Notas de Lógica Matemática I

David Meza Alcántara

Facultad de Ciencias, UNAM
Email address: dmeza@ciencias.unam.mx

Resumen. Las presentes notas de clase corresponden al curso de Lógica Matemática I impartido por el autor durante el semestre 2021-1 en la Facultad de Ciencias UNAM. El tema principal es la Lógica Proposicional Clásica, sin embargo se inicia con una discusión sobre el carácter de la Lógica Matemática en general.

El curso está pensado para estudiantes de semestres intermedios de la Licenciatura en Matemáticas, que han superado los primeros semestres de la carrera, se han empapado con la metodología y han adquirido cierta madurez matemática.

Índice general

Motivación 5

Introducción 7

Capítulo 1. Lógica Proposicional 9
1. Lenguajes Proposicionales 11
2. Semantica de la Lógica Proposicional 15
3. Teoría de la prueba de la Lógica Proposicional 40

Capítulo 2. Lógica de Predicados 51
1. Estructuras de Primer Orden 51
2. Lenguajes de Primer Orden 53
3. Semántica de la lógica de primer orden 56
4. Aritmética de Peano de primer orden 67
5. Compacidad de la lógica de primer orden 70

Motivación

Popularmente se conoce a la *lógica* como el arte de razonar correctamente, y se le incluye en el campo de la filosofía. En la actualidad la lógica es un área de estudio de gran amplitud, que llega incluso hasta las ciencias de la computación. Por *lógica matemática* entendemos la fundamentación de algunas formas de lógica en términos matemáticos. Los lenguajes, sus interpretaciones, las formulaciones bien formadas, las demostraciones, los teoremas, las teorías, se convierten en objetos matemáticos naturales, y con esto se puede hacer teoría sobre estos, es decir, se puede reflexionar organizadamente y hacer teoremas como en cualquier otro ámbito matemático. Los métodos comúnmente empleados por los matemáticos encuentran un campo de acción en la lógica. Algunas discusiones filosóficas se resuelven finalmente, de manera matemática: una polémica puede ser finiquitada en la forma de un teorema matemático.

Por el contrario, las matemáticas se fundamentan en la lógica de dos modos distintos: el modus operandi del matemático requiere que sus resultados se apeguen estrictamente a formas de razonamiento aceptadas comúnmente. La lógica es el árbitro que vigila que los razonamientos sean correctos. Por otro lado, la Teoría de Modelos es la constancia de lo fructífero que resulta hacer énfasis en el lenguaje en el quehacer matemático.

El curso de Lógica Matemática I se dedica al estudio de una forma de lógica particularmente relevante, la *Lógica Proposicional*, la cual se ocupa de evaluar la veracidad de una fórmula en función de los conectivos involucrados en ella. Si bien, la lógica proposicional tiene un alcance muy limitado en cuanto a su papel descriptivo de las formas correctas de razonamiento, por el contrario tiene una sencillez y belleza deslumbrantes. Su estudio es conveniente porque de modo sencillo revela los métodos usuales y los alcances de sus resultados. El presente curso, estudiaremos primordialmente la lógica proposicional *clásica*, aunque también se inspeccionan algunas lógicas no-clásicas, como la intuicionista y la paraconsistente. Nuestra presentación de la lógica proposicional clásica servirá como el *ejemplo canónico de un sistema*

de lógica, por lo que haremos énfasis en que en general las presentaciones de otros sistemas de lógica son análogos a esta, por lo que en general las propiedades de la lógica proposicional clásica se comparan con las de otros sistemas de lógica en un terreno común.

Introducción

Siguiendo la definición popular de lógica, (Lógica = el arte de razonar correctamente) podemos establecer las aspiraciones que un sistema lógico debe tener. En primer lugar, debe estar bien establecido qué *frases, afirmaciones, enunciados, fórmulas* están suficientemente bien formuladas como para ser calificadas como verdaderas o falsas. Con este fin, en primer lugar se establece un lenguaje y se definen las fórmulas de este lenguaje, con la intención de que estas eventualmente sean calificables por su valor de verdad. Por ejemplo, "hola", es una frase que tiene un significado en el español, pero que no puede ser calificada en cuanto a su veracidad. Sin embargo "toda función complipausada en un intervalo cerrado es acomentosa", sí puede ser calificada, naturalmente su veracidad dependerá de qué se entienda por "función complipausada", "intervalo cerrado" y "función acomentosa".

Algunas veces, una frase puede ser verdadera por su estructura lógica más que por su contenido. Por estructura lógica se entiende la disposición de las partículas simbólicas que componen tal frase. A manera de ejemplo considere la siguiente frase:

Si toda función continua en un intervalo cerrado alcanza valores máximo y mínimo, y la función seno es continua en el intervalo cerrado [0,1], entonces la función seno alcanza valores máximo y mínimo en [0,1].

Tal frase es verdadera independientemente de lo que entendamos por función continua, intervalo cerrado, función seno, alcanzar máximo y mínimo, pues al reemplazar estos términos, por cualesquiera otros, debemos aceptar su verdad. Para tal efecto podemos simbolizar la frase anterior de la siguiente manera:

Si para cualesquiera f *e* I, $\mathcal{C}(f, I)$ *implica* $M(f, I)$, *y* $\mathcal{C}(sen, [0, 1])$ *entonces* $M(sen, [0, 1])$.

donde

$\mathcal{C}(f, I)$ significa "f es continua en el intervalo I"
$M(f, I)$ significa "f alcanza sus valores máximo y mínimo en I"
sen representa a la función seno

$[0, 1]$ representa al intevalo $[0, 1]$.

Intente el lector reinterpretar estos términos y convénzase de aceptar la verdad de lo que resulte. Las lógicas que estudiaremos, intentarán caracterizar estas estructuras simbólicas que bajo cualquier interpretación resultan ser verdaderas.

Otro aspecto a estudiar será la noción de consecuencia lógica, tan presente en la vida del matemático. Los matemáticos estamos acostumbrados a *demostrar teoremas* en diferentes contextos. En términos precisos ¿qué es un teorema? ¿qué significa demostrar? Formalizaremos matemáticamente estas dos cuestiones, por un lado el enfoque sintáctico, en el que la noción de consecuencia lógica viene establecida por rigurosas reglas de manipulación de símbolos; y el enfoque semántico, que apela a la interpretación de esos símbolos. Se revisarán las demostraciones de teoremas clásicos como el de completud - correctud y el de compacidad en ambas lógicas, y además se ejemplificarán algunas de sus aplicaciones. Adicionalmente, en la parte de lógica de predicados estudiaremos los teoremas y las construcciones básicas de la Teoría de Modelos. Finalmente analizaremos varias teorías matemáticas populares a la luz de lo aprendido en el curso.

Capítulo 1

Lógica Proposicional

La lógica proposicional se ocupa de la verdad de fórmulas o validez de razonamientos cuando esta depende de la disposición de los *conectivos* involucrados. Un conectivo lógico es una palabra o conjunto de estas que vincula frases con el fin de construir nuevas frases. Considere la siguiente frase como ejemplo:

(*) *Llueve y hace frío*

La palabra "y" vincula las frases "Llueve" y "hace frío". El valor de verdad de (*) depende de los valores de verdad de las frases conectadas: si ambas son verdaderas entonces (*) será verdadera. Si una falla entonces (*) falla. Si vinculamos estas dos frases con otro conectivo, el significado cambia. Considere:

(**) *Llueve o hace frío*

El valor de verdad de (**) ahora se calcula de otro modo, pues para ser verdadera es suficiente con que una de las dos partículas lo sea. En conclusión, los conectivos lógicos vincularán frases y dotarán de sentido a una frase compuesta, en función del mismo conectivo y del valor de verdad de las subfrases conectadas.

A partir de ahora nos daremos el lujo de introducir una técnica usual en matemáticas: usar variables. Las letras P, Q, R,... representarán frases cualesquiera, es decir, actuarán como variables que recorren el dominio de *las frases en español suceptibles de ser calificadas como verdaderas o falsas*.

Los conectivos más usuales en el español son:

- La *conjunción*, cuya más frecuente forma es a través de la palabra "y". De este modo, "P y Q" es verdadera exactamente en el caso en que ambas, "P" y "Q" lo sean.
- La *disyunción*, cuya forma más frecuente es en la palabra "o". Así, la frase "P o Q" es verdadera exactamente en el caso en el que al menos una de las dos, "P" o "Q", lo sea. Esto claramente incluye el caso en el que ambas lo son.

- La *negación*, cuya forma más frecuente es la palabra "no", y que no conecta pares de frases, sino frases individuales. "no P" es verdadera exactamente en el caso en el que "P" es falsa.
- El *condicional*, cuya forma más usual es "Si P entonces Q", y que es verdadera cuando al ser "P" verdadera, "Q" también lo es. Probablemente el lector quede insatisfecho con esta definición, para lo cual se debe aclarar que cuando "P" es falsa, la implicación es verdadera, debido a que nuestra noción de implicación en *material*: la conclusión está comprometida sólo en el caso en el que el antecedente es verdadero.
- El *bicondicional*, cuya forma más usual es "P si y sólo si Q", que es verdadera cuando los valores de verdad de "P" y "Q" coinciden en todos los casos. Esto es, cuando no se dá el caso que "P" y "Q" tomen valores de verdad diferentes.

En el español existen muchos otros que se pueden definir en términos de los anteriores. Por ejemplo, "P a menos que Q", significa lo mismo que "si no Q entonces P".

Ejercicios 1. Para los siguientes conectivos del español, encuentre una traducción en términos de conjunciones, negaciones, disyunciones y condicionales.

1. P sin que Q
2. P a pesar de que Q
3. Ni P ni Q
4. P sólo si Q
5. P es necesario para que Q
6. P es suficiente para que Q
7. P es equivalente a Q
8. P es necesario y suficiente para que Q.

A continuación daremos tratamiento matemático al estudio de la lógica proposicional, lo cual quiere decir que enmarcaremos el estudio dentro de la teoría intuitiva de conjuntos, y en consecuencia, los objetos deberán ser tratados como usualmente se tratan los conjuntos.

0.1. Sobre la metateoría. Es relevante para el estudio de los sistemas lógicos, el poner a la vista cuál es el cuerpo de conocimientos que se dan por hechos al momento de estudiar un sistema lógico, lo cual es conocido como la *metateoría*. En el contexto de la fundamentación de las matemáticas, resulta vital minimizar o por lo menos poner de manifiesto la cantidad de suposiciones no-triviales que se asumen, para después poder medir la capacidad de las explicaciones que un sistema

de lógica puede ofrecer. Como se puso de manifiesto en el párrafo previo, nuestra metateoría será la teoría intuitiva de los conjuntos, la cual es una teoría no formal, que comprende las herramientas de uso común de los matemáticos, como el álgebra de conjuntos, los conceptos de función, relación, los números naturales y su aritmética, por ejemplo, en breve saltará a la vista el uso del principio de inducción matemática en la metateoría.

1. Lenguajes Proposicionales

La primera etapa en la matematización de la lógica proposicional consiste en dar tratamiento matemático a su lenguaje. Éste se construye a partir de los elementos más básicos, los *símbolos*, que serán unidades de lenguaje, en el sentido de que estos se considerarán indivisibles, es decir, se supondrá que ninguno de estos está formado por otros símbolos. Los lenguajes proposicionales contienen los siguientes símbolos:

- Letras Proposicionales:
  Las cuales están en algún conjunto no-vacío $\mathbb{P}$. Lo que de $\mathbb{P}$ podría ser relevante es su cardinalidad. Típicamente usaremos las letras $P, Q, R, P_1, P_2, \ldots$ como variables que recorren el conjunto de letras proposicionales.

- Conectivos lógicos:
  Estos son $\neg$ negación, $\vee$ disyunción, $\wedge$ conjunción, $\rightarrow$ condicional y $\leftrightarrow$ bicondicional.

- Símbolos auxiliares:
  parentésis derecho) e izquierdo (.

Por *expresión* entenderemos cualquier sucesión finita de símbolos. Un símbolo será considerado a la vez, como un átomo, y como la expresión de longitud 1 cuyo único término es el símbolo en cuestión. Si α y β son expresiones, podemos construír una tercera expresión por *yuxtaposición* de éstas, en el orden dado. Por ejemplo, de yuxtaponer la expresión $\vee PR$ con $RR\wedge \rightarrow$ resulta $\vee PRRR\wedge \rightarrow$. Si α y β son expresiones, $\alpha\beta$ denotará a la yuxtaposición de α con β. No sobra decir que dos expresiones se consideran iguales, si y sólamente si lo son símbolo por símbolo.

Las expresiones que podrán calificarse de verdaderas o falsas, serán llamadas *fórmulas*. **Recursivamente** se define el conjunto de fórmulas

proposicionales en el lenguaje $\mathbb{P}$, denotado por Φ (o $\Phi(\mathbb{P})$ cuando haya posibilidad de confusión), por:

1. $\Phi_0 = \mathbb{P}$
2. Φ_{n+1} es el mínimo conjunto de expresiones que contiene a Φ_n y a todas las expresiones de las formas
   - $(\neg\alpha)$
   - $(\alpha \wedge \beta)$
   - $(\alpha \vee \beta)$
   - $(\alpha \to \beta)$
   - $(\alpha \leftrightarrow \beta)$

   con α y β en Φ_n.
3. $\Phi = \bigcup_{n\in\mathbb{N}} \Phi_n$.

Se enfatiza el hecho de que la definición del conjunto de fórmulas es recursiva porque gracias esto la noción de "ser fórmula" es *decidible*. Distinguir de entre todas las expresiones del lenguaje $\mathbb{P}$, cuáles sí son fórmulas es fácil. Dada una expresión, siempre es posible discernir si esta se trata o no de una fórmula. Más que esto, es posible definir un *algoritmo* que nos permite *decidir* si una expresión es o no una fórmula. Queda como ejercicio para el lector describir de manera informal cómo sería un procedimiento algorítmico que permita distinguir si una expresión dada es o no una fórmula. El problema de la *decidibilidad* es crucial en lógica. Es una aspiración de la lógica que sus principios y procedimientos sean decidibles porque esta cualidad permitiría automatizarlos, es decir, abriría la posibilidad de programar una computadora que los verifique.

Para empezar, mostraremos que la naturaleza recursiva de esta definición provee un "metodo de demostración" utilizable cuando deseamos demostrar propiedades acerca de fórmulas.

TEOREMA 1.1 (Principio de Inducción sobre la Formación de Fórmulas). *Sea $\mathcal{P}$ una propiedad acerca de las expresiones de un lenguaje proposicional. Si todas las letras proposicionales tienen la propiedad $\mathcal{P}$ y cada vez que dos expresiones α y β la tienen, sucede que $(\neg\alpha)$, $(\alpha\wedge\beta)$, $(\alpha\vee\beta)$ y $(\alpha \to \beta)$ tienen la propiedad $\mathcal{P}$, entonces TODAS las fórmulas tiene la propiedad $\mathcal{P}$.*

La demostración queda como ejercicio al lector.

Adicionalmente, es posible definir las interpretaciones de los lenguajes proposicionales en términos de funciones, que a cada fórmula asignen su significado, es decir, su *valor de verdad*. Estos valores de verdad de las fórmulas deben pertenecer a un conjunto con suficiente estructura. Y como es natural, el valor de verdad de una fórmula

debería ser calculado en función de valores de verdad asignados a las letras proposicionales. En el siguiente teorema, la función v hace las veces de *asignación de valores de verdad a las letras proposicionales*, mientras que $\bar{v}$ extiende de manera natural a la asignación v, hasta asignar valores de verdad a todas las fórmulas.

Teorema 1.2 (Principio de Recursión sobre Fórmulas). *Sea $\mathbb{P}$ un conjunto de letras proposicionales y sea $\mathcal{B} = \langle B, \sim, \sqcap, \sqcup \Rightarrow, \Leftrightarrow \rangle$ una estructura algebraica donde $\sim$ es una operación unitaria (de B en B) y $\sqcap$, $\sqcup$, $\Rightarrow$ y $\Leftrightarrow$ son operaciones binarias (de $B \times B$ en B). Entonces, dada una función $v : \mathbb{P} \longrightarrow B$, existe una única función $\bar{v} : \Phi(\mathbb{P}) \longrightarrow B$ que satisface:*

- $\bar{v}(P) = v(P)$, *para toda P en $\mathbb{P}$.*
- $\bar{v}((\neg\alpha)) = \sim \bar{v}(\alpha)$
- $\bar{v}((\alpha \vee \beta)) = \bar{v}(\alpha) \sqcup \bar{v}(\beta)$
- $\bar{v}((\alpha \wedge \beta)) = \bar{v}(\alpha) \sqcap \bar{v}(\beta)$
- $\bar{v}((\alpha \to \beta)) = \bar{v}(\alpha) \Rightarrow \bar{v}(\beta)$
- $\bar{v}((\alpha \leftrightarrow \beta)) = \bar{v}(\alpha) \Leftrightarrow \bar{v}(\beta)$

La demostración de este hecho también queda como ejercicio para el lector (ver los ejercicios de esta sección).

Ejemplo 1.3. Sea $\mathbb{P} = \{P_0, P_1, P_2, \dots\}$, y definamos las siguientes operaciones sobre los números enteros:
$\sim: z \longmapsto 1 - z$
$\sqcap : (z, w) \longmapsto \text{mín}\{z, w\}$
$\sqcup : (z, w) \longmapsto \text{máx}\{z, w\}$
$\Rightarrow: (z, w) \longmapsto \text{máx}\{1 - z, w\}$.
$\Leftrightarrow: (z, w) \longmapsto \text{mín}\{\text{máx}\{1 - z, w\}, \text{máx}\{z, 1 - w\}\}$.
Con estas operaciones, si $v : \mathbb{P} \to \mathbb{Z}$ está dada por $v(P_n) = n$ entonces

	P_0	P_5	P_8	$(\neg P_0)$	$((\neg P_0) \wedge P_5)$	$(((\neg P_0) \wedge P_5) \to P_8)$
$\bar{v}$	0	5	8	1	1	8

Ejemplo 1.4. Nota que las operaciones definidas en el ejemplo anterior están cerradas en el subconjunto $\{0, 1\}$ de $\mathbb{Z}$. Si ahora definimos a $v : \mathbb{P} \to \{0, 1\}$ por

$$v(P_n) = \begin{cases} 1 & \text{si } n \text{ es par} \\ 0 & \text{si } n \text{ es impar} \end{cases}$$

entonces evaluando la fórmula $(((\neg P_0) \wedge P_5) \to P_8)$ tenemos

	P_0	P_5	P_8	$(\neg P_0)$	$((\neg P_0) \wedge P_5)$	$(((\neg P_0) \wedge P_5) \to P_8)$
$\bar{v}$	1	0	1	0	0	1

La interpretación clásica de la lógica proposicional es precisamente la dada por las operaciones del ejemplo anterior, en $\{0, 1\}$, con el 1 haciendo el papel de *verdadero* y 0 el de *falso*.

Una familia de estructuras donde de manera natural se puede interpretar la lógica de proposiciones es la formada por las álgebras potencia de conjuntos.

