichos valores en caso de haberla. Se define el modelo con la valuación $\ell(Alice, ab) = p_{A,a}$ y $\ell(Bob, ab) = p_{B,b}$ en ambos casos.

Nótese ahora que existe un morfismo δ que va de $Anomalia_1$ a $Anomalia_2$ definido como $\delta(Alice, ab) = (Alice, a\perp)$ y $\delta(Bob, ab) = (Bob, \perp b)$.

Lema 2.2.3 *δ es un morfismo simplicial.*

Prueba. Es inmediato que δ mapea vértices en vértices. Considérese ahora una arista $\{(Alice, ab), (Bob, ab)\}$, entonces $\delta[\{(Alice, ab), (Bob, ab)\}] = \{(Alice, a\perp), (Bob, \perp b)\}$ es una arista en $Anomalia_2$

Es obvio que es cromático por definición. Finalmente, nótese que también preserva la valuación ya que $\ell(Alice, a\perp) = \ell(Alice, ab)$ y $\ell(Bob, \perp b) = \ell(Bob, ab)$ ■

Considérese ahora la fórmula positiva $K_A(p_{B,1})$ que significa "Alice sabe que Bob tiene el 1". En el universo $Anomalia_2$ Alice nunca sabe el valor de Bob mientras que en

$Anomalia_1$ lo sabe en el mundo $X_{01} = \{(Alice, 01), (Bob, 01)\}$. Por tanto si se denotan $\mathcal{A}_1$ y $\mathcal{A}_2$ a los modelos simpliciales asociados a los universos entonces:

- $\mathcal{A}_1, X_{01} \models K_A(p_{B,1})$
- $\mathcal{A}_2, \delta(X_{01}) \not\models K_A(p_{B,1})$ o, lo que es equivalente, $\mathcal{A}_2, \delta(X_{01}) \models \neg K_A(p_{B,1})$

Sin embargo, si el Lema 2.2.2 admitiera fórmulas no positivas (como, por ejemplo, $\neg K_A(p_{B,1})$) entonces se tiene que $\mathcal{A}_2, \delta(X_{01}) \models \neg K_A(p_{B,1})$ implica $\mathcal{A}_1, X_{01} \models \neg K_A(p_{B,1})$, lo que contradice el análisis previo.

Por último, para definir la resolubilidad de tareas, hay un morfismo muy importante a tener en cuenta: las proyecciones canónicas de un producto simplicial. A continuación se presenta una versión explicada de la definición de [18]

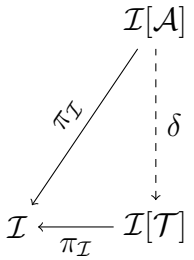
Definición 2.2.4 (Proyecciones canónicas simpliciales) *Dado $< R, \chi, l >$ modelo simplicial cromático de dimensión n, sean $< C, \chi, l' > y < T, \chi, l'' >$ modelos simpliciales cromáticos tales que $R = C \times T$. Entonces se definen las **proyecciones canónicas** como morfismos simpliciales tales que:*

- $\pi_C : R \to C$ *es tal que* $\pi_C((u, v)) = u$.
- $\pi_T : R \to C$ *es tal que* $\pi_T((u, v)) = v$.

Esto ya permite definir **resolubilidad de tareas** de manera formal.

Definición 2.2.5 (Resolubilidad de tareas [18]) *Sea $\mathcal{I}$ un modelo simplicial, $\mathcal{T}$ una tarea con misma coloración y $\mathcal{A}$ un modelo de acción también con misma coloración. La tarea $\mathcal{T}$ se puede resolver por el modelo de acción $\mathcal{A}$ si existe un morfismo simplicial $\delta : \mathcal{I}[\mathcal{A}] \to \mathcal{I}[\mathcal{T}]$ tal que $\pi_{\mathcal{I}} \circ \delta = \pi_{\mathcal{I}}$ (el diagrama de abajo conmuta).*

Para comprender esta definición, nótese que δ es un morfismo que indica qué conocimientos finales del modelo de acción $\mathcal{A}$ permiten deducir qué conocimientos finales de la tarea $\mathcal{T}$: **un valor final** a **de** $\mathcal{A}$ **permite deducir** $\delta(a)$ **en** $\mathcal{T}$. La propiedad conmutativa del diagrama asegura que a y $\delta(a)$ fueron obtenidos desde el mismo conocimiento inicial en $\mathcal{I}$.



Esta definición también funciona en mundos indistinguibles: considérese un vértice $(q, i, a) \in X \in F(\mathcal{I}[\mathcal{A}])$, entonces el agente q deduce el conocimiento final en $\mathcal{T}$ solamente acorde a su conocimiento en $\mathcal{I}[\mathcal{A}]$: si otra faceta X' contiene a (q, i, a) entonces $\delta((q, i, a)) \in \delta(X) \cap \delta(X')$ por lo que a tiene que realizar la misma acción en ambos mundos y por tanto resolver la tarea de la misma manera en dichos casos.

2.3. Preliminares para solucionar el problema de los memes robados

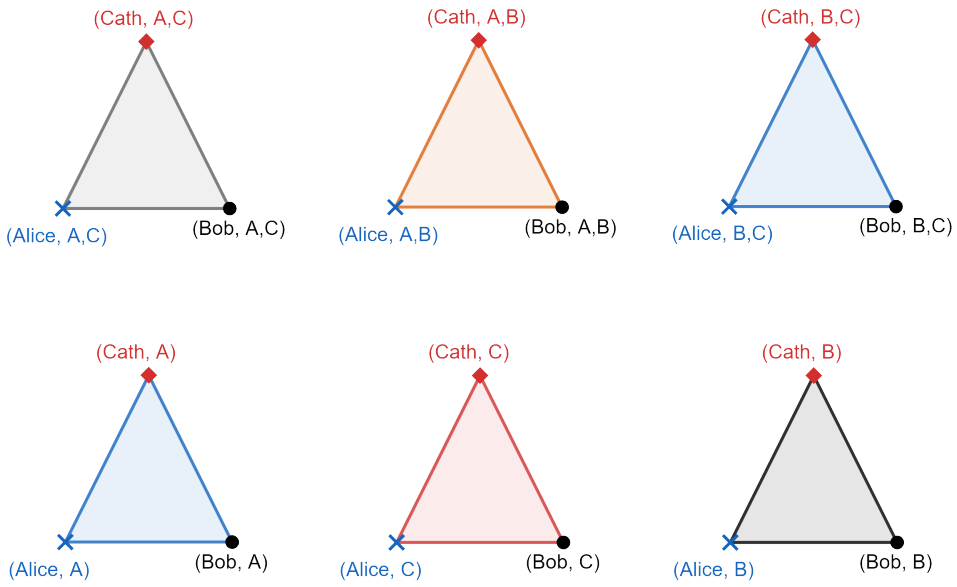
Recuérdese que, en el Problema de los ladrones de memes 1, la persona inocente debe descubrir la identidad de los ladrones. Por ejemplo, si Bob es inocente entonces existen tres posibilidades:

1. Que Alice o Catalina sea culpable.

2. Que ambas lo sean.

Esto induce los tres mundos correspondientes W_2, W_4 y W_5 en el modelo inicial de la Figura 1.2. Ahora bien, en la tarea a resolver es necesario que Bob pierda la indistinguibilidad, por lo que es necesario encontrar una tarea tal que estos tres mundos se separen en triángulos aislados en el *producto actualizado*. Haciendo este mismo procedimiento con Catalina y Alice inocentes, se tiene que la tarea de los memes robados es la de la Figura 2.3.

En este caso se prescinde de la notación $(B, \emptyset)$ y se sustituye con $(B, Culpables)$ pues el valor final de Bob es la identidad de los culpables. Nótese también que ninguno de los triángulos se intersecan con los otros, ni siquiera en los vértices correspondientes a agentes culpables, pues no existe indistinguibilidad alguna entre los diversos casos.



Formalmente, la tarea de los memes robados se define de la siguiente manera:

Definición 2.3.1 (Tarea de los memes robados) *Dado el conjunto de agentes* $\boldsymbol{A} = \{A, B, C\}$*, se define* $\mathcal{V} = \{D \subseteq \boldsymbol{A} | \emptyset \neq D \neq A\}$ *el conjunto de todos los valores finales posibles, consistentes en los conjuntos de culpables. Entonces la tarea de los memes robados* $\mathcal{R}$ *se define como:*

1. *El complejo simplicial cromático subyacente R tiene las siguientes facetas:*

$$F(R) = \bigcup_{D \in \mathcal{V}} \{(A, D), (B, D), (C, D)\}$$

Las cuales se denotan como X_D

2. *Las precondiciones $pre : V(R) \to \mathcal{L}_{\mathcal{K}}$ son tales que:*

$$pre((Q, D)) = \bigwedge_{q \in D} p_{q,1} \wedge \bigwedge_{q \notin D} p_{q,0}$$

Ahora bien, debido a las siguientes razones, queda evidenciada la similitud entre los ladrones de memes y el problema del consenso:

1. Todos los vértices de cada X_D tienen un mismo valor D asociado.
2. Gracias a las precondiciones, cada vértice de X_D tiene que venir de un mundo en el que los culpables sean los elementos de D
3. Mirando muy fijamente los mundos iniciales de la Figura 1.2, resulta que, en cada mundo donde los culpables son los elementos de D, hay al menos un agente cuyo valor asociado es D.

Por esta última razón la similitud es inmediata. Concretamente:

1. Los agentes tienen valores iniciales dados ($\emptyset$ o la lista de miembros de la conspiración).
2. Los agentes deben decidir uno de ellos (aunque aquí está la restricción de que no debe ser $\emptyset$).

Por lo tanto es legítimo pretender que, si se logra resolver el consenso, entonces se puede lograr también resolver el problema de los ladrones de memes. En el siguiente capítulo se presenta todo sobre la resolución del consenso, y finalmente se propone una forma de solucionar los memes robados a través del consenso en la Sección 4.2.1.

