Universidad Nacional Autónoma de México

facultad de ciencias

Modelos de topología combinatoria para problemas de cartas rusas

T E S I S

que para obtener el título de:

MATEMÁTICO

P R E S E N T A :

Jesús Jorge Armenta Segura

Tutor:
Dr. Sergio Rajsbaum Gorodezky

Ciudad Universitaria, CD. MX. 2020

A mis padres, por todo su apoyo y por haber creído siempre en mí.

A mis hermanos, por coincidir con ellos en este plano.

A mi perrito Winny (2003-2018), quien a su modo habría compartido la alegría de verme dar este paso.

Agradecimientos

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

Al Dr. Sergio Rajsbaum, por ayudarme a percibir con más claridad el enorme campo de la investigación que se encuentra mas allá de la licenciatura.

Al CONACyT, por su invaluable apoyo a este proyecto mediante la beca de ayudante de investigador.

A los asistentes a mi ponencia del LII Congreso Nacional de la Socieda Matemática Mexicana. En particular al dr. Omar Antolín y a Maria Teresa Hoejkstra por sus agudas e ingeniosas observaciones relacionadas con el tema de esta tesis.

Índice general

Resumen.

La presente tesis aborda el problema de las Cartas Rusas, el cual está relacionado con aspectos de criptografía e intercambio de información desde una perspectiva atípica. Se busca proporcionar una manera de verificar sus posibles soluciones, para lo que se construyen modelos de topología combinatoria y se generalizan algunas de las variables involucradas.

Este tipo de modelos son el resultado de 60 años de estudio de problemas y acertijos de intercambio de información (tan antiguos como la humanidad misma), y gracias a los recientes conceptos de *tarea* y *modelos de acción* permiten cumplir el objetivo deseado con gran rigor y formalidad.

Introducción.

El problema de las cartas rusas[1] *presenta a tres agentes Ana, Blas y Cruz que se reparten a,b y c cartas de un mazo con* $a+b+c$ *cartas. Ana y Blas quieren informarse entre ellos las cartas que poseen cada uno pero sin enterar a Cruz en el proceso. Si la única forma posible de comunicación es mediante anuncios públicos indecifrados (es decir, toda la información del anuncio es aprendida por todos, incluído Cruz), ¿cómo podrían lograr esto?.*

Al enfrentarse a este problema por primera vez suelen aparecer las siguientes dos preguntas: ¿realmente existen soluciones posibles?, y de ser así, ¿cómo podrían estudiarse?.

La primer pregunta surge a partir de lo distinto y *transgresor* del enfoque del problema al permitir a terceros todo acceso a la información intercambiada, lo que es contraintuitivo (¿ocultar la información sin ocultarla?) y contrario a lo históricamente usual en criptografía.

La segunda pregunta, por otra parte, es mucho más complicada de discutir ya que conlleva a una gran cantidad de cuestiones adicionales subyacentes. Por ejemplo, es necesario definir qué son las soluciones antes de discutir cómo estudiarlas,[2] lo que a su vez lleva tras de sí muchas otras cuestiones como la necesidad de definir qué es el conocimiento (¿qué significa que *Ana* conoce la mano de *Blas* pero que *Cruz* la ignora?) y qué es la incertidumbre que rodea a cada uno de los agentes (para así poder manipularla en términos de los intereses del problema). Dado que no tiene sentido seguir hablando del problema sin resolver primero estas cuestiones tan primordiales, ¿cuál sería un buen acercamiento para resolverlas?.

Un primer paso es darse cuenta de que el problema de las cartas rusas es en realidad un problema de la forma "ciertos sujetos quieren descubrir algo que desconocen, pero respetando ciertas restricciones", los cuales son problemas muy comunes en la vida diaria y que ya han sido analizados a lo largo de la historia desde múltiples perspectivas, como por ejemplo la lógica epistémica dinámica.

[1] Ver [8] para el enunciado clásico *de las siete cartas*. El problema ha sido estudiado desde sus orígenes en [7] (1847) y fue bautizado como *de las cartas rusas* por el Dr. Hans van Ditmarsch en [16] (2003). Pueden encontrarse soluciones para diversos casos particulares en [3, 5, 7, 8], entre otras fuentes.

[2] En [8] se discute esta cuestión.

En la década de los 60's, el filósofo norteamericano Saúl Kripke abordó desde una perspectiva muy abstracta el conocimiento así como la incertidumbre alrededor de él, dando lugar al nacimiento del lenguaje básico modal (ver **??**) y al posterior surgimiento de las gráficas de Kripke. A partir de ese momento comenzó un largo camino a través de múltiples problemas de computación y conocimiento que finalmente terminó en el surgimiento de una variante que consiguió simplificar la discusión sobre el conocimiento a algo en términos de unas pocas propiedades sobre un espacio topológico finito: los modelos de topología combinatoria.

La historia de estos modelos es curiosa y extraña, pues surgieron a mediados de los 80's motivados por la posibilidad de representar gráficamente a un sistema de múltiples computadoras que ejecutan un programa al mismo tiempo: en esos modelos, las computadoras fueron representadas como puntos en el espacio de n-dimensiones $\mathbb{R}^n$ (con $n \in \mathbb{N}$), se determinó que hubiera una línea entre dos computadoras si estas eran capaces de comunicarse entre sí, un triángulo entre tres computadoras en mismo caso, un tetraedro entre cuatro, etc. Y finalmente alcanzaron una madurez aceptable en el año 2018 en el artículo [6] cuando se definió de manera concreta la relación entre estos modelos y el conocimiento a través de teoría de categorías.

La principal ventaja de utilizar modelos de topología combinatoria sobre otro tipo de modelos formales para el conocimiento colectivo es la gran simpleza de sus términos: una complicada fórmula matemática como "$\mathcal{M}, s \models K_A(\phi)$ syss $\forall t, (t \sim_A s), \mathcal{M}, t \models \phi$" se convierte en una simple, precisa y elegante propiedad de conexidad entre dos simplejos (como se muestra en el capítulo 2). Así, el objetivo de la presente tesis es aprovechar este tipo de ventajas para el problema de las cartas rusas al construirle un modelo de topología combinatoria que va a formalizar el análisis de sus posibles soluciones y responderá a todas las cuestiones planteadas en esta introducción. Para lograr su cometido, la tesis se divide en dos grandes partes que a su vez se estructuran de la siguiente manera:

La primera parte pretende ser una especie de *proto-libro de texto* para introducir al lector a esta rama tan nueva de la topología y la epistemología, por lo que está colmado de ejemplos y prescinde totalmente de la parte técnica computacional (como por ejemplo el uso de la expresión *algoritmo distribuido*) para facilitar su comprensión. Se compone de los siguientes capítulos:

El capítulo 1 es un sumario de la discusión empezada por Saúl Kripke en torno al conocimiento y, mediante ejemplos y discusiones filosóficas, da la respuesta más conveniente sobre lo que es el conocimiento en términos de topología combinatoria. Cabe advertir que esta forma de ver el conocimiento sólo funciona para un tipo especial de casos que, afortunadamente, corresponde al problema de las cartas rusas y, en general, a los problemas de interés en las ciencias de la computación.

El capítulo 2 introduce al lector a los complejos simpliciales abstractos como herramientas para representar la incertidumbre de conocimiento.

El capítulo 3 muestra las pautas generales que deben cumplirse a la hora de manipular esa incertidumbre, y se definen los *modelos de acción* como una forma de representar todas las situaciones finales posibles una vez se ha resuelto el problema (es decir, *qué es una solución* para un problema de conocimiento como el de las cartas rusas).

Por último, en el capítulo 4 se muestra un ejemplo de la construcción de un modelo de topología combinatoria para problemas de este estilo.

La segunda parte consta de los resultados originales de esta investigación y se compone de los siguientes capítulos:

El capítulo 5 plantea la generalización del problema de las cartas rusas en términos de algunas de sus variables.

El capítulo 6 presenta el modelo de topología combinatoria para el problema con las generalizaciones del capítulo anterior.

Finalmente, en el capítulo 7 se establece una dialéctica entre el problema y el modelo para demostrar que este último es una representación legítima del problema en toda su extensión.

Si bien el texto está escrito de una manera *jovial* para acercar al lector a esta rama tan nueva de las matemáticas, se espera que se tengan los siguientes conocimientos previos:

- Lo básico de lógica matemática. No hay necesidad de estar familiarizado con el trabajo de Saúl Kripke ni con lógica modal pero se espera que se tenga conocimiento básico sobre sistemas formales de primer orden, más en particular el sistema con implicación material que describe la lógica clásica y que es el más extendido en toda la comunidad matemática mundial.
- Que se tenga algo de experiencia haciendo demostraciones, al menos la suficiente como para sobrevivir un primer año de licenciatura en la facultad de ciencias de la UNAM.[3]
- Lo básico de álgebra abstracta y matemáticas discretas, como por ejemplo álgebra de conjuntos, conjunto potencia, particiones, números naturales, inducción, recursión, teoría de gráficas, etc.
- Lo fundamental de gramáticas y lenguajes formales. Basta con que se conozca sobre reescritura, concatenación, clausura de Kleene y jerarquía de Chomsky.

En caso de no poseer dichos conocimientos previos, se recomienda consultar el libro [4] para la parte de lógica, el libro [17] para la parte de álgebra y matemáticas discretas

[3]En dicha facultad se pide, entre otras cosas, tener capacidad para probar propiedades elementales de los números reales y hacer construcciones con regla y compás a partir de los postulados de Euclides.

así como el libro [18] para teoría de gráficas (la topología manejada en este trabajo generaliza esta teoría en muchos aspectos), y el apéndice A en esta tesis para la parte de gramáticas formales.

Parte I

Marco teórico para modelos de topología combinatoria

Capítulo 1

Introducción al conocimiento y a su formalización.

En este capítulo se discute sobre el conocimiento y sobre el lenguaje básico modal. Se muestra cómo analizar un problema de incertidumbre definiendo todos los mundos posibles en los que se pueda vivir, a partir de los cuales se define provisionalmente el conocimiento.

A la hora de abordar un problema de la forma "¿cómo podría descubrirse tal cosa siguiendo ciertas restricciones?" es primordial determinar con precisión qué es lo que puede conocerse, antes de discutir sobre cómo conocerlo.

La lógica matemática ha aportado a la discusión la postura filosófica de que sólo se puede conocer lo que puede ser cierto o no.[1] Así, si se parte de ella, es necesario comenzar la descripción del conocimiento a partir de lenguajes formales.

1.1. El lenguaje básico modal.

En la década de los 60's surgió el lenguaje básico modal en el marco de una búsqueda para representar de manera precisa el conocimiento. En dicho lenguaje se retomaron los operadores lógicos tradicionales (conjunción y negación)[2] para formar las proposiciones a conocer, y se le añadió un operador *modal* para expresar el hecho de que un sujeto pudiera conocer alguna de estas proposiciones.

Si bien este lenguaje puede ser construido a la manera usual en la que se construyen los sistemas formales de primer orden, también puede construirse de una manera mucho

[1] Un buen chiste para persuadirse de la legitimidad de esta postura filosófica es ir a una plaza abarrotada de gente y gritar al mundo frases como *¡Escuchadme todos!, ¡yo conozco* ***zapato!*** (no confundir con *"yo conozco al zapato"*) o *¡yo conozco* ***hipopótamo!*** (no confundir con *"yo conozco al hipopótamo"*). El límite es el cielo (o el manicomio).

[2] La disyunción y la implicación material son lógicamente equivalentes a fórmulas compuestas por conjunciones y negaciones gracias a las leyes de De Morgan.

más compacta y práctica a partir de ciertas reglas descritas mediante una gramática en la forma de Backus-Naur[3] aplicadas a un conjunto AP de fórmulas atómicas. A continuación, se presenta dicha gramática correspondiente al lenguaje básico modal:

$$\phi ::= p \mid \neg\phi \mid (\phi \wedge \phi) \mid K_q(\phi)$$

Donde $p \in AP$ es una *metavariable* que indica que las fórmulas atómicas AP son parte del lenguaje, y q es un agente.[4] El símbolo $K_q(\phi)$ es el operador modal de conocimiento y se lee como "persona q conoce la fórmula ϕ".

Sobre el conjunto de fórmulas atómicas AP, estas deben ser predicados de la forma $p_{fulano,sutana}$ que, *grosso modo*, significan que el "agente *fulano* satisface la proposición *sutana*". Esto conlleva a que el paradigma tenga ciertas limitaciones que valen la pena tener en cuenta, como por ejemplo que el símbolo de conocimiento sólo puede expresar fórmulas del tipo $K_q(p_{p,sutana})$ (o compuestas) y no tiene la suficiente capacidad para hablar de conocimientos de otra especie. Así, lejos de ser un modelo para formalizar *todo conocimiento colectivo posible*, esto es más bien un *paradigma formal* para chismes y habladurías en los que *la comadre q* está muy interesada en saber que *la vecina p* satisface la proposición *sutana*.

A continuación se presenta un pequeño ejemplo del lenguaje básico modal, para ilustrar mejor sus alcances y limitaciones:

Ejemplo 1 (El novio loco)
En una noche de inseguridades, Ana intentó hablar por teléfono con su novio Paco pero no le contestó. Preocupada (y enfadada), Ana decidió averiguar qué estaba haciendo el susodicho por lo que, tras una exhaustiva investigación digna de una tesis de doctorado, redujo todas las opciones posibles a tres:

1. *Paco se fue de parranda y le puso los cuernos,* convirtiéndola en toda una antílope.
2. *Paco viajó a Timbuctú para cazar antílopes (Paco es una persona muy rara y con recursos).*
3. *Paco estuvo en su casa escribiendo su tesis de licenciatura*[5] *toda la noche.*

¿Qué podría ayudar a Ana a saber cuál es la correcta? (o al menos a saber que no puede descubrir la respuesta correcta a priori*).*

[3]Para más información sobre la forma Backus-Naur, véase el apéndice A.

[4]El término *agente* se utiliza para referirse a las personas involucradas en un problema de conocimiento. En este trabajo se usa indistintamente junto al término *persona*.

[5]Aunque versa sobre problemas de criptografía y aplicaciones de topología algebráica a la epistemología, no se trata de la presente tesis (se ha procurado evitar las autoreferencias en la medida de lo posible).

Un lenguaje básico modal que podría auxiliar a Ana es el siguiente:

Sean p, s y t símbolos primitivos interpretados como p = "irse de parranda" s = "irse de safari" t = "escribir la tesis". Si Ana y Paco son denotados como los agentes A y F (Francisco) respectivamente entonces las atómicas del lenguaje básico modal son $AP = \{p_{x,y} | x \in \{A, F\}, y \in \{p, s, t\}\}$. Algunas proposiciones este lenguaje básico modal son las siguientes:

- $p_{A,t} \wedge p_{F,t}$. Significa que tanto Ana como Paco estuvieron escribiendo la tesis. Esto contradice el hecho que Ana investigó toda la noche el paradero de su novio,[6] no obstante el lenguaje básico modal se caracteriza por ser demasiado *extenso* en su expresión, admitiendo este tipo de proposiciones inútiles *a priori*. ¿Cómo podría acotarse más para centrarse en el problema?.

- $\neg(p_{F,s} \wedge \neg p_{F,p})$. Significa que si Paco se fue de safari entonces estuvo de parranda, pues la implicación material $\alpha \rightarrow \beta$ equivale a $\neg(\alpha \wedge \neg\beta)$ (nótese cómo el lenguaje básico modal es lo suficientemente rico para expresar esquemas de razonamiento y deducciones como esta).

- $K_F(p_{A,p})$. Significa que Paco sabe que Ana se fue de parranda. Esta proposición describe una situación fuera del enunciado del problema ya que habla sobre las inquietudes de Paco en lugar de las de Ana (sobre las cuales trata el problema).

- $K_A(p_{F,s})$. Significa que Ana sabe que Paco se fue de safari. Esta proposición sí que es útil para los intereses del problema.

Ahora bien, ¿cómo podría *pulirse* este lenguaje básico modal para ayudar a eliminar la incertidumbre de Ana?. En realidad no hay necesidad de pulirlo como tal, sino de utilizarlo para describir dicha la incertidumbre mediante los *mundos posibles* en los que se pueda vivir.

1.2. Mundos posibles y conocimiento.

Dado que toda incertidumbre se encuentra en términos de lo que se desconoce sobre la situación en la que se encuentra uno, es posible representarla mediante todos los mundos posibles en los que se pudiera vivir, dado lo que se sabe. Así, en el ejemplo 1 del novio loco, Ana sabe que vive en uno de los siguientes tres mundos:

1. El mundo en el que Paco se fue de parranda y le puso los cuernos.

2. El mundo en el que Paco se fue de safari a Timbuctú.

[6] Nótese que ni siquiera está considerado en AP la opción de "investigar a la pareja". Es un buen ejercicio filosófico discutir por qué esto no afecta a los intereses de Ana ni representa una *anomalía en el paradigma*.

3. El mundo en el que pasó la noche escribiendo la tesis.

Dichos mundos pueden ser descritos fácilmente por las fórmulas del lenguaje básico modal $p_{F,p}$, $p_{F,s}$ y $p_{F,t}$ respectivamente. Así, eliminar la incertidumbre equivale a encontrar una manera en la que Ana descubra en cuál de esos tres mundos posibles vive, lo que equivale a demostrar cualesquiera de las fórmulas $K_A(p_{F,p})$, $K_A(p_{F,s})$ o $K_A(p_{F,t})$ a partir de lo dado en el problema.

Lo que sigue ahora es definir qué significa que Ana conozca algo en un mundo dado para poder demostrar alguna de esas fórmulas. De manera inmediata, dado que ella es incapaz de distinguir que vive en alguno de esos tres mundos, no tiene manera de *conocer* lo que los hace distintos, por lo que cabe suponer que conoce todo lo que tienen en común, lo que motiva a la siguiente definición provisional:[7]

Definición 1.2.1 (Definición provisional de conocimiento)
Sea S un conjunto de mundos y sea $\mathbf{A}$ el conjunto de personas o agentes que habitan cada uno de esos mundos. Sea $\mathcal{L}_K$ el lenguaje básico modal con fórmulas que describen lo que es cierto en cada $s \in S$. Un agente $p \in \mathbf{A}$ conoce una fórmula $\phi \in \mathcal{L}_K$ en el mundo $s \in S$ si dicha fórmula es cierta en todos los mundos entre los que es incapaz de distinguir, dado que vive en s.

Esta definición es la contrapositiva del siguiente argumento de sentido común: si dados todos los mundos indistinguibles para la persona A se tiene una fórmula ϕ que es cierta en algunos mundos y no lo es en algunos otros, entonces dicha fórmula marca una diferencia entre todos esos mundos. Así, si A la conociera entonces podría distinguir entre los mundos donde es cierta y los que no, al conocer algo que los hace diferentes.