Ejemplo 1.5. En $\mathcal{P}(\mathbb{N})$, la potencia de conjunto de números naturales, las siguientes operaciones están definidas:
$\sim: X \longmapsto \mathbb{N}\backslash X$
$\sqcap : (X, Y) \longmapsto X \cap Y$
$\sqcup : (X, Y) \longmapsto X \cup Y$
$\Rightarrow: (X, Y) \longmapsto Y \cup (\mathbb{N}\backslash X)$ [1]
$\Leftrightarrow: (X, Y) \longmapsto (X \cap Y) \cup [(\mathbb{N} \setminus X) \cap (\mathbb{N} \setminus Y)]$ [2]

Sea $\mathbb{P} = \{P_0, P_1, P_2, ...\}$ (como antes) y definamos $v : \mathbb{P} \to \mathcal{P}(\mathbb{N})$ por

$$v(P_n) = \{k \in \mathbb{N} : n \text{ divide a } k\}.$$

entonces el lector puede verificar que

$$\bar{v}((P_2 \to (\neg P_0 \wedge P_3)) = \{n : n = 0 \text{ o } n \text{ no es múltiplo de } 6\}.$$

Ejercicios 2.

1. Demuestra que $((\neg(P_0 \vee P_4)) \wedge (P_5 \to P_8))$ es una fórmula.
2. Demuestra que $(P_4 \to \neg(P_3 \vee P_1))$ no es una fórmula.
3. Calcula $\bar{v}((\neg(P_0 \vee P_4)) \wedge (P_5 \to P_8))$, para la asignación v de los ejemplos 1.3, 1.4 y 1.5.
4. Describe de manera informal un algoritmo que, dada una expresión del lenguaje de $\mathbb{P}$, decida si ésta es o no una fórmula.
5. Demuestra el Principio de Inducción sobre la Formación de Fórmulas (Teorema 1.1). En lo sucesivo lo abreviaremos con *issf*. Sugerencia: Inducción usual sobre $\mathbb{N}$.
6. Demuestra por isff que toda fórmula tiene tantos paréntesis izquierdos como derechos.

[1] esta operación se llama *complemento de X relativo a Y*.

[2] Esta operación que se podría llamar *coincidencia*, es el complemento de la mejor conocida *diferencia simétrica*.

7. Demuestra por isff que toda fórmula que no es letra proposicional, empieza con un paréntesis izquierdo y termina con un paréntesis derecho.
8. Demuestra por isff que ninguna fórmula contiene dos conectivos ubicados consecutivamente.
9. Demuestra por isff que ninguna fórmula contiene dos letras proposicionales ubicadas consecutivamente.
10. Describe de manera informal una noción de *complejidad* de las fórmulas. Dicho en otras palabras, ¿cuándo dirías que una fórmula es más compleja que otra?
11. Demuestra el Principio de Recursión sobre Fórmulas. Sugerencia: Para la existencia, haga lo usual. Considere la familia de extensiones parciales de v i.e. la familia V de todas las funciones de la forma $w : C \to B$ tales que:
    - $\mathbb{P} \subseteq C \subset \Phi(\mathbb{P})$,
    - $w \restriction \mathbb{P} = v$ y
    - si $(\neg\alpha)$, $(\alpha \vee \beta), (\alpha \wedge \beta), (\alpha \to \beta), (\alpha \leftrightarrow \beta) \in C$ entonces $\alpha, \beta \in C$, y además,
        - $w((\neg\alpha)) = \sim w(\alpha)$,
        - $w((\alpha \wedge \beta) = w(\alpha) \sqcap w(\beta)$,
        - $w((\alpha \vee \beta)) = w(\alpha) \sqcup w(\beta)$ y
        - $w((\alpha \to \beta)) = w(\alpha) \Rightarrow w(\beta)$
        - $w((\alpha \leftrightarrow \beta)) = w(\alpha) \Leftrightarrow w(\beta)$.

    Prueba por isff que si w_1 y w_2 están en V, entonces para toda fórmula α en $dom(w_1) \cap dom(w_2)$, $w_1(\alpha) = w_2(\alpha)$. Luego prueba (también por isff) que toda fórmula está en el dominio de alguna función en V. Finalmente, prueba la unicidad por isff.

2. Semantica de la Lógica Proposicional

2.1. Tautologías e Implicación Lógica. Dos aspiraciones fundamentales de cualquier sistema lógico son:

1. Establecer cuáles son las fórmulas *siempre verdaderas*.
2. Establecer cuándo una fórmula es *consecuencia* de otra fórmula, o de un conjunto de fórmulas.

El el caso de la lógica de proposiciones clásica, a las fórmulas que tienen la propiedad 1 se les llama tautologías, mientras que 2 corresponde a la noción de implicación lógica.

Definición 2.1. Sean $\mathbb{P}$ un conjunto de letras proposicionales y α una fórmula proposicional en el lenguaje $\mathbb{P}$. Decimos que α es una *tautología* si para toda $v : \mathbb{P} \longrightarrow \{0, 1\}$, ocurre que $\bar{v}(\alpha) = 1$.

En la presente definición de tautología estamos considerando al conjunto $\{0,1\}$ dotado con las operaciones descritas en el Ejemplo 1.3.

Queda como ejercicio al lector verificar las funciones definidas en el Ejemplo 1.3 coinciden con las bien conocidas *tablas de verdad*, cuando identificamos a 1 con "verdadero" y a 0 con "falso".

DEFINICIÓN 2.2. Sean $T \subseteq \Phi(\mathbb{P})$ y $\alpha \in \Phi(\mathbb{P})$. Decimos que T *implica lógicamente a* α si para cada $v : \mathbb{P} \to \{0,1\}$ que cumpla que para toda $\beta \in T$, $\bar{v}(\beta) = 1$, sucede que $\bar{v}(\alpha) = 1$. Denotaremos por $T \models \alpha$ el hecho de que T implica lógicamente a α.

Observe que $\emptyset \models \alpha$ equivale a que α sea una tautología, de ahí que la notación $\models \alpha$ significa α es una tautología. En el caso en que T esté formado por una sola fórmula, digamos β, la notación $\beta \models \alpha$ significará $\{\beta\} \models \alpha$.

Satisfecha la aspiración 2 se tiene gratuitamente la noción de equivalencia lógica: dos fórmulas serán *equivalentes* si son verdaderas exactamente en los mismos casos, es decir si una implica lógicamente a la otra, y viceversa.

Se recomienda al lector ver ejercicios de la sección para encontrar más propiedades de las relaciones de implicación y equivalencia lógica.

En términos de implicación lógica se puede enunciar el primer teorema no-trivial del curso, el Teorema de Compacidad: si $T \models \alpha$ entonces existe $T_0 \subseteq T$ finito tal que $T_0 \models \alpha$. Demostraremos este resultado más adelante.

En general (i.e, en cualquier sistema lógico) la aspiración 1 se puede conseguir simplemente al distinguir, de entre las fórmulas de un lenguaje a un subconjunto de estas. Por otro lado la aspiración 2 se puede conseguir ordenando (al menos parcialmente) a las interpretaciones (valores de verdad) de las fórmulas. Ordenar parcialmente a las interpretaciones de las fórmulas también resuelve el punto 1, si consideramos como verdaderas a las fórmulas "más verdaderas", es decir, aquellas cuyas interpretaciones siempre son el máximo de un tal orden parcial.

EJERCICIOS 3. Sean $\mathbb{P}$ un conjunto de letras proposicionales, S, T subconjuntos de $\Phi(\mathbb{P})$, $\alpha, \beta \in \Phi(\mathbb{P})$.

1. Verifica que las operaciones sobre $\{0,1\}$ definidas en el Ejemplo 1.3 coinciden con las bien conocidas tablas de verdad.
2. Demuestra que si $T \subseteq S$ y $T \models \alpha$ entonces $S \models \alpha$.
3. Demuestra que si para toda $\gamma \in S$, $T \models \gamma$ y $S \models \alpha$, entonces $T \models \alpha$.
4. Demuestra que $\emptyset \models \alpha$ si y sólo si α es una tautología.

5. Demuestra que $\alpha \to (\beta \to \gamma)$ es lógicamente equivalente a $(\alpha \wedge \beta) \to \gamma$.
6. Demuestra que $\beta \models \alpha$ si y sólo si $\models (\beta \to \alpha)$.
7. Demuestra que $\{\alpha_1, \ldots, \alpha_n\} \models \beta$ si y sólo si $\models (\alpha_1 \wedge \cdots \wedge \alpha_n) \to \beta$.
8. Demuestra que si α es tautología y $\alpha \models \beta$ entonces β es tautología.

2.2. Álgebras Booleanas. Con dos propósitos se presenta ahora la noción de álgebra booleana: Primero, establecer la esencia de la interpretación usual de los conectivos lógicos, que se pierde al considerar sólo dos valores de verdad. Segundo, poseer un lenguaje cómodo en el que se presenten teoremas importantes de manera sencilla.

De los cursos de álgebra superior, es conveniente recordar la siguiente definición.

Definición 2.3. Un relación entre pares de elementos de un conjunto $\mathbb{B}$ denotada por $\leq$ es un *orden parcial* si cumple que:

1. es *reflexiva*: $b \leq b$, para todo $b \in \mathbb{B}$,
2. es *antisimétrica*: si $a \leq b$ y $b \leq a$, entonces $a = b$.
3. es *transitiva*: si $a \leq b$ y $b \leq c$ entonces $a \leq c$.

El lector con seguridad conoce muchos ejemplos de órdenes parciales. Los más conocidos son los de las diferentes estructuras numéricas clásicas como los naturales, enteros, racionales y reales. Todos los anteriores son órdenes lineales, lo cual significa que los números se pueden pensar ubicados a lo largo de una línea, pero hay órdenes parciales que no son así. Por ejemplo, la relación de *contención* entre conjuntos o la de *ser subespacio* vectorial no son relaciones lineales.

2.2.1. Retículas. Recordemos que el *supremo* de un conjunto es la mínima cota superior de tal conjunto, es decir, el supremo de un conjunto A es un a tal que

1. para todo $x \in A$, $x \leq a$, y
2. si $x \leq a'$ para todo $x \in A$ entonces $a \leq a'$.

Por otro lado, el *ínfimo* de un conjunto A es la máxima cota inferior de tal conjunto, esto es, un a tal que

1. para todo $x \in A$, $a \leq x$, y
2. si $a' \leq x$ para todo $x \in A$ entonces $a' \leq a$.

Es sencillo probar (ver ejercicios) que supremos e ínfimos son únicos cuando existen.

Definición 2.4. Una *retícula* es un conjunto parcialmente ordenado $\mathbb{B} = \langle B, \leq \rangle$ tal que para cualesquiera $p, q \in B$, el par $\{p, q\}$ tiene supremo e ínfimo en $\mathbb{B}$.

Ejercicios 4. La contención de conjuntos es un orden parcial sobre el conjunto de partes de un conjunto dado X, que de hecho lo hace una retícula: el supremo de un par de conjuntos es la unión de estos, mientras que el ínfimo de dos conjuntos es la intersección de estos. La familia de subespacios de un espacio vectorial también es una retícula con respecto a la contención. En este ejemplo, la intersección de dos subespacios es el ínfimo de este par, pero la unión de subespacios de un espacio vectorial a veces no es subespacio, por lo que en este caso, el supremo no es la unión, sino el subespacio generado por la unión.

Notación: Si $\mathbb{B} = \langle B, \leq \rangle$ es una retícula con máximo y mínimo, se denota al máximo por 1 y al mínimo por 0. El ínfimo de $\{x, y\}$ se denotará por $x \wedge y$, mientras el supremo se denotará por $x \vee y$.

Proposición 2.5. *Sean $\mathbb{B} = \langle B, \leq \rangle$ una retícula y $a, b, c \in B$. Las siguientes condiciones son equivalentes:*

- $a \leq b$,
- $a \wedge b = a$, *y*
- $a \vee b = b$·

Además se cumple lo siguiente:

1. $a \wedge b \leq a \quad y \quad a \wedge b \leq b$.
2. $a \vee b \geq a \quad y \quad a \vee b \geq b$.
3. $a \wedge a = a \quad y \quad a \vee a = a$.
4. $a \wedge b = b \wedge a \quad y \quad a \vee b = b \vee a$.
5. $a \wedge (b \wedge c) = (a \wedge b) \wedge c \quad y \quad a \vee (b \vee c) = (a \vee b) \vee c$.
6. $c \vee (a \wedge b) \leq (c \vee a) \wedge (c \vee b) \quad y$
   $c \wedge (a \vee b) \geq (c \wedge a) \vee (c \wedge b)$.
7. *Si* $a \leq b$ *entonces* $a \wedge c \leq b \wedge c$ *y* $a \vee c \leq b \vee c$.
8. *Si* $\mathbb{B}$ *tiene máximo y mínimo entonces* $a \wedge 0 = 0$, $a \vee 0 = a$
   $a \wedge 1 = a$ *y* $a \vee 1 = 1$.

Demostración. Se deja como ejercicio al lector, salvo la primera parte del inciso 6, que se prueba a continuación. En primer lugar, por el inciso 2 se tiene que $c \leq c \vee a$ y $c \leq c \vee b$. En segundo lugar, por el inciso 1 se tiene que $a \wedge b \leq a$ y $a \wedge b \leq b$, por lo tanto $a \wedge b \leq c \vee a$ y $a \wedge b \leq c \vee b$. Luego $c \vee (a \wedge b)$ es cota inferior de $\{c \vee a, c \vee b\}$. Por lo tanto, usando nuevamente el inciso 2, $c \vee (a \wedge b) \leq (c \vee a) \wedge (c \vee b)$.
La segunda parte del inciso 6 se prueba de manera análoga a la primera. □

Definición 2.6. Una retícula $\mathbb{B}$ es *distributiva* si en el inciso 6 de la proposición anterior valen las igualdades, es decir, para cualesquiera a, b, c en B,

$$c \vee (a \wedge b) = (c \vee a) \wedge (c \vee b)$$

y

$$c \wedge (a \vee b) = (c \wedge a) \vee (c \wedge b).$$

2.2.2. Complementación. En esta sección escudriñaremos el concepto de negación. En un primer lugar, debemos acordar que una proposición y su negación deben ser incompatibles. No debería caber la posibilidad de que una proposición sea verdadera al mismo tiempo que lo sea también su negación. Si en una retícula $\mathbb{B}$ se asignan valores de verdad a las proposiciones, el valor que debería adquirir la conjunción de una proposición con su negación deberá ser 0, el mínimo de $\mathbb{B}$.

Volviendo a las retículas, diremos que dos elementos a y b de una retícula $\mathbb{B}$ son *incompatibles* si $a \wedge b = 0$. Es obvio que el 0 es incompatible con todos los elementos de una retícula (hasta consigo mismo). No se advierten motivos para pensar que, si a es un elemento cualquiera de B, el 0 debería ser el único elemento de B incompatible con a, probablemente hay más. Diremos que a y b son *compatibles* si no son incompatibles.

Proposición 2.7. *Sea $\mathbb{B}$ una retícula con máximo 1 y mínimo 0, y sean $a, b, c \in B$. Entonces:*

1. *a es compatible con b si y sólo si b es compatible con a.*
2. *Si a es incompatible con b y $c \leq b$, entonces a es incompatible con c.*
3. *Si a es compatible b y $c \geq b$ entonces a es compatible con c.*
4. *a es incompatible con $b \vee c$ si y sólo si a es incompatible con b y con c.*
5. *a es incompatible con 1 si y sólo si $a = 0$.*

Demostración. La demostración es un ejercicio sencillo para el lector. Sugerencia para el inciso 4: Usar la Proposición 2.5(6). □

La incompatibilidad no puede ser el único atributo de la negación. En los ejercicios se puede apreciar que en distintas retículas, un elemento puede tener muchos otros que le son incompatibles. Sin embargo, en algunos de estos ejemplos se puede encontrar un elemento incompatible especial: uno que es máximo con respecto a la incompatibilidad.

Definición 2.8. Sean $\mathbb{B}$ una retícula y $a \in B$. Un elemento b de B es el *pseudocomplemento* de a si es el máximo elemento incompatible con a, es decir, cumple que

- $a \wedge b = 0$, y
- si $x \wedge a = 0$ entonces $x \leq b$.

La condición de ser el máximo de un conjunto hace que este sea único, cuando existe. En los ejercicios se pedirá encontrar ejemplos (y contraejemplos) de elementos de retículas que tienen esta clase de elementos. Denotaremos por a^p al pseudocomplemento de a.

PROPOSICIÓN 2.9. *Sean $\mathbb{B}$ una retícula y a un elemento de B que tiene pseudocomplemento. Entonces, para todo x en $\mathbb{B}$, x es incompatible con a si y sólo si $x \leq a^p$. Además, las siguientes afirmaciones se cumplen para cualesquiera a, b, c para los cuales los pseudocomplementos involucrados existan.*

1. *$a \leq b$ si y sólo si $a^p \geq b^p$.*
2. *$a^p \wedge b^p \leq (a \vee b)^p$.*
3. *$(a \wedge b)^p \leq a^p \vee b^p$.*
4. *Si $b \neq 0$ entonces b es compatible con a o con a^p (o con ambos).*

DEMOSTRACIÓN. La ida es inmediata del inciso (2) de la definición de pseudocomplemento. El regreso se sigue de la parte (1) de la defincón, más el inciso (2) de la Proposición 2.7. Los incisos se dejan como ejercicios para el lector. □

La idea de la incompatibilidad también explica, al menos en parte, el carácter del conectivo implicación. Considerando que la verdad de una fórmula de la forma *si P entonces Q* es incompatible con la presencia de P en ausencia de Q, podemos considerar al valor de verdad de P *implica* Q como el máximo con respecto a esta condición, es decir, el si a y b son los valores de verdad de P y Q, respectivamente, el valor de verdad de P implica Q es el máximo c incompatible con $a \wedge b^p$. Esta caracterización tiene un pequeño defecto: recurre a la noción de psudocomplemento. Por suerte la defincón del valor de verdad de la implicación se puede enunciar equivalemente de la siguiente manera:

DEFINICIÓN 2.10. Sea $\mathbb{B}$ una retícula con 0 y 1. El *pseudocomplemento de a relativo a b* es el máximo elemento c de B tal que $a \wedge c \leq b$.

PROPOSICIÓN 2.11. *El pseudocomplemento de a relativo a b es el máximo elemento d de B que es incompatible con $a \wedge b^p$.*

DEMOSTRACIÓN. Sea c el pseudocomplemento de a relativo a b, y sea d como en la Proposición. Entonces, dado que $a \wedge c \leq b$, tenemos que $0 = (a \wedge c) \wedge b^p = (a \wedge b^p) \wedge c$, es decir, c es incompatible con $a \wedge b^p$. Por la maximalidad de d con respecto a esta propiedad, tenemos que $c \leq d$. Por otro lado, dado que d es incompatible con $a \wedge b^p$, tenemos

que $(a \wedge b^p) \wedge d = 0$, por lo que $(a \wedge d) \wedge b^p = 0$. Por 2.9, $a \wedge d \leq b$. Como c es maximal con respecto a esta propiedad, $d \leq c$. □

El pseudocomplemento de a relativo a b será denotado por $a \to b$.