Capítulo 3

Modelos de topología combinatoria para consenso

En este capítulo, se presenta un modelo de topología combinatoria para el problema del consenso.

3.1. Modelos iniciales

En la introducción se presentó el siguiente enunciado intuitivo que describe el problema del consenso:

El problema del consenso consiste en n agentes con valores iniciales dados que quieren decidir uno de ellos. ¿Cómo podrían lograrlo?

Sea $A = \{1, \ldots, n\}$ el conjunto de agentes. Un lenguaje básico epistémico modal útil es el generado por las variables proposicionales $AP = \{p_{q,v} | q \in A, v \in \mathcal{V}\}$ donde $p_{q,v}$ significa que el agente q tiene el valor v.

El siguiente paso es diseñar un modelo simplicial que contenga toda la información sobre los mundos iniciales posibles, como el de la Figura 1.2 para el problema de los memes robados. Para ello, lo primero es hablar sobre qué puede saber o no un agente al inicio del problema.

Al principio de los tiempos, cada agente recibe un valor de $\mathcal{V}$,[1] y posteriormente aprende o no valores de otros agentes. Es muy común asumir que cada agente conoce únicamente su propio valor inicial, sin embargo en este trabajo se generaliza esta noción, permitiendo que sea posible conocer otros valores además del propio (por ejemplo en el Problema de los memes robados 1, todos los culpables saben el valor inicial de los demás

[1]Hay una discusión amplia sobre cómo se reciben estos valores (incluso más allá del problema del consenso), por ejemplo en el artículo [15] se menciona una *caja negra* que entrega los valores al azar (en ese caso se trata de cartas), mientras que en [22] los valores son tomados a consciencia por cada agente y luego son propuestos públicamente por los mismos. El modelo propuesto en este trabajo es lo suficientemente general para que ello sea irrelevante.

culpables). De esta forma, las visiones iniciales de cada agente se determinan por un par ordenado $(a_1, \ldots, a_n)$ donde a_i es el valor del agente i en caso de **conocerse**, o bien $\perp$ en caso de **desconocerse**.

Definición 3.1.1 (Visiones iniciales) *Considérese un conjunto de n agentes enumerados $\{0, 1, \ldots, n-1\}$ y un dominio de valores $\mathcal{V}$. El conjunto de **visiones iniciales válidas** para el agente i-ésimo se define como:*

$$\mathcal{V}_i = \{(a_1, \ldots, a_n) \in (\mathcal{V} \cup \{\perp\})^n | a_i \neq \perp\}$$

En particular, se denota como $\hat{e_i}(x)$ al vector canónico que tiene todas las entradas como $\perp$ salvo la i-ésima, que vale x.

De esta forma, los **mundos iniciales** se definen como todas las combinaciones posibles de agentes con sus vistas tales que son consistentes entre sí: si el agente i sabe que el agente j tiene el valor k, y otro agente h conoce en el mismo mundo que el valor del agente j es k', entonces $k = k'$

Definición 3.1.2 (Mundos inciales) *Considérese un conjunto de n agentes enumerados $\{0, 1, \ldots, n-1\}$ y un dominio de valores $\mathcal{V}$. Se definen el conjunto de todos los **mundos iniciales** posibles como:*

$$F(I) := \{\{(1, \hat{v_1}), \ldots, (n, \hat{v_n})\} | \hat{v_i} \in \mathcal{V}_i \text{ y para todo } h, j, k \ \pi_j(\hat{v_k}) \neq \pi_j(\hat{v_h}) \text{ syss uno es } \perp\}$$

Donde $\pi_j(\hat{v_a})$ es la proyección canónica que arroja la j-ésima coordenada del vector $\hat{v_a}$

A continuación se demuestra que esta definición mantiene consistencia entre los conocimientos de los agentes en un mundo dado:

Teorema 3.1.1 *Sea $\{(1, \hat{v_1}), \ldots, (n, \hat{v_n})\} \in F(I)$, entonces si $\pi_j(\hat{v_i}) = k$ y $\pi_j(\hat{v_h}) = k'$ con $k \neq \perp \neq k'$ (es decir, los agentes i, h saben que j tiene el valor k y k' respectivamente) entonces $k = k'$*

Prueba.
Como $\{(1, \hat{v_1}), \ldots, (n, \hat{v_n})\} \in F(I)$, entonces se tiene que para todo i, h se cumple que $\pi_j(\hat{v_i}) \neq \pi_j(\hat{v_h})$ si y solo si uno es $\perp$. Sin embargo, para agentes i, h como en las hipótesis del enunciado del teorema se tiene que $\pi_j(\hat{v_i}) \neq \perp \neq \pi_j(\hat{v_h})$ por lo que $\pi_j(\hat{v_i}) = \pi_j(\hat{v_h})$, por lo que $k = k'$ ■

Es posible discutir aún más sobre la Definición 3.1.2 siendo una representación fiel de posibles configuraciones iniciales en el mundo real: por ejemplo es posible caer en un planteamiento inicial en el que ciertos mundos de $F(I)$ estén vetados, como aquellas situaciones en las que todos saben únicamente su propio valor inicial y nada más (es decir, solamente se cae en mundos de la forma $\{(1, \hat{e_1}(x_1)), \ldots, (n, \hat{e_n}(x_n))\}$), o bien sólo se vive en casos en los que la mitad de los agentes tienen el mismo valor, o mundos en los que la selección de fútbol de Armenia no puede coexistir en el mismo grupo de Eurocopa

que la selección de Azerbaiyán, y más aún el arreglo debe ser tal que su único encuentro sea hasta la final del torneo (cantadísima[2]), o mundos en los que si Alice tiene 0 entonces Bob no puede tener 5, etc.

Todas estas situaciones se pueden representar como subconjuntos de $F(I)$ sin ningún problema, por lo que vale la pena preguntarse si es posible encontrar casos fuera de $F(I)$. La respuesta es afirmativa ya que la Definición 3.1.1 no considera la situación en la que uno ignora su propio valor inicial, gracias a la petición $a_i \neq \perp$, sin embargo considerar este caso tiene consecuencias no triviales hasta el punto que es necesario renunciar a la pureza de los complejos simpliciales y cambiar el sistema axiomático $\mathbf{S5}_n$ por el sistema $\mathbf{KB4}_n$ (como se establece en [20], donde los agentes pueden morir y por tanto desconocer su propio valor inicial a partir de cierto momento).

3.2. La forma de modelos iniciales

En esta sección se discute la forma de ciertos modelos. A continuación se presenta terminología original:

Definición 3.2.1 (Modelos iniciales absolutos)
*El **modelo inicial absoluto** $\mathcal{I} =< I, \chi, \ell >$ es un modelo simplicial definido de la siguiente manera:*

1. *El complejo simplicial I es el inducido por el conjunto de facetas ya definido:*

$$F(I) := \{\{(1, \hat{v_1}), \ldots, (n, \hat{v_n})\} | \hat{v_i} \in \mathcal{V}_i, \ \ y \ \forall i, h \ \pi_j(\hat{v_i}) \neq \pi_j(\hat{v_h}) \ \ syss \ uno \ es \perp)\}$$

2. *La coloración χ es la primera proyección canónica: $\chi(i, v_i) = i$*

3. *La valuación se define como $\ell((q, \hat{v_q})) = p_{q,\pi_q(\hat{v_q})}$*

De estos modelos absolutos, un subconjunto importante son los **totales**, quienes corresponden al problema del consenso original en el que sólo se sabe el propio valor inicial:

Definición 3.2.2 (Modelos iniciales totales (basado en la definición de [18]))
*El **modelo inicial total** $\mathcal{I} =< I, \chi, \ell >$ es un modelo simplicial definido de la siguiente manera:*

1. *El complejo simplicial I es el inducido por el conjunto de facetas:*

$$F(I) := \{\{(1, \hat{e_1}(x_1)), \ldots, (n, \hat{e_n}(x_n))| x_i \in \mathcal{V}\}$$

2. *La coloración χ es la primera proyección canónica: $\chi(i, v_i) = i$*

[2]Como ya se explicó en los memes robados, este tipo de cosas pasan con mucha frecuencia en el fin del mundo.

3. La valuación se define como $\ell((q, \hat{e_q}(x_q))) = p_{q,x_q}$

A continuación se estudia la forma de los modelos totales, más en particular el caso más sencillo y fundamental de todos: el binario.

3.2.1. Modelos iniciales totales binarios

Considérese $\mathcal{V} = \{0, 1\}$, en este caso los conjuntos de valores iniciales posibles corresponden a las diversas palabras binarias de longitud n. Cuando $n = 2$ con agentes Alice y Bob, los mundos correspondientes son:

$$F(I) = \{\{(A, 1\bot), (B, \bot 1)\}, \{(A, 1\bot), (B, \bot 0)\}, \{(A, 0\bot), (B, \bot 1)\}, \{(A, 0\bot), (B, \bot 0)\}\}$$

Y es inmediato *pegarlos* entre sí para formar un grafo cíclico de orden 4. El resultado es un cuadrado ilustrado en la Figura 3.1a).