Es una definición provisional porque apela mucho a la intuición, pues todavía no se ha definido con precisión qué es la *indistinguibilidad* (Ana sabe que podría vivir en tres mundos distintos bien diferenciados entre sí, ¿cómo exáctamente es que no puede distinguir entre ellos si ya los conoce?) o que una fórmula *sea cierta* en un mundo $s \in S$. Así, un siguiente y natural paso es definir con precisión todas estas cuestiones, no obstante para ello es necesario motivar un puñado más de cosas que darán lugar al abordaje topológico del problema. Antes de eso, sin embargo, se presenta un último ejemplo basado en el bien conocido acertijo de Einstein para ilustrar la definición provisional de conocimiento:

Ejemplo 2 (Un pequeño acertijo tipo el de Einstein.)
Un viajero llega a una pequeña aldea perdida en Zacatecas donde viven un yucateco, un

[7]Cabe recalcar que es posible desconocer cosas que dos mundos tengan en común. Por tanto, esta definición sólo debe usarse cuando los agentes conocen todo lo que tienen en común los mundos indistinguibles para ellos. Por fortuna, como ya se mencionó en la introducción, este casi siempre será el caso para problemas de computación.

chilango y un regio en santa paz y armonía.[8] *Cada uno de ellos vive en una casa de un color distinto y tienen una mascota diferente. Tras hablar con ellos un rato, el viajero descubre lo siguiente sobre cada uno:*

- *El yucateco vive en la casa amarilla.*
- *El teporingo no es del regio.*
- *El cotorro no es del chilango.*
- *La vaca no es del yucateco.*
- *El teporingo no vive en la casa amarilla.*
- *El cotorro no vive en la casa azul.*

¿cómo podría el viajero descubrir quién es el dueño de la vaca, y quién vive en la casa roja?.[9]

Para resolver este problema vale la pena construir todos los mundos posibles a partir de la casa en la que puedan vivir los habitantes y las mascotas que pudieran tener, para posteriormente descartar los mundos que no satisfacen las hipótesis. Este proceso va a arrojar todos los mundos en los que el viajero pudiera vivir dada la información recabada. Para representar los mundos, pueden usarse las siguientes tablas:

Aldeano	Mascota	Casa
Chilango	su mascota	color de su casa
Regio	su mascota	color de su casa
Yucateco	su mascota	color de su casa

Y finalmente se "esculpen" todos los mundos que satisfacen las hipótesis con el siguiente esquema de razonamiento: en primer lugar, dado que el yucateco vive en la casa amarilla, todos estos mundos deben ser de la forma:

Aldeano	Mascota	Casa
Chilango	su mascota	color de su casa
Regio	su mascota	color de su casa
Yucateco	su mascota	**amarilla**

[8] Jaja.

[9] El acertijo original de Einstein consiste en cinco personas con cinco nacionalidades que viven en cinco casas, tienen cinco mascotas, beben cinco diferentes tipos de bebidas y fuman cinco diferentes tipos de cigarros. Es muy popular en la actualidad porque se publicita en internet como "el acertijo que sólo el 2 % de la población mundial puede resolver".

Posteriormente se tiene que el teporingo no vive en la casa amarilla, por lo que no es del yucateco al igual que la vaca. Así, la única mascota posible para el yucateco es el cotorro por lo que los mundos indistinguibles para el viajero quedan de la forma:

Aldeano	Mascota	Casa
Chilango	su mascota	color de su casa
Regio	su mascota	color de su casa
Yucateco	**cotorro**	**amarilla**

Y dado que el teporingo no es del regio y el cotorro ya está tomado, no queda otra alternativa mas que el regio tenga a la vaca (y el chilango al teporingo):

Aldeano	Mascota	Casa
Chilango	**teporingo**	color de su casa
Regio	**vaca**	color de su casa
Yucateco	**cotorro**	**amarilla**

Esto permite resolver la primera parte del entuerto ya que, en todo mundo indistinguible para el viajero, es cierto que el regio tiene a la vaca por lo que por la definición provisional de conocimiento, el viajero conoce que el regio tiene a la vaca (y para lograr deducirlo utiliza el esquema de razonamiento previamente planteado).

Hasta ahora se han reducido todos los mundos posibles en los que pueda vivir el viajero a los siguientes dos:

Aldeano	Mascota	Casa
Chilango	**teporingo**	azul
Regio	**vaca**	roja
Yucateco	**cotorro**	**amarilla**

Aldeano	Mascota	Casa
Chilango	**teporingo**	roja
Regio	**vaca**	azul
Yucateco	**cotorro**	**amarilla**

¿Sería posible reducirlos a uno sólo para determinar quién vive en la casa roja?.

Nótese que todas las hipótesis del problema se cumplen en ambos mundos a la vez: el yucateco vive en la casa amarilla, el teporingo no es del regio ya que es del chilango, el cotorro no es del chilango ya que es del yucateco, la vaca no es del yucateco ya que es del regio, el teporingo no vive en la casa amarilla ya que no es del yucateco y él vive en la casa amarilla, y finalmente el cotorro no vive en la casa azul ya que vive en la casa amarilla.

Como consecuencia de lo anterior, es imposible seguir reduciendo la cantidad de mundos a partir de las hipótesis dadas, por lo que el viajero no puede saber quién vive en la casa roja ya que en un mundo indistinguible para él vive ahí el chilango, y en el otro vive el regio. En próximos capítulos se estudiarán pautas sobre cómo reducir más los mundos mediante información adicional añadida.

1.3. Notas finales

En [12] se pueden encontrar las primeras formalizaciones (hasta donde mejor se sabe) sobre el concepto de indistinguibilidad (mediante *marcos y modelos de Kripke*) y el lenguaje básico modal.

La principal referencia para la elaboración de este capítulo fue el artículo [6]. La definición provisional de conocimiento no es mas que una interpretación intuitiva de la siguiente expresión matemática:

$$\mathcal{M}, s \models K_A(\phi) \text{ si y solo si } \forall t, (t \sim_A s),\ \mathcal{M}, t \models \phi$$

Donde $\mathcal{M}$ es un modelo de Kripke, s y t son mundos, A es una persona, $t \sim_A s$ significa que A no puede distinguir entre los mundos s y t, y $\mathcal{M}, s \models K_A(\phi)$ significa que, en un mundo s, es cierta la fórmula $K_A(\phi)$ (o dicho de manera correcta: "modela la fórmula $K_A(\phi)$").

Capítulo 2

Modelos simpliciales para problemas de conocimiento

En este capítulo se muestra una forma de representar los mundos posibles de un problema de conocimiento utilizando topología combinatoria. También se relaciona con el lenguaje básico modal mediante el operador de satisfacción.

Dados los mundos de un problema de incertidumbre, es posible caracterizarlos como todo lo que conocen los agentes sobre ellos, auxiliándose del lenguaje básico modal. Así, pueden definirse pares ordenados $(p, p(s))$ donde p es un agente y $p(s)$ lo que conoce de dicho mundo s puesto en términos de un lenguaje básico modal. De esta manera es posible representar los mundos como conjuntos $\{(p_1, p_1(s)), \ldots, (p_n, p_n(s))\}$ donde $p_1, \ldots, p_n$ son todas las personas involucradas.

Recordando que, por la definición provisional de conocimiento, dos mundos son indistinguibles para una persona si esta conoce lo mismo de ambos, resulta que esos dos mundos compartirán el vértice asociado a la persona incapaz de distinguir entre ellos. Dado que es posible visualizar estos conjuntos como puntos en el espacio, y a cada mundo como una *especie de poliedros* que envuelve firmemente a todos esos puntos, la indistinguibilidad es equivalente a que dos de estos *semi polígonos* compartan uno de sus vértices, convirtiendo así al conocimiento en una propiedad geométrica de conexidad entre estos cuerpos.

Por último, estas *envolventes de puntos* corresponden a un bien conocido espacio topológico denominado *complejo simplicial*. A continuación se da una introducción a su estudio.

2.1. Complejos simpliciales.

Una buena forma de motivar la definición del complejo simplicial es presentarlo como una generalización de la noción de gráfica en el siguiente sentido: mientras las gráficas constan de aristas que conectan vértices, los complejos simpliciales tienen la posibili-

dad de conectar vértices con planos, volúmenes, hiper-volúmenes, etc. En esta sección son definidos y estudiados para finalmente ser aterrizados en el tema central de esta tesis.

Definición 2.1.1 (Complejo simplicial abstracto)
Un complejo simplicial C sobre un conjunto finito V de vértices *es un $C \subseteq \mathscr{P}(V)$ que satisface lo siguiente:*

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

Generalmente el conjunto V se denota como $V(C)$ para enfatizar que se trata del conjunto de vértices de C.

Los elementos de un complejo simplicial se llaman *simplejos* y deben ser entendidos como la generalización de aristas de una gráfica. Visualmente corresponden a un arreglo de puntos en el espacio tales que están conectados dos a dos por segmentos de rectas (aristas), tres a tres por segmentos de planos, cuatro a cuatro por segmentos de espacios, etc. Así, un simplejo con tres vértices $\{a, b, c\}$ corresponde visualmente a un triángulo (pero nunca a tres puntos colineales), uno con cuatro vértices $\{a, b, c, d\}$ corresponde a un tetraedro (pero nunca a un cuadrado en el plano), etc. Para ver ejemplos consúltese la figura 2.1

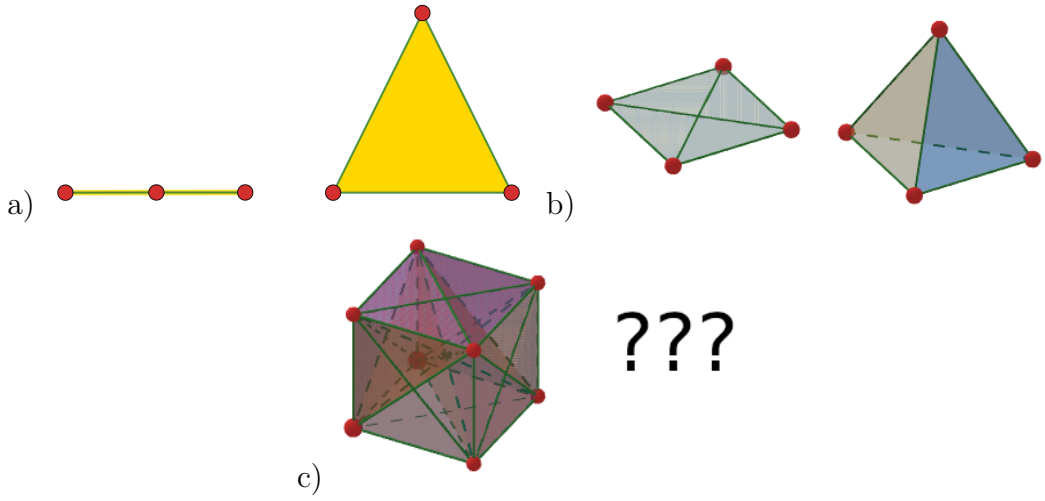

Figura 2.1: Todo simplejo corresponde a un arreglo de puntos en el espacio que son *geométricamente independientes*. Por ejemplo: (a) tres puntos colineales no representan a un simplejo mientras que un triángulo sí lo hace. b) Un cuadrado con sus diagonales no representa un simplejo mientras que un tetraedro sí. c) Este maravilloso poliedro de ocho vértices no representa a un simplejo, ¿pero cómo se vería el cuerpo geométrico correspondiente a un simplejo de ocho vértices?.

Dado un simplejo, todos sus sub-simplejos se denominan *caras* en alusión a dicha noción geométrica (el tetraedro de la figura 2.1 tiene triángulos como caras, que son simplejos con tres vértices). También es posible clasificarlos por su dimensión en el mismo sentido geométrico con el que se clasifica al espacio físico.

Definición 2.1.2 (Dimensiones)
Dado un complejo simplicial C sobre un conjunto finito V, un simplejo $s \in C$ tiene dimensión d si y solo si $|s| - 1 = d$. En ese caso s es un d-simplejo de C. Por último C tiene dimensión d si y solo si $d = Max\{|s| - 1 | s \in C\}$.

Así, tiene todo el sentido que un triángulo represente un simplejo de dimensión 2 (lo que corresponde al hecho de que son tres puntos unidos por un plano) y que un tetraedro represente un simplejo de dimensión 3 (acorde al hecho de que representa cuatro puntos unidos por un volumen).

Definición 2.1.3 (Facetas)
Un simplejo $s \in C$ es una faceta si para todo simplejo distinto $\sigma \in C$, es imposible que suceda que $s \subseteq \sigma$, es decir, es $\subseteq$-maximal en el conjunto de simplejos.
El conjunto de todas las facetas se denota como $F(C)$.

Este último concepto es de capital importancia para la presente tesis ya que los mundos posibles de un problema de conocimiento corresponden a las facetas del complejo simplicial asociado a dicho problema.

Definición 2.1.4 (Pureza)
Un complejo simplicial es puro si todas sus facetas tienen la misma dimensión.

Con todo esto ya definido, es posible hablar sobre complejos simpliciales para problemas de conocimiento. A continuación se presentan un par de ejemplos, el primero para ilustrar el procedimiento *per se* de construcción de modelos simpliciales, y el segundo para ilustrar cómo la indistinguibilidad se convierte en incidencia de facetas:

Ejemplo 3 (Adivina quien soy)
Dos amigos juegan al adivina quien soy *poniéndose en la frente cualesquiera de los siguientes personajes: Juan Gabriel, Pedro Infante y José José. ¿Cuáles son todas las posibilidades en las que puedan caer?*

Un lenguaje básico modal útil para la tarea es el generado por las atómicas $AP = \{p_{q,x} | q \in \{A, B\}, x \in \{Gabriel, Pedro, José\}\}$ que corresponden a $p_{i,Cantante}$ = "el amigo i es *tal cantante*". Así, un mundo donde el amigo A es Juan Gabriel y el amigo B es Pedro Infante puede representarse como la siguiente faceta:

$$X = \{(A, K_1(p_{2,pedro})), (B, K_2(p_{1,gabriel}))\}$$

En este caso particular el complejo simplicial es una gráfica ya que las facetas son de dimensión 1 (y por tanto corresponden a puntos unidos por rectas).

Dado un vértice $(Q, K_Q(p_{R,personaje}))$, el amigo Q puede ser cualquier personaje del conjunto $\{Gabriel, Pedro, José\} - \{personaje\}$ por lo que tiene grado 2 al ser adyacente a los vértices donde R sabe que él es cualesquiera de los dos elementos del conjunto previamente dado. Más aún, es una gráfica bipartita ya que cada amigo solo es adyacente a vértices del otro amigo. En la figura 2.2 se muestra el complejo simplicial asociado al problema, donde cada vértice incide en dos facetas correspondientes a los mundos que son incapaces de distinguir.

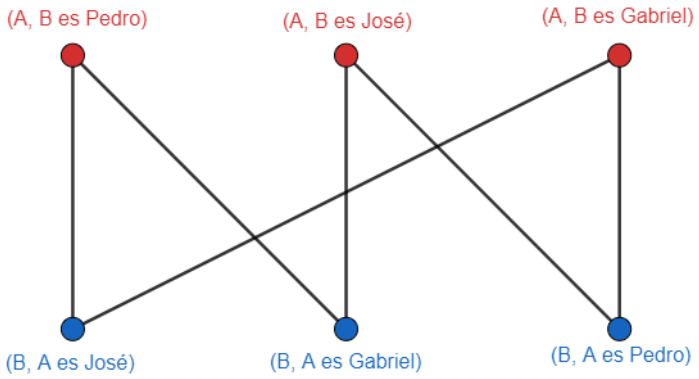

Figura 2.2: Si A vive en el mundo donde sabe que B es pedro, no puede vivir en el mundo donde B sabe que A es pedro, pero sí en todos los demás. En la gráfica los vértices del amigo A se colorean de rojo y los del amigo B de azul. Para simplificar en notación, en lugar de poner $K_R(p_{Q,personaje})$ se pone simplemente que "Q es *personaje*", sobreentendiéndose que R lo sabe.

Un muy buen ejercicio es pensar sobre cómo se vería el complejo simplicial si en lugar de dos amigos fueran tres. En este caso habría que tener en cuenta el incremento de información conocida *a priori* ya que cada amigo, a parte de conocer al personaje del segundo, también conocerá al del tercer amigo. En general, si los amigos se denotan como A, B, C entonces un posible vértice *abstracto* es $(A, K_A(p_{B,personaje} \wedge p_{C,cantante})$. Las facetas de este caso son de dimensión 2 y corresponden a triángulos en el espacio aislados entre sí como se muestra en la figura 2.3.

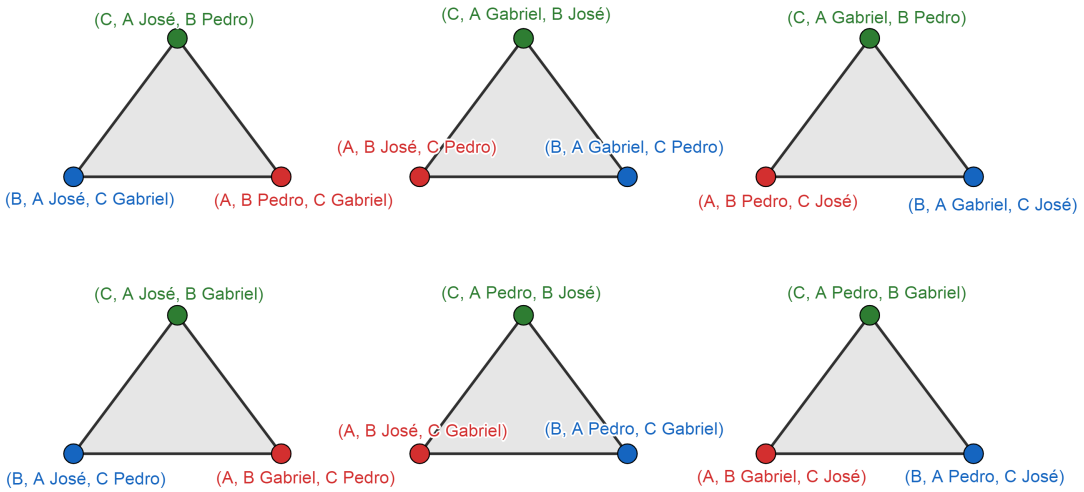

Figura 2.3: Con la llegada de un tercer amigo, las facetas del juego *adivina quien soy* se convierten en triángulos ajenos entre sí. Cada amigo puede deducir su propio personaje viendo a los de sus compañeros y concluyendo el suyo por descarte, lo que queda reflejado en el complejo simplicial con el hecho de que las facetas son disconexas entre sí. Es importante recordar que la definición provisional de conocimiento está en términos de si dos mundos (facetas) comparten vértices o no.