PROPOSICIÓN 2.12. *Sean $\mathbb{B}$ una retícula y $a, b, c \in B$. Las siguientes afirmaciones se cumplen.*

1. *$a \to b = 1$ si y sólo si $a \leq b$.*

DEFINICIÓN 2.13. Sea $\mathbb{B}$ una retícula con máximo y mínimo. Dados $p, q \in B$ decimos que q es *complemento* de p si $p \wedge q = 0$ y $p \vee q = 1$.

PROPOSICIÓN 2.14. *Si en una retícula distributiva $\mathbb{B}$ con máximo y mínimo, un elemento $a \in B$ tiene complemento, entonces éste es único.*

En virtud de este resultado, hablaremos de *el* complemento de a

DEMOSTRACIÓN. Sean q y q' complementos de p, es decir $q \wedge p = q' \wedge p = 0$ y $q \vee p = q' \vee p = 1$. Note que

$$q' = q' \wedge 1 = q' \wedge (q \vee p) = (q' \wedge q) \vee (q' \wedge p) = (q' \wedge q) \vee 0 = q' \wedge q$$

Por lo tanto $q' \leq q$. Análogamente se prueba que $q \leq q'$, y así, $q' = q$. □

NOTACIÓN: a^c denotará al complemento de a. Veamos las propiedades del complemento.

PROPOSICIÓN 2.15. *Sea $\mathbb{B}$ una retícula distributiva con máximo y mínimo, y sean a y b dos elementos de B que tienen complemento. Entonces,*

1. $(a^c)^c = a$, $1^c = 0$, $0^c = 1$.
2. $(a \wedge b)^c = a^c \vee b^c$,
3. $(a \vee b)^c = a^c \wedge b^c$,
4. *$a \leq b$ si y sólo si $a \wedge b^c = 0$ si y sólo si $a^c \vee b = 1$ si y sólo si $b^c \leq a^c$.*
5. *$a = b$ si y sólo si $(a^c \vee b) \wedge (b^c \vee a) = 1$ si y sólo si $(a^c \wedge b) \vee (a \wedge b^c) = 0$*

DEMOSTRACIÓN. Las demostracioones completas de todos los incisos, excepto el (4) quedan como ejercicio al lector. Aquí ponemos algunas pistas. (1) Observa que a satisface la definición de ser el complemento de a^c.
(2) Veamos que $a^c \vee b^c$ actúa como complemento de $a \wedge b$. En primer lugar,

$$(a \wedge b) \wedge (a^c \vee b^c) = ((a \wedge b) \wedge a^c) \vee ((a \wedge b) \wedge b^c) = (b \wedge (a \wedge a^c)) \vee (a \wedge (b \wedge b^c))$$
$$= (b \wedge 0) \vee (a \wedge 0) = 0 \vee 0 = 0.$$

En segundo lugar,

$$(a \wedge b) \vee (a^c \vee b^c) = (a \vee (a^c \vee b^c)) \wedge (b \vee (a^c \vee b^c)) = 1 \wedge 1 = 1.$$

(3) es muy parecido a (2).
(4) Si $a \leq b$ entonces $(a \wedge b^c) \leq (b \wedge b^c) = 0$, por lo tanto $a \wedge b^c = 0$.
Si $a \wedge b^c = 0$ entonces $a^c \vee b = ((a^c \vee b)^c)^c = (a^{c^c} \wedge b^c)^c = (a \wedge b^c)^c = 0^c = 1$.
Si $a^c \vee b = 1$, entonces $b^c = 1 \wedge b^c = (a^c \vee b) \wedge b^c = (a^c \wedge b^c) \vee (b \wedge b^c) = (a^c \wedge b^c) \vee 0 = (a^c \wedge b^c)$. Por la Proposición 2.5 $b^c \leq a^c$.

□

Definición 2.16. Un *álgebra booleana* es una retícula distributiva con máximo y mínimo en la que todo elemento tiene complemento.

El lector seguro conoce ejemplos de álgebras booleanas. Para empezar, las álgebras potencia de conjuntos lo son. En particular, el álgebra potencia de un conjunto unitario (i.e de la forma $\{e\}$) es isomorfa al conjunto $2 = \{0, 1\}$ dotado con las operaciones del ejemplo 1.3. Un célebre teorema de Marshall Stone proclama que de hecho todas las álgebras booleanas son isomorfas a álgebras de conjuntos (no necesariamente álgebras potencia), es decir, las operaciones de supremo, ínfimo y complemento son unión, intersección y complemento respecto al total. Un ejemplo de álgebra de conjuntos que no es (ni siquiera isomorfa a) un álgebra potencia es la que generamos con los subconjuntos finitos más los cofinitos de $\mathbb{N}$. Al ser un álgebra numerable, no puede ser la potencia de ningún conjunto.

En toda álgebra booleana están definidas las siguientes operaciones, es decir, para cualesquiera elementos a y b de un álgebra booleana $\mathcal{P}$ se define:

1. $a \to b := a^c \vee b$ (el complemento de a relativo a b).
2. $a \setminus b := a \wedge b^c$ (a menos b).
3. $a \triangle b := (a \setminus b) \vee (b \setminus a)$ (la diferencia simétrica).
4. $a \nabla b := (a \triangle b)^c$ (la coincidencia simétrica).

En los ejercicios de esta sección el lector se familiarizará con estas operaciones.

Ejemplo 2.17. Sea $\langle X, \tau \rangle$ un espacio topológico, y sean $CO(X)$ la familia de subconjuntos cerrados y abiertos de X, y $RO(X)$ la familia de los subconjuntos abiertos *regulares* de X. Se dice que A es abierto regular si $A = int(cl(A))$. El álgebra $CO(X)$ es un álgebra de conjuntos y está incluida en $RO(X)$, sin embargo esta última en general no es álgebra de conjuntos, pues el complemento de A es $int(X \setminus A)$, mientras que $A \vee B = int(cl(A \cup B))$.

EJERCICIOS 5.

1. Sea $B = \{1, 2, 3, \dots\}$, el conjunto de enteros positivos. Demuestra que la relación de *divisibilidad* es un orden parcial sobre B. ¿Tienen todos los pares de naturales un supremo con respecto a esta relación? ¿Tienen un ínfimo? Demuestra que 1 es el mínimo de la relación. ¿Hay un máximo? ¿Hay algo conocido qué agregar para que este orden tenga un máximo?
2. Reponde las preguntas del ejercicio anterior, cambiando $B = \mathbb{R}(x)$, el conjunto de polinomios en x con coeficientes reales. ¿Qué le cambiarías para que la relación de divisibilidad le de una estructura de retícula a este B, o a un subconjunto interesante de B?
3. Sea B el conjunto de todos los intervalos abiertos de números reales, es decir, $B = \{(r, s) : r, s \in \mathbb{R}, r \leq s\}$, ordenado por contención. ¿Es este conjunto ordenado una retícula? Observa que tiene mínimo, el $\emptyset$, pero no tiene máximo. ¿Qué cambiarías en este conjunto ordenado, para que hubiese un máximo?
4. Sea B el conjunto de todos los subespacios vectoriales de $\mathbb{R}^5$. Demuestra que si V, W son subespacios de $\mathbb{R}^5$ entonces $V \cap W$ es el ínfimo de $\{V, W\}$, y el subespacio de $\mathbb{R}^5$ generado por $V \cup W$ es el supremo de $\{V, W\}$. ¿Quiénes son el mínimo y el máximo elementos de B?

Para los siguientes ejercicios, sea $\mathbb{B} = \langle B, \leq \rangle$ un conjunto parcialmente ordenado.

5. Sea A un subconjunto de B que tiene supremo. Demuestra que éste es único. Medita y convéncete de que lo mismo pasa en el caso análogo para ínfimos.
6. Completa la demostración de la Proposición 2.5.
7. Da un ejemplo sencillo de una retícula que no sea distributiva. Es posible con un dibujo sencillo.
8. La relación de divisibilidad en el contexto del Ejercicio 1, ¿es distributiva?
9. La relación de contención en el Ejercicio 3, ¿es distributiva?
10. La relación de ser subespacio en el Ejercicio 4, ¿es distributiva?
11. Da un ejemplo de retícula distributiva con máximo y mínimo con un elemento que no tenga complemento.
12. Da un ejemplo de retícula con máximo y mínimo que tenga un elemento que a su vez tenga dos complementos diferentes.
13. Completa la demostración de la Proposición 2.15.

En los siguientes ejercicios, supondremos que $\mathcal{P}$ es un álgebra booleana.

14. $a \to b = 1$ si y sólo si $a \leq b$.
15. Demuestra que $a \triangle b = (a \vee b) \setminus (a \wedge b)$ y $a \triangledown b = (a \wedge b) \vee (a^c \wedge b^c) = (a \vee b^c) \wedge (b \vee a^c)$.
16. Demuestra que $a = b$ si y sólo si $a \triangle b = 0$.
17. Demuestra que en cualquier álgebra booleana, $\triangle$ es una operación de grupo abeliano, cuyo neutro es el 0 y en el que todos los elementos son autoinversos.
18. Use el ejercicio anterior para demostrar que en cualquier álgebra booleana, $\triangledown$ es una operación de grupo abeliano, cuyo neutro es el 1 y en el que todos los elementos son autoinversos.

2.3. La interpretación booleana. Filtros, homomorfismos, cocientes y ultrafiltros. La noción de tautología que fue definida en 2.1 parece ser restrictiva y artificial. ¿por qué admitir sólo dos valores de verdad? ¿qué se ganaría o perdería al admitir más valores de verdad, siempre que estos se encuentren en una estructura apropiada, como un álgebra booleana? Interpretemos un lenguaje proposicional $\mathbb{P}$ en un álgebra booleana $\mathcal{P}$. Por supuesto esto conlleva un cambio: ¿cuáles serán ahora las fórmulas válidas? Al igual que en el caso de las tautologías, digamos que una fórmula α es $\mathcal{P}$-válida si toda valuación de $\mathbb{P}$ en $\mathcal{P}$, asigna el valor 1 (el máximo de $\mathcal{P}$) a α. A partir de este momento, buscaremos demostrar que las tautologías son exactamente las fórmulas válidas en cualquier interpretación booleana. Para esto necesitamos incorporar al lenguaje la noción de filtro y estudiar los homomorfismos de álgebras booleanas.

Definición 2.18. Sea $\mathcal{P}$ un álgebra booleana. Un *filtro* F en $\mathcal{P}$ es un subconjunto de $\mathcal{P}$ tal que:

1. $1 \in F$, $0 \notin F$
2. Para todos $a \in F$ y $b \in \mathcal{P}$, si $b \geq a$ entonces $b \in F$.
3. Para todos $a, b \in F$ se tiene que $a \wedge b \in F$.

Dual a la noción de filtro, se define ideal.

Definición 2.19. Un ideal I en $\mathcal{P}$ es un subconjunto de $\mathcal{P}$ tal que:

1. $0 \in I$, $1 \notin I$
2. Para todos $a \in I$ y $b \in \mathcal{P}$, si $b \leq a$ entonces $b \in I$.
3. Para todos $a, b \in I$ se tiene que $a \vee b \in I$.

Observe que si I es un ideal sobre un álgebra booleana $\mathcal{P}$ entonces $I^* = \{a^c : a \in I\}$ es un filtro, llamado el *filtro dual* de I. Análogamente,

si F es un filtro, entonces $F^* = \{a^c : a \in F\}$ es un ideal, llamado el *ideal dual* de F.

Ejemplo 2.20. Sea $\mathcal{P}$ un álgebra booleana cualquiera. Trivialmente, el conjunto $\{1\}$ es un filtro y el conjunto $\{0\}$ es un ideal. En el álgebra potencia de $\mathbb{N}$, la familia $\mathbf{Fin}(\mathbb{N})$ de subconjuntos finitos de $\mathbb{N}$ es un ideal. Su filtro dual suele ser llamado el *filtro de Fréchet*.

Dado un elemento a de un álgebra booleana $\mathcal{P}$, la familia $F_a = \{b \in P : b \geq a\}$ es un filtro. Se dice que un filtro F es *fijo* cuando $F = F_a$ para algún $a \in P$. De lo contrario se dice que F es *libre*.

En la sección de ejercicios el lector podrá encontrar más ejemplos de filtros e ideales.

A continuación investigaremos cuándo un subconjunto cualquiera de un álgebra booleana está contenido en un filtro.

Definición 2.21. Decimos que $A \subseteq \mathcal{P}$ tiene la *propiedad de la intersección finita* (pif) si para cualesquiera $n \in \omega$ y $a_1, a_2, \ldots, a_n \in A$,

$$a_1 \wedge a_2 \wedge \ldots \wedge a_n \neq 0.$$

Note que los filtros siempre tienen esta propiedad. Inversamente, los conjuntos con esta propiedad son aquellos para los que hay un filtro que los contiene.

Proposición 2.22. *Sea A un subconjunto de un álgebra booleana $\mathcal{P}$. Entonces, A tiene la pif si y sólo si existe un filtro F tal que $A \subseteq F$.*

Demostración. $\Leftarrow$] Todo filtro tiene la pif, y subconjuntos de conjuntos con la pif tienen la pif.
$\Rightarrow$] Sea $F = \{b \in \mathcal{P} : \exists n \in \omega$ y $\exists a_1, a_2, \ldots, a_n \in A$ tal que $b \geq a_1 \wedge a_2 \wedge \ldots \wedge a_n\} \bigcup \{1\}$. Ver que esto es filtro se queda como ejercicio para el lector. □

Los filtros tienen la siguiente propiedad curiosa:

Proposición 2.23. *Sean F un filtro en un álgebra booleana $\mathcal{P}$, y $p \in \mathcal{P}$. Si $p \notin F$ entonces $F \cup \{p^c\}$ tiene la pif.*

Demostración. Supongamos que $F \cup \{p^c\}$ no tiene la pif. Entonces existe $a \in F$ tal que $a \wedge p^c = 0$ (piense el lector por qué). Por la Proposición 2.15 (4), existe a en F tal que $a \leq p$, y así tenemos que $p \in F$. □

Definición 2.24. Sean $\mathcal{P}$ y $\mathcal{Q}$ álgebras booleanas.
Un *homomorfismo* de $\mathcal{P}$ en $\mathcal{Q}$ es una función $\varphi : \mathcal{P} \longrightarrow \mathcal{Q}$ tal que:

1. $\varphi(0_{\mathcal{P}}) = 0_{\mathcal{Q}}$ y $\varphi(1_{\mathcal{P}}) = 1_{\mathcal{Q}}$.

2. $\varphi(a^c) = \varphi(a)^c$.
3. $\varphi(a \wedge b) = \varphi(a) \wedge \varphi(b)$.

Observe que todo homomorfismo φ es *creciente*, i.e. satisface que si $a \leq b$ entonces $\varphi(a) \leq \varphi(b)$. Más aún, satisface también que $\varphi(a \vee b) = \varphi(a) \vee \varphi(b)$. Por otro lado, note que no basta que una función sea creciente para que sea homomorfismo de álgebras booleanas (las demostraciones quedan como ejercicio).

Ejemplo 2.25.

1. El álgebra booleana 2 esta encajada en cualquier álgebra booleana $\mathcal{P}$ por la función φ dada por $\varphi(0) = 0$ y $\varphi(1) = 1$.
2. La función inclusión de $CO(X)$ en $RO(X)$ es un homomorfismo de álgebras booleanas (donde X es un espacio topológico).
3. Sean A cualquier conjunto y $B \subseteq A$. La función $\varphi : \mathcal{P}(A) \to \mathcal{P}(B)$ dada por $\varphi(a) = a \cap B$ es un homomorfismo. La inclusión de $\mathcal{P}(B)$ en $\mathcal{P}(A)$ no lo es.

De manera natural, los homomorfismos de álgebras booleanas determinan un filtro y un ideal en su dominio.

Definición 2.26. Sea $\varphi : \mathcal{P} \longrightarrow \mathcal{Q}$ un homomorfismo de álgebras booleanas. Se define la *coraza* de φ por

$$Shell(\varphi) = \{a \in \mathcal{P} : \varphi(a) = 1_{\mathcal{Q}}\},$$

y el *núcleo* de φ se define por

$$Ker(\varphi) = \{a \in \mathcal{P} : \varphi(a) = 0_{\mathcal{Q}}\}.$$

Proposición 2.27. *Sea φ un homomorfismo de álgebras booleanas. Entonces $Shell(\varphi)$ es un filtro, $Ker(\varphi)$ es un ideal y $Ker(\varphi) = Shell(\varphi)^*$.*

Dejamos al lector probar esta proposición, a manera de ejercicio.

Cada filtro (o ideal) define una relación de equivalencia sobre un álgebra booleana $\mathcal{P}$, cuyo cociente hereda de manera natural la estructura de álgebra booleana. A continuación los detalles.

Definición 2.28. Sean $\mathcal{P}$ un álgebra booleana y F un filtro en $\mathcal{P}$. Diremos que a y b elementos de $\mathcal{P}$, son *equivalentes módulo F* (denotado por $a \sim_F b$) si y sólo si $a \triangledown b \in F$.

Recuerde el lector que $a \triangledown b$ es la coincidencia simétrica definida en la sección 2.2. Claramente, la intención de esta definición es que dos elementos de $\mathcal{P}$ son equivalentes módulo F si "están de acuerdo en un elemento grande según F".

PROPOSICIÓN 2.29. *$\sim_F$ es una relación de equivalencia.*

DEMOSTRACIÓN. Usando el ejercicio 5 (incisos 8 y 11) esta prueba se torna muy simple. Reflexividad y simetría se dejan como ejercicio. Veamos la transitividad. Primero, note que si $r, s \in F$ entonces $r \nabla s = (r \vee s^c) \wedge (s \vee r^c) \geq r \wedge s \in F$. Sean $a, b, c \in \mathcal{P}$ tales que $a \nabla b$ y $b \nabla c \in F$. Entonces $a \nabla c = (a \nabla 1) \nabla c = (a \nabla (b \nabla b)) \nabla c = (a \nabla b) \nabla (b \nabla c) \in F$. □

La congruencia módulo F es además una relación de congruencia, es decir, se comporta correctamente con respecto a las operaciones de álgebra booleana.

PROPOSICIÓN 2.30. *Sean $\mathcal{P}$ un álgebra booleana, F un filtro en $\mathcal{P}$ y $a, b, c, d \in \mathcal{P}$ tales que $a \sim_F b$ y $c \sim_F d$, entonces:*

1. $a^c \sim_F b^c$
2. $(a \wedge c) \sim_F (b \wedge d)$
3. $(a \vee c) \sim_F (b \vee d)$

DEMOSTRACIÓN. 1 es inmediato del ejercicio 5.8. Para el inciso 2, observe que distribuyendo se obtiene que

$$(a \nabla b) \wedge (c \nabla d) = (a \wedge b \wedge c \wedge d) \vee (a \wedge b \wedge c^c \wedge d^c) \vee (a^c \wedge b^c \wedge c \wedge d) \vee (a^x \wedge b^c \wedge c^c \wedge d^c),$$

mientras que

$$(a \wedge c) \nabla (b \wedge c) = (a \wedge b \wedge c \wedge d) \vee (c^c \wedge d^c) \vee (a^c \wedge b^c) \vee (a^c \wedge d^c) \vee (\wedge b^c \wedge c^c).$$

Finalmente, note que cada disyunto de la primera ecuación es menor o igual que algún disyunto de la segunda. □

DEFINICIÓN 2.31. $[a] \sqsubseteq [b]$ si $a^c \vee b \in F$.