Cuando se involucra una tercer agente Catalina, la dimensión del complejo simplicial se incrementa y deja de ser un grafo para convertirse en un poliedro, más en particular en un octaedro con caras correspondientes a las siguientes facetas:

$$\begin{aligned} F(I) \quad = \{&\{(A, 1\bot\bot), (B, \bot 1\bot), (C, \bot\bot 1)\}, \{(A, 1\bot\bot), (B, \bot 0\bot), (C, \bot\bot 1)\}, \\ &\{(A, 0\bot\bot), (B, \bot 1\bot), (C, \bot\bot 1)\}, \{(A, 0\bot\bot), (B, \bot 0\bot), (C, \bot\bot 1)\}, \\ &\{(A, 1\bot\bot), (B, \bot 1\bot), (C, \bot\bot 0)\}, \{(A, 1\bot\bot), (B, \bot 0\bot), (C, \bot\bot 0)\}, \\ &\{(A, 0\bot\bot), (B, \bot 1\bot), (C, \bot\bot 0)\}, \{(A, 0\bot\bot), (B, \bot 0\bot), (C, \bot\bot 0)\}\} \end{aligned}$$

Como puede verse en la Figura 3.1b)

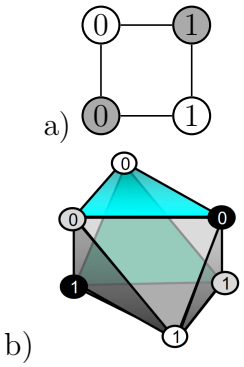


Figura 3.1: a) El complejo inicial binario de dos agentes. Alice es gris y Bob es blanco. b) El complejo inicial binario para tres agentes. Alice es gris, Bob es blanco y Catalina es negra. Los mundos de hasta arriba y abajo son aquellos donde todos tienen el mismo valor inicial.
Tanto en a) como en b), el vértice $(agente, \hat{e}_{agente}(x))$ es representado como un círculo coloreado por el agente y con el valor x dentro del mismo, por ejemplo $(Bob, \bot 0\bot)$ se representa como un círculo blanco con el valor 0 dentro. Fuente: [18]

Cabe ahora preguntarse cómo se vería el modelo inicial total si de pronto se integra a la fiesta el cocodrilo **D**ante (un cuarto agente **D**), y luego le sucede la zombi sanguinaria

de **E**lizabeth Bathory (una quinta agente **E**), etc. En general, ¿qué clase de figura se formaría para n agentes? pegar faceta por faceta de manera artesanal podría no brindar la suficiente información topológica (sin mencionar que tomaría muchísimo tiempo), por lo que es necesario tomar otro camino.

Ahora bien, si se observan con atención los complejos simpliciales de la Figura 3.1 entonces se notará algo muy interesante: el complejo de dos agentes es la triangulación de una circunferencia, mientras que el complejo de tres agentes es la triangulación de una esfera (es decir, son homeomorfos a dichos objetos), lo que se hace obvio si las aristas se curvan y las caras se abomban. Es entonces una buena conjetura el pretender que el complejo inicial binario de n agentes es homeomorfo a una $(n-1)$-esfera, lo que de hecho es cierto como es asegurado en [22] (donde se le deja como ejercicio al lector). En este trabajo se demuestra dicho teorema, pero antes de ello es necesario discutir una serie de cuestiones. En primer lugar, los autores de [22] son crueles pero justos y, siendo conscientes de la dificultad intrínseca de este teorema,[3] dejaron la sugerencia de notar que el complejo en cuestión es una bola abierta acorde a la *distancia Manhattan*.

Definición 3.2.3 (Distancia Manhattan o métrica del taxista [9]) *Dados dos vectores $(x_1,\ldots,x_n),(y_1,\ldots,y_n)\in\mathbb{R}^n$, se define su* ***distancia Manhattan*** *como:*

$$d((x_1,\ldots,x_n),(y_1,\ldots,y_n))=\sum_{i=1}^{n}|x_i-y_i|$$

Para finalmente aplicar el siguiente lema de análisis matemático:[4]

Teorema 3.2.1 *Sean d_1,d_2 distancias en $\mathbb{R}^n$, sean τ_1,τ_2 las topologías inducidas por estas métricas y sea $B_r^i(\hat{x})=\{\hat{y}\in\mathbb{R}^n|d_i(\hat{x},\hat{y})<r\}$ la bola de radio r y centrada en $\hat{x}$ con la métrica inducida por d_i. Entonces para todo $r>0$, $B_r^1(\hat{0})$ es homeomorfa a $B_r^2(\hat{0})$.[5] Más aún, las fronteras de ambas bolas también son homeomorfas.*

Existen también otras pruebas para este teorema, destacando la de [26], Capítulo 4, Ejemplo 4.2.2, (también encontrada en el libro [21], Capítulo 0, sección correspondiente al "Join") donde se construye paso a paso el complejo inicial correspondiente utilizando herramientas topológica más avanzadas, de manera que el homeomorfismo es casi inmediato.[6] En este trabajo se realizará la prueba esbozada en [22],

A continuación se demuestra:

Teorema 3.2.2 *El complejo inicial binario de n agentes es homeomorfo a una $(n-1)$-esfera.*

[3] De hecho es el más extenso y complicado de esta tesis.

[4] Este enunciado es una paráfrasis del que puede encontrarse en la fuente no primaria [9], Definición 3.8, Desigualdades (3.2), (3.1).

[5] El resultado es generalizable a cualquier centro distinto del origen gracias a que las traslaciones son isometrías. Sin embargo para los intereses de esta tesis no hay necesidad.

[6] Aunque en esta fuente no se considera el aspecto epistémico y cromático, sino únicamente la naturaleza topológica del objeto.

Prueba.
Considérese el siguiente morfismo $G : I \to \mathbb{R}^n$ definido como:

$$G(i, \hat{e}_i(x_i)) = \begin{cases} e_i & si \quad x_i = 1 \\ -e_i & si \quad x_i = 0 \end{cases}$$

Donde $e_i \in \mathbb{R}^n$ es el vector canónico que tiene todas las coordenadas 0 salvo la i-ésima, que vale 1.

Nótese ahora que el conjunto de vértices es $\{\pm e_i | 1 \leq i \leq n\}$ y que, para todo i, el conjunto $\{\pm e_i \mp e_j | 1 \leq j \leq n\} \cup \{\pm e_i \pm e_j | 1 \leq j \leq n\}$ es linealmente independiente por lo que G es una realización geométrica.

Posteriormente, el morfismo G se puede extender a simplejos *rellenando el cascarón* con la **envolvente convexa**: la arista $\{(i, \hat{e}_i(x_i)), (j, \hat{e}_i(x_j))\}$ se mapea a la recta que va de $G(i, \hat{e}_i(x_i))$ a $G(j, \hat{e}_i(x_j))$, la imagen de un 3-simplejo bajo G es un triángulo con vértices los tres elementos del 3-simplejo, y así sucesivamente. En general, un k-simplejo $K = \{(i_1, \hat{e}(x_{i_1})), \ldots, (i_k, \hat{e}(x_{i_k}))\}$ es mapeado al siguiente conjunto:

$$G[K] = \left\{ \sum_{j=1}^{k} a_j G(i_j, \hat{e}(x_{i_j})) \mid a_j \geq 0, \sum_{j=1}^{k} a_j = 1 \right\}$$

El cual es la envolvente convexa de las imágenes de sus vértices $conv(G[K])$. Además, satisface la siguiente propiedad:

Lema 3.2.1 *Un escalar a_j es nulo si y solo si $a_j G(i_j, \hat{e}_i(x_{i_j})) = 0$*

Prueba.
La ida de la prueba es trivial ya que $a_j = 0$ implica que $a_j G(i_j, \hat{e}_i(x_{i_j})) = 0$. La vuelta es inmediata ya que $G(i_j, \hat{e}_i(x_{i_j})) \in \{e_i, -e_i\}$ no es un vector nulo por lo que $a_j = 0$ forzosamente. ■

El siguiente paso es demostrar que la imagen de esta realización geométrica es homeomorfa a una $(n-1)$-esfera, para ello basta con notar que es una bola con la distancia Manhattan. Para notar ello, sea $\sum_{j=1}^{k} a_j G(i_j, \hat{e}(x_{i_j})) \in G[I]$ y defínase:

$$\delta(i, j) = \begin{cases} 0 & si \quad x_{i_j} = 1 \\ 1 & si \quad x_{i_j} = 0 \end{cases}$$

Esto permite hacer $\sum_{j=1}^{k} a_j G(i_j, \hat{e}(x_{i_j})) = \sum_{j=1}^{k} a_j (-1)^{\delta(i,j)} e_{i_j}$. Ahora bien, el vector $a_j (-1)^{\delta(i,j)} e_{i_j}$ es aquel que tiene todas las coordenadas nulas salvo la i_j-ésima, que vale $a_j (-1)^{\delta(i,j)}$, por lo que $\sum_{j=1}^{k} a_j (-1)^{\delta(i,j)} e_{i_j}$ es el vector que tiene todas las coordenadas

nulas salvo las i_j-ésimas para toda $1 \leq j \leq k$, las cuales valen $a_j(-1)^{\delta(i,j)}$ cada una. De esta forma:

$$\begin{aligned}
\ell_1\left(\sum_{j=1}^{k} a_j G(i_j, \hat{e}(x_{i_j})), \hat{0}\right) &= \ell_1\left(\sum_{j=1}^{k} a_j(-1)^{\delta(i,j)} e_{i_j}, \hat{0}\right) \\
&= \sum_{j=1}^{k} |a_j(-1)^{\delta(i,j)}| \\
&= \sum_{j=1}^{k} |a_j| \\
&= \sum_{j=1}^{k} a_j \\
&= 1
\end{aligned}$$

La igualdad no es "menor-qué" gracias al Lema 3.2.1, y por lo tanto $G[I] \subseteq \partial(B_1(\hat{0}))$

Finalmente, para revisar que $\partial(B_1(\hat{0})) \subseteq G[I]$ y por tanto concluir que la realización geométrica es efectivamente una bola con la distancia Manhattan, considérese $\hat{x} \in B_1(\hat{0})$ tal que $\hat{x} = (x_1, \ldots, x_n)$, entonces $\ell_1(\hat{x}, \hat{0}) = \sum_{i=1}^{n} |x_i| = 1$. Sean $x_{i_1}, \ldots, x_{i_k}$ las coordenadas no nulas de $\hat{x}$, entonces $\sum_{j=1}^{k} |x_{i_j}| = 1$. Sea ahora $a_j = |x_{i_j}|$ y se define:

$$\delta_0(i,j) = \begin{cases} 0 & si \quad x_{i_j} \geq 0 \\ 1 & si \quad x_{i_j} \leq 0 \end{cases}$$