A continuación se presenta el segundo ejemplo, en el cual se muestra con mayor énfasis cómo la indistinguibilidad se traduce en incidencia de facetas:

Ejemplo 4 (Ladrones de memes)
En un mundo postapocalíptico donde el internet ha muerto, los últimos memes que quedan sobre la faz de la tierra son pequeñas hojitas de papel bond impresas (en blanco y negro), muy vulnerables a las inundaciones y a las llamas (lo que los hace todavía más valiosos).
Un grupo de tres amigos: Armanda, Belindo y Calixta, tienen en su poder un gran tesoro de memes para su deleite personal que, un mal día, desaparece misteriosamente.
Dado que no hay animales salvajes cercanos ni humanos adicionales, el ladron (o ladrones) está(n) entre los tres. ¿Cómo podrían encontrar al culpable?.

Para describir los mundos posibles basta notar que tan sólo hay dos tipos de conocimientos posibles en un inicio: el no saber nada sobre la identidad del ladrón, o el saber la identidad del ladrón o ladrones porque se está dentro de la conspiración (por simplicidad no se toman en cuenta los casos en los que alguien sabe del robo pero no toma parte). Así, los diversos pares ordenados asociados a los mundos posibles son:

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

Donde A, B, C representan a los tres amigos, el valor vacío representa que no saben nada sobre la identidad del ladrón y el valor k se compone de todos los involucrados en el robo, incluyendo al propio q, pero sin ser el total (¿qué punto habría en robar los memes si todos lo saben?).

Lo que procede ahora es construir las facetas del complejo simplicial. Por ejemplo considérese el mundo en el que Armanda es la única ladrona, entonces los vértices asociados a dicho mundo son:

$$(A, \{A\}), (B, \emptyset)(C, \emptyset)$$

Lo que determina un triángulo cuyos vértices representan los conocimientos descritos.

Ahora bien, en esta faceta Belindo ignora la identidad del ladrón, ¿pero es la única donde pasa esto?, Si Calixta fuera la ladrona entonces Belindo tampoco lo sabría (ni Armanda), y la faceta asociada es:

$$(A, \emptyset), (B, \emptyset), (C, \{C\})$$

Más aún, si Armanda y Calixta estan coludidas, Belindo tampoco tendría manera de saberlo en un inicio y la faceta correspondiente es:

$$(A, \{A, C\}), (B, \emptyset)(C, \{A, C\})$$

Por lo que el Belindo ignorante de la identidad del criminal vive en estas tres facetas a la vez, las cuales pueden verse como triángulos en el espacio que inciden en dicho vértice (véase figura 2.4).

Ahora bien, ¿cómo Belindo podría descubrir a las ladronas?. Lo *inmediato* es que empiece a interrogarlas con la finalidad de obtener información adicional que le permita descartar mundos y quedarse con uno solo, no obstante ¿cómo podría describirse esta evolución del conocimiento en términos de complejos simpliciales?. Esa pregunta será respondida en el siguiente capítulo, pero para ello antes es necesario estudiar cómo puede expresarse *la verdad* en términos de complejos simpliciales.

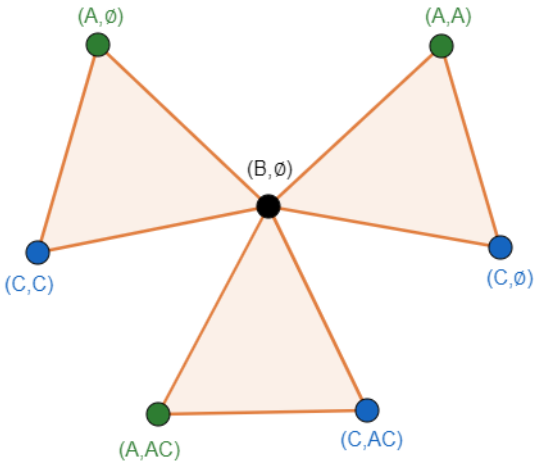

Figura 2.4: La incapacidad de Belindo de saber cuál de las tres posibilidades es la correcta. Por estándar computacional los conjuntos $\{A, C\}$ se suelen denotar como palabras AC.

2.2. Proposiciones verdaderas en complejos simpliciales.

En el ejemplo 3 de *Adivina quien soy* se vio que, para el caso con dos amigos y tres personajes, cada amigo es incapaz de distinguir entre dos mundos distintos. Por otra parte, en el caso con tres amigos y tres personajes cada uno sí que era capaz de distinguir entre todos los mundos, lo que les permitía deducir cuál era su personaje a partir de sus conocimientos iniciales.

En ese ejemplo, el complejo simplicial únicamente modela el hecho de que no existe indistinguibilidad para ningún amigo en ningún mundo, pero no explica directamente por qué y cómo cada amigo podría descubrir eso (el razonamiento dado en la figura 2.3 está fuera del modelo). Para resanar esa *anomalía en el pardigma* vale la pena encontrar una manera de representar estos *procesos de pensamiento* en términos del complejo simplicial.

Antes de entrar en materia es necesario dar un par de conceptos previos:

Definición 2.2.1 (Etiquetado)
Sea C un complejo simplicial y sea Q un conjunto contable. Un etiquetado es una función f que asigna a cada vértice de $V(C)$ una etiqueta *en el conjunto Q.*

La idea de un etiquetado es asignar a cada vértice algún valor que ilustre lo que significa. En problemas de conocimiento ya se ha dado un etiquetado implícito mediante el representar lo que la persona conoce de un mundo en la segunda coordenada del par ordenado.

Por otra parte, el nombre de la persona colocado en la primera coordenada del vértice también puede verse como una etiqueta, no obstante esta satisface la propiedad de que,

en cada faceta, no puede haber dos vértices asociados a la misma persona ya que basta con uno solo para representar todo su conocimiento sobre el mundo. Este tipo de etiquetados se denominan *cromáticos* ya que en gráficas corresponden a las bien conocidas coloraciones.

Definición 2.2.2 (Coloración)
Sea C un complejo simplicial sobre un conjunto finito V y sea K otro conjunto finito. $\chi : V(C) \to K$ es una K-coloración si es inyectivo al restringirlo en cualquier faceta.[1] *Si un complejo simplicial C tiene asociada una coloración χ, la estructura $< C, \chi >$ se denomina complejo simplicial K-cromático.*

Esto también permite saber sin pasos intermedios que, cuando el problema involucra únicamente a dos personas, el complejo simplicial será una gráfica bipartita ya que tiene una 2-coloración.

Ahora bien, en ciertos problemas de conocimiento se espera que el conocimiento de las personas involucradas equivalga a lo que las describa en todos los mundos entre los que no pueden distinguir: se espera que el hecho de conocer algo esté íntimamente relacionado con sus propias situaciones.[2] A partir de dicho estatuto filosófico es que se definen los modelos simpliciales, los cuales constan de un complejo cromático al que se le añade una valuación en términos de un lenguaje básico modal que asigna a cada vértice lo que es cierto sobre la persona de su color.

Definición 2.2.3 (Modelo simplicial)
Sea $\mathcal{L}_K$ un lenguaje básico modal generado por las atómicas AP, en términos del conjunto de personas $\boldsymbol{A}$. Un modelo simplicial $\mathcal{C} =< C, \chi, l >$ es un complejo simplicial $\boldsymbol{A}$-cromático y puro $< C, \chi >$ denominado subyacente, asociado a un etiquetado $l : V(C) \to \mathscr{P}(AP)$ tal que para todo $u \in V(C)$, $p_{i,j} \in l(u)$ si y solo si $i = \chi(u)$ se compone únicamente de proposiciones que describen a la persona asociada a u en dicho mundo.

Es posible empezar el diseño de un modelo simplicial a partir de estas valuaciones en lugar de los conocimientos de los agentes como se he hecho hasta ahora siempre que el problema satisfaga el estatuto filosófico de que el conocimiento está en correlación con la propia naturaleza.

Dado que la valuación determina lo que es cierto *a priori* sobre un agente en términos del lenguaje básico modal, es necesario encontrar una manera de poder deducir las proposiciones que se escinden de ello. Aprovechando la definición del lenguaje básico modal

[1] Es muy fácil probar que esta definición de coloración equivale a la habitual de decir que χ es inyectivo al restringirlo a cualquier simplejo, y se le deja al lector.

[2] Por supuesto podrían haber problemas que no satisfagan esto, pero por fortuna no será el caso de las cartas rusas.

en la forma de Backus-Naur, puede definirse un operador que determine en esos términos la verdad de una proposición dada su especie. Así, se define lo siguiente:

Definición 2.2.4 (Estado epistémico)
Sea $\mathcal{C} =< C, \chi, l >$ un modelo simplicial. Los estados epistémicos se definen como los elementos del conjunto $Eps = \{\mathcal{C}\} \times F(C)$ (recordamos que $F(C)$ son las facetas del complejo simplicial C) y, para $(\mathcal{C}, X) \in Eps$, se denota como $(\mathcal{C}, X) = \mathcal{C}, X$.

Estos estados epistémicos son un preámbulo relativamente indefinido que se utilizan para dar pie a decir que $\mathcal{C}, X =$"La faceta X, considerada en el modelo simplicial $\mathcal{C}$, cumple/satisface tales proposiciones...".

Definición 2.2.5 (Operador de satisfacción)
Sea $\mathcal{C} =< C, \chi, l >$ un modelo simplicial. Se define la verdad de una fórmula $\phi \in \mathcal{L}_K$ en un estado epistémico $\mathcal{C}, X$ como el siguiente operador $\models \subseteq Eps \times \mathcal{L}_K$ definido de la siguiente manera:

$$\begin{array}{lll} \mathcal{C}, X \models p & syss & p \in l[X] \\ \mathcal{C}, X \models \neg\phi & syss & \mathcal{C}, X \not\models \phi \\ \mathcal{C}, X \models (\phi \wedge \psi) & syss & \mathcal{C}, X \models \phi \wedge \mathcal{C}, X \models \psi \\ \mathcal{C}, X \models K_q(\phi) & syss & \forall Y \in F(C), q \in \chi(X \cap Y) \Rightarrow \mathcal{C}, Y \models \phi \end{array}$$

Donde $\chi(X \cap Y) = \{\chi(v) | v \in X \cap Y\}$ es el conjunto de todos los colores de los vértices en común entre ambas facetas, y $\mathcal{C}, X \models p$ significa que $((\mathcal{C}, X), p) \in \models$.

Nótese que el operador está definido para cada una de las posibles reescrituras de la gramática básica modal. Más aún, finalmente el conocimiento se define formalmente ya que una persona conoce la fórmula ϕ en el mundo X si es verdadera en todo mundo Y indistinguible para la persona (representado con la petición de que $q \in \chi(X \cap Y)$). Además si existe correlación entre lo que uno es y lo que se conoce (es decir, que en todos los mundos indistinguibles uno es la misma cosa) entonces este operador prueba que ambos modelos simpliciales (el construido a partir de la valuación y el construido a partir de los conocimientos) son idénticos. Por ejemplo, en el juego de *adivina quien soy* con tres agentes y tres personajes, el mundo X donde A es Pedro infante, B es José José y C es Juan Gabriel satisface lo siguiente:

$$\mathcal{C}, X \models p_{A,Pedro} \wedge p_{C,Gabriel}$$

Y dado que todos los mundos son aislados entre sí ($X \cap Y = \emptyset$ para todo Y),

$$\mathcal{C}, X \models K_B(p_{A,Pedro} \wedge p_{C,Gabriel})$$

Por la definición de conocimiento y por vacuidad. Lo que corresponde a la segunda coordenada del vértice definido en la sección anterior (es análogo con todos los demás agentes). Recíprocamente, se tiene que estas segundas coordenadas modelan los elementos de $l[X] = \{p_{A,Pedro}, p_{B,Gabriel}, p_{C,José}\}$ ya que:

$$\begin{aligned} \mathcal{C}, X \models & \quad K_A(p_{B,Gabriel} \wedge p_{C,José}) \wedge K_B(p_{A,Pedro} \wedge p_{C,José}) \\ \models & \quad p_{B,Gabriel} \wedge p_{C,José} \wedge p_{A,Pedro} \end{aligned}$$

Puesto que $A, B \in \chi(X \cap X)$.

El caso con dos amigos es más interesante pero también satisface el estatuto filosófico: por ejemplo en una arista X donde A es (sin pérdida de generalidad) Pedro, y B es José José, se tiene lo siguiente:

$$\begin{aligned} \mathcal{C}, X \models & \quad K_A(p_{B,José}) \\ \models & \quad p_{B,José} \end{aligned}$$

Ya que $p_{B,José}$ se cumple en todos los mundos entre los que A no puede distinguir. Además se tiene que:

$$\begin{aligned} \mathcal{C}, X \models & \quad K_B(p_{A,Pedro}) \\ \models & \quad p_{A,Pedro} \end{aligned}$$

Por lo que cada mundo puede ser caracterizado mediante la valuación $l[X] = \{p_{A,Personaje}, p_{B,Cantante}\}$ sin muchos problemas.

2.3. Notas finales

Los modelos simpliciales han sido discutidos a lo largo del siglo XXI con diversos nombres y enfoques, no obstante -y como ya se comentó en la introducción- alcanzaron su madurez en el año 2018 en el artículo [6] aunque no están tan orientados al conocimiento como aquí se describen.

Las principales referencias de este capítulo son [10, 11], de las que se extrajeron las definiciones básicas sobre complejos simpliciales abstractos.

Capítulo 3

Evolución del conocimiento

A lo largo de este trabajo se han mostrado varios ejemplos en los que no se puede encontrar una solución a partir de la información de las hipótesis como en el ejemplo 2 del *acertijo tipo Einstein* o en el ejemplo 4 de los *ladrones de memes*. Ambos tienen en común que los protagonistas son incapaces de distinguir entre varios mundos posibles. Así, para poder encontrar una solución es necesario encontrar formas de aumentar su conocimiento inicial rumbo a una situación que les permita alcanzar sus objetivos. En el presente capítulo se presenta cómo es la evolución del conocimiento en modelos simpliciales.

3.1. Modelos de acción.

En el ejemplo 4 de *ladrones de memes*, Belindo puede empezar a interrogar a sus compañeras para obtener más información. Supóngase que recibe las siguientes respuestas si preguntara a ambas la identidad de la ladrona:

- Armanda asegura que Calixta es la ladrona.
- Calixta asegura que ambas lo son.

Un lenguaje básico modal que puede ayudar a Belindo es el conformado por las atómicas $AP = \{p_{q,i} | q \in \{A, B, C\}, i \in \{0, 1\}\}$ el cual asigna a la persona q el 1 si es ladrón y el 0 si no lo es. Así, la faceta correspondiente a que Armanda es la ladrona es:

$$\{(A, K_A(p_{A,1})), (B, K_B(p_{B,0})), (C, K_B(p_{C,0}))\}$$

Y el mundo donde sólo Belindo quedó fuera de la conspiración es:

$$\{(A, K_A(p_{A,1} \wedge p_{C,1})), (B, K_B(p_{B,0})), (C, K_B(p_{C,1} \wedge p_{A,1}))\}$$

De esta forma las respuestas de ambas se convierten en las siguientes proposiciones acorde a cada uno de los escenarios posibles: si Armanda miente y Calixta dice la verdad

entonces sería cierto que $\neg p_{C,1} \wedge p_{A,1} \wedge p_{C,1} = (\neg p_{C,1} \wedge p_{C,1}) \wedge p_{A,1}$; si es el caso recíproco entonces sería $p_{C,1} \wedge (\neg p_{A,1} \vee \neg p_{C,1})$; si ambas mienten entonces sería $\neg p_{C,1} \wedge (\neg p_{A,1} \vee \neg p_{C,1})$; y finalmente si ambas dicen la verdad sería $p_{C,1} \wedge p_{A,1} \wedge p_{C,1} = p_{C,1} \wedge p_{A,1}$.

En el caso en el que Armanda miente y Calixta dice la verdad hay una contradicción $(\neg p_{C,1} \wedge p_{C,1})$, por lo que no puede suceder. Descartando este, ¿cómo podría expresarse con precisión la evolución del conocimiento de Belindo tras el interrogatorio?. Un modelo de acción es un complejo simplicial que representa todos los conocimientos posibles al final de la evolución.

Definición 3.1.1 (Modelos simpliciales de acción)
Un modelo simplicial de acción $\mathcal{A} =< T, \sim, pre >$ *consiste en un complejo simplicial cromático puro* $< T, \sim >$ *y en una función* $pre : V(T) \to \mathcal{L}_K$ *que asigna a cada vértice una precondición representada con una fórmula en* $\mathcal{L}_K$*. Las precondiciones se extienden a simplejos de la siguiente manera:* $pre : T \to \mathcal{L}_K$ *es tal que* $pre(s) = \bigwedge_{u \in s} pre(u)$*.*

Estos modelos de acción funcionan *casi* igual que los modelos simpliciales para problemas de conocimiento presentados en el capítulo anterior: las facetas de un modelo de acción también representan mundos posibles en los que se pueda caer, y dos facetas comparten un vértice si la persona que colorea a dicho vértice es incapaz de distinguir entre ambos mundos. La diferencia radica en la interpretación: los modelos de acción deben ir acompañados por los conocimientos finales adquiridos tras una evolución del conocimiento, y en lugar de una valuación que defina qué es cierto sobre cada agente en cada mundo, va acompañado por unas precondiciones que definen qué conocimiento inicial conlleva a qué conocimiento final.

En el ejemplo del interrogatorio de Belindo, los únicos casos en donde las respuestas no generan paradojas implican los siguientes aumentos en el conocimiento, ya descartado el caso paradójico:[1]

- Si Calixta miente y Armanda dice la verdad, entonces es cierto que $p_{C,1}$ y $\neg p_{A,1} \vee \neg p_{C,1}$ por lo que Calixta es la ladrona y Armanda no lo es.
- Si ambas mienten entonces $\neg p_{C,1}$ y $\neg p_{A,1} \vee \neg p_{C,1}$ por lo que Calixta es la ladrona, pero Armanda también podría serlo.
- Si ambas dicen la verdad entonces $p_{C,1}$ y $p_{A,1} \wedge p_{C,1}$ por lo que ambas son las ladronas.

De manera que el conocimiento de Belindo evoluciona a que descubre que Calixta es la ladrona, aunque permanece en la incertidumbre sobre si Armanda estaba coludida o no. Esto último puede representarse con un vértice $(B, K_B(p_{B,0} \wedge p_{C,1}))$ en el modelo de

[1] Este tipo de esquemas de razonamiento podrían recordar al empleo que daba Hércules Poirot a sus *células grises* para resolver los más difíciles casos.

acción, el cuál deberá tener por precondición el hecho $p_{B,0}$ de que Belindo es inocente. Más aún, el vértice en el modelo de acción vive en dos facetas: una donde Armanda es cómplice de Calixta y otra donde no lo es.