Verifiquemos que esta definición no depende de representantes. Supongamos que $a_1 \sim_F a_2$, $b_1 \sim_F b_2$ y $a_1^c \vee b_1 \in F$. Entonces $(a_1^c \vee b_1) \vee (a_1 \nabla a_2) \vee (b_1 \nabla b_2) \in F$. Distribuyendo y cancelando adecuadamente se tiene que

$$(a_1^c \vee b_1) \vee (a_1 \nabla a_2) \vee (b_1 \nabla b_2) =$$
$$(b_1 \wedge b_2 \wedge a_1^c \wedge a_2^c) \vee (b_1 \wedge b_2 \wedge a_1 \wedge a_2) \vee (b_1^c \wedge b_2^c \wedge a_1^c \wedge a_2^c).$$

Note que cada disyunto de la ecuación anterior es menor o igual que $a_2^c \vee b_2$, por lo que $a_2^c \vee b_2 \in F$.

PROPOSICIÓN 2.32. *La relación $\sqsubseteq$ es un orden parcial sobre $\mathcal{P}/F$*

DEMOSTRACIÓN. La reflexividad es trivial, la antisimetría se obtiene fćilmente del ejercicio 5.8. Demostraremos la transitividad. Supongamos que $a^c \vee b$ y $b^c \vee c$ están en F. Así basta observar que $(a^c \vee b) \wedge (b^c \wedge c) = (a^c \wedge (b^c \vee c)) \vee (b \wedge c) \leq a^c \vee c$. □

PROPOSICIÓN 2.33. *Sean $\mathcal{P}$ un álgebra booleana , F un filtro en $\mathcal{P}$ y $\mathcal{P}/F$ el cociente.*
Si $[a], [b] \in \mathcal{P}/F$, entonces:

1. $[a]^C = [a]^c$.
2. $[a] \bigwedge [b] = [a \wedge b]$.
3. $[a] \bigvee [b] = [a \vee b]$.

DEMOSTRACIÓN. Por la Proposición 2.30, estas definiciones no dependen de representantes. Tan solo probaremos la ecuacuón (2), dejando el resto como ejercicio para el lector. Probemos que $\bigwedge$ se comporta como el ínfimo con respecto a $\sqsubseteq$. Claramente, $(a \wedge b)^c \vee a = (a^c \vee b^c) \vee a = 1 \in F$, por lo tanto $[a \wedge b] \sqsubseteq [a]$, y análogamente se prueba que $[a \wedge b] \sqsubseteq [b]$. Por lo tanto $[a \wedge b]$ es cota inferior de $\{[a], [b]\}$. Sea $c \in \mathcal{P}$ tal que $[c] \sqsubseteq [a]$ y $[c] \sqsubseteq [b]$, entonces $c^c \vee a \in F$ y $c^c \vee b \in F$, de donde $(c^c \vee a) \wedge (c^c \vee b) = c^c \vee (a \wedge b) \in F$. Luego $[c] \sqsubseteq [a \wedge b]$. □

Observe que, como de costumbre, la función $\varphi : \mathcal{P} \longrightarrow \mathcal{P}/F$ dada por $\varphi(a) = [a]_F$ es un homomorfismo suprayectivo. A continuación discutiremos el caso en el que $\mathcal{P}/F$ es isomorfa al álgebra 2.

DEFINICIÓN 2.34. Un filtro F sobre un álgebra booleana $\mathcal{P}$ es un *ultrafiltro* si es un filtro maximal con respecto a la contención.

Los ejemplos de ultrafiltros están en dos extremos: o son muy triviales o son imposibles de describir. Se dice que un elemento a de un álgebra booleana $\mathcal{P}$ es un *átomo* si no existe $x \in \mathcal{P}$ tal que $0 < x < a$. De este modo, el filtro fijo $F_a = \{p \in \mathcal{P} : p \geq a\}$ es un ultrafiltro cuando a es un átomo. Queda como ejercicio probar que si F_a es un ultrafiltro, entonces a es un átomo. La existencia de ultrafiltros libres está garantizada por el siguiente Teorema.

TEOREMA 2.35. *(del ultrafiltro, Tarski) En cualquier álgebra booleana $\mathcal{P}$, para cada conjunto $A \subseteq \mathcal{P}$ con la pif, existe un ultrafiltro F en $\mathcal{P}$ tal que $A \subseteq F$.*

DEMOSTRACIÓN. Sea $\mathcal{R}$ la familia de todos los filtros $G \subseteq \mathcal{P}$ tales que $A \subseteq G$, y considere a $\mathcal{R}$ ordenado por contención. Por la Proposición 2.22, $\mathcal{R}$ es no vacío. Sea $\mathcal{C} \subseteq \mathcal{R}$ una cadena. Supongamos que $\bigcup \mathcal{C}$ no tiene la pif. Entonces existen $n \in \omega$ y $c_1, c_2, \ldots, c_n \in \bigcup \mathcal{C}$ tales que $c_1 \wedge c_2 \wedge \ldots \wedge c_n = 0$. Por ser una cantidad finita existe $G \in \mathcal{C}$ tal que $c_1, c_2, \ldots, c_n \in G$, lo cual implica que G no tiene la pif, una contradicción. Por lo tanto $\bigcup \mathcal{C}$ tiene la pif. Por el Lema de Kuratowski-Zorn existe un maximal $F \in \mathcal{R}$. □

El siguiente teorema muestra varias equivalencias de ser ultrafiltro.

TEOREMA 2.36. *Sea $\mathcal{P}$ un álgebra booleana, y $F \subseteq \mathcal{P}$ un filtro. Entonces las siguientes afirmaciones son equivalentes:*

1. *F es un ultrafiltro.*
2. *Para todos $p, q \in \mathcal{P}$, si $p \vee q \in F$ entonces, o bien $p \in F$, o $q \in F$.*
3. *Para todo $p \in \mathcal{P}$, o bien $p \in F$, o $p^c \in F$.*
4. *$\mathcal{P}/F \cong \{0, 1\}$.*
5. *F^* es un ideal maximal.*

DEMOSTRACIÓN. $(1 \Rightarrow 2)$. Supongamos que $p \notin F$ y $q \notin F$. Por la Proposición 2.23, $F \cup \{p^c\}$ y $F \cup \{q^c\}$ tienen la pif, pero por la maximalidad de F, ambos conjuntos están contenidos en F y por tanto, $(p \vee q)^c = p^c \wedge q^c \in F$. Como F tiene la pif, $p \vee q \notin F$. $(2 \Rightarrow 3)$. Sea $p \in \mathcal{P}$. Entonces $p \vee p^c = 1 \in F$, y por (2), $p \in F$ o $p^c \in F$. $(3 \Rightarrow 4)$. Es un trámite burocrático verificar que la función $\varphi : \mathcal{P} \to 2$ dada por $\varphi(p) = 1$ si y sólo si $p \in F$ es un isomorfismo de álgebras booleanas. $(4 \Rightarrow 1)$. Sea $\varphi : \mathcal{P}/F \to 2$ un isomorfismo de álgebras booleanas. Claramente $F = Shell(\varphi)$ es un filtro. Si $p \notin F$ entonces $\varphi(p) = 0$ por tanto $p \in Ker(\varphi) = F^*$, y por tanto $p^c \in F$. Como F tiene la pif, p no puede estar en un filtro que extienda a F, con lo cual queda establecida la maximalidad de F. $(1 \Leftrightarrow 5)$ es inmediato. □

Ahora estamos en posición de regresar a la interpretación booleana de las fórmulas proposicionales.

TEOREMA 2.37. *Sea $\mathbb{P}$ un conjunto de letras proposicionales y α una fórmula en $\mathbb{P}$. Entonces las siguientes afirmaciones son equivalentes:*

1. *α es una tautología,*
2. *existe un álgebra booleana $\mathcal{P}$ tal que para toda $v : \mathbb{P} \longrightarrow \mathcal{P}$, $v^*(\alpha) = 1_{\mathcal{P}}$, y*
3. *para toda álgebra booleana $\mathcal{P}$ y toda $V : \mathbb{P} \longrightarrow \mathcal{P}$, $V^*(\alpha) = 1_{\mathcal{P}}$.*

DEMOSTRACIÓN. $(3 \Rightarrow 2)$ es inmediato.

$(2 \Rightarrow 1)$ Supongamos α no es una tautología, sea $v : \mathbb{P} \longrightarrow 2$ tal que $v^*(\alpha) = 0$. Sea $\mathcal{P}$ cualquier álgebra booleana. Consideremos el homomorfismo $\varphi : 2 \longrightarrow \mathcal{P}$ dado por $\varphi(0) = 0_{\mathcal{P}}$ y $\varphi(1) = 1_{\mathcal{P}}$. De este modo, $w := \varphi \circ v : \mathbb{P} \to \mathcal{P}$ es una asignación tal que $w^*(\alpha) = 0$.

$(1 \Rightarrow 3)$ Supongamos que existe un álgebra booleana $\mathcal{P}$ y una función $v : \mathbb{P} \to \mathcal{P}$ tal que $v^*(\alpha) \neq 1_{\mathcal{P}}$. Entonces $v^*(\neg\alpha) = v^*(\alpha)^c \neq 0_{\mathcal{P}}$. De este modo, el conjunto $\{v^*(\neg\alpha)\}$ tiene la pif. Por Teorema del Ultrafiltro 2.35 existe un ultrafiltro F en $\mathcal{P}$ tal que $v^*(\neg\alpha) \in F$. Ahora definamos $w : \mathbb{P} \longrightarrow 2$ de la siguiente manera: $w(P) = 1$ si y sólo si

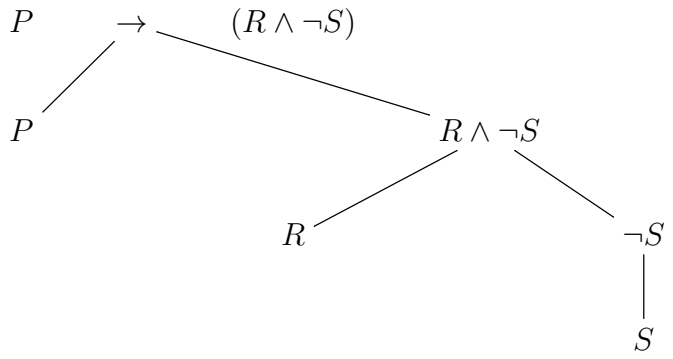
$v(P) \in F$. Se deja como ejercicio demostrar por inducción que para cada fórmula β, $w^*(\beta) = 1$ si y sólo si $v^*(\beta) \in F$. Así w es una asignación para la cual $w(\alpha) = 0$, demostrando que α no es tautología. □

Ejercicios 6.

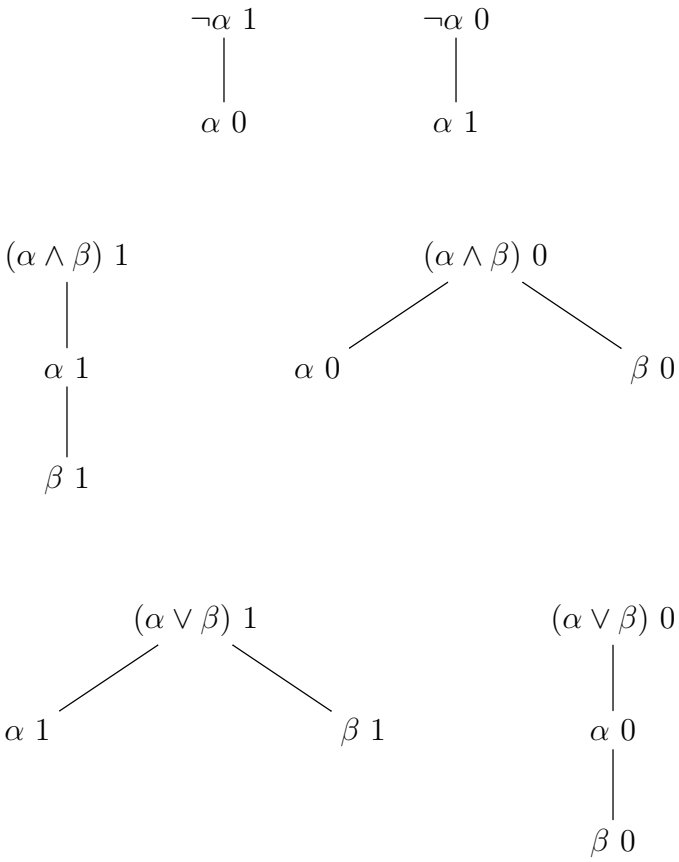
1. Demuestre que las siguientes familias de conjuntos tienen la pif. Describa al filtro generado por ellos y a su ideal dual.
   a) $\{(a, \infty) \subseteq \mathbb{R} : a \in \mathbb{R}\}$
   b) $\{A \subseteq \kappa : A$ es cerrado y no acotado$\}$, donde κ es un cardinal.
   c) $\{A \subseteq \mathbb{R} : A$ denso y abierto$\}$
   d) $\{A \subseteq [0,1] : \lambda(A) = 1\}$, donde λ es la medida de Labesgue sobre $[0,1]$.
2. Sea φ un homomorfismo de álgebras booleanas y a y b en el dominio de φ. Demuestre que $\varphi(a \vee b) = \varphi(a) \vee \varphi(b)$ y que si $a \leq b$ entonces $\varphi(a) \leq \varphi(b)$.
3. Complete la demostración de la Proposición 2.22.
4. Demuestre la proposición 2.27.
5. Demuestre la reflexividad y simetría en la Proposición 2.29.
6. Demuestre (3) en la proposición 2.30.
7. Complete la demostración de la Proposición 2.33.
8. Demuestre que si el filtro fijo F_a es ultrafiltro entonces a es un átomo.
9. Complete la demostración del Teorema 2.37.

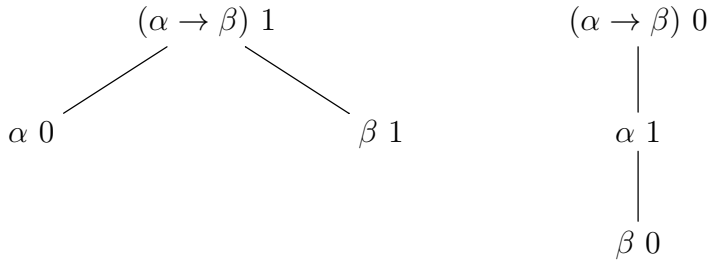
2.4. Árboles signados. En esta sección estudiaremos el método de *árboles signados* que de modo ágil permite reconocer tautologías e implicación y equivalencia lógica. Su agilidad es notable comparada con las tablas de verdad, las cuales suelen requerir demasiados cálculos cuando quedan involucradas muchas letras proposicionales.

Recuerde el lector que las fórmulas proposicionales han sido construidas recursivamente, teniendo como base a las letras proposicionales, de modo que cada fórmula lleva implícito un *árbol de construcción*, en cuyos nodos quedan las subfórmulas de la fórmula dada. Por ejemplo, el árbol de construcción para la fórmula $P \to (R \wedge \neg S)$ se muestra a continuación:



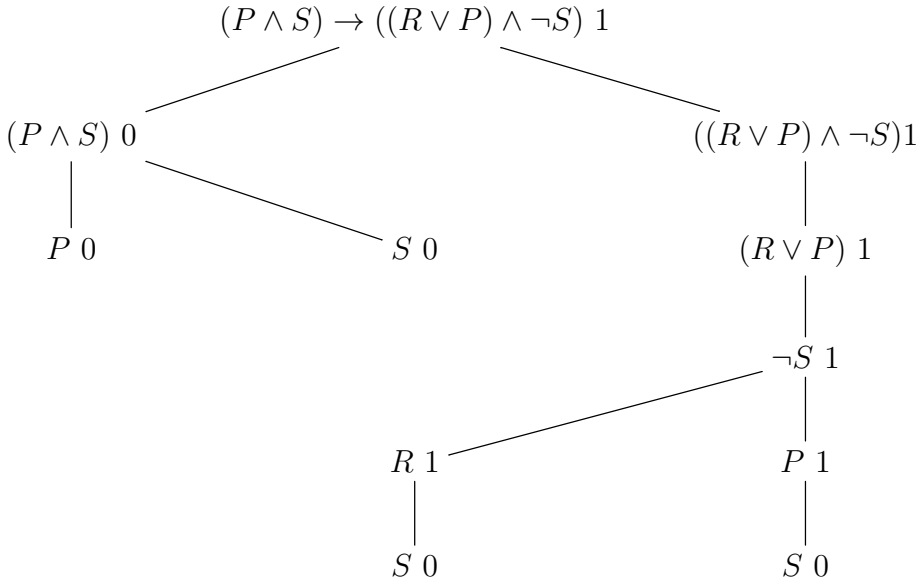
En un árbol signado igualmente descompondremos una fórmula en sus subfórmulas, pero ahora en términos de un *signo* previamente establecido. Este signo será 0 o 1, y se seguirán las siguientes reglas de descomposición de nodos.





Observe que hay dos tipos de reglas: las de *bifurcación* y las *descendentes*. Las reglas descendentes tienen prioridad sobre las de bifurcación y el desglose de fórmulas deberá ser exhaustivo, es decir, antes de desglosar una fórmula deben haber sido desglosadas las fórmulas de nivel superior.

EJEMPLO 2.38. El árbol signado para la fórmula $(P \wedge S) \to ((R \vee P) \wedge \neg S)\ 1$ es:



DEFINICIÓN 2.39. Decimos que una rama está *muerta* si hay una letra proposicional P tal que $P\ 0$ y $P\ 1$ aparecen en tal rama. Una rama esta *viva* si y sólo si no esta muerta.

PROPOSICIÓN 2.40. *Sea $S = 0$ o $S = 1$. Entonces toda rama viva para el árbol signado $\alpha\ S$ induce una asignación v tal que $v^*(\alpha) = S$. Tal asignación consiste simplemente en $v(P) = 1$, si $P\ 0$ no aparece en tal rama, y $v(P) = 0$ en otro caso. Inversamente, para cada asignación v, si $v^*(\alpha) = S$ entonces el árbol $\alpha\ S$ tiene una rama viva tal que*

para cada letra proposicional P, si en tal rama aparece P c entonces $v(P) = c$.

Demostración. Demostraremos la primera parte por inducción sobre la formación de α. El caso base es obvio. Mostraremos los casos más ilustrativos, dejando el resto como ejercicio para el lector. Supongamos que α es de la forma $\neg\beta$ y $S = 1$. Por hipótesis de inducción, una rama viva del árbol signado β 0 nos da una asignación v que satisface que $v^*(\beta) = 0$. Por lo tanto $v^*(\neg\beta) = 1$. Si α es de la forma $\beta \wedge \gamma$ y $S = 0$ entonces una rama viva para α 0 es o bien una rama viva para β 0 o una rama viva para γ 0. Supongamos que β 0 tiene tal rama viva. Por hipótesis de inducción, existe una asignación v tal que $v^*(\beta) = 0$. Por tanto, $v^*(\alpha) = 0$. Si α es de la forma $\beta \wedge \gamma$ y $S = 1$, entonces la rama viva de α 1se puede descomponer en dos ramas vivas de β 1 y γ 1 respectivamente, que además están de acuerdo en sus letras proposicionales, es decir, no hay una letra proposicional P de modo tal que P 0 aparezca en una de ellas y P 1 aparezca en la otra. Por hipótesis de inducción, tendremos una asignación v tal que $v^*(\beta) = 1 = v^*(\gamma)$. Por lo tanto, $v^*(\alpha) = 1$.