Esta δ_0 es una especie de *recíproco* de la $\delta(i,j)$ definida para probar la otra contención, y además con la propiedad útil de que $x_{i_j} = (-1)^{\delta_0(i,j)}|x_{i_j}|$ para todo $x_{i,j}$

Finalmente, nótese que:

$$\begin{aligned}
\hat{x} &= \sum_{j=1}^{k} x_{i_j} e_{i_j} \\
&= \sum_{j=1}^{k} (-1)^{\delta_0(i,j)} |x_{i_j}| e_{i_j} \\
&= \sum_{j=1}^{k} |x_{i_j}| (-1)^{\delta_0(i,j)} e_{i_j}
\end{aligned}$$

Y dado que $1 = \sum_{j=1}^{k} |x_{i_j}|$, y además $G[I]$ es la envolvente convexa, se tiene que $\hat{x} \in G[I]$

Por último, gracias al Teorema 3.2.1, $G[I]$ es homeomorfa a la frontera de la bola euclidiana centrada en el origen y de radio 1, o lo que es lo mismo: a la $(n-1)$-esfera ■

3.3. Tareas de consenso

En el problema del consenso, todos los agentes necesitan decidir uno de los valores iniciales. Como ya fue mencionado en el Capítulo 2, la tarea del consenso es un cúmulo de facetas aisladas, una para cada posible decisión.

En el artículo [38] se señala una lista de propiedades importantes que formalizan la tarea del consenso de una manera axiomática. Dado un protocolo ejecutado por los agentes, este protocolo resuelve el consenso si y solo si satisface las siguientes propiedades:

- ***Terminación***. Cada agente debe decidir eventualmente un valor.[7]
- ***Acuerdo***. Todos los valores decididos son el mismo.
- ***Validez***. El valor decidido fue el valor inicial de alguien.

De esta manera, si la tarea del consenso se denota como un modelo de acción $\mathcal{T} =< T, \chi, pre >$ entonces T debe ser el siguiente cúmulo de facetas:

$$F(T) = \bigcup_{d \in \mathcal{V}} \{\{(p,d) | p \in A\}\}$$

Una por cada posible decisión marcada por la condición de *terminación*. Además en cada faceta todos los agentes tienen el mismo valor, lo que corresponde a la condición de ***acuerdo***.

Estas facetas pueden denotarse como $\{(p,d)|p \in A\} = X_d$, y es muy fácil demostrar que están aisladas:

Teorema 3.3.1 *Si $X_d \cap X_f \neq \emptyset$ entonces $d = f$*

Prueba. Sea $(a,i) \in V(X_d \cap X_f)$, entonces por definición $i = d$ e $i = f$ por lo que $d = f$ ■

Como corolario inmediato, las facetas X_d están aisladas entre sí.

Finalmente, la tarea del consenso se define formalmente como sigue:

Definición 3.3.1 (Tarea del consenso [18]) *Considérese un conjunto de n agentes A y un dominio de valores $\mathcal{V}$. Sea $V \subseteq \mathcal{V}$ el conjunto de todos los valores iniciales posibles ($V = \mathcal{V}$ para modelos totales), entonces la tarea del consenso $\mathcal{T}$ se define como sigue:*

[7] Nótese que esto implica que todo protocolo que resuelva el consenso debe terminar algún día.

1. *El complejo simplicial cromático subyacente T tiene facetas:*

$$F(T) = \bigcup_{d \in V} \{\{(p, d) | p \in A\}\}$$

Y tiene la coloración usual $\chi = \pi_1$

2. *Las precondiciones $pre : V(T) \to \mathcal{L}_{\mathcal{K}}$ son tales que:*

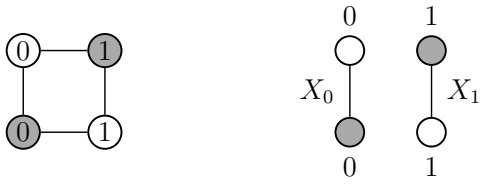
$$pre((p, d)) = \bigvee_{q \in A} p_{q,d}$$

Nótese que las tres condiciones de [38] salvo la de terminación[8] quedan bien representadas en esta definición:

- ***Acuerdo***. Dada una faceta X_d, todos tienen el valor d en ella.
- ***Validez***. Formalizada por la precondición. Si p decidió d entonces p vivía en un mundo donde alguien tenía p, lo que equivale a la siguiente fórmula:

$$\bigvee_{q \in A} p_{q,d}$$

Para estudiar el producto actualizado, a continuación se presentan un par de ejemplos. En primer lugar, en la figura de abajo se ilustra el modelo inicial $\mathcal{I}$ (izquierda) y el modelo de acción $\mathcal{C}$ (derecha) para el caso binario con dos agentes Alice (blanco) y Bob (gris):



$\mathcal{I}$ $\mathcal{C}$

Los números de los nodos son proposiciones atómicas que describen valores iniciales de $\mathcal{I}$.

Para obtener el producto actualizado, basta con emparejar cada acción X_i con los mundos donde alguien tiene el valor inicial i. Para casos pequeños como este es posible enlistar cada uno de ellos, por ejemplo si $i = 0$ entonces los mundos que satisfacen $pre(X_0)$ son:

- $\{(A, 0), (B, 0)\}$

[8]Puede quedar representado por el hecho de que aplicar la acción implica que, eventualmente, algo sucederá. Sin embargo es posible representar acciones que suceden en el infinito con este mismo marco teórico.

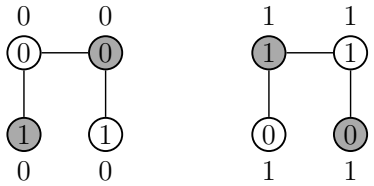
- $\{(A,0),(B,1)\}$
- $\{(A,1),(B,0)\}$

Luego, en el producto actualizado, evolucionarán a los siguientes mundos:

- $\{(A,0,0),(B,0,0)\}$
- $\{(A,0,0),(B,1,0)\}$
- $\{(A,1,0),(B,0,0)\}$

Como nota curiosa, nótese que el vértice $(A,1)$ también podría evolucionar a $(A,1,1)$ ya que $\{(A,1),(B,0)\}$ cumple además con $pre(X_1)$. En general, siempre es posible que un vértice evolucione a múltiples vértices en el producto actualizado (concretamente, a tantos como precondiciones satisfaga).

Ahora bien, gracias a la estructura topológica del producto actualizado, las indistinguibilidades se comportan de manera *adecuada*: las facetas se intersecan en los vértices que tienen en común. Por ejemplo, $(A,0,0)$ pertenece a dos facetas del producto actualizado. De esta forma, es posible construirlo de manera *artesanal*, pegando cuidadosamente las facetas conforme corresponda. En este caso, el resultado es el siguiente:



$\mathcal{I}[\mathcal{C}]$

A la izquierda están todos los mundos donde deciden 0 mientras que a la derecha donde deciden 1. En general, el producto actualizado del problema del consenso es tal que cada acción X_d conforma una componente conexa, lo que es intuitivamente cierto ya que lo contrario implicaría que un agente no podría distinguir entre un mundo donde eligieron d de otro donde eligieron algún otro valor, lo que es una contradicción a lo previamente discutido.

Teorema 3.3.2 *El subcomplejo C_d del producto actualizado $\mathcal{I}[\mathcal{C}]$ consistente en el subcomplejo inducido por los vértices $\{(q,v,d)|q \in A, v \in \mathcal{V}\}$ es conexo. Además, si $d \neq e$ entonces C_d y C_e están aislados.*

Prueba.
Conexidad:

Sean $(q,v,d),(p,b,d) \in V(C_d)$. Nótese que $(q,v) \in V(I)$ comparten facetas con algún vértice (r,d), pero $(r,d) \in \{(a,d)|a \in A\} \in F(I)$. Así, el siguiente camino está en $I[C]$:

$$(q,v,d),(r,d,d)$$

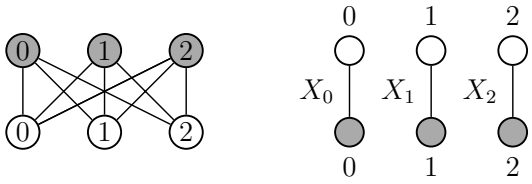
Finalmente, por argumento análogo, tenemos el camino $(r,d,d),(p,b,d)$ y por tanto el camino $(q,v,d),(r,d,d),(p,b,d)$. Nótese que esto también demuestra que los C_d tienen forma de estrella cuyo núcleo es el mundo donde inicialmente todos tenían d.

Componentes aislados:

Aprovechando la prueba previa, será suficiente mostrar que los mundos $\{(q,d,d)|q \in A\}$ y $\{(q,e,e)|q \in A\}$ están aislados.