Algo muy interesante es ver qué pasaría si Belindo no fuera inocente pero aún así hace el interrogatorio (para disimular) y obtiene las mismas respuestas. Es un un buen ejercicio revisar esto de forma similar a como se hizo el otro caso.[2]

3.2. El efecto de un modelo de acción sobre un modelo simplicial.

Un modelo de acción determina en qué conocimientos finales acaba cada persona tras un evento que haga evolucionar su conocimiento. Es hora de juntar *adecuadamente* esto con los modelos simpliciales del capítulo anterior para construir un único modelo simplicial que dentro de sí guarde toda la información sobre la evolución de conocimiento:

- Qué conocimientos iniciales terminan en qué conocimientos finales tras el evento.
- Una vez obtenidos los conocimientos finales, ¿cómo es la nueva indistinguibilidad?.

Para ello es necesario definir un concepto previo fundamental: el producto cartesiano simplicial.

Definición 3.2.1 (Producto cartesiano cromático)
Sean $< C, \chi >$ *y* $< T, \chi >$ *complejos simpliciales cromáticos puros de misma dimensión y coloración. Se define el producto cartesiano como el complejo simplicial cromático* $< C \times T, \chi >$ *tal que:*

- $V(C \times T) = \{(u, v) \in V(C) \times V(T) | \chi(u) = \chi(v)\}$.
- $\{(u_0, v_0), \ldots, (u_k, v_k)\} \in C \times T$ *si y solo si* $\{u_0, \ldots, u_k\} \in C, \{v_0, \ldots, v_k\} \in T$ *y* $\forall 0 \leq i \leq k$, $\chi(u_i) = \chi(v_i)$.

En algunas ocasiones el simplejo $\{(u_0, v_0), \ldots, (u_k, v_k)\} \in C \times T$ *se denota como* $\{u_0, \ldots, u_k\} \times \{v_0, \ldots, v_k\}$.

Pueden verse algunos ejemplos en la figura 3.1. Cuando se dice que dos complejos simpliciales *tienen la misma coloración* no se refiere necesariamente a que las funciones χ sean iguales. Más bien, se refiere a que sus coloraciones tienen el mismo contradominio de colores.

De esta forma, el modelo simplicial que representa de manera adecuada toda la evolución del conocimiento es un sub-modelo del producto cartesiano entre el modelo inicial y

[2]Gran pista: eso sólo puede pasar en el mundo donde Belindo y Calixta están coludidos en el robo.

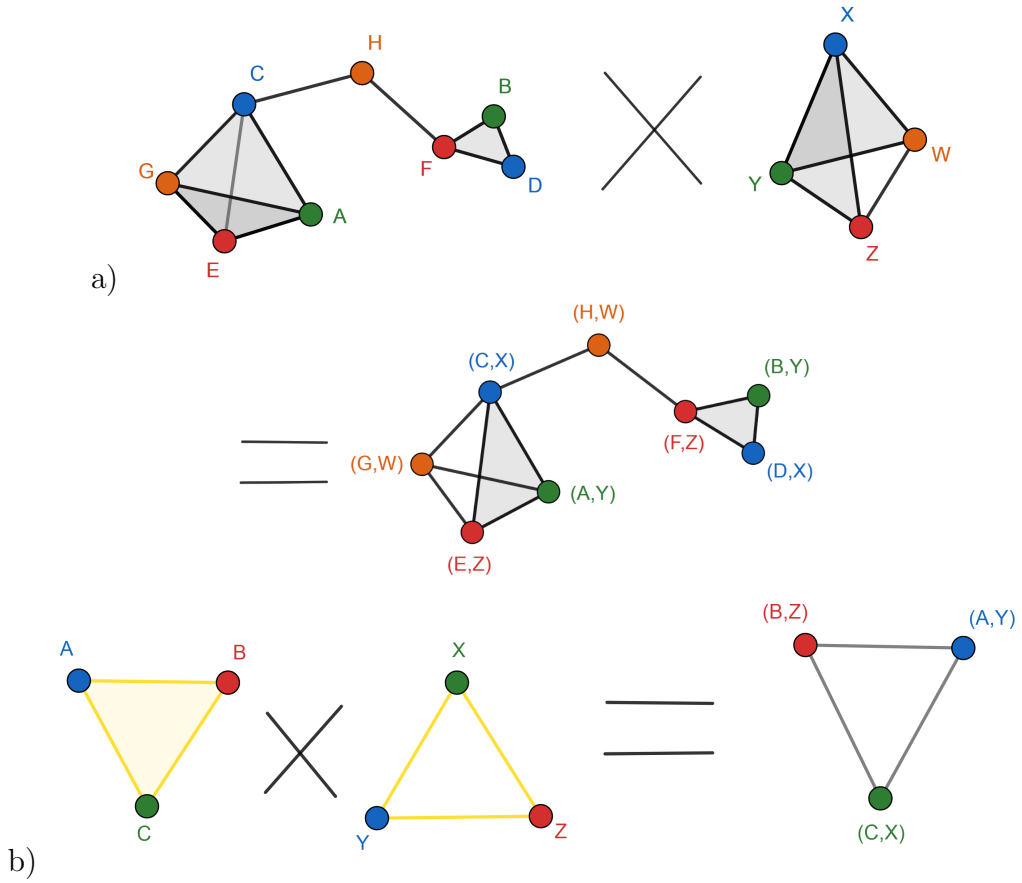

Figura 3.1: Ejemplos de productos cartesianos: a) Dos complejos simpliciales impuros. b) Dos complejos simpliciales puros. Contrario a la intuición vectorial, el producto cartesiano simplicial no aumenta la dimensión de los complejos simpliciales (y hasta parece reducirlo).

el modelo de acción al que se le denomina *Efecto de la acción sobre un modelo simplicial* y se define de la siguiente manera:

Definición 3.2.2 (Efecto de un modelo de acción sobre un modelo simplicial)

Sea $\mathcal{C} =< C, \chi, l >$ *un modelo simplicial y* $\mathcal{A} =< A, \chi, pre >$ *un modelo de acción, ambos con la misma coloración y dimensión. Se define el efecto de* $\mathcal{A}$ *sobre* $\mathcal{C}$ *como el modelo simplicial* $\mathcal{C}[\mathcal{A}] =< C[A], \chi[A], l[A] >$ *tal que*

a) $C[A] \subseteq C \times A$ *es tal que* $\{u_0, \ldots, u_k\} \times \{v_0, \ldots, v_k\} \in F(C[A])$ *si y solo si* $\mathcal{C}, \{u_0, \ldots, u_k\} \models pre(\{v_0, \ldots, v_k\})$.

b) $\chi[A]$ *es la coloración del producto cartesiano* $C \times A$.

c) La valuación $l[A] : V(C[A]) \to \mathscr{P}(AP)$ *se define como* $l[A]((u, v)) = l(u)$.

El punto b) formaliza el deseo de que las precondiciones indiquen qué mundos en el modelo inicial terminan en qué mundos en el modelo de acción. Los vértices quedan de la forma $((A, K_A(\phi_1)), (A, K_A(\phi_2)))$, pero para economizar en notación puede representarse como $(A, K_A(\phi_1), K_A(\phi_2))$, lo que permite interpretar cada vértice como que el agente A, al empezar con el conocimiento $K_A(\phi_1)$, debe terminar con el conocimiento $K_A(\phi_2)$ al final del evento que representa el modelo de acción.

En este punto es posible hablar de *aprendizaje* en estos términos para aterrizar la intuición alrededor de los modelos. Se dice que un agente A aprende una fórmula ϕ en el efecto de un modelo de acción sobre un modelo simplicial si en este modelo es falso que A conoce ϕ, pero en el efecto es cierto. Dicho en términos formales, y considerando los mundos posibles, es como sigue:

Definición 3.2.3 (Aprendizaje)
Sea $\mathcal{C} =< C, \chi, l >$ un modelo simplicial y $\mathcal{A} =< A, \chi, pre >$ un modelo de acción, ambos con la misma coloración y dimensión. Sea ϕ una fórmula en el lenguaje básico modal asociado a ambos y sea p un color (agente). p aprende la fórmula ϕ en un mundo $f \in F(C)$ si y solo si:

a) $\mathcal{C}, f \not\models K_p(\phi)$

b) Si $f \times g \in F(C[A])$ *entonces* $\mathcal{C}[\mathcal{A}], f \times g \models K_p(\phi)$.

Este concepto es de capital importancia ya que la resolución o no de un problema de intercambio de información depende fuertemente del aprendizaje de los involucrados.

3.2.1. Tareas.

Si bien los modelos de acción representan la evolución del conocimiento obtenido tras un evento determinado, en realidad no dependen de dicho evento *per se* ya que únicamente definen con precisión los conocimientos finales adquiridos. Así, es posible abstraer todavía más a los modelos de acción para representar todos los estados finales de conocimiento que deben alcanzarse para solucionar un problema de incertidumbre.

Definición 3.2.4 (Tarea)
Dado un problema de conocimiento, sea $\mathcal{C}$ un modelo simplicial que represente los conocimientos iniciales del problema. Una tarea $\mathcal{T}$ es un modelo de acción con misma dimensión y coloración que $\mathcal{C}$ tal que representa todos los conocimientos finales válidos en los que deberían terminar los agentes para dar por resuelto el problema.

Esta definición es una muy importante herramienta que permite verificar si un evento tiene la capacidad de hacer evolucionar lo suficiente el conocimiento de los involucrados como para que sean capaces de deducir los conocimientos finales deseados (bien definidos

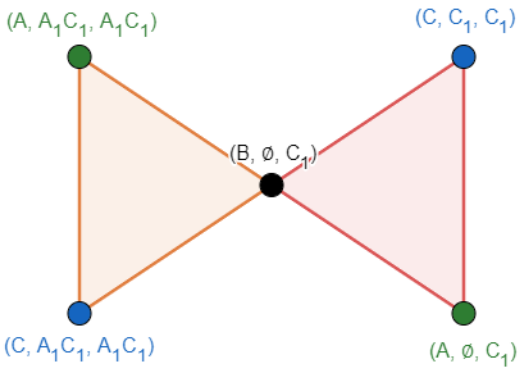

Figura 3.2: Parte del efecto del modelo que representa el interrogatorio de Belindo sobre sus compañeras, centrada en los mundos donde Belindo es inocente. La segunda coordenada de los vértices representa los conocimientos iniciales y la tercera coordenada los finales, por ejemplo el vértice $(B, \emptyset, C_1)$ significa que, al inicio del problema, Belindo no sabía nada de los culpables (representado por la segunda coordenada $\emptyset$) pero que al final consiguió descubrir que Calixta estaba involucrada (representado por la tercera coordenada $C1$) aunque sin poder decir nada sobre Armanda. El vértice de Armanda en la faceta roja (donde es inocente) muestra como conocimiento final que ella descubre la culpabilidad de Calixta, aunque realmente no puede decir nada sobre la de Belindo (¿y si montó un *teatrito* para disimular su culpabilidad y le prometió una suculenta tajada de memes a Calixta a cambio de entregarse?) por lo que puede deducirse que dicho vértice debe incidir en otras facetas.

por la tarea).

Retomando nuevamente el ejemplo 4 de los ladrones de memes, los mundos donde Belindo es inocente deben ser llevados en la *tarea* asociada al problema a mundos donde conoce a los culpables del crimen. ¿Es el interrogatorio suficiente para ello?, recuérdese que, a pesar de haber logrado aprender que Calixta forma parte de la conspiración, Belindo sigue sin tener certeza sobre la inocencia de Armanda por lo que dicho interrogatorio no basta para resolver el problema. Dado que la conexidad está íntimamente ligada con la indistinguibilidad, este argumento parece equivaler al hecho de que, como se muestra en la figura 3.2, hay dos mundos conectados en el efecto del interrogatorio mientras que en el efecto de la tarea (figura 3.3) todos los mundos son ajenos entre sí.

En la figura 3.4 se muestran dos modelos que no son lo *lo suficientemente parecidos* como para decir que representan los mismos conocimientos finales ya que el conocimiento es visualizable en complejos simpliciales mediante las intersecciones entre los simplejos. En general, es posible hacer este tipo de análisis visuales en general, pero antes es necesario formalizarlo adecuadamente para comprender sus alcances y limitaciones.

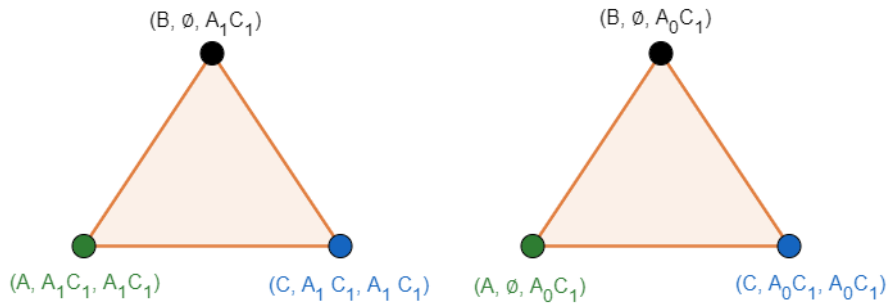

Figura 3.3: Parte del efecto de la tarea sobre el modelo para el problema de los ladrones de memes, centrada en los mundos donde Belindo es inocente. Por ejemplo el vértice $(B, \emptyset, A_1C_1)$ significa que, al inicio del problema, Belindo no sabía nada de los culpables (representado por $\emptyset$) pero que al final consiguió descubrir que las ladronas eran Armanda y Calixta (representado por la tercera coordenada A_1C_1).

3.3. Funciones continuas para comparar efectos.

La manera inmediata de comparar el efecto de un modelo de acción con el efecto de la tarea que pretende resolver es mediante cotejar las indistinguibilidades. Si un modelo de acción resuelve la tarea entonces las indistinguibilidades de su efecto deben ser lo suficientemente parecidas a las del efecto de la tarea.

La pregunta ahora es qué tan parecidos deben ser ambos efectos. Dado que se espera que tengan conexidades equivalentes (ya que de ello depende la indistinguibilidad), sería bueno que existiera alguna especie de *morfismo* que haga explícito tal cosa, y dado que la conexidad depende de las intersecciones entre los simplejos, un buen punto de partida es pedir que estos morfismos guarden cierta similitud estructural al respecto.

Definición 3.3.1 (Mapeos simpliciales)
Sean C y D complejos simpliciales (no necesariamente con el mismo conjunto de vértices). Se define un mapeo simplicial como una función f que lleva a los vértices de C a vértices de D y que satisface que $\forall s \in C$, $f[s] \in D$.

Es necesario también pedir un par de cosas más a los mapeos simpliciales: que no hagan cosas extrañas con los nombres de los agentes ni con lo que es cierto en ellos en cada mundo (sus valuaciones).

Definición 3.3.2 (Mapeos cromáticos)
Sean $< C, \chi >$ y $< D, \chi >$ complejos simpliciales cromáticos con la misma coloración. Un mapeo simplicial $f : V(C) \to V(D)$ es cromático si preserva colores. Es decir $\chi(v) = \chi(f(v))$ para todo $v \in V(C)$.

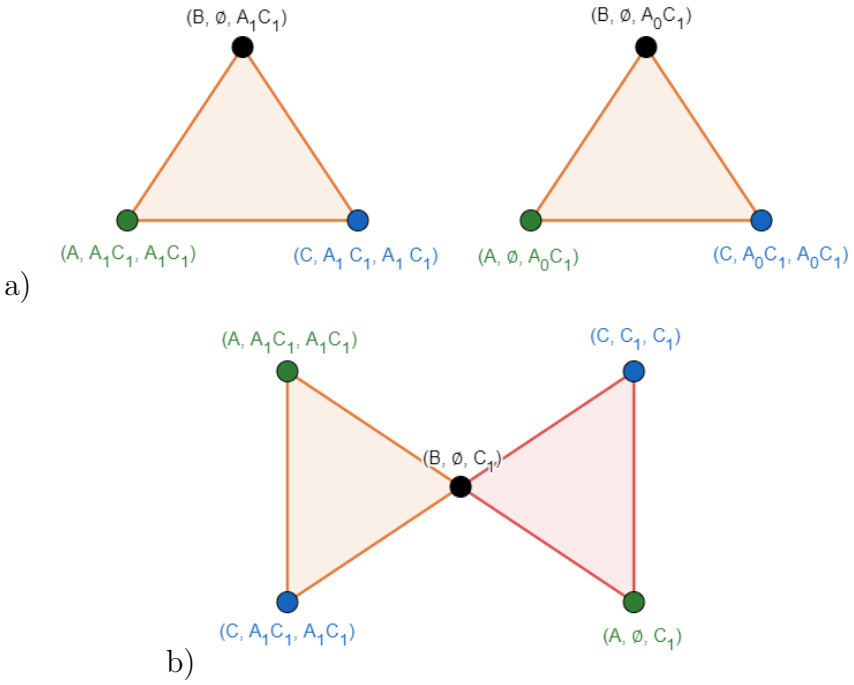

Figura 3.4: a) Efecto del interrogatorio sobre el modelo inicial. b) Efecto de la tarea sobre el modelo inicial.

De esta forma, un mapeo cromático no va a hacer cosas extrañas como asociar el vértice de Belindo inocente con el poco relacionado vértice de Armanda culpable.

Definición 3.3.3 (Morfismo de modelos)
Un morfismo entre modelos simpliciales $M =< C, \chi, l >$ *y* $M' =< C', \chi', l' >$*, denotado* $f : M \to M'$ *es un mapeo simplicial cromático que preserva a los etiquetados* l *y* l'*, es decir,* $l(v) = l'(f(v))$ *para todo vértice* v*.*

De esta forma, un morfismo de modelos no va a hacer cosas extrañas como asociar el vértice de Belindo inocente a un vértice donde sea culpable y esté coludido con Calixta.

Así, es legítimo determinar que dos efectos son *equivalentes* si existe un morfismo de modelos entre ambos, pues con eso se garantiza que cada simplejo de un efecto tenga un equivalente en el otro efecto, y que las indistinguibilidades son lo suficientemente parecidas (gracias a la preservación de la valuación, y a lo íntimamente relacionada que está esta con la indistinguibilidad gracias al operador de satisfacción).

Más aún, al dicho morfismo ser cromático y preservador de valuaciones, puede caracterizarse como una función que lleva los conocimientos finales del modelo de acción a los conocimientos finales del modelo simplicial, representando así el que cada involucrado es capaz de deducir los conocimientos finales determinados en la tarea a partir de los

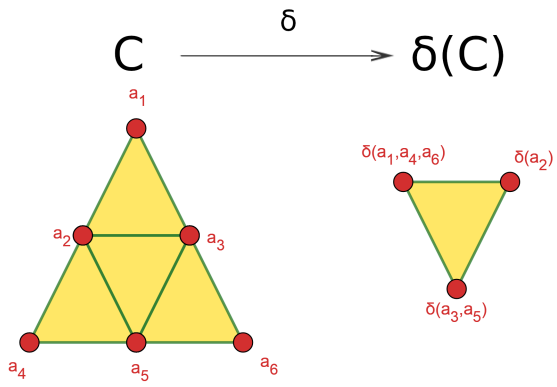

Figura 3.5: Ejemplo de un mapeo simplicial δ que lleva cuatro triángulos a uno sólo. Claramente no es un ejemplo inyectivo. ¿Existe una coloración que lo volviera cromático?.

obtenidos en el otro modelo de acción.