Para la segunda parte también procederemos por inducción sobre la formación de α. El caso en el que α es una letra proposicional es trivial. El caso en el que α es de la forma $\neg\beta$ se sigue directamente de la hipótesis de inducción, lo mismo que en los casos en los que el árbol se bifurca. El caso representativo del árbol que se extiende de manera descendente es cuando α es de la forma $\beta \wedge \gamma$ y $S = 1$. Por hipótesis de inducción, β 1 y γ 1 tienen (cada uno) una rama viva, en las que ambas satisfacen que para cada letra proposicional P, si en tal rama aparece P c, entonces $v(P) = c$. Esto quiere decir que para este par de ramas, no habrá una letra proposicional P tal que P 0 aparezca en una mientras que P 1 aparece en la otra. Por tanto, trenzando estas dos ramas, obtendremos una rama de α 1 que satisface las condiciones del teorema. □

Teorema 2.41 (Completud-Correctud). *α es una tautología si y sólo si todas las ramas del árbol α 0 están muertas.*

Demostración. ($\Rightarrow$) Por la Proposición 2.40, si α 0 tiene una rama viva, entonces hay una asignación v tal que $v^*(\alpha) = 0$, por lo que tal α no es tautología. ($\Leftarrow$) Si α no es tautología entonces hay una asignación v el árbol α 0 tiene una rama viva. □

Ejercicios 7.

1. Mediante el método de árboles signados determine cuáles de las siguientes fórmulas son tautologías:

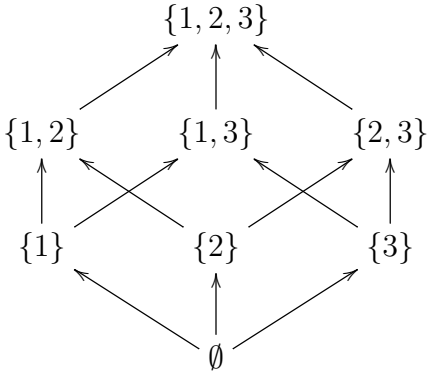
a) $((\neg P \vee Q) \wedge R) \to (Q \wedge R)$
b) $(P \to (Q \to R)) \to ((P \to Q) \to (P \to R))$
c) $((P \to R) \wedge (P \to S)) \to (R \to S)$
d) $(P \to R) \wedge (P \to S) \to (P \to R \wedge S)$

2. Mediante el método de árboles signados, pruebe o refute que el conjunto $\{P \wedge Q, (R \vee Q) \to M\}$ implica lógicamente a la fórmula $(M \wedge P) \vee \neg R$.
3. Demuestra que $\{\alpha, \beta\} \models (\alpha \wedge \beta)$.
4. Demuestra que $\alpha \models (\alpha \vee \beta)$.
5. Demuestra que $\{\alpha, (\alpha \to \beta)\} \models \beta$.
6. Agregue las reglas que faltan a nuestra lista para fórmulas que contienen el signo de bicondicional.
7. Complete la demostración de la proposición 2.40.

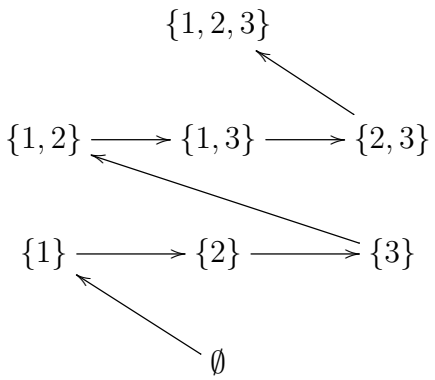
2.5. Satisfacibilidad e implicación lógica. Comenzaremos por plantear un problema aparentemente ajeno a la Lógica Proposicional.

PROBLEMA 2.42. *Dado un conjunto parcialmente ordenado* $(\mathcal{P}, \leq)$*, ¿existe un orden total para* $\mathcal{P}$ *que extienda a* $\leq$*?*

Consideremos el siguiente ejemplo. Sea $\mathcal{P} = \mathcal{P}\{1, 2, 3\}$ ordenado por contención. El siguiente diagrama nos muestra a $\mathcal{P}$ con este orden.



Es sencillo encontrar muchos órdenes lineales que extienden al anterior. El mismo dibujo por niveles nos sugiere que con tan solo definir un orden lineal entre los elementos de un mismo nivel podemos obtener un orden lineal en todo nuestro conjunto $\mathcal{P}$. Una forma podría ser la siguiente (se omiten algunas flechas que se sobreentiende que están):



En general, para cualquier conjunto parcialmente ordenado finito podemos hacer una extensión de este estilo, ordenando nivel por nivel. Sin embargo cuando el conjunto es infinito, no queda claro que haya niveles ni que los niveles estén linelmente ordenados, como en los conjuntos finitos. En este caso es en el que podemos utilizar la Lógica Proposicional.

Definamos un lenguaje de proposiciones

$$\mathbb{P} = \{A(p,q) : p, q \in \mathcal{P}\}, \tag{1}$$

es decir asignemos una letra proposicional a cada par ordenado de puntos del conjunto. Codifiquemos al orden parcial considerando el siguiente conjunto

$$B = \{A(p,q) : p \leq q\}.$$

La propiedad de orden parcial se puede codificar a través el conjunto

$$C = \{A(p,p) : p \in \mathcal{P}\} \cup \{\neg(A(p,q) \wedge A(q,p)) : p \neq q\}$$
$$\cup\{(A(p,q) \wedge A(q,r)) \to A(p,r) : p, q, r \in \mathcal{P}\}.$$

Y el siguiente conjunto B codifica la propiedad de ser orden total.

$$D = \{(A(p,q) \vee A(q,p)) : p, q, \in \mathcal{P}\}.$$

Nuestro sueño dorado sería encontrar una asignación $v : \mathbb{P} \to 2$ tal que para toda α en $B \cup C \cup D$, $v^*(\alpha) = 1$, pues en caso de tenerla, el orden total $\sqsubseteq$ que extendería a $\leq$ podría quedar definido por:

$$a \sqsubseteq b \text{ si y sólo si } v^*(A(a,b)) = 1. \tag{2}$$

El lector queda comprometido a verificar los detalles a manera de ejercicio. La pregunta es ¿existe tal asignación? Hagamos un poco de teoría al respecto

Definición 2.43. Un conjunto T de fórmulas proposicionales en un lenguaje $\mathbb{P}$ es *satisfacible* si existe una asignación $v : \mathbb{P} \to 2$ tal que para toda fórmula α en T, $v^*(\alpha) = 1$.

En el caso del problema anterior, precisamente el sueño dorado consiste en ver si $T = B \cup C \cup D$ es satisfacible. Cuando T consta de una sola fórmula α, T es satisfacible si y sólo si α no es una contradicción. Cuando T es finito, T es satisfacible si y sólo si la conjunción de sus fórmulas no es una contradicción. En consecuencia, verificar la satisfacibilidad de un conjunto finito de fórmulas se reduce al problema dual de verificar si una fórmula es una tautología. En términos de árboles signados, α es satisfacible si y sólo si el árbol $\alpha 1$ tiene una rama viva. El lector encontrará la oportunidad de divertirse demostrando todos estos hechos a la manera de un ejercicio.

En oposición a la sencillez del problema de la satisfacibilidad finita, se encuentra el problema de verificar que una familia infinta de fórmulas es satisfacible. Con el fin de ahorrar escritura, diremos que un conjunto de fórmulas proposicionales T es *finitamente satisfacible* (finsat) si cada subconjunto finito de T es satisfacible. El siguiente teoremón resuelve el problema de la satisfacibilidad de conjuntos infinitos de fórmulas.

TEOREMA 2.44. *(Compacidad) Sea T un conjunto de fórmulas de un lenguaje proporcional $\mathbb{P}$. Si T es finsat entonces T es satisfacible.*

Daremos dos pruebas distintas para este teorema.

2.5.1. Primera prueba (usando Lema de König, para T numerable). Para esta demostración del teorema necesitamos demostrar primero el *Lema de König.*

DEFINICIÓN 2.45. Un árbol A es un conjunto parcialmente ordenado con elemento mínimo (llamado *raíz*) y tal que para cada $t \in A$, el conjuntos de predecesores de t, $pred_A(t) = \{s \in A : s \leq t\}$ está bien ordenado.

Observe que todo nodo $s \in A$, el cual tenga un sucesor $t > s$, tiene un sucesor inmediato. Denotaremos:

$$succ_A(s) = \{t \in A : t \text{ es sucesor inmediato de } s\}.$$

Decimos que A tiene *ramificación finita* si para cada $s \in A$, el conjunto de sucesores inmediatos de s es finito. Una *rama* de A es un subconjuntos R de$A$ linealmente ordenado maximal respecto a la contención.

LEMA 2.46. *(König) Si A es un árbol infinito con ramificación finita, entonces A tiene una rama infinita.*

DEMOSTRACIÓN. Sea $B = \{s \in A : s$ tiene una infinidad de sucesores$\}$. Es claro que la raíz está en B. Además, cada que $s \in B$ existe $s' \in succ_A(s)$ tal que $s' \in B$, ya que de lo contrario, si cada

$s' \in succ_A(s)$ tuviese una cantidad finita de sucesores entonces, como unión finita de finitos es finito, tenemos que $s \notin B$, contradicción. Sea x_0 la raíz de A, supongamos definido x_n y elijamos $x_{n+1} \in succ_A(x_n)$ con la única restricción de que tenga una infinidad de sucesores. Sea $R \subseteq A$ una rama tal que $\{x_n : n \in \omega\} \subseteq R$. Tal rama existe por zornificación, y claramente es infinita. □

Ahora si, la demostración del Teorema de Compacidad, para T numerable.

Demostración. Sea $T = \{\alpha_n : n < \omega\}$, definimos un árbol A como sigue: Llamaremos A_0 al árbol signado de α_0 1. Supongamos que está definido el árbol A_n. Al final de cada rama viva de A_n colgaremos una copia del árbol signado α_{n+1} 1. Note que A_{n+1} tiene una rama viva ya que $\{\alpha_k : k \leq n+1\}$ es satisfacible. Sea $A = \bigcup_{n=0}^{\infty} A_n$. Observe que A es un árbol infinito de ramificación finita. Por Lema de König, A tiene una rama infinita R. Observe que una rama infinita debe seguir una infinidad de ramas vivas de árboles α_k 1. Sea $v : \mathbb{P} \to 2$ tal que $v(P) = 1$ si P 1 está en R y $v(P) = 0$ si P 1 no está en R. Así, $v(\alpha_n) = 1$ para toda $n \in \omega$. □

2.5.2. Segunda Prueba (definiendo el álgebra de Lindenbaum y usando el Teorema del Ultrafiltro). El *álgebra de Lindenbaum* $\mathbb{L}$ para un lenguaje proposicional $\mathbb{P}$, se define como el cociente de la familia de $\mathbb{P}$-fórmulas, módulo la siguiente relación de equivalencia:

$$\beta \sim \gamma \text{ si y sólo si } \models \beta \leftrightarrow \gamma.$$

Ordenamos a $\mathbb{L}$ como sigue:

$$[\alpha] \leq [\beta] \text{ si y sólo si } \alpha \models \beta.$$

Se verifica facilmente que (ver ejercicios):

Proposición 2.47. *Se cumplen las siguientes afirmaciones.*

- $\leq$ *no depende de representantes*
- *Las tautologías forman una clase de equivalencia, y ésta es el máximo de* $\mathbb{L}$.
- *Las contradicciones también forman una clase de equivalencia y ésta es el mínimo de* $\mathbb{L}$.
- $[\alpha \wedge \beta] = [\alpha] \wedge [\beta]$ *y* $[\alpha \vee \beta] = [\alpha] \vee [\beta]$
- *Todo subconjunto finito de* T *es satisfacible si y sólo si* $\bar{T} = \{[\alpha] : \alpha \in T\}$ *tiene la p.i.f.*

Sea U un ultrafiltro en $\mathbb{L}$ que extienda a $\bar{T}$, definamos $v : \mathbb{P} \to 2$ por $v(P) = 1$ si y sólo si $[P] \in U$. Es fácil demostrar por inducción sobre la formación de fórmulas, que para cada fórmula β, $v^*(\beta) = 1$ si

y sólo si $[\beta] \in U$ (ver ejercicios). Así, como para toda $\alpha \in T$, $[\alpha] \in U$, tenemos que $v^*(\alpha) = 1$. Por lo tanto T es satisfacible. □

Ejercicios 8.

1. Demuestra que si $T = \{\alpha\}$ entonces T es satisfacible si y sólo si α no es una contradicción si y sólo si α 1 tiene una rama viva.
2. Demuestra que si $T = \{\alpha_1, \ldots, \alpha_n\}$ entonces T es satisfacible si y sólo si $\alpha_1 \wedge \cdots \wedge \alpha_n$ es satisfacible.
3. Considere el lenguaje $\mathbb{P}$ definido en la ecuación (1) 1. Sea $v : \mathbb{P} \to 2$ de modo tal que para cada fórmula α en $B \cup C \cup D$, se cumple que $v^*(\alpha) = 1$. Sea $\sqsubseteq$ la relación definida en 2. Dé una demostración detallada de que $\sqsubseteq$ es un orden total sobre $\mathcal{P}$ que extiende a $\leq$.
4. Dé una prueba detallada de que la asignación v definida en el ejercicio anterior existe.
5. Demuestre la proposición 2.47.

2.6. Consecuencias del Teorema de Compacidad.

En esta sección daremos algunos ejemplos de la vida real (de un matemático) donde se resuelven problemas usando el Teorema de Compacidad para la Lógica Proposicional.

2.6.1. Graficas.

Una *gráfica* es un par $\langle G, E\rangle$ donde $G \neq \emptyset$ y $E \subseteq [G]^2 = \{\{n, m\} : n \neq m \in E\}$. Una *coloración* para una gráfica $\langle G, E\rangle$ es una función $f : G \to k$, tal que si $\{a, b\} \in E$ entonces $f(a) \neq f(b)$. A tal k se le considera el conjunto de colores. Decimos que $\langle G, E\rangle$ es *k-coloreable* si hay una coloración de $\langle G, E\rangle$ en un conjunto con k colores.

Diremos que una gráfica $\langle H, F\rangle$ es una *subgráfica* de $\langle G, E\rangle$ si $H \subseteq G$ y $F \subseteq E$. Observe que si $\langle H, F\rangle$ es subgráfica de $\langle G, E\rangle$ y $\langle G, E\rangle$ es k-coloreable entonces $\langle H, E\rangle$ también es k-coloreable.

Proposición 2.48. *Si todas las subgráficas finitas de $\langle G, E\rangle$ son k-coloreables, entonces $\langle G, E\rangle$ es k-coloreable.*

Demostración. Sea $k \in \omega$, $\mathbb{P} = \{P(p, c) : p \in G, c \in k\}$. Considere los siguientes conjuntos de fórmulas:

- $A_1 = \{P(p, c) \to \neg(\bigvee_{d \neq c \in k} P(p, d)) : p \in G \wedge c \in k\}$.
- $A_2 = \{\neg(P(p, c) \wedge P(q, c)) : \{p, q\} \in E, c \in k\}$.
- $A_3 = \{\bigvee_{c \in k} P(p, c) : p \in G\}$.

Queda como ejercicio para el lector demostrar lo siguiente:

PROPOSICIÓN 2.49. *Una asignación v que satisface al conjunto $A_1 \cup A_2 \cup A_3$ induce una coloración f para nuestra gráfica en k colores: simplemente, sea $f(p) = c$ si y sólo si $v(P(p,c)) = 1$. Por el contrario, una coloración f para $\langle G, E\rangle$ induce una asignación v tal que $v(\alpha) = 1$ para toda fórmula α en $A_1 \cup A_2 \cup A_3$: simplemente definamos $v(P(p,c)) = 1$ si y sólo si $f(p) = c$.*

Y en efecto, tal asignación v existe porque que $A = A_1 \bigcup A_2 \bigcup A_3$ es finitamente satisfacible, lo cual es cierto poque precisamente en virtud de la proposición anterior y de la hipótesis, cada subconjunto finito de A es satisfacible. □

2.6.2. Órdenes parciales. Recuerde que una *cadena* en un conjunto parcialmente ordenado $\mathcal{P}$ es un subconjunto de $\mathbb{P}$ que está ordenado linealmente.

PROPOSICIÓN 2.50. *Si $\mathbb{P}$ es un conjunto parcialmente ordenado y $k \in \omega$, si cada subconjunto finito de $\mathbb{P}$ puede cubrirse con a lo más k cadenas, entonces $\mathbb{P}$ puede ser cubierto con a lo más k cadenas.*

DEMOSTRACIÓN. Sea $\mathbb{P} = \{A(p,q) : p, q \in \mathcal{P}\} \cup \{P(p,i) : p \in \mathbb{P} \wedge 0 \leq i < k\}$, y sean B y C como en el Problema 2.42. Defina un conjunto de fórmulas D que expresen el hecho de que un elemento p de $\mathcal{P}$ debe pertenecer a alguna cadena K_i. Defina otro conjunto de fórmulas E que exprese que cada K_i es una cadena. Verifique que $B \cup C \cup D \cup E$ es finitamente satisfacible y use el Teorema de Compacidad. □

2.6.3. Consecuencia lógica. La siguiente aplicación del Teorema de Compacidad es sobre la misma Lógica Proposicional.

El lector inspirado en la Proposición 2.23 puede demostrar el siguiente lema.

LEMA 2.51. *Sea T un conjunto satisfacible de fórmulas en un lenguaje proposicional $\mathbb{P}$, y sea α una fórmula del lenguaje $\mathbb{P}$. Entonces, $T \models \alpha$ si y sólo si $T \bigcup \{\neg\alpha\}$ no es satisfacible.*

Ahora bien, el siguiente Teorema es la versión del Teorema de Compacidad que fue enunciada en la Subsección 2.1.

TEOREMA 2.52. *Sea T un conjunto de fórmulas en un lenguaje proposicional $\mathbb{P}$, y sea α una fórmula del lenguaje $\mathbb{P}$. Entonces $T \models \alpha$ si y sólo si existe $T' \subseteq T$ finito tal que $T' \models \alpha$.*

DEMOSTRACIÓN. Note que el regreso es trivial. Probemos la ida. Si $T \models \alpha$ entonces $T \bigcup \{\neg\alpha\}$ no es satisfacible. Por Teorema de Compacidad, existe $T' \subseteq T$ finito tal que $T' \bigcup \{\neg\alpha\}$ no es satisfacible. Por el Lema anterior, $T' \models \alpha$. □

Ejercicios 9.

1. Demuestre la Proposición 2.49.
2. Complete la demostración del la Proposición 2.50.
3. Demuestre el Lema 2.51.
4. Demuestre el regreso del Teorema 2.52.
5. Demuestre que el Teorema 2.52 implica al Teorema de Compacidad.