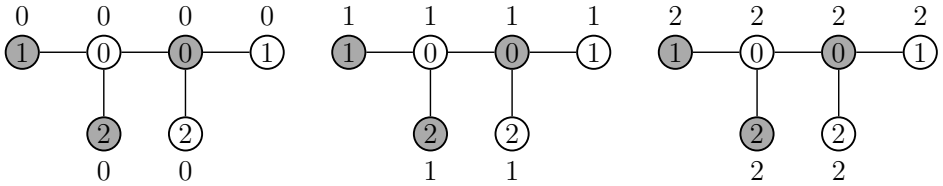
Supóngase que existe un camino $(q,d,d),(q_1,v_1,d_1),\ldots,(q_k,v_k,d_k),(q,e,e)$, entonces debe haber algún momento i tal que $d_i \neq d_{i+1}$ (defínase $d_0 = d$ y $d_{k+1} = e$, $q_0 = q = q_{k+1}$) y por tanto la decisión hecha en esos mundos debe ser diferente. Considérese el primero de estos i's y considérese el agente del vértice (q_i,v_i,d_i)), entonces q_i no puede distinguir entre mundos donde todos decidieron lo tomado en $\{(q_{i-1},v_{i-1},d_{i-1}),(q_i,v_i,d_i)\}$ de mundos donde todos decidieron lo tomado en $\{(q_{i+1},v_{i+1},d_{i+1}),(q_i,v_i,d_i)\}$, lo que es una contradicción. ■

Para un ejemplo más elaborado, supóngase que Alice y Bob también pueden tomar un tercer valor 2, entonces el modelo inicial es más complicado (aunque aún posible de dibujar), consistente en el grafo $K_{3,3}$ completo bipartito con tres vértices de cada color/agente,[9] mientras que el modelo de acción consiste en un cúmulo de tres aristas ajenas X_0, X_1, X_2:



$\mathcal{I}$ $\mathcal{C}$

En este caso, el producto actualizado es como sigue:



$\mathcal{I}[\mathcal{C}]$

Nótese que se mantiene el hecho discutido en la prueba del Teorema 3.3.2 de que las componentes conexas del producto actualizado tienen forma de estrella cuyo núcleo es el mundo en el que todos tienen el mismo valor inicial.

[9]Este grafo no es plano por el teorema de Kuratowski [8]. En general, ningún complejo de dos agentes es plano si $\mathcal{V}$ tiene tres o más elementos.

El siguiente paso es discutir el problema principal del presente trabajo: responder a la pregunta de cuándo el consenso se puede resolver y cuándo no. Para resolver esta cuestión va a aglomerarse todo lo visto en capítulos previos.

Capítulo 4

Sobre la resolubilidad del consenso

En este capítulo, se discute a profundidad la resolubilidad del consenso desde el punto de vista topológico-epistémico. Finalmente, se presentan dos resultados famosos de consenso y se discuten bajo esta misma perspectiva.

4.1. Una caracterización con conocimiento común

Existe una relación íntima entre la resolución del consenso y el conocimiento común: si todo el mundo sabe que resolvió el consenso entonces puede resolverlo (esto fue ampliamente discutido en el libro [32] capítulo 6, pero desde una perspectiva lógica). Sin embargo cabe preguntarse si aquello no sería una condición equivalente y, más en particular, qué significa "saber que se resolvió la tarea".

Para aterrizar lo anterior, recuérdese que el conocimiento grupal (Definición 1.4.1) fue definido como $E(\varphi) = \bigwedge_{a\in A} K_a(\varphi)$. En estos términos, las tres propiedades del consenso discutidas en el Capítulo 3, Sección 3.3 se pueden traducir a las siguientes fórmulas epistémicas:

- *Acuerdo.* $\mathcal{I}[\mathcal{T}], I \times X_d \models \bigwedge_{a\in A} p_{a,d}$
- *Validez.* Si $\mathcal{I}[\mathcal{T}], I \times X_d \models \bigwedge_{a\in A} p_{a,d}$ entonces $\mathcal{I}, I \models \bigvee_{a\in A} p_{a,d}$.
- *Terminación.* $\mathcal{I}[\mathcal{T}], I \times X_d \models E^\infty(\bigwedge_{a\in A} p_{a,d})$.

Sobre el conocimiento común usado en la terminación, nótese que, para poder decidir un valor final, los agentes deben estar seguros de que, si alguien no ha tomado aún una decisión, eventualmente lo hará (y será la misma que la de ellos). Más aún, **esta cuestión proporciona una caracterización para el consenso**, lo cual es el resultado más importante de esta tesis:

Teorema 4.1.1 *Un protocolo distribuido representado mediante un modelo de acción $\mathcal{T}$ resuelve el consenso si y solo si $\mathcal{I}[\mathcal{T}], X \models \bigvee_{v\in\mathcal{V}} E^\infty(\bigvee_{a\in A} p_{a,v})$ para toda faceta $X \in \mathcal{I}[\mathcal{T}]$. En otras palabras, existe un valor $v \in \mathcal{V}$ tal que el que alguien lo tenga como valor inicial es de conocimiento común.*

Prueba.

Supóngase que la tarea $\mathcal{T}$ resuelve el consenso.

A continuación se procede por inducción a partir de $n = 1$, sobre la cantidad de veces que se anida el operador de conocimiento grupal en la fórmula $\bigvee_{a\in A} p_{a,v}$

Para probar que $\mathcal{I}[\mathcal{T}], X \models E^1(\bigvee_{a\in A} p_{a,d})$, considérese $\delta : \mathcal{I}[\mathcal{C}] \to \mathcal{I}[\mathcal{T}]$ el morfismo como en la Definición 2.2.5, y considérese la componente conexa C_d en $I[C]$ para un $d \in \mathcal{V}$ arbitrario, entonces la imagen directa $\delta[C_d]$ es una componente conexa aislada en $\mathcal{I}[\mathcal{T}]$ por el Lema 2.2.1. Más aún, todas las facetas en $\delta[C_d]$ provienen de una configuración inicial donde alguien tiene d como valor inicial (pues $\pi_{\mathcal{I}} \circ \delta = \pi_{\mathcal{I}}$) por lo que, para toda faceta $X \in \delta[C_d]$, se tiene que $\mathcal{I}[\mathcal{T}], X \models \bigvee_{a\in A} p_{a,d}$. Finalmente, ello implica que $\mathcal{I}[\mathcal{T}], X \models E(\bigvee_{a\in A} p_{a,d})$

Ahora bien, supóngase que para toda faceta $X \in \mathcal{I}[\mathcal{T}]$ se tiene que $\mathcal{I}[\mathcal{T}], X \models E^n(\bigvee_{a\in A} p_{a,d})$ para alguna $n \in \mathbb{N}$, entonces por argumento análogo al de la base inductiva se tiene que $\mathcal{I}[\mathcal{T}], X \models E^{n+1}(\bigvee_{a\in A} p_{a,d})$

Finalmente, nótese que $\delta[\mathcal{I}[\mathcal{C}]] = \mathcal{I}[\mathcal{T}]$ por lo que $\bigcup_{v\in\mathcal{C}} \delta[C_v] = \mathcal{I}[\mathcal{T}]$ y por tanto $\mathcal{I}[\mathcal{T}], X \models \bigvee_{v\in\mathcal{V}} E^\infty_A(\bigvee_{a\in A} p_{a,v})$ para toda faceta X de $X \in \mathcal{I}[\mathcal{T}]$

Supóngase que $\mathcal{I}[\mathcal{T}], X \models \bigvee_{v\in\mathcal{V}} E^\infty(\bigvee_{a\in A} p_{a,v})$ para toda faceta $X \in \mathcal{I}[\mathcal{T}]$

Al final de la ejecución es posible alcanzar consenso con el siguiente algoritmo:

Sea I el conjunto de todos los valores que satisfacen la condición del conocimiento común.

- **PASO 1:** Asígnese un orden parcial para I. Esto puede hacerse de manera *greedy* tomando elementos al azar e irlos enumerando conforme vayan saliendo.
- **PASO 2:** Decidir $Max(I)$

Este algoritmo es correcto ya que toda I es igual para todos los agentes en el mismo mundo gracias al conocimiento común. ■

Para terminar, vale la pena recalcar una nota importante: en los ejemplos del consenso binario y ternario presentados en la Sección 3.3, el diámetro de las componentes C_d es de a lo más dos, por lo que $E^2(\varphi) = E^\infty(\varphi)$. Sin embargo esto sólo pasa en la tarea del consenso y es posible construir una componente conexa con un diámetro mayor y que también satisfaga conocimiento común.

4.2. Un método de coloración para resolubilidad del consenso

Otra consecuencia del Teorema 4.1.1 es que permite saber si un protocolo resuelve o no el consenso a través del siguiente método que recuerda al análisis topológico de datos:

1. Primero se asigna un color a cada valor de $\mathcal{V}$.
2. Considérese el modelo de acción $\mathcal{A}$ asociado al protocolo, entonces se asigna el color d a cada mundo en $I[A]$ si y solo si ese mundo proviene de un mundo donde alguien tiene d como valor inicial (es posible que haya mundos multicolores. Por ejemplo para $\mathcal{A} = \mathcal{T}$, un mundo tiene tantos colores como elementos del conjunto I descrito en la prueba del Teorema 4.1.1).
3. Considérese una componente conexa K de $I[A]$. Si existe un valor d que colorea todos los mundos de K entonces se tiene conocimiento común sobre d siendo el valor inicial de alguien.
4. En cada K quítense todos los colores que no satisfacen la propiedad del conocimiento común. Los colores sobrevivientes son los elementos del conjunto I.

Teorema 4.2.1 *El consenso no se puede resolver en $\mathcal{A}$ si y solo si existe una componente conexa $K \subseteq T$ sin color alguno en el algoritmo previo.*

Prueba.

Supóngase que el consenso no se puede resolver en $\mathcal{A}$

Supóngase también que toda componente conexa $K \subseteq T$ tiene color al finalizar el algoritmo previo, entonces en cada una de ellas se puede resolver el consenso ejecutando el algoritmo de la prueba del Teorema 4.1.1 ya que el conjunto I nunca es vacío (sus elementos son los colores que pintan la componente conexa en la que viven los agentes, como ya se mencionó), lo que es una contradicción.

Supóngase que existe componente conexa $K \subseteq T$ sin color alguno.