Por último, es necesario pedir que cada conocimiento final *equivalente* del modelo de acción y de la tarea hayan sido deducidos a partir del mismo mundo (lo que equivale a que tengan la misma precondición). Una forma topológica de manejar esto a partir del producto cartesiano simplicial son las proyecciones canónicas.

Definición 3.3.4 (Proyecciones canónicas simpliciales)
Dado $< R, \chi, l >$ *modelo simplicial cromático puro de dimensión* n*, sean* $< C, \chi, l' >$ *y* $< T, \chi, l'' >$ *modelos simpliciales tales que* $R = C \times T$*, entonces las proyecciones canónicas son morfismos simpliciales cromáticos tales que:*

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

De esta manera, $\pi_C((u, v)) = u$ manda el par $(sujeto, inicial, final)$ a $(sujeto, inicial)$ si y solamente si el sujeto obtuvo el conocimiento final a partir del conocimiento "*inicial*", lo que formaliza la noción de precondición.

Finalmente, todo lo anterior converge a la siguiente definición.

Definición 3.3.5 (Resolución de una tarea)
Sea $\mathcal{I}$ *un modelo simplicial,* $\mathcal{T}$ *una tarea asociada a dicho modelo simplicial y* $\mathcal{A}$ *un modelo de acción también asociado a* $\mathcal{I}$*. La tarea* $\mathcal{T}$ *se resuelve por el modelo de acción* $\mathcal{A}$ *(o que es posible llegar a* $\mathcal{T}$ *desde* $\mathcal{A}$*) si existe un morfismo de modelos* $\delta : \mathcal{I}[\mathcal{A}] \to \mathcal{I}[\mathcal{T}]$ *tal que* $\pi_{\mathcal{I}} \circ \delta = \pi_{\mathcal{I}}$.

Esta definición puede visualizarse como que el diagrama de la figura 3.6 conmuta, y formaliza toda la discusión previa: δ es el morfismo que indica qué conocimiento final del modelo de acción $\mathcal{A}$ permite deducir qué conocimiento final de la tarea $\mathcal{T}$, y la petición de conmutatividad del diagrama equivale a la petición de que, si el conocimiento final k de $\mathcal{A}$ es llevado al conocimiento final $\delta(k)$ de $\mathcal{T}$, entonces ambos fueron obtenidos a partir de un mismo conocimiento inicial.

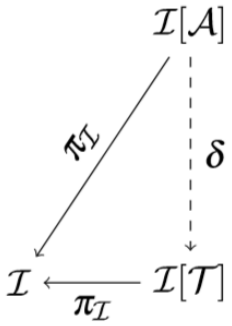

Figura 3.6: Diagrama conmutativo que representa el que un modelo de acción resuelva una tarea. Estos diagramas son muy usados en álgebra abstracta y teoría de categorías. Fuente: [6].

3.4. Notas finales

Las principales referencias de este capítulo son [10, 11, 6]. El tercero es la fuente primaria de la definición de resolución de tareas.

La discusión de la última sección permite poner un punto final a la discusión empezada en [8] sobre lo que es una solución para el problema de las cartas rusas: dada una tarea que represente todos los conocimientos finales admitidos (que *Ana* y *Blas* conozcan sus cartas mutuamente mientras que *Cruz* sólo conozca las propias), una solución para el problema es un evento que haga evolucionar los conocimientos de *Ana* y *Blas* hasta un punto que les permita deducir la mano de *Cruz*, sin que este pueda adivinar ninguna de las cartas de ellos. Es decir, un modelo de acción que resuelva la tarea.

Sobre lógica epistémica dinámica vista desde el punto de vista de la topología combinatoria, el artículo [15] es una fuente bastante reciente[3] (data de febrero del 2020) y concisa que la abarca a la perfección. Es una lectura ampliamente recomendada para quienes deseen un enfoque mucho más especializado del tema, orientado a teoría de la computación.

[3]Esta tesis se imprimió en noviembre del 2020

Capítulo 4

El problema del consenso binario: un ejemplo de modelos de topología combinatoria para problemas de conocimiento

En el presente capítulo se muestra un pequeño ejemplo que aglomera todo lo previamente visto y construye un modelo de topología combinatoria para el bien conocido *problema del consenso binario*. Más aún, se establecen una serie de pautas generales para hacer mucho más amigable la aparatosa notación derivada del lenguaje básico modal y del producto cartesiano simplicial, y se comparten una serie de tips muy útiles a la hora de hacer modelos de este tipo.

Problema 1 (El problema del consenso binario.)
Dos amigos Ariadno y Bibiano quieren decidir si ir al cine o a la discoteca. Si al principio no saben lo que quiere el otro, ¿cómo podría representarse el problema para poder estudiar formas de ponerse de acuerdo?.

Como cabe esperarse, la forma en la que se representará este problema es mediante un modelo de topología combinatoria que permitirá estudiar formas de ponerse de acuerdo.

Definición 4.0.1 (Modelos de topología combinatoria)
Un modelo τ de topología combinatoria para un problema de conocimiento que involucra a varias personas deseosas de descubrir algo pero siguiendo ciertas restricciones se compone de lo siguiente:

- *Un modelo simplicial $\mathcal{I}$ denominado* inicial *que representa todos los mundos en los que pueden caer los involucrados al inicio del problema.*
- *Una tarea $\mathcal{T}$ que representa todos los conocimientos finales que se deben obtener para eliminar la incertidumbre, cumpliendo con las restricciones impuestas.*

En general, el modelo de topología combinatoria es representado simbólicamente con el efecto $\tau := \mathcal{I}[\mathcal{T}]$.

A continuación se muestra la construcción del modelo para el problema del consenso.

4.1. Los mundos posibles

Un buen consejo a la hora de elegir un lenguaje básico modal para trabajar un problema es pensar sobre lo que los protagonistas del problema desean conocer, para luego *reducirlo a su mínima expresión*. Los amigos tienen la tarea de llegar a un acuerdo sobre si ir al cine o a la discoteca, por lo que un lenguaje básico modal útil para ello es el generado por el conjunto de atómicas $AP = \{p_{i,j} | i \in \{A, B\}, j \in \{cine, discoteca\}\}$.

A fin de simplificar la notación, se hace $cine = 1$ y $discoteca = 0$ de manera que $p_{q,1}$ significa que "el amigo q quiere ir al cine".

Una vez con un buen lenguaje, se procede a determinar los mundos posibles. A la hora de hacer esto, es recomendable recordar que la finalidad de definir *mundos* es describir la incertidumbre que se desea eliminar. Así, dado que los amigos desconocen los deseos del otro, cada uno de ellos genera los siguientes dos mundos:

1. El mundo donde Ariadno (o Bibiano) quiere ir al cine.
2. El mundo donde Ariadno (o Bibiano) quiere ir a la discoteca.

Posteriormente se pule más la definición de los mundos, buscando que cada uno diga algo sobre todos los involucrados a la vez. Ya que los deseos de Bibiano son independientes de los de Ariadno (y visceversa), los mundos posibles pueden definirse como todas las posibles combinaciones de deseos en una forma vectorial como la siguiente:

$$S := \{0, 1\}^2$$

Por estandar se le asignará la primera coordenada a Ariadno y la segunda a Bibiano, por lo que el mundo $(0, 1)$ es aquel donde Ariadno quiere ir a la discoteca mientras que Bibiano quiere ir al cine. El mundo $(1, 1)$ es aquel donde ambos quieren ir al cine (y para resolver el problema del consenso únicamente basta con que se pregunten entre ellos).

4.2. Modelo inicial

Dados los mundos, lo que procede es preguntarse qué conoce cada amigo de ellos. En este caso esto corresponde a la siguiente proposición en el lenguaje básico modal para, sin pérdida de generalidad, Bibiano:

$$K_B(p_{B,j}) \wedge \neg K_B(p_{A,1} \vee p_{A,0})$$

Con $j \in \{0, 1\}$, la segunda parte de la expresión significa que desconoce los deseos de Ariadno.

Sería bueno ahora cambiar a una notación mucho más fácil de entender. Un buen consejo para esto es buscar reducir todo a las *certezas* de los involucrados, lo que en este caso corresponde únicamente a los deseos del propio agente (por ejemplo la expresión $\neg K_B(p_{A,1} \vee p_{A,0})$ significa que Bibiano no tiene certezas sobre Ariadno).

Posteriormente hay que buscar una manera de expresar las certezas en algún vector fácil de escribir y entender, para finalmente extenderlo para expresar las incertidumbres con un símbolo $\perp$. En este caso, el conocimiento de Bibiano se convierte en lo siguiente:

$$K_B(p_{B,j}) \wedge \neg K_B(p_{A,1} \vee p_{A,0}) \longrightarrow (\perp, j)$$

Lo que es maravillosamente compacto respecto a la fórmula original, y guarda la misma información. La flecha larga significa que lo de la izquierda va a denotarse como lo de la derecha, y es notación tomada prestada de la teoría de gramáticas y lenguajes formales.

Finalmente se procede a construir el modelo inicial. Un buen consejo a la hora de construir modelos simpliciales para problemas de conocimiento es empezar mediante la construcción de las facetas, y luego completar recursivamente el complejo simplicial metiendo todos los subconjuntos de las facetas. En este caso cada faceta es como sigue, para un mundo $(s_1, s_2) \in S$:

$$f(s_1, s_2) = \{(A, (s_1, \perp)), (B, (\perp, s_2))\}$$

Lo que puede expresarse de manera aún más compacta así:

$$f(s_1, s_2) = \{(A, s_1\perp), (B, \perp s_2)\}$$

Una vez dadas las facetas, lo que sigue es darse una idea de cómo luce el complejo simplicial para poder ir adivinando las indistinguibilidades.[1] Para estudiar las adyacencias y conexidades del complejo es bueno empezar contando la cantidad de mundos indistinguibles. En este caso los únicos mundos indistinguibles son aquellos donde el otro amigo varía su deseo, por ejemplo el vértice $(A, 1\perp)$ es adyacente a los vértices $(B, \perp 1)$

[1] Y hasta quizá concebir alguna forma de resolver el problema.

y $(B, \perp 0)$ gracias a la independencia entre deseos. Así, el modelo inicial $\mathcal{I}$ es una gráfica bipartita regular de grado 2 (véase figura 4.1).

Es inmediato notar que este problema sí satisface la petición filosófica de que lo que conozca cada amigo esté relacionado con su propia naturaleza ya que, de manera trivial, cada amigo únicamente conoce sus propios deseos. Así, la valuación se define de la siguiente manera para un vértice (Q, q_1q_2) (con $Q \in \{A, B\}$ y $q_i \in \{0, 1, \perp\}$):

$$l((Q, q_1q_2)) = p_{q,\pi_Q(q_1,q_2)}$$

Donde π_Q es la proyección de la primera coordenada si $Q = A$ o de la segunda coordenada si $Q = B$. Esta valuación únicamente asigna a cada agente su propio deseo. Por ejemplo para el vértice en el que Bibiano quiere ir al cine, $l((B, \perp 1)) = p_{B,1}$.

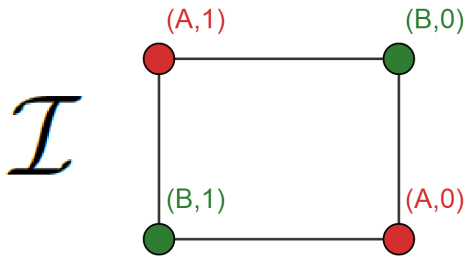

Figura 4.1: Como sólo hay dos agentes, el modelo simplicial es una gráfica bipartita que se ve muy bonita puesta como un cuadrado (en teoría de gráficas [18] es mejor conocida como el 2-cubo Q_2). Los vértices son denotados como $v = (\chi(v), l(v))$ en lugar de con la forma definida $v = (Q, q_1q_2)$ ya que el problema del consenso binario es del tipo de problemas en los que el conocimiento inicial total corresponde de manera biunívoca a lo que se conoce de sí mismo.

4.3. La tarea a resolver

Visto desde un punto de vista *recalcitrantemente práctico*, el problema del consensos puede considerarse resuelto si ambos amigos llegan a un acuerdo independientemente de los conocimientos iniciales. Dado que se están representando las elecciones posibles como 0 y 1, se espera que las facetas de la tarea a resolver sean dos aristas ajenas de la siguiente forma:

$$\{(A, \text{elegir } 0), (B, \text{elegir } 0)\}$$
$$\{(A, \text{elegir } 1), (B, \text{elegir } 1)\}$$

En términos de conocimiento y recordando la necesidad del diálogo, esto equivale a que la tarea tenga vértices de la forma:

$$(Q, K_Q(p_{A,i} \wedge p_{B,i}))$$

De manera que dos vértices $(Q, K_Q(p_{A,i} \wedge p_{B,i}))$ y $(R, K_R(p_{A,j} \wedge p_{B,j}))$ conforman una faceta si $i = j$ (es decir, se llegó a un concenso). Nuevamente se puede economizar notación de la siguiente manera:

$$(Q, K_Q(p_{A,i} \wedge p_{B,i})) \longrightarrow (Q, i)$$

Así, el vértice (Q, i) debe leerse como "el amigo Q al final decidió ir a i".

Nótese que, si bien $K_Q(p_{A,i} \wedge p_{B,i})$ significa que Q sabe que Ariadno quiere ir al lugar i y Bibiano también, no significa que se vino de un mundo inicial en donde esto pasó. Más aún, pudo haber provenido de cualquier mundo gracias a la independencia de los deseos, por lo que las precondiciones deben tener en cuenta esta situación a la hora de definirse:

$$pre((Q, K_Q(p_{A,i} \wedge p_{B,i}))) = (p_{A,1} \vee p_{A,0}) \wedge (p_{B,1} \vee p_{B,0})$$

La cual significa que tanto Ariadno como Bibiano originalmente querían ir al cine o a la discoteca, es decir, provienen de cualquier mundo del modelo inicial.

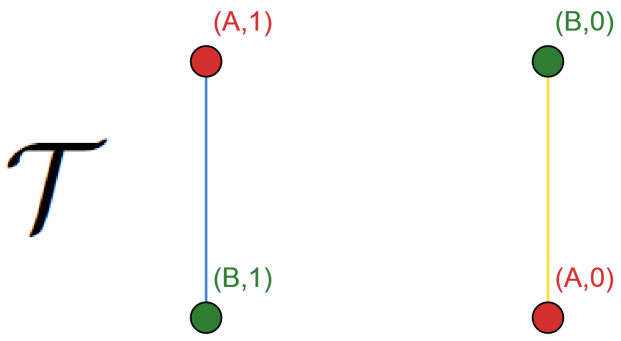

Figura 4.2: La tarea a resolver, con la notación hipercompacta.

Por último se procede a hacer el efecto $\mathcal{I}[\mathcal{T}]$. En este caso dicho efecto se compone de

vértices $(Q, q_1q_2) \times (Q, j)$ donde $q_1, q_2, j \in \{0, 1\}$ son valores arbitrarios (pues cualquier mundo puede terminar en cualquier consenso). Para denotar de manera *elegante* estos vértices, debe recordarse que significan que "el amigo Q originalmente quería ir al lugar $\pi_Q(q_1, q_2)$,[2] pero al final decidió ir al lugar j", por lo que la siguiente notación es más que adecuada:

$$(Q, q_1q_2) \times (Q, j) \longrightarrow (Q, \pi_Q(q_1, q_2), j)$$

Ya que $(Q, \pi_Q(q_1, q_2), j)$ puede fácilmente leerse en el sentido descrito. Por ejemplo $(A, 1, 1)$ significa que Ariadno quería ir al cine y al final efectivamente fue, mientras que $(B, 0, 1)$ significa que Bibiano quería ir a la discoteca pero al final fue persuadido por Ariadno de ir al cine.

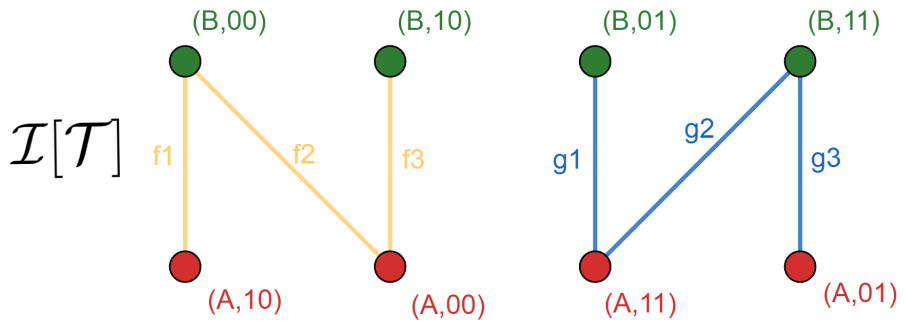

Figura 4.3: Modelo de topología combinatoria para el problema del consenso.

4.4. Notas finales

El problema del consenso binario es un problema original de la computación distribuida, y su planteamiento original prescinde de salidas nocturnas y de personas nombradas por entrañables santorales patronales. Para el lector más interesado en el tema se recomiendan las fuentes [11, 6] donde el problema es abordado desde un punto de vista mucho más formal.

[2]En este caso $\pi_Q(q_1, q_2)$ corresponde a la proyección canónica correspondiente al agente Q, dado que a Ariadno se le asocia la primera coordenada y a Bibiano la segunda. En decir, $\pi_A(q_1, q_2) = q_1$ y $\pi_B(q_1, q_2) = q_2$.

Parte II

Modelos de topología combinatoria para problemas de cartas rusas

Capítulo 5

Generalización y mundos posibles para el problema de las cartas rusas

En este capítulo se plantea de manera completa y precisa el problema de las cartas rusas para después generalizar algunas de sus variables. Finalmente se definen los conjuntos de mundos que son la base para el modelo de topología combinatoria para el problema.

Problema 2 (Las cartas rusas generalizadas.)
Tres agentes Ana, Blas y Cruz toman a, b y c cartas respectivamente de un mazo de $a+b+c$ *cartas.*
Todos los agentes saben qué cartas habían en el mazo y cuántas tomaron cada uno de los otros agentes, pero también sólo pueden ver las cartas de su propia mano.
Ana y Blas, sin embargo, quieren saben exactamente qué cartas tomó Cruz. Más aún, no quieren que él descubra quien tiene cualquier carta -a parte por supuesto de las de él-. Sin embargo solamente pueden hacerse anuncios públicos indecifrados, por lo que Cruz puede aprender toda la información que intercambien Ana y Blas. ¿Podrá el par lograr esto?.
Se dice que el problema tiene parámetros (a, b, c).