3. Teoría de la prueba de la Lógica Proposicional

En esta sección, ejemplificaremos el modus operandi de la *teoría de la prueba* con el caso específico de la lógica proposicional. Enmarcaremos ahora a la lógica proposicional en un sistema deductivo *tipo Hilbert*. En general estos sistemas involucran los siguientes elementos:

1. Un lenguaje, que incluye símbolos y fórmulas.
2. Axiomas, que son algunas fórmulas particulares, y que típicamente son fáciles de reconocer.
3. Reglas de inferencia, que especifican cuándo una fórmula se deduce inmediatamente de otras, y que típicamente son sintácticas, es decir, están definida en términos de la formación de los símbolos, y no apelan al significado de las fórmulas.
4. Una noción de deducción, que especifica cuándo una fórmula se deduce (no necesariamente de manera inmediata) de otras, la cual también debe estar formulada en términos de la formación de los símbolos involucrados.

La notación es sugestiva: $T \vdash \alpha$ significa que la fórmula α se deduce de T (en un sistema específico). En nuestro caso:

1. El lenguaje y las fórmulas son un lenguaje proposicional $\mathbb{P}$, con las fórmulas que conocemos $\Phi(\mathbb{P})$.
2. Los axiomas son las fórmulas que están en la unión de los siguientes conjuntos:
   - $A1 = \{\alpha \to (\beta \to \alpha) : \alpha, \beta \in \Phi(\mathbb{P})\}$
   - $A2 = \{(\alpha \to \beta) \to ((\alpha \to (\beta \to \gamma)) \to (\alpha \to \gamma)) : \alpha, \beta, \gamma \in \Phi(\mathbb{P})\}$
   - $A3 = \{(\alpha \wedge \beta) \to \alpha : \alpha, \beta \in \Phi(\mathbb{P})\}$
   - $A4 = \{(\alpha \wedge \beta) \to \beta : \alpha, \beta \in \Phi(\mathbb{P})\}$
   - $A5 = \{\alpha \to (\beta \to (\alpha \wedge \beta)) : \alpha, \beta \in \Phi(\mathbb{P})\}$
   - $A6 = \{\alpha \to (\alpha \vee \beta) : \alpha, \beta \in \Phi(\mathbb{P})\}$
   - $A7 = \{\beta \to (\alpha \vee \beta) : \alpha, \beta \in \Phi(\mathbb{P})\}$
   - $A8 = \{(\alpha \to \gamma) \to [(\beta \to \gamma) \to (\alpha \vee \beta \to \gamma)] : \alpha, \beta, \gamma \in \Phi(\mathbb{P})\}$
   - $A9 = \{(\alpha \to \beta) \to ((\alpha \to \neg\beta) \to \neg\alpha) : \alpha, \beta \in \Phi(\mathbb{P})\}$

- $A10 = \{(\alpha \to \beta) \wedge (\beta \to \alpha)\} \to (\alpha \leftrightarrow \beta) : \alpha, \beta \in \Phi(\mathbb{P})\}$
- $A11 = \{(\alpha \leftrightarrow \beta) \to (\alpha \to \beta) : \alpha, \beta \in \Phi(\mathbb{P})\}$
- $A12 = \{(\alpha \leftrightarrow \beta) \to (\beta \to \alpha) : \alpha, \beta \in \Phi(\mathbb{P})\}$
- $A13 = \{\neg(\neg\alpha) \to \alpha : \alpha \in \Phi(\mathbb{P})\}$

3. La única regla de inferencia que consideraremos se llama *modus ponens* y actua como sigue. De las fórmulas α y $\alpha \to \beta$ se deduce β.
4. Una deducción en este sistema es una sucesión finita $\alpha_1, \ldots, \alpha_n$ de fórmulas tal que para cada $k \leq n$, o bien, α_k es un axioma (es decir, está en $A_1 \cup \cdots \cup A_{13}$), o bien existen $i, j < k$ tales que α_k se deduce por modus ponens de α_i y α_j, es decir, α_i es de la forma $\alpha_j \to \alpha_k$.

El sistema recién presentado fue tomado del libro de S. C. Kleene [**?**], y se le conoce como el *Cálculo Proposicional de Kleene*. Estrenemos el juguete nuevo.

Ejemplo 3.1. Haremos una deducción de la fórmula $P \to P$:

1. $P \to ((P \to P) \to P)$	$A1$
2. $(P \to (P \to P)) \to ((P \to ((P \to P) \to P)) \to (P \to P))$	$A2$
3. $P \to (P \to P)$	$A1$
4. $(P \to ((P \to P) \to P)) \to (P \to P)$	MP 2, 3
5. $P \to P$	MP 1, 4.

Es una buena costumbre enumerar el lugar que cada fórmula ocupa en la deducción, a la vez que se acompaña por la justificación de su presencia. Claramente, en el ejemplo anterior, la fórmula 1 está justificada por pertenecer al esquema A_1, mientras que la fórmula 4 se obtuvo por Modus Ponens a partir de las fórmulas 2 y 3.

La noción de deducción del Cálculo de Kleene se puede extender de modo que podamos hacer deducciónes utilizando *hipótesis*. Decimos que α se deduce de un conjunto de fórmulas (hipótesis) Γ si existe una sucesión finita de fórmulas $\alpha_1, \ldots, \alpha_n$ tales que $\alpha = \alpha_n$ y para cada $i = 1, \ldots, n$, o bien α_i esta en Γ, o α_i es un axioma (es decir, está en $A_1 \cup \cdots \cup A_{13}$), o bien se obtiene por Modus Ponens de α_j y α_l para algunos $j, l < i$.
Notación:

1. $\Gamma \vdash \alpha$ significa que α se deduce de Γ.
2. $\varnothing \vdash \alpha$ también se denotará por $\vdash \alpha$.
3. $\beta_1, \ldots, \beta_n \vdash \alpha$ significa que $\{\beta_1, \ldots, \beta_n\} \vdash \alpha$

Ejemplo 3.2. Demostremos que $A \wedge B, A \to (B \to C) \vdash C$.

1. $(A \wedge B) \to A$	$A3$
2. $A \wedge B$	Hipótesis
3. A	MP 1, 2
4. $(A \wedge B) \to B$	$A4$
5. B	MP 2, 4
6. $A \to (B \to C)$	Hip
7. $B \to C$	MP 3, 6
8. C	MP 5, 7.

Estamos en posición de hacer unas cuantas observaciones sencillas.

PROPOSICIÓN 3.3. *El Cálculo Proposicional de Kleene tiene las siguientes propiedades:*

- *Si* $\Delta \vdash \alpha$ *y* $\Delta \subseteq \Gamma$ *entonces* $\Gamma \vdash \alpha$.
- *Si* $\alpha_1, \ldots, \alpha_k$ *son fórmulas tales que* $\Gamma \vdash \alpha_i$ *para toda* $i = 1, .., k$ *y* $\{\alpha_1, \ldots, \alpha_k\} \vdash \beta$ *entonces* $\Gamma \vdash \beta$.
- *Si* $\Gamma \vdash \alpha \to \beta$ *entonces* $\Gamma, \alpha \vdash \beta$.
- *(Lema de finitud) Si* $\Gamma \vdash \alpha$ *entonces existe* $\Gamma_0 \subseteq \Gamma$ *tal que* $\Gamma_0 \vdash \Gamma$.

DEMOSTRACIÓN. (1) Toda deducción a partir de Δ lo es a partir de Γ cuando $\Delta \subseteq \Gamma$. (2) Si $L_1, L_2, \ldots, L_k$ son, respectivamente, deducciones de $\alpha_1, \alpha_2, \ldots, \alpha_k$ a partir de Γ, y L es una deducción de β a partir de $\{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ entonces la concatenación de las listas $L_1, L_2, \ldots, L_k, L$ es una deducción de β a partir de Γ (se deja como ejercicio al lector verificarlo). (3) Use la regla MP. (4) Sea $\alpha_1, \ldots, \alpha_n$ una deducción de α a partir de Γ, y sea $\Gamma_0 = \Gamma \cap \{\alpha_1, \ldots, \alpha_n\}$. Entonces $\alpha_1, \ldots, \alpha_n$ es una deducción de α a partir de Γ_0 (la verificación de este hecho queda también como ejercicio para el lector). □

Dos trucos útiles en la construcción de deducciones se muestran en la siguiente proposición.

PROPOSICIÓN 3.4.
1. *Si* $\Gamma \vdash \alpha$ *y* β *es cualquier fórmula, entonces* $\Gamma \vdash \beta \to \alpha$.
2. *Si* α *y* β *son dos fórmulas cualesquiera, entonces* $\alpha, \neg\alpha \vdash \beta$.

DEMOSTRACIÓN. Construyamos las deducciones correspondientes. (1) Supongamos que $\Gamma \vdash \alpha$. Como $\alpha \to (\beta \to \alpha)$ está en A_1, haciendo MP con esta fórmula y α obtenemos $\beta \to \alpha$. (2) Por (1), a partir de α y $\neg\alpha$ se obtiene $\neg\beta \to \alpha$ y $\neg\beta \to \neg\alpha$. Haciendo MP sucesivamente con la fórmula $(\neg\beta \to \neg\alpha) \to ((\neg\beta \to \alpha) \to \neg\neg\beta)$, la cual está en A_9,

obtenemos $\neg\neg\beta$. Haciendo MP con esta fórmula y $\neg\neg\beta \to \beta$, la cual está en $A13$, obtenemos β. □

El trucazo más popular es el siguiente, llamado también *Teorema de la Deducción*

TEOREMA 3.5. *Sea* $\Gamma \cup \{\alpha, \beta\}$ *un conjunto de fórmulas. Si* $\Gamma, \alpha \vdash \beta$ *entonces* $\Gamma \vdash \alpha \to \beta$.

DEMOSTRACIÓN. Supongamos que $\beta_1, \beta_2, \ldots, \beta_n$ es una deducción que muestra que $\Gamma, \alpha \vdash \beta$. Mostraremos inductivamente que para todo $i = 1, \ldots, n$, sucede que $\Gamma \vdash \alpha \to \beta_i$. Sea $i \in \{1, \ldots, n\}$.

- Si β_i es un axioma o está en Γ entonces $\Gamma \vdash \beta_i$, y por la Proposición 3.4(1), $\Gamma \vdash \alpha \to \beta_i$.
- Si β_i es α, entonces, en vista del ejemplo 3.1 tenemos que $\Gamma \vdash \alpha \to \alpha$.
- Si β_i se obtuvo por MP a partir de β_j y β_l con $j, l < i$, digamos β_l es $\beta_j \to \beta_i$ y suponemos que β_j y β_l cumplen el resultado, entonces:

1. $\Gamma \vdash \alpha \to \beta_j$	*hip*
2. $\Gamma \vdash \alpha \to (\beta_j \to \beta_i)$	*hip*
3. $\Gamma \vdash (\alpha \to \beta_j) \to ((\alpha \to (\beta_j \to \beta_i)) \to (\alpha \to \beta_i))$	$A2$
4. $\Gamma \vdash (\alpha \to (\beta_j \to \beta_i)) \to (\alpha \to \beta_i)$	MP 4, 1
5. $\Gamma \vdash \alpha \to \beta_i$	MP 3, 6

□

EJEMPLO 3.6. Daremos una deducción completa que muestre que

$$A \wedge B \vdash (A \to (B \to C)) \to C$$

Nótese que por el Teorema de la Deducción y el ejemplo 3.2 tenemos demostrado que $A \wedge B \vdash (A \to (B \to C)) \to C$. Este argumento esconde la demostración explícita, sin embargo, es posible reconstruirla siguiendo el algoritmo descrito en la demotración del TD. El algoritmo suele no ser eficiente, como se pordrá ver a continuación.

Conviene tener a la mano los 8 pasos de la deducción hecha en el ejemplo 3.2

1. $(A \wedge B) \to A$ $A3$
2. $((A \wedge B) \to A) \to ((A \to (B \to C)) \to ((A \wedge B) \to A))$ $A1$
3. $(A \to (B \to C)) \to ((A \wedge B) \to A)$ $MP1, 2$
4. $A \wedge B$ Hip
5. $(A \wedge B) \to (A \to (B \to C)) \to ((A \wedge B))$ $A1$
6. $((A \to (B \to C)) \to (A \wedge B)$ $MP5, 6$
7. $((A \to (B \to C)) \to (A \wedge B)) \to$
   $[(A \to (B \to C)) \to ((A \wedge B) \to A)] \to ((A \to (B \to C)) \to A)$ $A2$
8. $[(A \to (B \to C)) \to ((A \wedge B) \to A)] \to ((A \to (B \to C)) \to A)$ $MP6, 7$
9. $(A \to (B \to C)) \to A$ $MP9, 10$
10. $(A \wedge B) \to B$ $A4$
11. $((A \wedge B) \to B) \to ((A \to (B \to C)) \to ((A \wedge B) \to B))$ $A1$
12. $(A \to (B \to C)) \to ((A \wedge B) \to B)$ $MP10, 11$
13. $((A \to (B \to C)) \to (A \wedge B)) \to$
    $[(A \to (B \to C)) \to ((A \wedge B) \to B)] \to ((A \to (B \to C)) \to B)$ $A2$
14. $[(A \to (B \to C)) \to ((A \wedge B) \to B)] \to ((A \to (B \to C)) \to B)$ $MP6, 13$
15. $(A \to (B \to C)) \to B$ $MP12, 14$
16. $(A \to (B \to C)) \to$
    $(((A \to (B \to C)) \to (A \to (B \to C))) \to (A \to (B \to C)))$ $A1$
17. $((A \to (B \to C)) \to ((A \to (B \to C)) \to (A \to (B \to C))))$
    $\to (((A \to (B \to C)) \to (((A \to (B \to C)) \to (A \to (B \to C)))$
    $\to (A \to (B \to C))))) \to ((A \to (B \to C)) \to (A \to (B \to C))))$ $A2$
18. $(A \to (B \to C)) \to ((A \to (B \to C)) \to (A \to (B \to C)))$ $A1$
19. $((A \to (B \to C)) \to (((A \to (B \to C)) \to (A \to (B \to C)))$
    $\to (A \to (B \to C))))) \to ((A \to (B \to C)) \to (A \to (B \to C)))$ $MP\ 16, 17$
20. $(A \to (B \to C)) \to (A \to (B \to C))$ $MP\ 16, 19$
21. $(A \to (B \to C)) \to (A \to (B \to C)) \to$
    $[(A \to (B \to C)) \to A] \to [(A \to (B \to C)) \to (B \to C)]$ $A3$
22. $[(A \to (B \to C)) \to A] \to [(A \to (B \to C)) \to (B \to C)]$ $MP20, 21$
23. $(A \to (B \to C)) \to (B \to C)$ $MP9, 22$
24. $(A \to (B \to C)) \to (B \to C) \to$
    $[((A \to (B \to C)) \to B) \to ((A \to (B \to C)) \to C)]$ $A3$
25. $((A \to (B \to C)) \to B) \to ((A \to (B \to C)) \to C)$ $MP23, 24$
26. $(A \to (B \to C)) \to C$ $MP15, 25$

Analicemos la deducción anterior, a la luz de la deducción del ejemplo 3.2. Los pasos 1, 2 y 3 fueron la ejecución de la rutina que hay que seguir cuando tenemos un axioma, en este caso, uno que está en A3. Según la demostración del TD, esa misma rutina es la que se sigue cuando tenemos una fórmula del conjunto de hipótesis, el cual es el caso de la fórmula 2 de 3.2, así que los pasos 4 a 6 se dedicaron a ello. La fórmula 3 de 3.2 se obtiene por MP de los dos anteriores, y para ocuparnos de ello se ejecutó la rutina que marca la demostración del TD en los pasos 7 a 9. Las fórmulas 4 y 5 de 3.2 vuelven a ser obtenidas de los modos anteriormente descritos en los pasos 10 a 15, pero la fórmula 6 de 3.2, empleamos, como lo marca la demostración del TD, la rutina dada en el ejemplo 3.1, la cual consta de los pasos 16 a 20. El resto son dos aplicaciones de MP, para lo cual se emplea dos veces la rutina del TD para MP en los pasos 21 a 26.

PROPOSICIÓN 3.7. *Las siguientes reglas se pueden derivar en el Cálculo de Kleene.*

1. $\alpha \wedge \beta \vdash \alpha$
2. $\alpha \wedge \beta \vdash \beta$
3. $\alpha \vdash \neg\neg\alpha$
4. $\neg\neg\alpha \vdash \alpha$
5. $\alpha \vdash \alpha \vee \beta$
6. $\beta \vdash \alpha \vee \beta$
7. $\alpha, \beta \vdash \alpha \wedge \beta$
8. $\alpha, \beta \vdash \alpha \wedge \beta$
9. $\alpha \to \gamma, \beta \to \gamma \vdash (\alpha \vee \beta) \to \gamma$
10. $\neg\beta, \alpha \to \beta \vdash \neg\alpha$
11. $\alpha \to \beta, \beta \to \alpha \vdash \alpha \leftrightarrow \beta$
12. $\alpha \leftrightarrow \beta \vdash \alpha \to \beta$
13. $\alpha \leftrightarrow \beta \vdash \beta \to \alpha$
14. $\alpha \to \beta, \alpha \to \neg\beta \vdash \neg\alpha$
15. $\neg\alpha \to \beta, \neg\alpha \to \neg\beta \vdash \alpha$
16. $\alpha \vee \beta, \neg\beta \vdash \alpha$
17. $\alpha \vee \beta, \neg\alpha \vdash \beta$
18. $\alpha \to \beta \vdash \neg\beta \to \neg\alpha$
19. $\alpha \to \neg\beta \vdash \beta \to \neg\alpha$
20. $\neg\alpha \to \beta \vdash \neg\beta \to \alpha$
21. $\neg\alpha \to \neg\beta \vdash \beta \to \alpha$

Demostración. Derivaremos únicamente la regla 17, el resto quedará como ejercicio para el lector.

1. $\alpha \vee \beta, \neg\alpha, \alpha \vdash \beta$	regla derivada 4
2. $\alpha \vee \beta, \neg\alpha \vdash \alpha \to \beta$	TD
3. $\alpha \vee \beta, \neg\alpha \vdash \beta \to \beta$	Ejemplo 3.1
3. $\alpha \vee \beta, \neg\alpha \vdash (\alpha \vee \beta) \to \beta$	regla derivada 11
4. $\alpha \vee \beta, \neg\alpha \vdash \alpha \vee \beta$	Hipótesis
5. $\alpha \vee \beta, \neg\alpha \vdash \beta$	MP 4 y 5.

□

Ejercicios 10.

1. Demuestre que las Leyes de DeMorgan se deducen en Cálculo de Kleene.
2. Demuestre que si hay una deducción de $\vdash \alpha$ que consta de dos fórmulas, entonces hay una que consta de una sóla fórmula. ¿Podemos decir algo análogo sobre una deducción que conste de cuatro fórmulas?
3. Verifique los detalles faltantes en las demostraciones de los incisos 2, 3 y 4 de la Proposición **??**.
4. Calcule una cota para la cantidad de pasos que debería tener una deducción de $\Gamma \vdash \alpha \to \beta$, si se dispone de una deducción de $\Gamma \cup \{\alpha\} \vdash \beta$ que consta de 3 pasos. Haga lo mismo para una deducción que conste de n pasos.
5. Demuestre que todas las fórmulas de $A1$ a $A13$ son tatutologías. Si le duele la mano al arrastrar el lápiz, al menos convénzase de que lo son.
6. Demuestre que si α y $\alpha \to \beta$ son tautologias entonces β es una tautología.