Entonces para todo valor d existe un mundo en K donde alguien no tiene d por lo que para todo X faceta de K se tiene que $\mathcal{I}[\mathcal{A}], X \models \bigwedge_{d\in\mathcal{V}} \neg E^{\infty}(\bigvee_{a\in A} p_{a,d})$ (intuitivamente, no se tiene conocimiento común sobre la posesión de ningún valor por parte de alguien) por lo que, por el Teorema 4.1.1, el consenso es imposible. ■

4.2.1. Resolviendo el problema de los memes robados

Como ya se mencionó en el capítulo anterior, es legítimo sospechar que el problema de los memes robados puede resolverse a partir del problema del consenso ya que es un caso particular del mismo. Para corroborarlo formalmente basta con ver que el modelo

inicial de los memes robados está contenido dentro del modelo inicial del problema del consenso, sin embargo ello no tiene sentido *a priori* ya que los vértices del modelo de los memes robados son de la forma $(A, (\emptyset, \perp, \perp))$ mientras que los del modelo del consenso son $(A, valor)$. Para sortear esta dificultad, nótese que la *vista* $(\emptyset, \perp, \perp)$ de ser inocente e ignorar a los culpables corresponde al valor inicial $\emptyset$ de manera biunívoca, por lo que existe un submodelo del modelo inicial absoluto que es isomorfo (es decir, que existe un morfismo biyectivo) al modelo de los memes robados.

Teorema 4.2.2 *Considérese el modelo inicial absoluto* $\mathcal{I} =< I, \chi, \ell >$ *con el conjunto de valores* $\mathcal{V} = \{X \subseteq \{A, B, C\} | X \neq \{A, B, C\}\}$ *Entonces el modelo inicial de los memes robados, denotado* $\mathcal{M} =< M, \chi, \ell >$ *es isomorfo a un submodelo de* $\mathcal{I}$*.*

Prueba. Para esta prueba, se presentan también los lemas auxiliares anidados Lema 4.2.1 y Lema 4.2.2.

Recuérdese que $\mathcal{M}$ se define con los siguientes vértices:

$$V(C) = \{(q, \emptyset), (q, \mathcal{K}) | q \in \{A, B, C\}, \{q\} \subseteq \mathcal{K} \subsetneq \{A, B, C\}\}$$

También recuérdese que los agentes culpables conocen la identidad de todos los culpables (y por tanto saben quienes son inocentes) mientras que los inocentes no tienen la menor idea de lo que está pasando, lo que induce los siguientes subconjuntos de vistas:

1. **Vistas posibles de Alice**:
   $\mathcal{B}_A = \{(\emptyset, \perp, \perp), (\{A\}, \emptyset, \emptyset), (\{A, B\}, \{A, B\}, \emptyset), (\{A, C\}, \emptyset, \{A, B\})\} \subseteq \mathcal{V}_1$
2. **Vistas posibles de Bob**:
   $\mathcal{B}_B = \{(\perp, \emptyset, \perp), (\emptyset, \{B\}, \emptyset), (\{A, B\}, \{A, B\}, \emptyset), (\emptyset, \{B, C\}, \{B, C\})\} \subseteq \mathcal{V}_2$
3. **Vistas posibles de Catalina**:
   $\mathcal{B}_C = \{(\perp, \perp, \emptyset), (\emptyset, \emptyset, \{C\}), (\{A, C\}, \emptyset, \{A, C\}), (\emptyset, \{B, C\}, \{B, C\})\} \subseteq \mathcal{V}_3$

De esta manera, el submodelo isomorfo $\mathcal{M}' \subseteq \mathcal{I}$ se define con las siguientes facetas:

$$F(M') = \{\{(A, \hat{v}_A), (B, \hat{v}_B), (C, \hat{v}_C)\} | \hat{v}_X \in \mathcal{B}_X, \text{ y } \forall X, Y, j \ \pi_j(\hat{v}_X) \neq \pi_j(\hat{v}_Y) \text{ syss uno es } \perp\}$$

Debido a su definición, $\mathcal{M}'$ es submodelo de $\mathcal{I}$ por lo que basta rectificar que es isomorfo a $\mathcal{M}$. Para ello considérese la siguiente función $\varphi : V(M) \to V(M')$ definida por casos como sigue:

1. $\varphi((A, \emptyset)) = (A, (\emptyset, \perp, \perp))$, $\varphi((B, \emptyset)) = (B, (\perp, \emptyset, \perp))$, $\varphi((C, \emptyset)) = (C, (\perp, \perp, \emptyset))$
2. Para $\mathcal{K}$ conjunto unitario, $\varphi((q, \mathcal{K}))$ es el vértice cuya vista tiene todas las coordenadas $\emptyset$ excepto la correspondiente al único elemento de $\mathcal{K}$. Por ejemplo,
   $\varphi(A, \{A\}) = (A, (\{A\}, \emptyset, \emptyset))$
3. Para $\mathcal{K}$ con dos elementos, $\varphi((q, \mathcal{K}))$ es el vértice cuya vista tiene única coordenada $\emptyset$ la correspondiente al único elemento de $\{A, B, C\} - \mathcal{K}$. Por ejemplo,
   $\varphi(B, \{B, C\}) = (B, (\emptyset, \{B, C\}, \{B, C\}))$

Lema 4.2.1 *φ es biyectiva.*

Prueba.

1. **Inyectividad**: Sean $(X, V_X), (Y, V_Y) \in V(M)$ tales que $\varphi((X, V_X)) = \varphi((Y, V_Y))$. Si $\varphi((X, V_X)) = \varphi((Y, V_Y))$ y tienen "$\perp$" en alguna coordenada entonces $V_X = V_Y = \emptyset$. En particular, si la i-ésima coordenada no es $\perp$ entonces X y Y coinciden con el agente correspondiente a dicha coordenada, por lo que $X = Y$. Por otra parte, si $\varphi((X, V_X)) = \varphi((Y, V_Y))$ tienen $\emptyset$ en todas sus entradas salvo en una, donde tienen al conjunto unitario $\{q\}$, entonces $V_X = V_Y = \{q\}$ y además $X = Y = q$. Finalmente, si $\varphi((X, V_X)) = \varphi((Y, V_Y))$ y además tienen dos coordenadas con el conjunto $\{q, k\}$ entonces $V_X = V_Y = \{q, k\}$. Además, como $\varphi((X, V_X)) = \varphi((Y, V_Y))$, el agente de ambos es el mismo por lo que $X = Y$

2. **Suprayectividad**: La definición por casos de φ permite revisar suprayectividad de manera inmediata, ya que todos los vértices de M' caen en uno de esos casos.

■

Lema 4.2.2 *φ es cromática y preserva valuaciones.*

Prueba. El cromatismo es inmediato por la definición por casos: el color de un vértice $(X, V_X) \in V(M)$ es X, y la imagen $\varphi((X, V_X))$ tiene siempre color X por definición. Sobre las valuaciones, se tiene que se define explícitamente como sigue:

$$\ell(X, V_X) = \begin{cases} p_{X,0} & si \quad X \notin V_X \\ p_{X,1} & si \quad X \in V_X \end{cases}$$

Mientras que la valuación en M' se define como $\ell((X, \hat{v}_X)) = p_{X,\pi_X(\hat{v}_X)}$. Caso por caso, se tiene que:

1. $\ell(\varphi((X, \emptyset)) = \ell(A, (\emptyset, \perp, \perp)) = p_{A,0}$, $\ell(\varphi((B, \emptyset)) = \ell(B, (\perp, \emptyset, \perp)) = p_{B,0}$ y $\ell(\varphi((C, \emptyset))) = \ell(C, (\perp, \perp, \emptyset)) = p_{C,0}$

2. Para $\mathcal{K}$ conjunto unitario, $\ell(\varphi((q, \mathcal{K}))) = p_{q,1}$ ya que es el vértice cuyas coordenadas son todas "$\emptyset$" salvo la correspondiente al único elemento de $\mathcal{K}$, pero $\ell((q, \mathcal{K})) = p_{q,1}$.

3. Para $\mathcal{K}$ con dos elementos, $\ell(\varphi((q, \mathcal{K}))) = p_{q,1}$ ya que $q \in \mathcal{K}$, pero también $\ell((q, \mathcal{K})) = p_{q,1}$

■

Gracias a los Lemas 4.2.1 y 4.2.2, se concluye entonces la existencia del isomorfismo. ■

Nótese ahora que la tarea de los memes robados está contenida en la tarea del consenso con valores $\mathcal{V} = \{X \subseteq \{A, B, C\} | X \neq \{A, B, C\}\}$, pues esta última consiste en un cúmulo de siete triángulos aislados: seis correspondientes a los de la tarea de los memes robados (donde deciden $\{A\}, \{B\}, \{C\}, \{A, B\}, \{A, C\}$ o $\{B, C\}$ respectivamente) junto con aquel en el que deciden $\emptyset$. Por lo tanto, es legítimo pretender que, si $\mathcal{R}$ es la tarea de los memes robados entonces $\mathcal{M}'[\mathcal{R}] \subseteq \mathcal{I}[\mathcal{C}]$, y por tanto resolver el consenso conlleva a resolver los memes robados.

Si bien esta solución es válida, no necesariamente es la única posible: debido a que $\mathcal{M}'[\mathcal{R}] \subseteq \mathcal{I}[\mathcal{C}]$, existen mundos en $\mathcal{I}[\mathcal{C}]$ que no están en $\mathcal{M}'[\mathcal{R}]$ por lo que existen indistinguibilidades en $\mathcal{I}[\mathcal{C}]$ que no están en $\mathcal{M}'[\mathcal{R}]$. Así, en los memes robados hay más conocimiento que en el consenso ordinario (lo que concuerda con el hecho de que los culpables se conocen entre sí), por lo que no debe descartarse la existencia de una solución que tome ventaja de esto.