Esta versión *generalizada* del problema es la que se enuncia en [5]. Ahí, el mazo de cartas es el conjunto I_{a+b+c} de los primeros $a+b+c$ naturales y cada combinación de manos posibles corresponde a una partición $\{A, B, C\}$ del mazo cuyos elementos tienen a, b y c elementos respectivamente.

Un modelo de topología combinatoria para este problema consiste en complejos simpliciales puros de dimensión 2 y cuya tarea elimina la indistinguibilidad para *Ana* y *Blas*, pero manteniéndola para *Cruz*. Así, es posible generalizar la dimensión del complejo tomando al conjunto $\mathbf{A} = \{A_1, \ldots, A_n\}$ de n agentes en lugar de a los amigables *Ana*, *Blas* y *Cruz*.

Esta generalización de la dimensión saca a la luz una serie de consideraciones adicionales, pues al poder haber más de tres agentes, el maquiavélico *Cruz* podría tener

más aliados que desean descubrir las cartas de *Ana* y *Blas* (quienes a su vez también podrían tener más cómplices). Así, es conveniente particionar al conjunto $\mathbf{A}$ con dos subconjuntos propios $\mathbf{E}$ y $\mathbf{P}$.[1] En este trabajo se ha decidido nombrar al bando de *Cruz* como "los espías" (ya que desean robar información), y al bando de *Ana* y *Blas* como "los no-espías"[2] por lo que los conjuntos $\mathbf{E}$ y $\mathbf{P}$ son denominados *de espías* y *de no-espías* respectivamente.

El incremento de agentes trae consigo también un incremento en los parámetros del problema, por lo que el vector (a, b, c) debe generalizarse a un vector $(a_1, \ldots, a_n) \in (\mathbb{Z}^+)^n$ donde el agente i-ésimo recibe a_i cartas.[3]

Otra consecuencia de aumentar la cantidad de agentes es que se abre la posibilidad de considerar casos en los que no se reparten r cartas del mazo (con $r > 0$), al poder pensarse esto como un $n+1$-ésimo *agente vacío* (que actuaría como un espía mudo).

Finalmente, el mazo de cartas I_{a+b+c} es generalizado al enorme conjunto $I_{\Sigma_{i=1}^n a_i + r}$ de los primeros $\Sigma_{i=1}^n a_i + r$ naturales. Para evitar complicaciones de notación, se denota $cards := I_{\Sigma_{i=1}^n a_i + r}$ como la mano.

Problema 3 (El muy generalizado problema de las cartas rusas.)
Un conjunto de $n \geq 2$ agentes $A_1, \ldots, A_n$ toman $a_1, \ldots, a_n$ elementos respectivamente de $cards = I_{\Sigma_{i=1}^n a_i + r}$. Todos los agentes saben cuántos elementos tomaron cada uno, pero sólo conocen los que tomaron ellos mismos. Por una parte hay un grupo de agentes $\{P_1, \ldots, P_k\} \subsetneq \{A_1, \ldots, A_n\}$ que quieren saber qué elementos tomaron todos ellos pero sin que el resto de los agentes $\{E_1, \ldots, E_m\}$, denominados espías*, se enteren. Dado que únicamente pueden hacerse anuncios públicos indecifrados, los espías podrán aprender toda la información que los no-espías intercambien entre ellos. ¿Como sería posible lograr esto?. En este caso el problema tiene parámetros $(a_1, \ldots, a_n) = \overline{a} \in (\mathbb{Z}^+)^n$.*

A partir de este momento se da por sentado que se trabaja sobre el conjunto abstracto de agentes $\mathbf{A} = \{A_1, \ldots, A_n\}$ y que está particionado en $\mathbf{P}$ y $\mathbf{E}$. Además $\overline{a} = (a_1, \ldots, a_n) \in (\mathbb{Z}^+)^n$.

5.1. Mundos posibles.

La incertidumbre del problema está en términos de las cartas de los demás. Así, un conjunto útil de atómicas es el siguiente:

$$AP = \{p_{a,x} | a \in \mathbf{A}, x \in cards\}$$

[1] Y por tanto $\mathbf{P} := \mathbf{A} - \mathbf{E}$.
[2] ¡Ingenioso nombre! ¿eh?.
[3] $(\mathbb{Z}^+)^n = \underbrace{\mathbb{Z}^+ \times \cdots \times \mathbb{Z}^+}_{n \text{ veces}}$. El exponente aquí es relativo al producto cartesiano.

Donde la variable $p_{a,x}$ significa que "el agente a tiene la carta x". Finalmente el lenguaje básico modal se denota $\mathcal{L}_K(cards)$ para indicar que se trabaja sobre dicho mazo de cartas.

Para construir los mundos posibles, hay que recordar que la incertidumbre que se desea eliminar es que los no-espías descubran las cartas que tienen entre todos al tiempo que los espías permanecen en la ignorancia, por lo que es aceptable definir los mundos en términos de las cartas que tienen cada uno. De esta forma se definen todos los mundos como el conjunto de todos los arreglos de cartas posibles.

El conjunto de cartas que recibe el agente A_i es un $X_i \in \mathscr{P}_{a_i}(cards)$.[4] Así, es posible representar un mundo como un vector $\overline{X} = (X_1, \ldots, X_n)$ que es tal que $X_i \cap X_j = \emptyset$ si y solo si $i \neq j$. Así, el conjunto de mundos queda como:

$$S = \{(X_1, \ldots, X_n) \in \mathscr{P}_{a_1}(cards) \times \cdots \times \mathscr{P}_{a_n}(cards) \mid X_i \cap X_j = \emptyset \text{ si y solo si } i \neq j\}$$

Los mundos posibles son también denominados *arreglos de cartas* y se dice que tienen parámetros $\overline{a}$. Por último, para economizar en notación vale la pena establecer que $\overline{X} = (X_1, \ldots, X_n)$ por lo que la mano de A_i en el mundo $\overline{X}$ es X_i. En general, cualquier mundo denotado como una mayúscula con barra superior es tal que sus entradas son esa misma mayúscula pero sin la barra y con subíndices numéricos para indicar la coordenada.

[4]Donde $\mathscr{P}_{a_i}(cards) = \{X \subseteq cards \mid |X| = a_i\}$ es la potencia de a_i-subconjuntos de $cards$.

Capítulo 6

Modelos de topología combinatoria para el muy generalizado problema de las cartas rusas.

En este capítulo se alcanzan los objetivos de la presente tesis. Primero se construye el modelo inicial convirtiendo a los mundos en facetas, después se construye la tarea y finalmente se da el efecto de esta sobre el modelo inicial.

6.1. Modelo simplicial inicial para cartas rusas.

Para convertir un arreglo de cartas en una faceta, es necesario discutir los conocimientos iniciales que puedan tener los agentes. Por hipótesis, este corresponde a únicamente sus propias cartas, lo que equivale a la siguiente enorme fórmula:

$$K_{A_i}(\bigwedge_{x\in X_i} p_{A_i,x}) \wedge \bigwedge_{j\neq i} \neg K_{A_i}(\bigvee_{x\in cards-X_i} p_{A_j,x})$$

Donde $i, j \in \{1, \ldots, n\}$. Ahora bien, utilizando el símbolo $\perp$ para expresar incertidumbre, esta enorme fórmula se comprime de la siguiente manera:

$$(A_i, \overline{X}_i)$$

Donde $\overline{X}_i = \{f : \{1, \ldots, n\} \to \mathscr{P}(cards) \cup \{\perp\} | f(j) = \perp, f(i) = X_i\}$ es una forma con funciones de expresar al enorme vector cuyas entradas son todas $\perp$ excepto la asociada al agente A_i. Por ejemplo, para las cartas rusas originales con tres agentes, $\overline{X}_1 = (X_1, \perp, \perp)$, y para el caso $n = 7$, $\overline{X}_7 = (\perp, \perp, \perp, \perp, \perp, \perp, X_7)$.

De antemano es posible asegurar que este modelo simplicial satisface el estatuto fi-

losófico de que el conocimiento está en correspondencia con la propia naturaleza ya que lo único que conoce cada agente son sus propias cartas. Así, de antemano ya se sabe que la valuación es el mazo propio de cartas:

$$l((A_i, \overline{X}_i) = \bigwedge_{x \in X_i} p_{A_i,x}$$

Lo que permite definir de una forma mucho más rápida a los vértices como pares (A_i, X_i). Finalmente, las facetas del complejo simplicial I subyacente al modelo inicial $\mathcal{I}$ son:

$$F(I) = \{\{(A_1, X_1), \ldots, (A_n, X_n)\} | (X_1, \ldots, X_n) \in S\}$$

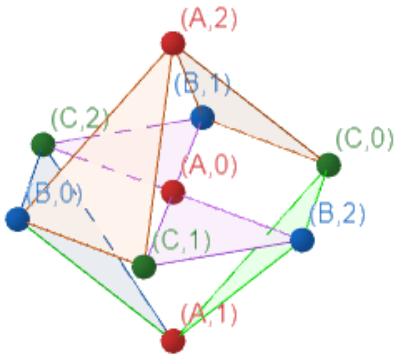

Figura 6.1: Modelo simplicial para el problema tradicional con parámetros $(1, 1, 1)$. Los vértices corresponden a $(Q, \{q\}) = (Q, q)$ para mayor simpleza.

Antes de terminar la sección vale la pena definir un par de notaciones para un conjunto $\Gamma \subseteq cards$ arbitrario:

$$p_{i,\Gamma} = \bigwedge_{x \in \Gamma} p_{i,x}$$

$$P_{i,\Gamma} = \bigcup_{x \in \Gamma} \{p_{i,x}\}$$

Esto permite escribir de manera compacta $l((A_i, \overline{X}_i) = \bigwedge_{x \in X_i} p_{A_i,x}$ como simplemente $l((A_i, \overline{X}_i) = p_{A_i,X_i}$, lo que es bastante útil en las demostraciones.

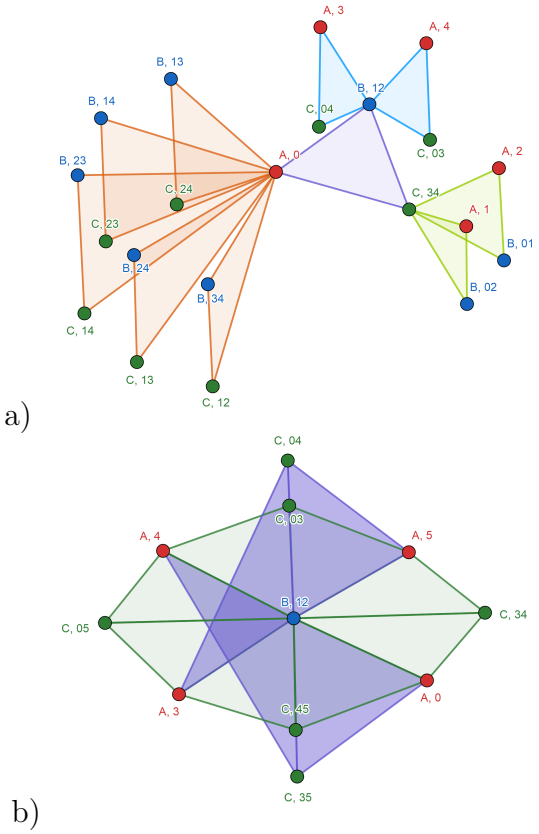

Figura 6.2: a) Incidencias del mundo $(0, 12, 34)$ en el modelo inicial del caso $(1, 2, 2)$ sin cartas sin repartir. b) Incidencias del vértice donde *Blas* tiene la mano 12 en el modelo inicial del caso $(1, 2, 2)$ con una carta sin repartir. En a) los triángulos sólo comparten vértices, mientras que en b) pueden compartir compartir aristas. Los vértices se denotan como $(Q, \{q_1, \ldots, q_n\}) = Q, q_1 \ldots q_n$.

6.2. La tarea a resolver para cartas rusas

El problema únicamente puede considerarse resuelto si, tras un procedimiento de intercambios de información que haga evolucionar los conocimientos de los involucrados, los no-espías conocen sus cartas entre ellos pero los espías desconocen el paradero exacto de cualquiera de estas.[1]

Dado un mundo $\overline{X} \in S$, un agente espía tan sólo se le tiene permitido conocer cartas de otros espías mientras que un agente no-espía debe conocer las cartas de todos sus compañeros no-espías (es irrelevante el conocer cartas de espías, aunque para casos sin cartas sin repartir es un buen auxiliar).

Así, para un mundo dado $\overline{X} \in S$, se esperan que los vértices sean de la forma $(A_i, K_{A_i}(\bigwedge_{A_k \in \mathbf{P}} p_{A_k, X_k}))$ para $A_i \in \mathbf{P}$ no-espía, mientras que sean de la forma

[1]No hay que olvidar que los anuncios son públicos, lo que significa que todo el mundo aprende la información intercambiada.

$(A_i, \neg K_{A_i}(\bigwedge_{A_k \in \mathbf{P}} p_{A_k,X_k}))$ para $A_i \in \mathbf{E}$ espía.

Se puede economizar notación de la siguiente manera:

$$(A_i, K_{A_i}(\bigwedge_{A_k \in \mathbf{P}} p_{A_k,X_k})) \longrightarrow (A_i, P_i(\overline{X}))$$

Y para espías:

$$(A_i, \neg K_{A_i}(\bigwedge_{A_k \in \mathbf{P}} p_{A_k,X_k})) \longrightarrow (A_i, E_i(\overline{X}))$$

Donde $P_i(\overline{X})$ es un vector con n entradas que asigna $\perp$ a los espías y su mano en $\overline{X}$ a los no-espías, mientras que $E_i(\overline{X})$ es un vector que asigna $\perp$ a los no-espías y su mano en $\overline{X}$ a los espías. Por ejemplo para el problema tradicional, $P_1(\overline{X}) = P_2(\overline{X}) = (X_1, X_2, \perp)$ y $P_3(\overline{X}) = (\perp, \perp, X_3)$. En el caso con parámetros $(1, 2, 2)$, en el mundo $\overline{X} = \{0, 12, 34\}$, la faceta asociada en la tarea es:

$$\{(A, (0, 12, \perp)), (B, (0, 12, \perp)), (C, (\perp, \perp, 34))\}$$

De esta manera, *Ana* y *Blas* viven en esa única faceta mientras que *Cruz* vive en cualquiera donde los no-espías tengan sus manos en $\{0, 1, 2\}$.

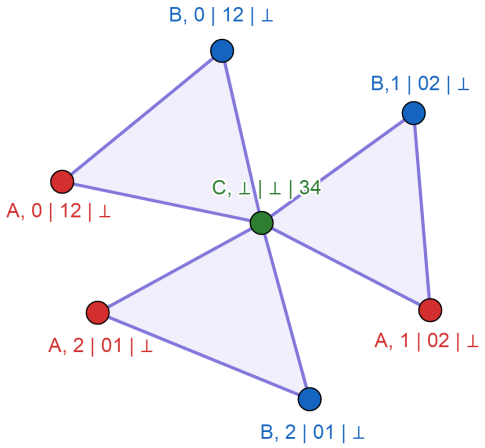

Figura 6.3: La tarea para el caso $(1, 2, 2)$ centrada en la indistinguibilidad de C con la mano $\{3, 4\}$). El vector $(Q, (q_1, q_2, q_3))$ se denota como $Q,\ q_1 \mid q_2 \mid q_3$ para mayor claridad.

Ahora bien, ese mismo ejemplo puede complicarse si se supone que hay una carta sin repartir, entonces *Ana* y *Blas* ya no viven en una única faceta al vivir en varias donde *Cruz* tiene su mano contenida en $\{3,4,5\}$ (en este caso son tres facetas en total). ¿Eso significa que la tarea falla en modelar que *Ana* y *Blas* pierden su indistinguibilidad? sí, pero no falla en modelar que *Ana* y *Blas* conocen sus propias cartas ya que la arista de ambos vive en todas las facetas que comparten, lo que epistémicamente significa que, sin importar cual sea la mano de *Cruz*, ellos ya saben la mano del otro. De ahí que al final se tomó la decisión de definir $P_i(\overline{X})$ como se hizo, incluyendo $\perp$ a los espías. Véase la figura 6.2 para ejemplos.

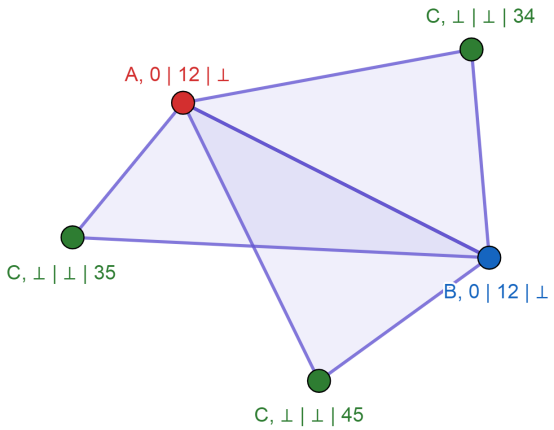

Figura 6.4: La tarea para el caso $(1,2,2)$ pero con una carta no repartida. Cada arista de *Ana* y *Blas* viven en los mismos mundos indistinguibles, lo que significa que, aunque no puedan saber la mano de *Cruz*, sí pueden saber sus propias cartas.

Las precondiciones de cada vértice deben ser que provengan de un mundo en el que tienen la mano X_i (no necesariamente el mismo $\overline{X}$), lo que se traduce en:

$$pre(A_i, P_i(\overline{X})) = p_{A_i,X_i}$$
$$pre(A_i, E_i(\overline{X})) = p_{A_i,X_i}$$

Formalmente, la tarea a resolver es la siguiente:

Definición 6.2.1 (Tarea para el muy generalizado problema)
La tarea para el muy generalizado problema de las cartas rusas se define como el siguiente modelo de acción $\mathcal{T} =< T, \chi, pre >$*:*

- $V(T) = \bigcup_{\overline{X}\in S}\{(A_i, P_i(\overline{X}))|A_i \in \mathbf{P}\} \cup \{(A_i, E_i(\overline{X}))|A_i \in \mathbf{E}\}$
- $F(T) = \bigcup_{\overline{X}\in S}\{(A_1, G_1(\overline{X})), \ldots, (A_n, G_n(\overline{X})\}$ *donde* $G_i = P_i$ *si* $A_i \in \mathbf{P}$*, y* $G_i = E_i$ *si* $A_i \in \mathbf{E}$*.*

- $\chi = \pi_1$ *es la primera proyección canónica y es tal que* $\chi(A_i, G_i(\overline{X})) = A_i$.
- $pre(A_i, G_i(\overline{X})) = p_{A_i,X_i}$

Puede consultarse un ejemplo para un caso poco estudiado del problema en la figura 6.4.