3.1. Correctud consistencia y completud. El Cálculo de Proposiciones de Kleene pretende *producir* a todas las tautologías, es decir, toda tautología debe ser deducible en el Cálculo de Kleene, y sólo se deberían deducir tautologías en este cálculo. Empecempos por esto último.

Teorema 3.8. *(De correctud) Si* $\vdash \alpha$ *entonces* $\vDash \alpha$.

Demostración. Se sigue inmediatamente del ejercicio 10, incisos 5 y 6. □

La noción de deducción a partir de un conjunto de hipótesis también es correcta con respecto a la de consecuencia lógica, como se prueba en el siguiente Teorema.

Por útimo, la versión extendida del Teorema de Completud

TEOREMA 3.9. *(De correctud extendido) Si* $\Gamma \vdash \alpha$ *entonces* $\Gamma \vDash \alpha$.

DEMOSTRACIÓN. Sea $v : \mathbb{P} \longrightarrow 2$ tal que $\overline{v}(\beta) = 1$ para toda β en Γ. Entonces v también hace verdaderos a todos los axiomas y además, si $\overline{v}(\phi) = 1$ y $\overline{v}(\phi \to \psi) = 1$ entonces $\overline{v}(\psi) = 1$, es decir, MP preserva verdad. En consecuencia, v hará verdadera a cualquier fórmula que aparezca en una deducción desde Γ. □

En particular, no es posible deducir cualquier fórmula en el cálculo de Kleene, desde que no cualquiera es tautología. Más aún, el Cálculo de Kleene no puede deducir una fórmula a la vez que a la negación de tal fórmula.

DEFINICIÓN 3.10. Un conjunto Γ de fórmulas es *consistente* si no existe una fórmula α tal que $\Gamma \vdash \alpha$ y $\Gamma \vdash \neg\alpha$.

Inconsistencia implica trivialidad. La siguiente Proposición se queda como ejercicio para el lector.

La siguiente proposición es un hecho útil, que permite establecer que una proposición se sigue, cuando se sigue de una fórmula dada e independientemente, también de su negación.

PROPOSICIÓN 3.11. Γ *es inconsistente si y sólo si* $\Gamma \vdash \beta$ *para toda fórmula* β.

LEMA 3.12. *Sean* α *y* β *fórmulas y* Γ *un conjunto de fórmulas, entonces si* $\Gamma, \neg\beta \vdash \alpha$ *y* $\Gamma, \beta \vdash \alpha$ *entonces:* $\Gamma \vdash \alpha$

DEMOSTRACIÓN. Por teorema de la deducción y la hipótesis, tenemos que $\Gamma \vdash \neg\beta \to \alpha$ y $\Gamma \vdash \beta \to \alpha$. Usando las reglas derivadas (18) y (20) de 3.7, tenemos que $\Gamma \vdash \neg\alpha \to \neg\beta$ y $\Gamma \vdash \neg\alpha \to \beta$. Finalmente, usando la regla derivada (15) de 3.7, se tiene que $\Gamma \vdash \alpha$. □

En el sentido opuesto, veamos que todas las tautologías son deducibles en el Cálculo de Kleene.

TEOREMA 3.13. *(Completud) Si* $\vDash \alpha$ *entonces* $\vdash \alpha$.

DEMOSTRACIÓN. (Kálmar): Sea α cualquier fórmula proposicional, sean $P_1, \ldots, P_k$ las letras que aparecen en α y sea $v : \mathbb{P} \longrightarrow 2$ fija. Se define $\bar{P}_j$ y $\bar{\alpha}$ como sigue:

$$\bar{P}_j = \begin{cases} P_j & \text{si } v(P_j) = 1 \\ \neg P_j & \text{si } v(p_j) = 0 \end{cases}$$

y

$$\bar{\alpha} = \begin{cases} \alpha & \text{si } \overline{v}(\alpha) = 1 \\ \neg\alpha & \text{si } \overline{v}(\alpha) = 0 \end{cases}$$

LEMA 3.14. $\bar{p_1}, \ldots, \bar{p_k} \vdash \bar{\alpha}$.

DEMOSTRACIÓN. (del lema) Inducción sobre la formación de α.

1. Si α es una letra proposicional, entonces $k = 1$, α es P_1, y claramente $P_1 \vdash P_1$ y $\neg P_1 \vdash \neg P_1$, así que en ambos casos se tiene que $\bar{P_1} \vdash \bar{P_1}$.
2. Supongamos que α es la negación de β y β cumple. Si $\overline{v}(\alpha) = 1$ entonces $\overline{v}(\beta) = 0$ y por tanto $\bar{\beta}$ es α, así que por hipótesis de inducción, $\bar{P_1}, \ldots, \bar{P_k} \vdash \alpha$. Si $\overline{v}(\alpha) = 0$ entonces $\overline{v}(\beta) = 1$ y consecuentemente $\bar{\beta}$ es β. Por hipótesis de inducción $\bar{P_1}, \ldots, \bar{P_k} \vdash \beta$, pero $\bar{\alpha}$ es $\neg\alpha$ y por tanto $\bar{\alpha}$ es $\neg\neg\beta$, así que usando la regla derivada 3.7(3), tenemos que $\bar{p_1}, \ldots, \bar{p_k} \vdash \neg\neg\beta$.
3. Si α es $\beta \wedge \gamma$ y β y γ cumplen, entonces consideramos dos casos:
   Caso 1. Si $\overline{v}(\alpha) = 1$, entonces $\overline{v}(\beta) = 1 = \overline{v}(\gamma)$, por lo tanto $\bar{\alpha}$ es α, $\bar{\beta}$ es β y $\bar{\gamma}$ es γ. Por hipótesis de inducción se tiene que $\bar{p_1}, \ldots, \bar{p_k} \vdash \beta$ y $\bar{p_1}, \ldots, \bar{p_k} \vdash \gamma$ y por tanto, $\bar{p_1}, \ldots, \bar{p_k} \vdash \beta \wedge \gamma$.
   Caso 2. Si $\overline{v}(\alpha) = 0$, entonces: $\overline{v}(\beta) = 0$ o $\overline{v}(\gamma) = 0$. Supongamos lo primero, en vista de que el otro caso es análogo. De este modo, $\bar{\alpha}$ es $\neg\alpha$ y $\bar{\beta}$ es $\neg\beta$. Por hipótesis de inducción se tiene que $\bar{p_1}, \ldots, \bar{p_k} \vdash \neg\beta$. Observe además que $\bar{p_1}, \ldots, \bar{p_k} \vdash (\beta \wedge \gamma) \to \beta$, por ser un axioma de $A3$. Por la regla derivada 10, tenemos que $\bar{p_1}, \ldots, \bar{p_k} \vdash \neg(\beta \wedge \gamma)$.
4. El resto de la demostración se deja como ejercicio al lector, con la pista de que la estrategia es la misma que la utilizada en el caso de la conjunción.

□

Regresando a la prueba del Teorema de Completud, sea $LP(\alpha) = \{p_1, \ldots, p_n\}$ el conjunto de letras proporcionales que aparecen en α. Como α es una tautología, para cada asignación v, $\bar{\alpha}$ es α. Por el lema anterior, $\bar{p_1}, \ldots \bar{p_k} \vdash \alpha$. Por lo tanto $\bar{p_1}, \ldots \bar{p_{k-1}}, p_k \vdash \alpha$ y $\bar{p_1}, \ldots \bar{p_{k-1}}, \neg p_k \vdash \alpha$. Por el Lema 3.12 se tiene que $\bar{p_1}, \ldots \bar{p_{k-1}} \vdash \alpha$. Repitiendo ese argumento $k - 1$ veces tenemos que $\vdash \alpha$. □

Por último, enunciaremos la versión extendida del Teorema de Completud, dejando su demostración al lector,

TEOREMA 3.15. *(Completud extendido) Si* $\Gamma \models \alpha$ *entonces* $\Gamma \vdash \alpha$.

EJERCICIOS 11.

1. Demuestre la proposición 3.11.
2. Demuestre que si Γ es consistente entonces $\Gamma \cup \{\alpha\}$ es consistente o $\Gamma \cup \{\neg\alpha\}$ lo es, para cualquier fórmula α.
3. Demuestre el Teorema de Completud Extendido. Sugerencia: use el Teorema de Compacidad.

3.2. Formas Normales.

1. Disyuntiva:
   Sea α una fórmula con $P_1, \ldots, P_n$ letras proposicionales. Si α no es una contradicción, entonces existe una única (salvo permutaciones) fórmula β de la forma $\bigvee_{j=1}^{k} \beta_j$ donde cada β_j es de la forma

   $$\bar{P}_1 \wedge \ldots \wedge \bar{P}_n \text{ y cada } \bar{P}_i \text{ es o bien } P_i \text{ o } \neg P_i$$

   tal que $\beta \equiv \alpha$.
2. Conjuntiva:
   Sea α una fórmula con $P_1, \ldots, P_n$ letras proposicionales. Si α no es una tautología, entonces existe una única (salvo permutaciones) fórmula β de la forma $\bigwedge_{j=1}^{k} \beta_j$ donde cada β_j es de la forma

   $$\bar{P}_1 \vee \ldots \vee \bar{P}_n \text{ y cada } \bar{P}_i \text{ es o bien } P_i \text{ o } \neg P_i$$

   tal que $\beta \equiv \alpha$.

Demostración:

1. Para cada asignación $V : \mathbb{P} = \{P_1, \ldots, P_n\} \longrightarrow 2$ tal que $V^*(\alpha) = 1$, definamos

   $$\bar{P_i}^V = P_i \text{ si } V(P_i) = 1 \text{ o bien } \neg P_i \text{ si } V(P_i) = 0.$$

   Observe que $\bar{P_1}^V \wedge \ldots \wedge \bar{P_n}^V \models \alpha$, por que la única asignación W que hace verdaderas a todas $\bar{P_i}^V$ es V.

   Por lo tanto $\bar{P_1}^V \wedge \ldots \wedge \bar{P_n}^V \models \alpha$ para toda asignación V que haga verdadera a α.
   entonces $\beta := \bigvee \{\bar{P_1}^V \wedge \ldots \wedge \bar{P_n}^V : V^*(\alpha) = 1\} \models \alpha$.
   Ahora bien, sea $W : \mathbb{P} \longrightarrow 2$ tal que $W^*(\alpha) = 1$.
   Por lo tanto $W^*(\bar{P_1}^w \wedge \ldots \wedge \bar{P_n}^w) = 1$, entonces $W^*(\beta) = 1$.
2. Es la demostración dual de la Disyuntiva, es decir se hace considerando $V^*(\alpha) = 0$, y definiendo $\bar{P_i}^V$ para cada $i = 1, \ldots, n$ de modo que $\bar{P_i}^V = P_i$ si $V(P_i) = 0$ o bien $\neg P_i$ si $V(P_i) = 1$. $\square$

Ejemplo:

La forma normal disyuntiva: $P_1 \wedge (P_2 \rightarrow P_3) \equiv (P_1 \wedge P_2 \wedge P_3) \vee (P_1 \wedge \neg P_2 \wedge P_3) \vee (P_1 \wedge \neg P_2 \wedge \neg P_3)$

La forma normal conjuntiva: $P_1 \wedge (P_2 \rightarrow P_3) \equiv (\neg P_1 \vee \neg P_2 \vee \neg P_3) \wedge (P_1 \vee P_2 \vee \neg P_3) \wedge (P_1 \vee \neg P_2 \vee P_3) \wedge (P_1 \vee P_2 \vee \neg P_3) \wedge (P_1 \vee P_2 \vee P_3)$.

COROLARIO 3.16. *Toda fórmula proposicional equivalente a otra escrita sólo con* $\neg, \wedge, \vee$.

Más aún, toda fórmula proposicional equivale a otra escrita únicamente con $\neg, \vee$. Esto se puede por las Leyes de Morgan.

DEFINICIÓN 3.17. Un conjunto de conectivos G es completo si toda fórmula proposicional es equivalente a otra escrita únicamente usando conectivos de G.

Ejemplo:

- $\{\neg, \vee\}$, $\{\neg, \wedge\}$ son completos.
- $\{\neg, \rightarrow\}$ es completo, ya que $\beta \vee \gamma \equiv \neg\beta \rightarrow \gamma$.
- $\{\neg, \leftrightarrow\}$ no es completo, ya que por ejemplo no se puede deducir $\neg\beta \rightarrow \gamma$.

¿Existe algún conectivo el cual es completo por si solo?

Es decir, ¿ existe algún $*$ tal que $V(P * P) = 0 \Leftrightarrow V(P) = 1$?

Si existen, estos son $NAND$ y NOR.

Definimos $NAND$ y NOR como sigue:

$P \ \ NAND \ \ Q \equiv \neg(P \wedge Q)$.

$P \ \ NOR \ \ Q \quad \equiv \neg(P \vee Q)$.

EJERCICIOS 12. 1. Demostrar que $\{NAND\}$ y $\{NOR\}$ son conjuntos completos.

Capítulo 2

Lógica de Predicados

En cierto sentido la lógica de predicados es una extensión de la lógica de proposiciones ya que hereda los conectivos y los interpreta de la misma forma. Adicionalmente la lógica de predicados permite expresar relaciones entre individuos de un universo, operarlos, representar elementos arbitrarios a través de variables y cuantificar sobre ellos.

La lógica de predicados suele recurrir a símbolos de diferentes naturalezas. Un grupo de simbolos es común a cualquier interpretación de tal lenguaje, pero otros pueden o no ser necesarios. Esto dependerá del tipo de estructuras que se tengan en consideración.

1. Estructuras de Primer Orden

Antes de presentar los lenguajes de Primer Orden, delimitaremos los objetos a los que tienen como referente. Para nuestra fortuna, podemos echar mano de nuestra experiencia como matemáticos para extraer ejemplos. Uno clásico es $\mathbb{Z}$ el *anillo de los enteros*. Éste consta de un conjunto (que damos por bien conocido) Z, en el cual están definidas dos operaciones, la suma y la multiplicación. Cero se llama el elemento de Z que hace las veces de neutro aditivo, y uno se llama el neutro multiplicativo. Tanto la suma como la multiplicación son *operaciones binarias*, es decir son funciones que a pares (ordenados) de números enteros, asignan nuevos números enteros, por ejemplo, la suma al par (3,2) le asigna el 5. Cero y uno son simples elementos de Z, pero distinguidos. En principio, carece de sentido sumar conjuntos de enteros, o funciones de enteros, las operaciones de suma y multiplicación sólo trabajan con elementos de Z y devuelven siempre elementos de Z.

En $\mathbb{Z}$ hay todavía más estructura que la de ser anillo. Todos conocemos bien el orden de $\mathbb{Z}$, el cual es una *relación binaria*, esto es, compete a pares de número enteros. Por ejemplo, $3 < 5$ pero no es el caso que $8 > 2$. No tiene sentido (al menos no en principio) preguntarse si un conjunto de enteros es menor que otro, o si una operación es menor que otra.

Definición 1.1. Una *estructura de primer orden* es una tupla $\mathbb{A} = \langle A, \mathcal{R}, \mathcal{O}, \mathcal{E} \rangle$ donde:

- A es un conjunto no vacío, llamado el *universo* o *dominio* de $\mathbb{A}$.
- $\mathcal{R}$ es una familia de relaciones sobre A, cada una de ellas con una *aridad*, es decir, para cada $R \in \mathcal{R}$ existe un entero positivo n tal que $R \subseteq A^n$. En este caso decimos que R es una relación n-aria.
- $\mathcal{O}$ es una familia de operaciones sobre A, cada una con su *aridad*, es decir, cada f en $\mathcal{O}$ es una función de A^n en A, donde n es la aridad de f.
- Los elementos de $\mathcal{E}$ son llamados *elementos distinguidos* de A, y no tienen más requisitos qué cumplir, que ser elementos de A.

Volviendo al ejemplo de los enteros, pordemos considerar a estos de diferentes maneras. Como anillo, los enteros se ven así:

$$\mathbb{Z} = \langle Z, \emptyset, \{+, \times\}, \{0, 1\}\rangle$$

donde $\emptyset$ significa que no se consideran relaciones, $+$ y $\times$ son dos operaciones, debiendo especificar que ambas son binarias, y 0 y 1 son elementos distinguidos.

Como estructura ordenada, podemos considerar a los enteros como

$$\mathbb{Z}' = \langle Z, \{<\}, \emptyset, \emptyset\rangle$$

debiendo especificar que $<$ es una relación binaria.

La definición de estructura de primer orden nos autoriza a considerar a los enteros con todas o más o ninguna de estas relaciones, operaciones y elementos distinguidos. Por ejemplo, podemos *expandir* a $\mathbb{Z}$ agregando el orden, y obtenemos

$$\mathbb{Z}'' = \langle Z, \{<\}, \{+, \times\}, \{0, 1\}\rangle.$$

En general, las estructuras de primer orden se pueden expandir o reducir, lo cual sólo significa que se va a poner atención a algunas de las relaciones, operaciones o elementos de éstas, sin que por ello los objetos matemáticos cambien. Sólo por no dejar pasar la ocasión daremos la definición precisa de expansión y reducción.

Definición 1.2. Sean $\mathbb{A} = \langle A, \mathcal{R}, \mathcal{O}, \mathcal{E}\rangle$ y $\mathbb{B} = \langle B, \mathcal{R}', \mathcal{O}', \mathcal{E}'\rangle$ dos estructuras de primer orden. Decimos que $\mathbb{A}$ es un reducto de $\mathbb{B}$, o que $\mathbb{B}$ es una expansión de $\mathbb{A}$ si $A = B$, $\mathcal{R} \subseteq \mathcal{R}'$, $\mathcal{O} \subseteq \mathcal{O}'$ y $\mathcal{E} \subseteq \mathcal{E}'$.

Otro modo de comparar estructuras es por su tipo. No daremos ahora una definición del tipo de una estructura, lo cual es útil pero engorroso, mejor diremos cuándo dos de ellas tienen el mismo tipo.

Definición 1.3. Decimos que $\mathbb{A}$ y $\mathbb{B}$ *tienen el mismo tipo* si hay biyecciones t_1, t_2, t_3 de $\mathcal{R}$, $\mathcal{O}$ y $\mathcal{E}$ en $\mathcal{R}'$, $\mathcal{O}'$ y $\mathcal{E}'$ respectivamente, que preservan aridades, es decir, si $R \in \mathcal{R}$ entonces la aridad de $t_1(R)$ es

igual a la aridad de R y si $f \in \mathcal{O}$ entonces la aridad de $t_2(f)$ es igual a la aridad de f.

Por ejemplo, todos los anillos y los campos tienen el mismo tipo, mientras que los grupos aditivos de anillos son reductos de anillos.