4.3. Resolución del consenso en otros modelos

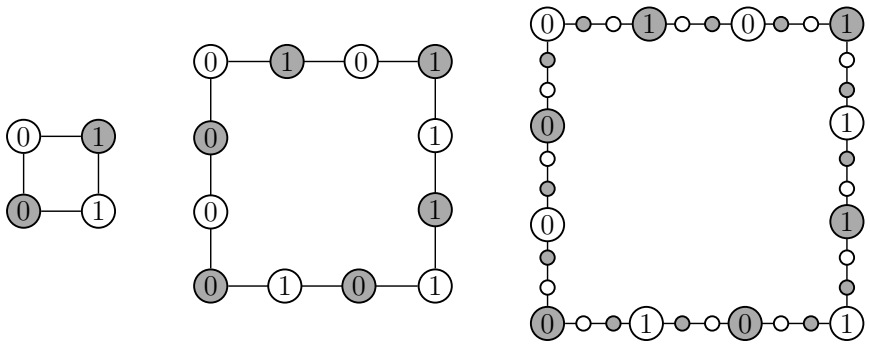
En esta sección se presentan dos resultados sobre la resolubilidad del consenso: el de Moses-Winkler-Schmidt [39] para sistemas síncronos *compactos*[1] y el más reciente de [31] para todo tipo de sistemas síncronos. Son discutidos bajo la perspectiva topológico-combinatoria.

4.3.1. Sistemas síncronos con redes dinámicas

En el artículo [31], el problema del consenso es estudiado en sistemas donde los medios de comunicación están determinados por redes dinámicas, las cuales son un sistema basado en rondas (síncronos) de envío de mensajes sin intermediarios como una memoria compartida o un búfer de mensajes (por ejemplo comunicación por radiofrecuencias). El interés de las redes dinámicas es que no están exentas de fallas y existe la posibilidad de que un mensaje no pueda llegar a su destino (esto ha sido entendido con el concepto de Adversario de Mensajes, presentado en [1]).

Un ejemplo de redes dinámicas es el **modelo de gráficas dinámicas**, denotado $\mathcal{DG}^r$, y estudiado en [4]:

[1]Para ver más sobre la *compacidad*, se recomienda revisar [39]. En este trabajo no se utiliza el hecho de *ser compacto* en ningún momento de las pruebas.



$\mathcal{I}$ $\mathcal{I}[\mathcal{DG}]$ $\mathcal{I}[\mathcal{DG}^2]$

Aquí, las comunicaciones admitidas son $\{A \to B, A \leftarrow B, A \leftrightarrow B\}$ (donde $Q \to P$ significa que el mensaje enviado por Q llega a P, lo mismo que $P \leftarrow Q$) y los conocimientos evolucionan acorde a $\mathcal{I}[\mathcal{DG}^r]$, lo que es un ciclo con $4 \times 3^{r-1}$ vértices. El consenso es imposible aquí [5, 6, 22, 29].

En general, la pregunta de interés es saber en qué redes dinámicas el consenso puede ser alcanzado. En [31] se definió una métrica para medir la "cercanía en conocimiento" de las diversas ejecuciones. En dicho trabajo las ejecuciones son denotadas por letras griegas y se definen como una configuración inicial, un algoritmo y un adversario de mensajes (dicho concepto equivale al medio de comunicación en este caso). Nótese que una ejecución en la ronda r tiene asociada una faceta en $\mathcal{I}[\mathcal{MA}^r]$, por lo que se denotan las facetas de dicho producto actualizado con letras griegas.

La métrica del mínimo La distancia entre dos facetas/ejecuciones α, β se define como $d_{min}(\alpha, \beta) = 1/2^r$ si y solo si $r-1$ es la última ronda donde los agentes son incapaces de distinguir entre α y β (equivalentemente, r es la primer ronda cuando al menos un agente puede distinguir entre α y β). De esta forma, si $d_{min}(\alpha, \beta) = 1/2^r$ entonces α y β serán la misma faceta hasta $\mathcal{I}[\mathcal{MA}^r]$. Una bola abierta con radio r centrada en α es entonces el conjunto de todas las facetas β que comparten todos los vértices de P con α al menos hasta la ronda r.

Teorema 4.3.1 (Nowak-Schmid-Winkler [31]) *Existe una ronda r tal que $\mathcal{I}[\mathcal{MA}^r]$ resuelve el consenso si y solo si existe una partición $\{PS(v)|v \in \mathcal{V}_O\}$ de las facetas de $\mathcal{MA}^r$ tal que:*

1. *Cada $PS(v)$ es un conjunto abierto.*
2. *Si Z_v es una faceta de una configuración inicial donde todos tienen valor inicial v entonces $Z_v \in PS(v)$ (Z_v es una faceta z-valente).*

Esto es otra forma de comprender el resultado de los colores que mostramos previamente: en $PS(v)$ se decide v, por lo que corresponde a un cúmulo coloreado con v.

4.3.2. Adversarios de mensajes cerrados

La topología mínima descrita previamente fue definida en términos de ejecuciones, por lo que un adversario de mensajes puede ser un conjunto cerrado de ejecuciones (es decir, su complemento es abierto).

Este caso fue ampliamente estudiado en [39], donde los autores definieron que un agente A *influye* otro agente B en la ronda r si existe una secuencia de agentes $A_1, \ldots, A_{r-1}$ tales que A envía mensaje a A_1 en la ronda 1, luego A_1 envía a A_2 en la ronda 2 y así sucesivamente hasta llegar al agente A_{r-1}, que finalmente envía mensaje a B en la ronda r: es una cadena de mensajes desde A hasta B a lo largo de las rondas. El núcleo de una secuencia de comunicaciones se define como el conjunto de agentes que influencian a todos los demás en dicha secuencia.

Entonces definieron indistinguibilidad entre secuencias de comunicación en términos de relaciones de equivalencia, y finalmente el ***Kernel*** de una clase de indistinguiblidad como la intersección de todos los núcleos de los elementos de la clase. Finalmente, dieron su teorema principal:

Teorema 4.3.2 (Moses-Schmid-Winkler [39]) *Un adversario de mensajes cerrado resuelve el consenso si y solo si el Kernel de todas sus clases de indistinguibilidad es no vacío.*

De esta forma, en la ronda r, si un agente no puede distinguir entre dos secuencias de comunicación entonces las facetas asociadas compartirán el vértice coloreado con ese agente. Así, las clases de indistinguibilidad son componentes conexas del producto actualizado $\mathcal{I}[\mathcal{MA}]$. Finalmente, tener un Kernel no vacío en cada componente conexa significa que existe un agente que logró comunicar su valor inicial a todo el mundo. En otras palabras, si v es dicho valor inicial, entonces la fórmula $E(\bigvee_{a\in A} p_{a,v})$ se satisfará en la clase de indistinguibilidad. Por tanto, en adversarios de mensajes cerrados, un conocimiento grupal equivale a conocimiento común:

Teorema 4.3.3 *Un adversario de mensajes cerrado $\mathcal{MA}$ resuelve consenso en la ronda r si y solo si $\mathcal{I}[\mathcal{MA}^r], X \models \bigvee_{v\in\mathcal{V}} E_A(\bigvee_{a\in A} p_{a,v})$ para toda faceta $X \in \mathcal{I}[\mathcal{MA}^r]$.*

La moraleja principal de estas dos últimas secciones es que, bajo la lupa de la topología combinatoria, resultados tan teóricamente distantes como los de Moses-Schmid-Winkler y Fischer-Lynch-Paterson de pronto se tornan demasiado cercanos y estrechos entre sí gracias al Teorema 4.1.1, lo que es una evidencia más del gran poder que tiene esta rama de las matemáticas al ser aplicada en computación.

Capítulo 5

Conclusiones

El problema del consenso consiste en n agentes con valores iniciales dados que quieren decidir uno de ellos. ¿Cómo podrían lograrlo?

Una de las metas más importantes de la computación distribuida es *imitar* el cómputo secuencial mediante sistemas de múltiples computadoras para mejorar el rendimiento. Una forma de lograrlo es a través del consenso, lo que desafortunadamente no siempre es posible.

En esta tesis de maestría, se demostró en el Teorema 4.1.1 que el consenso es posible si y solamente si existe conocimiento común sobre la tenencia de uno de los valores iniciales, lo que tiene como consecuencia que el problema del consenso sea uno de esos casos descritos en el libro [32] donde el acuerdo y el conocimiento común son equivalentes.

Para obtener este resultado se utilizó el modelo de topología combinatoria basado en lógica epistémica mostrado en [18], pero generalizado en la Sección 3.2. Usando este modelo, se estudiaron algunos resultados conocidos sobre el problema y se obtuvieron visiones frescas. Por ejemplo se mostró el hecho de que, en conjuntos de ejecuciones cerrados en la topología de Alpern-Schneider (véase [2]), el conocimiento común equivale a conocimiento grupal.

Desafortunadamente, las lógica epistémica y la topología combinatoria son áreas famosas por ser oscuras y difíciles de comprender ya que requieren muchos conocimientos previos y un gran esfuerzo. Para resolver esta vicisitud se proporcionó una introducción jovial y fácil de entender a través del Ejemplo 1 de los **ladrones de memes**, el cual resultó tener conexiones íntimas con el problema del consenso.

En síntesis, las contribuciones principales de este trabajo son:

1. El Teorema 4.1.1

2. El método de la Sección 4.2, que se aprovecha del Teorema 4.1.1 para determinar si el consenso es posible o no a partir de colores en componentes conexas del producto acutalizado (donde tener el color p es igual a tener conocimiento común sobre p).

3. La presentación de los resultados de [39] y [31], más en particular el Teorema 4.3.3 el cual tiene como corolario inmediato que, en conjuntos cerrados de la topología de Alpern-Schneider, el conocimiento común equivale a conocimiento grupal.

4. Una introducción jovial a la topología epistémica a través del problema de los ladrones de memes.

Por otra parte, existe el siguiente trabajo a futuro:

1. En el Teorema 4.1.1, la fórmula que debe satisfacer conocimiento común es la condición de **terminación**, ¿y si todos los problemas de decisión se pueden reducir a este tipo de condiciones? Entonces podría obtenerse una caracterización universal.