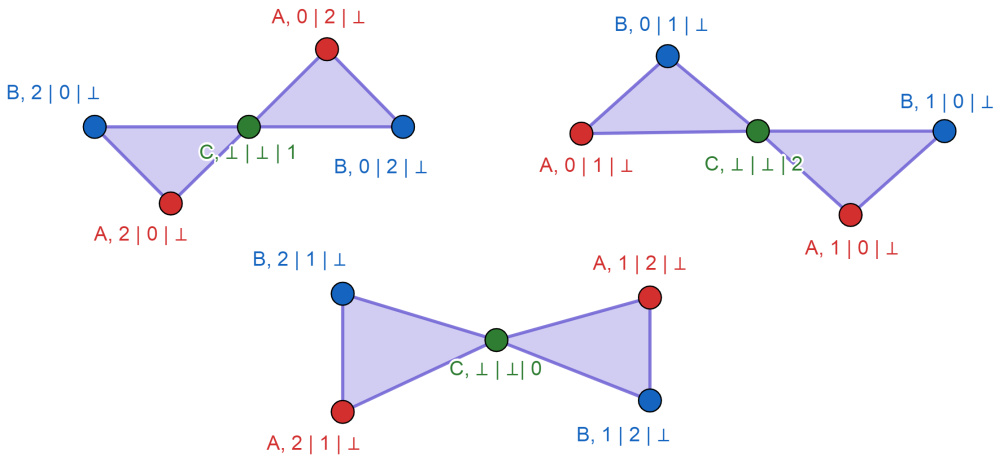

Figura 6.5: Tarea para el caso $(1, 1, 1)$ del problema tradicional de las cartas rusas. Consta de *tres elegantes moñitos*.

6.3. El efecto de la tarea sobre el modelo inicial.

Por último, sólo queda revisar el efecto de la tarea sobre el modelo inicial. En esta sección se procede *recalcitrantemente formal* por lo que se le pide al lector que conceda algo de paciencia para adentrarse en la brutal notación del lenguaje básico modal.

El objetivo principal es describir los vértices del efecto en un estilo $(A_i, inicio, final)$, para ello vale la pena recordar que el problema es muy claro a la hora de determinar qué conocimientos iniciales deben terminar en qué conocimientos finales, por lo que se espera que todos los vértices sean de la forma $(A_i, X_i, G_i(\overline{Y}))$ si y solamente si X_i es la i-ésima coordenada del mundo $\overline{Y}$, $G_i = E_i$ si A_i es espía y $G_i = P_i$ en caso contrario.

Un análisis inmediato revela que la faceta del producto cartesiano $\{(A_1, X_1, G_1(\overline{Y})), \ldots, (A_n, X_n, G_i(\overline{Y}))\}$ pertenece al efecto únicamente si $X_i = Y_i$ para todo i, gracias a la precondición. Esto es tan importante que vale la pena probarlo mediante un teorema:

Lema 6.3.1 (Efecto diagonal identidad generalizado)
Sean $\overline{X}, \overline{Y} \in S$*, entonces* $\mathcal{I}, \{(A_1, X_1), \ldots, (A_n, X_n)\} \models pre(\{(A_1, G_1(\overline{Y})), \ldots, (A_n, G_n(\overline{Y}))\})$ *si y solo si* $\overline{X} = \overline{Y}$

Demostración.
Para economizar en notación, sean $f = \{(A_1, X_1), \ldots, (A_n, X_n)\}$ y $g = \{(A_1, G_1(\overline{Y})), \ldots, (A_n, G_n(\overline{Y}))\}$.

Para la ida, supóngase que $\mathcal{I}, f \models pre(\{(A_1, G_1(\overline{Y})), \ldots, (A_n, G_n(\overline{Y}))\})$, entonces $\mathcal{I}, f \models \bigwedge_{1 \leq i \leq n} p_{A_i, Y_i}$ ya que las precondiciones se extienden a simplejos mediante la conjunción.
Utilizando la definición del operador de satisfacción, se tiene que $\mathcal{I}, f \models \bigwedge_{1 \leq i \leq n} p_{A_i, Y_i}$ equivale a que, para todo $1 \leq i \leq n$, $P_{A_i, Y_i} \subseteq l[f]$. Así, $\{p_{A_i, y} | 1 \leq i \leq n, y \in Y_i\} \subseteq l[f]$ pero además se tiene que:

$$l[f] = \{p_{A_i, x} | 1 \leq i \leq n, y \in X_i\}$$

Y dado que ambos conjuntos tienen la misma cardinalidad y son finitos, no queda otra opción mas que $\{p_{A_i, y} | 1 \leq i \leq n, y \in Y_i\} = \{p_{A_i, x} | 1 \leq i \leq n, y \in X_i\}$. Finalmente, dado que $A_i \neq A_j$ si y solo si $i \neq j$, cada $p_{A_i, y}$ es igual a algún $p_{A_i, x}$ por lo que $Y_i \subseteq X_i$, y dado que tienen la misma cantidad de elementos, $Y_i = X_i$.

Al pasar lo anterior para toda i, se concluye que $\overline{X} = \overline{Y}$.

Para la vuelta, únicamente basta con notar que es trivial, ya que:

$$\begin{aligned} l[f] &= \{p_{A_i, x} | 1 \leq i \leq n, y \in X_i\} \\ &= \{p_{A_i, y} | 1 \leq i \leq n, y \in Y_i\} \end{aligned}$$

Por lo que:

$$\begin{aligned} \mathcal{I}, f &\models \bigwedge p_{A_i, X_i} \\ &\models \bigwedge p_{A_i, Y_i} \\ &\models pre(g) \end{aligned} \quad \blacksquare$$

El significado de este teorema es mayúsculo: un vértice $(A_i, X_i, G_i(\overline{Y}))$ estará en el efecto si y solamente si $X_i = Y_i$ (pues, por el teorema del efecto diagonal, $(A_i, X_i, G_i(\overline{Y})) = (A_i, Y_i, G_i(\overline{Y}))$). Así, un mazo de cartas inicial X_i sólo puede llevar a conocimientos finales sobre mundos donde el agente tiene ese mismo mazo de cartas iniciales. Un ejemplo de las consecuencias de este teorema se puede encontrar en la figura 6.5.

Así, ya es posible definir el modelo de topología combinatoria para el muy generalizado problema de las cartas rusas:

Definición 6.3.1 (Modelos de topología combinatoria para problemas de cartas rusas)

Dado el modelo inicial para cartas rusas $\mathcal{I}$ y la tarea $\mathcal{T}$ definida previamente, el modelo de topología combinatoria es el siguiente efecto $\mathcal{I}[\mathcal{T}] =< I[T], \chi, l >$:

- $V(I[T]) = \{(A_i, X_i, G_i(\overline{Y}))|X_i = Y_i\}$.
- $F(I[T]) = \bigcup_{\overline{X}\in S}\{\{(A_1, X_1, G_1(\overline{X})), \ldots, (A_n, X_n, G_n(\overline{X}))\}\}$.
- $\chi = \pi_1$.
- $l(A_i, X_i, G_i(\overline{Y})) = p_{A_i,X_i}$.

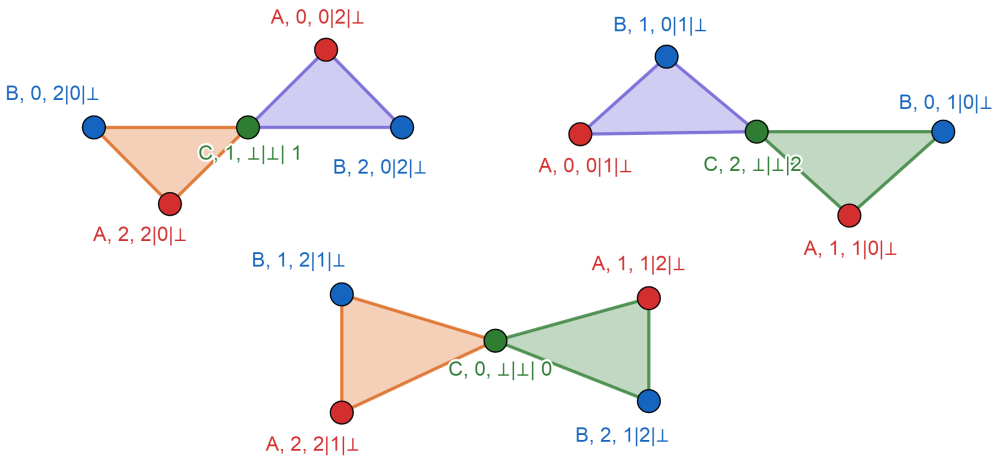

Figura 6.6: Modelo de topología combinatoria para el caso $(1, 1, 1)$. ¿Por qué es isomorfo a la tarea?.

Esta definición permite percatarse de que los conocimientos finales tienen una fuerte dependencia con los conocimientos iniciales: para el agente A_i, la i-ésima entrada de su conocimiento final siempre es igual a su conocimiento inicial. ¿Ello podría significar que la tarea es isomorfa al modelo de topología combinatoria?, de ser así, sería posible economizar todavía más la notación. Las figuras 6.6 y 6.7 hacen pensar que sí sucede, lo que motiva al enunciado del siguiente teorema:

Teorema 6.3.1 *Para todo posible problema de cartas rusas, el complejo simplicial subyacente de su modelo de topología combinatoria es isomorfo al complejo simplicial subyacente de su tarea, es decir, $I[T] \cong T$.*

Demostración. El isomorfismo entre complejos simpliciales se define como la existencia de un mapeo simplicial cromático y biyectivo δ cuya función inversa sea también un mapeo simplicial cromático. Se propone el siguiente mapeo $\delta : V(I[T]) \to V(T)$ definido como:

$$\delta((A_i, X_i, G_i(\overline{X}))) = (A_i, G_i(\overline{X}))$$

Por lo que sólo hace falta demostrar que es mapeo simplicial cromático, biyectivo y que su inversa es también mapeo simplicial cromático.

Para probar que es un mapeo simplicial, basta tomarse un simplejo $s = \{(A_{i_1}, X_{i_1}, G_{i_1}(\overline{X})), \ldots, (A_{i_k}, X_{i_k}, G_{i_k}(\overline{X}))\}$ de $I[T]$, entonces se cumple que:

$$\begin{aligned}\delta[s] &= \{\delta((A_{i_1}, X_{i_1}, G_{i_1}(\overline{X}))), \ldots, \delta((A_{i_k}, X_{i_k}, G_{i_k}(\overline{X})))\} \\ &= \{(A_{i_1}, G_{i_1}(\overline{X})), \ldots, (A_{i_k}, G_{i_k}(\overline{X}))\}\end{aligned}$$

Lo que es un simplejo de T al estar contenido en la faceta $\{(A_1, G_1(\overline{X})), \ldots, (A_n, G_n(\overline{X}))\}$

Ahora bien, es inmediato percatarse de que es cromático ya que:

$$\chi((A_i, X_i, G_i(\overline{X}))) = A_i = \chi((A_i, G_i(\overline{X})))$$

A continuación, se prueba que es una función biyectiva:

Para la inyectividad, basta tomar dos vértices $(A_i, X_i, G_i(\overline{X})), (A_j, Y_j, G_j(\overline{Y})) \in V(I[T])$ tales que $\delta((A_i, X_i, G_i(\overline{X}))) = \delta((A_j, Y_j, G_j(\overline{Y})))$. Entonces $(A_i, G_i(\overline{X})) = (A_j, G_j(\overline{Y}))$ por lo que $A_i = A_j$ y $G_i(\overline{X}) = G_i(\overline{Y})$. Así, $i = j$ y dado que la i-ésima coordenada de $G_i(\overline{X})$ y $G_i(\overline{Y})$ es X_i y Y_i respectivamente, $X_i = Y_i$ por lo que $(A_i, X_i, G_i(\overline{X})) = (A_j, Y_j, G_j(\overline{Y}))$

Para la suprayectividad, sea $(A_i, G_i(\overline{X})) \in V(T)$, entonces $\delta((A_i, X_i, G_i(\overline{X}))) = (A_i, G_i(\overline{X}))$.

Por último, para ver que δ^{-1} (definida como $\delta^{-1}((A_i, G_i(\overline{X}))) = (A_i, X_i, G_i(\overline{X}))$) es un mapeo simplicial cromático, sea $s = \{(A_{i_1}, G_{i_1}(\overline{X})), \ldots, (A_{i_k}, G_{i_k}(\overline{X}))\}$ un simplejo de T, entonces: [2]

$$\begin{aligned}(\delta^{-1})[s] &= \{\delta^{-1}((A_{i_1}, G_{i_1}(\overline{X}))), \ldots, \delta^{-1}((A_{i_k}, G_{i_k}(\overline{X})))\} \\ &= \{(A_{i_1}, X_{i_1}, G_{i_1}(\overline{X})), \ldots, (A_{i_k}, X_{i_k}, G_{i_k}(\overline{X}))\}\end{aligned}$$

Lo que es un simplejo de $I[T]$. La prueba de que es cromático es análoga a la de δ. ■

Este isomorfismo no debe interpretarse como que en ambos modelos se tienen las mismas verdades (principalmente porque las precondiciones de la tarea no son un etiquetado del mismo tipo que la valuación del modelo de topología combinatoria). Más bien, su principal utilidad radica en que facilita sobremanera el diseño visual, ya que basta con obtener la tarea para saber cómo se verá el efecto.

Con esto se han alcanzado los objetivos de la presente tesis, sin embargo todavía

[2]La imagen directa $(\delta^{-1})[s]$ no debe confundirse con la imagen inversa $\delta^{-1}[s]$.

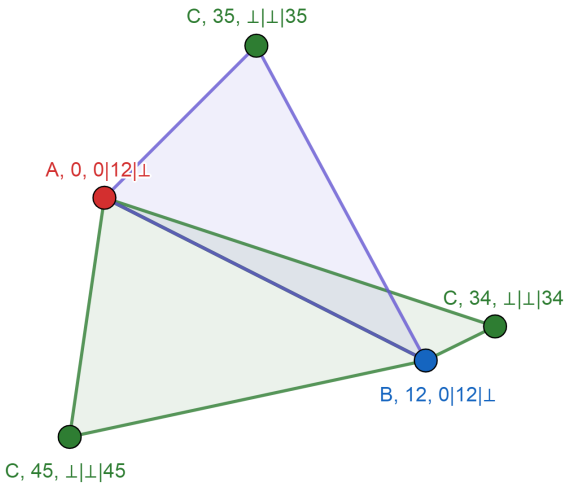

Figura 6.7: Modelo de topología combinatoria para el caso $(1, 2, 2)$ cuando sobra una carta, centrado en las adyacencias del vértice $(B, 12, 0|12|\perp)$. Aprovechando que la tarea es isomorfa al modelo de topología combinatoria, se hizo este diseño con bastante rapidez.

quedan un par de detalles a discutir: se han tomado ciertas licencias en el diseño de la tarea como poner que los espías conocen todas sus cartas aunque pueda ser imposible o aunque ese conocimiento conlleve a que adivinen el paradero de cartas de no-espías (como en el ejemplo con un sólo no-espía). Más aún, ¡falta corroborar que el *muy generalizado problema* realmente generaliza al problema original!. En el siguiente capítulo se hace todo eso utilizando el lenguaje básico modal.

Capítulo 7

Legitimidad del modelo como representación fiel del problema.

El problema es clarísimo en su planteamiento: el espía no debe conocer ninguna carta de los no-espías, y estos deben conocer sus cartas entre sí. Estas condiciones epistémicas no son un tema nuevo y han sido previamente planteadas en el artículo [14] para el caso con tres agentes:[1]

- a_knows_bs = $\bigwedge_{n=0}^{d-1} K_A(n_B \vee \neg n_B)$.
- b_knows_as = $\bigwedge_{n=0}^{d-1} K_B(n_A \vee \neg n_A)$.
- c_ignorant = $\bigwedge_{n=0}^{d-1} \neg K_C(n_A) \wedge \neg K_C(n_B)$.

Donde $d = a + b + c$ es el tamaño del mazo de cartas, $n_Q := p_{Q,n}$ y se dice que los agentes han resuelto el problema si, tras un intercambio de anuncios públicos que les haga evolucionar su conocimiento, al final es cierto que a_knows_bs, b_knows_as y c_ignorant. Esta propuesta es legítima ya que la proposición $p_{q,x} \vee \neg p_{q,x}$ literalmente significa "el agente q tiene o no tiene la carta x" por lo que $K_A(p_{q,x} \vee \neg p_{q,x})$ significa que el agente A conoce si la carta x está o no en manos de q, de manera que a_knows_bs significa que *Ana* conoce el paradero de todas las cartas de *Blas* mientras que b_knows_as significa que *Blas* conoce el paradero de todas las cartas de *Ana*. Finalmente c_ignorant significa que, para toda carta del mazo, *Cruz* no sabe que *Ana* tiene la carta ni tampoco que *Blas* la tiene.

A continuación se proponen las siguientes generalizaciones de estas premisas tipo *knows* e *ignorant* para el *muy generalizado problema*:[2]

- i_sabe_j = $\bigwedge_{x \in cards} K_i(p_{j,x} \vee \neg p_{j,x})$.

[1] Puede parecer extraña la elección de nombres del estilo de "a_knows_bs". La razón es que corresponden a la idiosincracia de los comandos del lenguaje Haskell ya que se diseñaron para ser verificados por un programa en dicho lenguaje. El código fuente completo puede encontrarse en [14].

[2] En este trabajo se seguirá una idiosincracia *parecida* al lenguaje Haskell para mantener cierta consistencia con [14].

- i_ignorant$(\mathbf{P}) = \bigwedge_{x \in cards} \bigwedge_{A_j \in \mathbf{P}} \neg K_i(p_{x,j})$.

Donde $1 \leq i, j \leq n$ y $\mathbf{E}$ es el conjunto de espías y $\mathbf{P} = \mathbf{A} - \mathbf{E}$.

i_sabe_j significa de que, para toda $x \in \mathbb{N}$, A_i sabe si A_j tiene la carta x o no. i_ignorant$(\mathbf{P})$ es una generalización de c_ignorant pero para conjuntos completos de agentes.

A continuación se demuestra que estas propuestas son generalizaciones legítimas del caso de tres agentes, cero cartas residuales y un único espía, por lo que el enunciado inédito planteado aquí realmente generaliza al problema de las cartas rusas.

Teorema 7.0.1
Si $\mathbf{A} = \{A_1, A_2, A_3\}$ *y* $\mathbf{E} = \{A_3\}$ *entonces para* $A = A_1$, $B = A_2$ *Y* $C = A_3$ *se tiene que:*

1. 1_*sabe*_2 *si y solo si a_knows_bs.*
2. 2_*sabe*_1 *si y solo si b_knows_as.*
3. 3_*ignorant*$(\{A_1, A_2\})$*si y solo si c_ignorant.*

Demostración.
La prueba sale de notar que son iguales.