2. El método de color de la Sección 4.2 es, como ya se señaló, muy similar a los métodos de análisis topológico de datos (ATD). Por tanto, es posible tender un puente entre ATD y topología epistémica tomando esto como punto de partida. Más aún, colorear un producto actualizado e informar si hay una componente sin colorear puede ser un programa computacional.

Sin duda alguna hay muchas más preguntas que se pueden derivar de este trabajo, siendo estas tres algunas de las más importantes.

Por último, esperamos que este proyecto impulse el enfoque de la topología combinatoria para abordar problemas de conocimiento y que, en general, se extienda hacia el estudio generalizado de problemas de decisión o, ¿por qué no?, todo tipo de problemas distribuidos.

Bibliografía

[1] Afek, Y., Gafni, E.: Asynchrony from synchrony. In: Frey, D., Raynal, M., Sarkar, S., Shyamasundar, R.K., Sinha, P. (eds.) Distributed Computing and Networking, 14th International Conference, ICDCN 2013, Mumbai, India, January 3-6, 2013. Proceedings. Lecture Notes in Computer Science, vol. 7730, pp. 225–239. Springer (2013). https://doi.org/10.1007/978-3-642-35668-1_16, https://doi.org/10.1007/978-3-642-35668-1_16

[2] Alpern, B., Schneider, F.B.: Defining liveness. Inf. Process. Lett. **21**(4), 181–185 (1985). https://doi.org/10.1016/0020-0190(85)90056-0, https://doi.org/10.1016/0020-0190(85)90056-0

[3] Armenta-Segura, J.: Modelos de topología combinatoria para problemas de Cartas Rusas. B.S. Thesis, Universidad Nacional Autónoma de México, México (2020)

[4] Armenta-Segura, J., Ledent, J., Rajsbaum, S.: Two-agent approximate agreement from an epistemic logic perspective. In: 13th Latin American Workshop on Logic/-Languages, Algorithms and New Methods of Reasoning, LANMR 2020 (2020)

[5] Attiya, H., Rajsbaum, S.: Indistinguishability. Commun. ACM **63**(5), 90–99 (Apr 2020). https://doi.org/10.1145/3376902, https://doi.org/10.1145/3376902

[6] Biran, O., Moran, S., Zaks, S.: A Combinatorial Characterization of the Distributed 1-Solvable Tasks. J. Algorithms **11**(3), 420–440 (1990). https://doi.org/10.1016/0196-6774(90)90020-F

[7] Blackburn, P., de Rijke, M., Venema, Y.: Modal Logic, Cambridge Tracts in Theoretical Computer Science, vol. 53. Cambridge University Press (2001). https://doi.org/10.1017/CBO9781107050884, https://doi.org/10.1017/CBO9781107050884

[8] Bondy, J.A., Murty, U.S.R.: Graph Theory with Applications. Elsevier, New York (1976)

[9] Clapp, M.: Análisis matemático. papirhos, IM-UNAM, México (2015)

[10] Coulouma, É., Godard, E., Peters, J.G.: A characterization of oblivious message adversaries for which consensus is solvable. Theor. Comput. Sci. **584**, 80–90 (2015). https://doi.org/10.1016/j.tcs.2015.01.024, https://doi.org/10.1016/j.tcs.2015.01.024

[11] Davis, M., Sigal, R., Weyuker, E., Sigal, D.: Computability, Complexity, and Languages: Fundamentals of Theoretical Computer Science. Computer Science and Scientific Computing, Elsevier Science (1994), https://books.google.com.mx/books?id=GRWOqKwZGRAC

[12] Ditmarsch, H.v., van der Hoek, W., Kooi, B.: Dynamic Epistemic Logic. Springer (2007). https://doi.org/10.1007/978-1-4020-5839-4

[13] Enderton, H.B.: A mathematical introduction to logic. Academic Press (1972)

[14] Euclid: The Elements of Euclid. Dover Publications Inc., New York, 2nd edn. (1956), https://archive.org/details/euclid_heath_2nd_ed

[15] Fernández-Duque, D., Soler-Toscano, F., Cordón-Franco, A., van Ditmarsch., H.: A colouring protocol for the generalized russian cards problem. Theoretical Computer Science (495), 81–95 (2013)

[16] Fischer, M., Lynch, N.A., Paterson, M.S.: Impossibility Of Distributed Commit With One Faulty Process. Journal of the ACM **32**(2), 374–382 (Apr 1985). https://doi.org/10.1145/3149.214121

[17] Fraleigh, J.: A First Course in Abstract Algebra. Pearson Education (2003), https://books.google.com.mx/books?id=gGJ2c6db8tYC

[18] Éric Goubault, Ledent, J., Rajsbaum, S.: A simplicial complex model for dynamic epistemic logic to study distributed task computability. Information and Computation p. 104597 (2020). https://doi.org/https://doi.org/10.1016/j.ic.2020.104597, in print, a preliminary version appeared in Proc. of GandALF 2018

[19] Goubault, E., Lazic, M., Ledent, J., Rajsbaum:, S.: A dynamic epistemic logic analysis of the equality negation task. DaLí pp. 53–70 (2019)

[20] Goubault, É., Ledent, J., Rajsbaum, S.: A simplicial model for kb4_n: Epistemic logic with agents that may die. In: Berenbrink, P., Monmege, B. (eds.) 39th International Symposium on Theoretical Aspects of Computer Science, STACS 2022, March 15-18, 2022, Marseille, France (Virtual Conference). LIPIcs, vol. 219, pp. 33:1–33:20. Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2022). https://doi.org/10.4230/LIPIcs.STACS.2022.33, https://doi.org/10.4230/LIPIcs.STACS.2022.33

[21] Hatcher, A.: Algebraic topology. Cambridge Univ. Press, Cambridge (2000), https://cds.cern.ch/record/478079

[22] Herlihy, M., Kozlov, D., Rajsbaum, S.: Distributed Computing Through Combinatorial Topology. Elsevier-Morgan Kaufmann (2013). https://doi.org/10.1016/C2011-0-07032-1

[23] Herlihy, M., Shavit, N.: The Art of Multiprocessor Programming. Elsevier (2012)

[24] Laveaga, C.: Álgebra superior: curso completo. Universidad Nacional Autónoma de México (2014), https://books.google.com.mx/books?id=RjjyvQEACAAJ

[25] Lewis, D.: Convention: a philosophical study, by David K. Lewis. Harvard University Press Cambridge (1969)

[26] Matousek, J.: Using the Borsuk-Ulam Theorem: Lectures on Topological Methods in Combinatorics and Geometry. Springer Publishing Company, Incorporated (2007)

[27] Mizrahi, T., Moses, Y.: Continuous consensus with ambiguous failures. Theor. Comput. Sci. **411**(34-36), 3031–3041 (2010). https://doi.org/10.1016/j.tcs.2010.04.025, https://doi.org/10.1016/j.tcs.2010.04.025

[28] Moses, Y.: Knowledge in distributed systems pp. 1051–1055 (2016). https://doi.org/10.1007/978-1-4939-2864-4_606, https://doi.org/10.1007/978-1-4939-2864-4_606

[29] Moses, Y., Rajsbaum, S.: A layered analysis of consensus. SIAM J. Comput. **31**(4), 989–1021 (Apr 2002)

[30] Munkres, J.: Elements of Algebraic Topology. Addison-Wesley Publishing Company, 2 edn. (1984)

[31] Nowak, T., Schmid, U., Winkler, K.: Topological characterization of consensus under general message adversaries. In: Robinson, P., Ellen, F. (eds.) Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing, PODC 2019, Toronto, ON, Canada, July 29 - August 2, 2019. pp. 218–227. ACM (2019). https://doi.org/10.1145/3293611.3331624, https://doi.org/10.1145/3293611.3331624

[32] R. Fagin, J. Halpern, Y.M., Vardi, M.: Reasoning About Knowledge. MIT Press (1995)

[33] Rotman, J.: A First Course in Abstract Algebra. Prentice Hall (1996), https://books.google.com.mx/books?id=rlorAAAAYAAJ

[34] Santoro, N., Widmayer, P.: Time is not a healer. In: Monien, B., Cori, R. (eds.) STACS 89, 6th Annual Symposium on Theoretical Aspects of Computer Science, Paderborn, FRG, February 16-18, 1989, Proceedings. Lecture Notes in Computer Science, vol. 349, pp. 304–313. Springer (1989). https://doi.org/10.1007/BFb0028994, https://doi.org/10.1007/BFb0028994

[35] Schmid, U., Weiss, B., Keidar, I.: Impossibility results and lower bounds for consensus under link failures. SIAM J. Comput. **38**(5), 1912–1951 (2009). https://doi.org/10.1137/S009753970443999X, https://doi.org/10.1137/S009753970443999X

[36] Sipser, M.: Introduction to the Theory of Computation. Course Technology, Boston, MA, third edn. (2013)

[37] van Ditmarsch, H., Goubault, E., Ledent, J., Rajsbaum, S.: Knowledge and simplicial complexes. arXiv e-prints (Feb 2020), https://arxiv.org/abs/2002.08863, to appear in the journal Information and Computation, Elsevier.

[38] Winkler, K., Schmid, U.: An overview of recent results for consensus in directed dynamic networks. Bull. EATCS **128** (2019), http://bulletin.eatcs.org/index.php/beatcs/article/view/581/585

[39] Winkler, K., Schmid, U., Moses, Y.: A characterization of consensus solvability for closed message adversaries. In: Felber, P., Friedman, R., Gilbert, S., Miller, A. (eds.) 23rd International Conference on Principles of Distributed Systems, OPODIS 2019, December 17-19, 2019, Neuchâtel, Switzerland. LIPIcs, vol. 153, pp. 17:1–17:16. Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2019). https://doi.org/10.4230/LIPIcs.OPODIS.2019.17, https://doi.org/10.4230/LIPIcs.OPODIS.2019.17