Prueba de 1 y 2:

Hay que tener en cuenta que $cards = I_d = \{0, \ldots, d-1\}$ es el conjunto de los primeros d naturales. Así,

$$\begin{aligned} 1\_\text{sabe}\_2 &= \textstyle\bigwedge_{x \in cards} K_1(p_{x,2} \vee \neg p_{x,2}) \\ &= \textstyle\bigwedge_{x \in cards} K_A(p_{x,B} \vee \neg p_{x,B}) \\ &= \textstyle\bigwedge_{x=0}^{d-1} K_A(p_{x,B} \vee \neg p_{x,B}) \\ &= a\_\text{knows}\_bs. \end{aligned}$$

Análogamente para 2_sabe_1

Prueba de 3:

$$\begin{aligned} 3\_\text{ignorant}(\{A_1, A_2\}) &= \textstyle\bigwedge_{x \in cards} \bigwedge_{A_j \in \{A_1, A_2\}} \neg K_3(p_{x,j}) \\ &= \textstyle\bigwedge_{x \in cards} \neg K_3(p_{x,1}) \wedge \neg K_3(p_{x,2}) \\ &= \textstyle\bigwedge_{x \in cards} \neg K_C(p_{x,A}) \wedge \neg K_C(p_{x,B}) \quad \blacksquare \\ &= \textstyle\bigwedge_{x=0}^{d-1} \neg K_C(p_{x,A}) \wedge \neg K_C(p_{x,B}) \\ &= c\_\text{ignorant}. \end{aligned}$$

Finalmente se generalizan las condiciones de haber resuelto el problema a_knows_bs, b_knows_as y C_ignorant a que todo no-espía A_i conozca las cartas de los demás agentes de su tipo mientras que los espías las ignoren por completo, es decir,

$(\bigwedge_{A_i \in \mathbf{P}} \bigwedge_{A_j \in \mathbf{P}} i\_\text{sabe}\_j) \wedge (\bigwedge_{A_k \in \mathbf{E}} k\_\text{ignorant}(\mathbf{P}))$.

Dado un intercambio de anuncios públicos y su modelo de acción asociado, basta con probar que todas sus facetas modelan estas condiciones de término para concluir que el problema se ha resuelto. Así, para demostrar que la tarea definida en el capítulo anterior realmente representa la solución del problema, se probará que sus facetas modelan estas condiciones de término, lo que traerá como consecuencia que todos los "*peros*" y objeciones planteadas al final del capítulo anterior se tornen completamente irrelevantes.

Teorema 7.0.2 (Legitimidad de la tarea)
$\forall f \in F(I[T]), \mathcal{I}[\mathcal{T}], f \models (\bigwedge_{A_i \in \mathbf{P}} \bigwedge_{A_j \in \mathbf{P}} i\_sabe\_j) \wedge (\bigwedge_{A_k \in \mathbf{E}} k\_ignorant(\mathbf{P}))$.

Demostración.
Para demostrar que para todo $A_i \in \mathbf{P}$, $\mathcal{I}[\mathcal{T}], f \models \bigwedge_{A_j \in \mathbf{P}} i\_\text{sabe}\_j$, se tomarán en primer lugar a dos no-espías $A_i, A_j \in \mathbf{P}$. Así, basta con demostrar que $\mathcal{I}[\mathcal{T}], f \models i\_\text{sabe}\_j$.

Sea $x \in cards$ y sea $g \in F(\mathcal{I}[\mathcal{T}])$ tal que comparte con f el vértice de A_i (es decir, $A_i \in \chi(f \cap g)$). Basta probar que $\mathcal{I}[\mathcal{T}], f \models p_{j,x} \vee \neg p_{j,x}$ pues hay que recordar que A_i sabe algo en el mundo f si ese tal algo es cierto en todos los mundos g entre los que A_i no puede distinguir.

Nótese ahora que estas proposiciones del tipo *ignorant* y *knows* son *"muy trampo-sas"* desde su concepción ya que la proposición $p_{j,x} \vee \neg p_{j,x}$ es siempre una tautología puesto que equivale a $(\neg p_{j,x} \wedge p_{j,x})$, lo que es la negación de una contradicción ya que si $\mathcal{I}[\mathcal{T}], f \models \neg p_{j,x} \wedge p_{j,x}$ entonces $p_{j,x} \in l[f]$ y $p_{j,x} \notin l[f]$, lo que contradice al axioma de extensionalidad de Zermelo-Fraenkel.[3]

Así, $\mathcal{I}[\mathcal{T}], g \models p_{j,x} \vee \neg p_{j,x}$ por lo que $\mathcal{I}[\mathcal{T}], f \models K_{A_i}(p_{j,x} \vee \neg p_{j,x})$.

Finalmente, para demostrar que todo $A_k \in \mathbf{E}$ satisface que $\mathcal{I}[\mathcal{T}], f \models k\_\text{ignorant}(\mathbf{P})$, basta con tomar $x \in cards$ y $A_j \in \mathbf{P}$, y demostrar que $\mathcal{I}[\mathcal{T}], f \models \neg K_k(p_{x,j})$.

En efecto, dados $x \in cards$ y $A_j \in \mathbf{P}$, es suficiente con probar que existe un mundo $g \in F(I[T])$ indistinguible para A_k tal que es falso que $p_{x,j}$.

CASO 1: En el mundo $\overline{X}$ asociado a f, A_j no tiene la carta x. Entonces basta con hacer $f = g$.

CASO 2: En el mundo $\overline{X}$ asociado a f, A_j sí tiene la carta x. En este caso, el mundo $\overline{Y}$ asociado a g puede construirse con el siguiente procedimiento:

1. Dado el mundo $\overline{X}$ asociado a f, considérense dos no-espías A_i y A_j.
2. Tómese $w \in X_j$.

[3]Se sabe que $l[g] \subseteq l[g]$ por lo que $\forall y(y \in l[g] \rightarrow y \in l[g])$, pero literalmente se llegó a la negación de esto.

3. Se define el mundo $\overline{Y}$ como $Y_n = X_n$ siempre que $n \neq i, j$, $Y_i = X_i - \{x\} \cup \{w\}$ y $Y_j = X_j - \{w\} \cup \{x\}$.

Como $i \neq k \neq j$, se tiene que $X_k = Y_k$. Más aún, dado que la única diferencia entre $\overline{X}$ y $\overline{Y}$ sucede en manos de no-espías, y estas corresponden a símbolos $\perp$ en E_k, se tiene que $(A_k, X_k, E_k(\overline{X})) = (A_k, Y_k, E_k(\overline{Y}))$ por lo que la faceta g asociada a $\overline{Y}$ comparte vértice de A_k con la faceta f, y además $\mathcal{I}[\mathcal{T}], g \models \neg p_{i,x}$ por construcción.

Para el caso donde hay un único no-espía, si hubieran cartas sin repartir podría hacerse el intercambio entre x y w con las cartas no repartidas. Si, por otro lado, no hubieran cartas sin repartir, entonces el problema está resuelto *a priori* y no hay necesidad de considerar una tarea ya que desde el principio el único no-espía ya conoce las cartas de los otros no-espías (osea él). Peor aún, los espías podrían intercambiar sus cartas entre ellos y, tomando el complemento, encontrar la mano del no-espía sin que este pueda hacer nada para evitarlo.

Discutir esta última problemática es importante, pero es motivada una vez ha sido construido el modelo de topología combinatoria por lo que ahondar más al respecto trasciende los intereses de la presente tesis. Lo único que se dirá aquí es que en ese caso el problema no puede solucionarse debido a lo comentado en el párrafo anterior. ■

Capítulo 8

Conclusiones

Gracias a este trabajo, estudiar posibles soluciones para el problema de las cartas rusas se reduce a definir un modelo de acción que represente dicha solución, y luego rectificar si resuelve la tarea.

El conocimiento que los agentes puedan tener en un problema de cartas rusas ha sido definido con precisión como que un agente conoce una fórmula si y solo si esa fórmula es cierta en todos sus mundos indistinguibles, es decir, que un agente sabe que otro tiene una carta si y solo si la tiene en todos los mundos entre los que no puede distinguir.

La indistinguibilidad fue definida en términos de los mundos para determinar sin lugar a ambigüedades la incertidumbre de los agentes involucrados en el problema, y visualmente corresponde a la propiedad de conexidad de que dos facetas inciden en un mismo vértice.

Así, el que *Ana* conoce la mano de *Blas* pero que *Cruz* la ignora significa que *Ana* y *Blas* carecen de indistinguiblidad entre ellos (es decir, cada vértice asociado a *Ana* es a lo más adyacente a un único vértice de *Blas*) mientras que *Cruz* sí la tiene.

Si bien a lo largo de este texto no se sacrificó en formalidad ni precisión, sí que se prescindió de toda la cuestión computacional intrínseca en las motivaciones de cada unas de las definiciones. Por ejemplo un modelo de acción está pensado para describir un *algoritmo o protocolo de un sistema distribuido*, mientras que la noción de resolver la tarea corresponde al concepto de *solublidad* (palabra que ni siquiera existe en español como tal). Los involucrados en un problema no suelen ser personas, sino más bien *procesos* que deben ser ejecutados en un programa. Finalmente las proposiciones atómicas de los conjuntos AP son tales que $p_{i,j}$ equivale a *el proceso i tiene asignado el valor j*.

Futuras investigaciones pueden orientarse a analizar propuestas conocidas de soluciones como las presentadas en [14, 5, 7], estudiar otras variantes del problema como la posibilidad de que los anuncios de los agentes no lleguen siempre a su destino (en un modelo del tipo *libre de espera*, muy estudiados en computación distribuida), ahondar en soluciones para casos con más de tres agentes, o incluso buscar un *meta-protocolo* que

resuelva la mayor cantidad de casos posibles.

Por último, esperamos que este pequeño proyecto impulse el bonito enfoque de la topología combinatoria para abordar problemas de conocimiento y que, en general, se extienda hacia el estudio generalizado de protocolos de criptografía, ya que todos ellos son de esta especie.

Gracias por leer.

Bibliografía

[1] Chomsky, N. Three models for the description of language. *IRE Transactions on Information Theory*, Vol. 2 (1956), 113–124.

[2] Chomsky, N. *Syntactic Structures*, 1 ed. Mouton CO., 1957.

[3] Cordon-Franco, A., van Ditmarsch, H., Fernandez-Duque, D., Joosten, J. J., and Soler-Toscano, F. A secure additive protocol for card players. *Australas J. Combin*, 54 (2012), 163–175.

[4] Enderton, H. *A mathematical introduction to logic*, 1 ed. Boston Academic Press, 1972.

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

[6] Goubault, E., Ledent, J., and Rajsbaum, S. A simplicial complex model for dynamic epistemic logic to study distributed task computability. *Proceedings Ninth International Symposium on Games, Automata, Logics, and Formal Verification, GandALF 2018, Saarbrücken, Germany, 26-28th September 2018.* (2018), 73–87.

[7] Kirkman, T. On a problem in combinations. *Cambridge an Dublin Math journal*, 2 (1847), 191–204.

[8] Makarychev, Y. S., and Makarychev., K. S. The importance of being formal. *Springer-Verlag New York*, 23.1 (2001), 41–42.

[9] Martin, J. C. *Introduction to languages and the theory of computation*, 4 ed. Mc Graw Hill, 2011.

[10] Munkres, J. *Elements of Algebraic Topology*, 2 ed. Addison-Wesley Publishing Company, 1984.

[11] Rajsbaum, S., Herlihy, M., and Kozlov., D. *Distributed Computing Through Combinatorial Topology*, 1 ed. Elsevier, 2013.

[12] S., K. A semantic analysis of modal logic. *Zeitschr. f. math. Logik und Grundlagen d. Math*, 9 (1963), 67–96.

[13] Sisper, M. *Introduction of the Theory of Computation*, 2 ed. Thomson, 2006.

[14] Soler-Toscano, F., and van Ditmarsch., H. Three steps. *Conference paper* (2011).

[15] v. Ditmarsch, H., Goubault, E., Ledent, J., and Rajsbaum, S. Knowledge and simplicial complexes. *CoRR abs/2002.08863* (2020).

[16] van Ditmarsch, H. The russian cards problem. *Studia Logica*, 75 (2003), 31–62.

[17] y H. Rincón y C. Rincón, A. B. *Álgebra Superior*, 1 ed. 3 reimp. ed. Las Prensas de Ciencias, 2013.

[18] y U. Murty, J. B. *Graph Theory*, 1 ed. Springer, 2008.

Parte III

Apéndices

Apéndice A

Forma de Backus-Naur y lenguajes formales.

En este apartado se define lo que es una gramática formal y la forma Backus-Naur. Por último se explica la gramática básica modal dada en el capítulo 1.

Las gramáticas formales fueron introducidas por Noam Chomsky en la década de los 50's como una forma de determinar todas las palabras de un lenguaje en términos relativamente sencillos e intuitivos.

Definición A.0.1 (Clausura de Kleene)
Sea Σ un conjunto finito de símbolos indivisibles denominado alfabeto*. Dada la operación de concatenación que junta cualesquiera letras $a_1, \ldots, a_n \in \Sigma$ en la palabra $a_1 \ldots a_n$, la clausura de Kleene se define como el operador unario:*

$$\Sigma^* := \bigcup_{n \in \mathbb{N}} \{a_1 \ldots a_n | a_i \in \Sigma\}$$

Definición A.0.2 (Gramática formal)
Una gramática formal es una cuarteta $G = (N, \Sigma, S, P)$ tal que:

- *N y Σ son conjuntos finitos de símbolos indivisibles tal que $N \cap \Sigma = \emptyset$. Los elementos de N se denotan con mayúsculas y se denominan* símbolos no-terminales*, y los elementos de Σ se denotan con minúsculas y se denominan* símbolos terminales*.*
- *$S \in N$ es una variable distinguida llamada* símbolo inicial*.*
- *$P \subseteq \{(\alpha, \beta) | \alpha \in (N \cup \Sigma)^* - \Sigma^*, \beta \in (N \cup \Sigma)^*\}$ es una familia de pares ordenados denominados* reglas de reescritura *o* de producción*, y cada $(\alpha, \beta) \in P$ se denota como $\alpha \to \beta$, diciendo que "α produce β".*

Las gramáticas se clasifican en términos de la jerarquía de Chomsky. El lector interesado en el tema puede consultar las referencias dadas en las notas finales del apéndice.

Podría haber el caso en el que hubieran varias reglas de producción con la misma primera coordenada. En esos casos se denotan, para $(\alpha, \beta_1), \ldots, (\alpha, \beta_n) \in P$, $\alpha \to \beta_1|\beta_2|\ldots|\beta_n$ lo que se lee como que "α produce β_1, o produce β_2, o ..., o produce β_n". La barra vertical debe interpretarse como un símbolo de disyunción.

Definición A.0.3 (Lenguaje generado)
Dada una gramática $G = (N, \Sigma, S, P)$, se define lo siguiente:

- *La derivación formal de una palabra $v \in (N \cup \Sigma)^*$ a partir de $w \in (N \cup \Sigma)^*$ en un paso como la existencia de una regla de producción $\alpha \to \beta \in P$ y de palabras $\gamma_1, \gamma_2 \in (N \cup \Sigma)^*$ tal que $w = \gamma_1\alpha\gamma_2$ y $v = \gamma_1\beta\gamma_2$. Lo que se denota como $w \Rightarrow v$.*
- *Una cadena v es* derivable *a partir de la cadena w si existen palabras $\gamma_1, \ldots, \gamma_n$ tal que $w = \gamma_1 \Rightarrow \cdots \Rightarrow \gamma_n = v$, lo que se denota como $w \Rightarrow^* v$.*
- *Se define el lenguaje generado por la gramática G como*

$$L(G) = \{w \in \Sigma^* | S \Rightarrow^* w\}$$

Finalmente, la forma Backus-Naur es una forma de denotar cierto tipo de gramáticas (las que son libres de contexto en la jerarquía de Chomsky) y se define como sigue:

Definición A.0.4 (Forma Backus-Naur)
Dada una gramática $G = (N, \Sigma, S, P)$. Su notación en la forma Backus-Naur es como sigue:

- *Para cada $< expr > \in N$, si $(< expr >, \beta) \in P$ entonces se denota $< expr > ::= \beta$, lo que se lee como "la expresión $< expr >$ consiste en β" y si $\beta \in (N \cup \Sigma)^*$ es una expresión compuesta $\beta = a_1 \ldots a_n$ entonces es "la expresión $< expr >$ consiste en a_1 seguido de a_2 ... finalizando con a_n".*
- *Si hay $(< expr >, \beta_1), \ldots, (< expr >, \beta_n) \in P$ entonces se denota $< expr > ::= \beta_1|\ldots|\beta_n$, lo que se lee como "la expresión $< expr >$ consiste en β_1 o consiste en β_2 o $\ldots$ o consiste en β_n".*

Es claro que no toda gramática puede expresarse en la forma Backus-Naur ya que es necesario que todas sus reglas de derivación tengan a la izquierda un único símbolo no terminal.[1]

Por último se estudia el lenguaje básico modal. Recordando que su forma de Backus-Naur es:

$$\phi ::= p \mid \neg\phi \mid (\phi \wedge \phi) \mid K_q(\phi)$$

Se tiene que su gramática $G = (N, \Sigma, S, P)$ es tal que:

[1]Quizá una gramática carezca de esto, pero puede hallarse otra equivalente que genere el mismo lenguaje que sí lo satisfaga. A este tipo de gramáticas se les conoce como *libres de contexto*.

- $N = \{S\} := \{\phi\}$. Y sólo se tiene un único símbolo no terminal $S = \phi$.
- $\Sigma = \{\wedge,), (, \neg\} \cup \{K_q | q \in \mathbf{A}\} \cup AP$.
- $P = \{(\phi, p) | p \in AP\} \cup \{(\phi, \neg\phi), (\phi, (\phi \wedge \phi))\} \cup \{(\phi, K_q(\phi)) | q \in \mathbf{A}\}$.

Re-denotada, $G = (\{\phi\}, \Sigma, \phi, P)$. Finalmente el lenguaje básico modal se define formalmente como $\mathcal{L}_K := L(G)$.

Por último, en este caso Σ es un conjunto de conectivos lógicos y variables proposicionales a la usanza de la lógica de primer orden, la cual puede estudiarse extensamente en [4].

A.1. Notas finales del apéndice.

Noam Chomsky introdujo las gramáticas formales en [1, 2]. Posteriormente John Backus propuso un metalenguaje que a la postre se convertiría en la forma Backus-Naur que actualmente está muy extendida.

Buenas referencias para profundizar en el estudio de gramáticas y en la jerarquía de Chomsky son los libros [13, 9] donde el lector puede empaparse de contexto al ubicar el tema en términos de máquinas de Turing, lenguajes de programación y compiladores. En mismos libros el lector puede estudiar más a fondo los operadores sobre alfabetos como la clausura de Kleene y la concatenación.