Ahora explicaremos qué tiene de *primero* el primer orden de estas estructuras. El asunto es sencillo. La estructura considerada concierne sólo a *individuos de un universo*. Relacionar individuos, operar individuos y distinguir individuos es lo que se permite en primer orden. Lo que no se permite es operar o relacionar conjuntos de inviduos, operar o relacionar operaciones o relaciones entre individuos, ni entre conjuntos de conjuntos de individuos, etc. Las estructuras que consideran tales posibilidades no son de primer orden, por ejemplo los espacios topológicos son estructuras de segundo orden. Teniendo la herramienta del lenguaje, podremos abundar sobre esta diferencia.

Como comentario final, se debe señalar que el estudio de las estructuras matemáticas, es decir, su clasificación y demás aspectos, son lo que se conoce como *álgebra universal*. En lo sucesivo seguiremos estudiando más de esos aspectos, pero por lo pronto conviene regresar a los lenguajes de predicados de primer orden.

Ejercicios 13.

1. Es obvio que el grupo aditivo de un anillo es un reducto de tal anillo. ¿Será que todo grupo es reducto de un anillo? Sugerencia: consulte un algebrista.
2. ¿Es posible expandir o reducir a un anillo para que sea del mismo tipo que una álgebra booleana?
3. ¿Los espacios vectoriales son estructuras de primer orden? ¿y los grafos (dirigidos y sin dirigir)?

2. Lenguajes de Primer Orden

Los lenguajes de primer orden están diseñados para ser interpretados en estructuras de primer orden, así que para diferentes tipos de estructuras, serán adecuados diferentes tipos de lenguajes. En común, los lenguajes de primer orden incluyen los siguientes símbolos básicos:

1. Variables individuales: Un conjunto infinito numerable, típicamente usaremos $v_0, v_1, v_2, \ldots$.
2. Símbolo de igualdad $=$
3. Conectivos: Los mismos que en lógica proposicional.
4. Cuantificadores: Universal $\forall$ y existencial $\exists$.
5. Símbolos auxiliares: paréntesis derecho), coma , y paréntesis izquierdo (.

Y según el tipo de estructuras que deseemos discutir, un lenguaje de predicados de primer orden (en lo sucesivo lppo) contendrá símbolos de relación que se llamarán *letras predicativas*, símbolos de operación que llamaremos *letras funcionales* y símbolos de constante que llamaremos *constantes individuales*. Los lenguajes se vincularán con las estructuras en virtud de su tipo.

DEFINICIÓN 2.1. Un *tipo* es un par $\rho = \langle \mathcal{L}, a \rangle$ donde $\mathcal{L}$ es un conjunto de símbolos, conformado por la unión de tres conjuntos ajenos y posiblemente vacíos, $\mathcal{P}$, $\mathcal{F}$ y $\mathcal{C}$, y a es una función de $\mathcal{P} \bigcup \mathcal{F}$ en los enteros positivos, que por razones naturales, llamaremos *aridad*.

La interpretación de un lppo de un tipo, debe ser una estructura del mismo tipo, es decir,

DEFINICIÓN 2.2. Sean ρ un tipo y $\mathbb{A} = \langle A, \mathcal{R}, \mathcal{O}, \mathcal{E} \rangle$ una estructura. Diremos que $\mathbb{A}$ es de tipo ρ, (o ρ-estructura) si existe una función $I : \mathcal{L} \to \mathcal{R} \cup \mathcal{O} \cup \mathcal{E}$ tal que

1. $I \restriction \mathcal{P}$ es una biyección de $\mathcal{P}$ sobre $\mathcal{R}$ que respeta aridades, es decir, la aridad de $I(P)$ es $a(p)$.
2. $I \restriction \mathcal{F}$ en una biyección de $\mathcal{F}$ sobre $\mathcal{O}$ que respeta aridades, es decir, la aridad de $I(f)$ es $a(f)$.
3. $I \restriction \mathcal{C}$ es una función de $\mathcal{C}$ sobre $\mathcal{E}$. Ojo: sólo tiene que ser suprayectiva, no tiene por qué ser biyectiva.

Una función I de este estilo se llama *función de interpretación*, y da la clave para interpretar todo lo correctamente escribible en el lenguaje $\mathcal{L}$ en una estructura del mismo tipo.

Volviendo al ejemplo de los enteros, un lenguaje del tipo adecuado para $\mathbb{Z}$ debe incluir dos letras funcionales digamos f y g con $a(f) = 2 = a(g)$ y dos constantes individuales, digamos c y d. Una interpretación posible es $I(f) = +$, $I(g) = \times$, $I(c) = 0$, $I(d) = 1$[1].

A continuación formaremos las expresiones de los lppo que pueden tener sentido. En este caso consideraremos dos sentidos diferentes. En primer lugar las expresiones cuyo referente es un elemento del universo, y en segundo lugar las que expresan que alguna relación se da entre individuos de ese universo.

DEFINICIÓN 2.3. (Informal) Término es una expresión que representa a un individuo de un universo.

[1]Conviene en este punto aclarar que estas ecuaciones intentan abreviar frases como *La interpretación de f es la operación suma*. De ningún modo se pretende decir que $I(f)$ es una crucecita

La anterior definición parece bien hecha, pero es un reto para el lector determinar si la expresión del español "Sinforiano" es o no un término de este lenguaje. El español carece de reglas para formar términos, pero un lenguaje que se precie de ser formal sí debe tenerlas. Procedemos a dar una definición formal de manera recursiva.

DEFINICIÓN 2.4. (Recursiva) Son términos de un lenguaje $\mathcal{L}$

- las variables,
- las constantes de $\mathcal{L}$, y
- las expresiones de la forma $f(t_1, \ldots, t_n)$ donde cada t_i es un término.

Entrados en gastos, distinguiremos las fórmulas de un lenguaje de predicados, dejando para después las interpretaciones.

DEFINICIÓN 2.5. (Informal) Fórmula es una expresión que se interpreta como alguna relación que puede ocurrir o no entre individuos del universo de interpretación.

Nuevamente, en el lenguaje español no tenemos un criterio para decidir si una expresión tiene sentido, o ya no digamos, que se pueda calcular su valor de verdad. En los lenguajes de predicados siempre hay reglas para definir las fórmulas, que capturan la intención de la definición informal, y que sirven como criterio para decidir cuándo una expresión es fórmula. La construcción de las fórmulas es recursiva, y a las expresiones que sirven como base se les llama *fórmulas atómicas*, que se pueden obtener de dos modos:

- Si t_1 y t_2 son términos $t_1 = t_2$ es fórmula atómica.
- Si P es un símbolo de relación de aridad n, y $t_1, \ldots, t_n$ son términos entonces $P(t_1, \ldots, t_n)$ es una fórmula atómica.

El paso recursivo de la construcción de fórmulas se describe como sigue:

- Las fórmulas atómicas son fórmulas.
- Si α y β son fórmulas entonces: $(\neg\alpha)$, $(\alpha \wedge \beta)$, $(\alpha \vee \beta)$, $(\alpha \to \beta)$, $(\alpha \leftrightarrow \beta)$ son fórmulas.
- Si α es una fórmula y x es variable, entonces: $\exists x\alpha$ y $\forall x\alpha$ son fórmulas.

EJERCICIOS 14.

1. Decida si las siguientes expresiones del español son o no términos:

   a) "La tierra"
   b) "Las pirámides de Egipto"
   c) "El amigo de la hermana de un señor que no vino a la fiesta"
   d) "El ave fénix"
2. Enumere los términos construibles en el lenguaje $\mathcal{L} = \emptyset$.
3. Demuestre que un término sólo involucra una cantidad finita de símbolos, lo mismo que una fórmula.
4. Si $\mathcal{L}$ es un lenguaje de primer orden que tiene una cantidad finita de símbolos, ¿cuántos términos del lenguaje $\mathcal{L}$ hay? ¿y si $\mathcal{L}$ es infinito numerable? ¿y si es infinito no numerable? ¿y cuántas fórmulas en cada caso?
5. Como ejercicio de inducción, pruebe que todo término y toda fórmula tienen tantos paréntesis izquierdos como derechos.
6. Enuncie y demuestre un principio de recursión para términos y otro para fórmulas, en el sentido del Teorema 1.2.

3. Semántica de la lógica de primer orden

Sean ρ un tipo con lenguaje $\mathcal{L}$, y $\mathbb{A}$ una estructura de tipo ρ, con función de interpretación I. La función de interpretación da la clave con la que podemos interpretar términos y calificar de verdaderas o falsas a las fórmulas.

3.1. Interpretación de términos. La interpretación de los ρ-términos se hace de manera recursiva, esto quiere decir que interpretaremos primero los términos más básicos, y luego los que se forman recursivamente. La función de interpretación hace la mitad del trabajo, pues las constantes y las letras funcionales están en el dominio de I, pero las variables no tienen modo de quedar interpretadas desde el principio, y qué bueno que así sea! La intención de tener variables es que éstas sean interpretables como cualquier individuo de su dominio de interpretación, sin restricciones. Así pues, la intepretación de términos se conseguirá con el auxilio de una especie de interpretación *ocasional* de las variables.

Un segundo detalle sobre las interpretaciones ocasionales es que probablemente tengamos que hacer muchas. Si un término incluye muchas variables, tenemos la obligación de interpretar a todas las que aparecen. Ya entrados en gastos, podemos de plano considerar a todas las posibles interpretaciones de todas las variables a la vez. Cada una de ellas no es más que una función s cuyo dominio es el conjunto de variables Var y su contradominio es A, el universo de $\mathbb{A}$. Llamaremos *asignación de valores a las variables* (avv) a las funciones de esta clase. Con esto, ahora definiremos la interpretación I_s de todos los términos en $\mathfrak{A}$,

bajo una avv s, recursivamente. Notemos ahora que tal interpretación es una función que va del conjunto de ρ-términos en A.

- Si t es una variable, digamos x, $I_s(t)$ es $s(x)$, es decir, el valor que s asigna a x.
- Si t es una constante, digamos c, $I_s(t)$ es el elemento distinguido $I(c)$ de $\mathfrak{A}$. También suele denotarse a $I_s(c)$ por $c^{\mathfrak{A}}$.
- Sea f una letra de funcional de aridad n, y sean $t_1, \ldots, t_n$ términos. Entonces la intepretación $I_s(f(t_1, \ldots, t_n))$ es el resultado de evaluar a $I(f)$ en la n-tupla $(I_s(t_1), I_s(t_2), \ldots, I_s(t_n))$.

Una primera observación destacable es que no hay términos que incluyan a todas las variables a la vez, puesto que éstas son una infinidad mientras que sólo una cantidad finita de ellas pueden estar incluidas en un término dado. La siguiente observación puntualiza el hecho de que la interpretación de variables que no aparecen en un término, es irrelevante para la interpretación de éste.

Observación 3.1. *Sean t un término, $x_1, x_2, \ldots x_n$ las variables que aparecen en t y s_1 y s_2 dos avv tales que $s_1(x_i) = s_2(x_i)$, para todo $i = 1, \ldots, n$. Entonces $I_{s_1}(t) = I_{s_2}(t)$.*

La demostración de este hecho queda como un sencillo ejercicio de inducción para el lector. Como consecuencia directa de 3.1 se tiene que $I_s(c) = I_{s'}(c)$ para cualesquiera asignaciones s y s' y toda constante c.

Una popular forma de definir términos es por sustitución. Dentro de un término, es posible distinguir términos más simples, por ejemplo, variables. Si disponemos de dos términos, digamos t y r, y la variable x aparece en t, podríamos reemplazar todas las apariciones de la variable x para poner en su lugar al término r.

Notación 3.2. *Denotaremos por $t(x/r)$ al término que resulta al reemplazar todas las apariciones de la variable x por r en t.*

Es más engorroso que útil, pero definiremos recursivamente esta operación, incluyendo el caso en el que x no apareciera en t.

Definición 3.3. Sean t y r dos términos y x una variable.

1. Si t es una variable, entonces tenemos dos casos:
   a) si t es la variable x entonces $t(x/r)$ es r,
   b) si t no es x entonces $t(x/r)$ es t.
2. Si t es una constante, entonces $t(x/r)$ es t.
3. Si existen una letra funcional f de aridad n y términos $t_1, \ldots, t_n$ tales que t es $f(t_1, \ldots, t_n)$, entonces $t(x/r)$ es el término $f(t_1(x/r), \ldots, t_n(x/r))$.

Es claro que $t(x/r)$ es un término, aunque una demostración formal de este hecho se debería hacer por inducción. Ahora bien, la interpretación de un término de esta forma se puede calcular en base a la interpretación de t, pero no necesariamente con la misma asignación de valores a las variables.

NOTACIÓN 3.4. *Sean s una avv, x una variable y a un elemento de A. Denotaremos por $s(x/a)$ a la avv definida por*

$$s(x/a)(y) = \begin{cases} s(y) & \text{si } y \text{ no es } x \\ \\ a & \text{si } y \text{ es } x \end{cases}$$

En otras palabras, $s(x/a)$ actúa exactamente de la misma manera que lo hace s en todas las variables excepto x, a la cual le asigna el valor a. La siguiente proposición nos dice cómo calcular la interpretación de un término que se ha obtenido por reemplazar una variable por otro término.

PROPOSICIÓN 3.5. *Sean t y r términos y s una avv. Entonces $I_s\left(t(x/r)\right)$ es igual a $I_{s(x/I_s(r))}(t)$.*

DEMOSTRACIÓN. Procederemos por inducción sobre la formación de t. Para ahorrar escritura, denotemos por s' a $s(x/I_s(r))$.

Si t es la variable x entonces $t(x/r)$ es r, y por tanto $I_{s'}(t) = I_{s'}(x) = s'(x) = I_s(r) = I_s\left(t(x/r)\right)$.

Si t es una variable y distinta de x o una constante, entonces $t(x/r)$ es t, y así $I_{s'}(t) = I_s(t(x/r))$, pues s y s' coinciden en todas las variables que aparecen en t.

Supongamos que f es una letra funcional de aridad n y $t_1, \ldots, t_n$ son términos que cumplen $I_{s'}(t_j) = I_s(t_j(x/r))$ para todo $j = 1, \ldots, n$, entonces:

$$I_{s'}(f(t_1, \ldots, t_n)) = I(f)\left(I_{s'}(t_1), \ldots, I_{s'}(t_n)\right)$$
$$= I(f)\left(I_s\left(t_1(x/r)\right), \ldots, I_s\left(t_n(x/r)\right)\right) = I_s\left(f(t_1, \ldots, t_n)(x/r)\right).$$

□

3.2. Interpretación de fórmulas. Ahora definiremos cómo es que se interpretan las fórmulas de un lenguaje de primer orden. Esto significa que daremos una definición formal de cuándo una fórmula es verdadera en alguna de sus interpretaciones. Al igual que en el caso de las interpretaciones de términos, determinar si una fórmula se satisface en una interpretación depende de una interpretación de sus variables, es decir, de una avv. Por ejemplo, la verdad de una ecuación como

$x^3 - 3x - 3 = 0$ depende del valor que le estemos asignando a x. La definición de la relación de satisfacción se debe a Alfred Tarski, no es más que el establecimiento del significado de los conectivos y cuantificadores clásicos. En un sentido más teórico, se puede decir que la definición de Tarski es una fórmula de la Teoría de Conjuntos clásica, que establece la relación de satisfacción, la cual es una relación ternaria, entre estructuras, fórmulas y asignaciones de valores a las variables. Como de costumbre, la definición de Tarski es recursiva, sobre la formación de fórmulas.

DEFINICIÓN 3.6. (De satisfacción de Tarski) Para cualesquiera $\mathfrak{A}$ estructura, s avv en A y fórmula α, todas del mismo tipo, se define la relación "$\mathfrak{A}$ satisface a α bajo s, denotada por $\mathfrak{A} \models \alpha[s]$ por recursión sobre la formación de α como sigue:

- Si α es la igualdad entre términos, digamos t_1 y t_2, entonces $\mathfrak{A} \models (t_1 = t_2)[s]$ si y sólo si $I_s(t_1) = I_s(t_2)$ (es decir, t_1 y t_2 se interpretan como el mismo objeto de A).
- Si P es una letra relacional de aridad n y $t_1 \ldots, t_n$ son términos entoces $\mathfrak{A} \models P(t_1 \ldots, t_n)[s]$ si y sólo si la tupla $\langle I_s(t_1), \ldots, I_s(t_n)\rangle$ está en la relación $I(P)$.
- Si α es de la forma $\neg\beta$ entonces $\mathfrak{A} \models \alpha[s]$ si y sólo si no es el caso que $\mathfrak{A} \models\beta[s]$.
- Si α es de la forma $\beta \wedge \gamma$ entonces $\mathfrak{A} \models\alpha[s]$ si y sólo si $\mathfrak{A} \models\beta[s]$ y $\mathfrak{A} \models\gamma[s]$.
- Si α es de la forma $\beta \vee \gamma$ entonces $\mathfrak{A} \models\alpha[s]$ si y sólo si $\mathfrak{A} \models\beta[s]$ o $\mathfrak{A} \models\gamma[s]$.
- Si α es de la forma $\beta \to \gamma$ entonces $\mathfrak{A} \models\alpha[s]$ si y sólo si $\mathfrak{A} \models\neg\beta[s]$ o $\mathfrak{A} \models\gamma[s]$.
- Si α es de la forma $\forall x\beta$ entonces $\mathfrak{A} \models \alpha[s]$ si y sólo si para todo a en A sucede que $\mathfrak{A} \models \beta[s(x/a)]$.
- Si α es de la forma $\exists x\beta$ entonces $\mathfrak{A} \models \alpha[s]$ si y sólo si existe a en A para el cual $\mathfrak{A} \models \beta[s(x/a)]$.

Si el lector se ha quedado amargado por el hecho de que la verdad de una fórmula dependa de las avv, no se mortifique más. Bertrand Russell opinó que ese desencanto viene de querer que las fórmulas sean sólo verdaderas o sólo falsas, independientemente de más consideraciones que el universo donde se interpretan, pero lo que en general una fórmula representa es una *función*, cuyo dominio son las avv y que a cada una de ellas asigna un valor de verdad. Sin embargo algunas de estas funciones son constantes. Más aún, tales funciones nunca dependen de todas las variables del lenguaje, ni siquiera de todas las variables que aparecen en la fórmula. Los cuantificadores tienen precisamente la función de

enmudecer a las variables, en el sentido de que una variable cuantificada hace irrelevante el valor que una avv le asigna. Sin embargo una variable puede aparecer cuantificada en algunos tramos y en otros no, dentro de una misma fórmula. Empezaremos por definir (recursivamente) la situación en la que una variable no queda cuantificada en todas sus apariciones. A continuación los detalles.

DEFINICIÓN 3.7. Sea α una fórmula y x una variable. Diremos que x *aparece libre* en α si

- α es atómica y x aparece en α,
- α es de la forma $\beta \wedge \gamma$ y x aparece libre en β o en γ; lo mismo con el resto de conectivos,
- α es de la forma $\forall y\beta$ o de la forma $\exists y\beta$, y x aparece libre en β y x no es y.

Ahora bien, la siguiente proposición muestra claramente que sólo la interpretación de las variables que aparecen libres en una fórmula dada puede hacer una diferencia en la satisfacción de ésta.

PROPOSICIÓN 3.8. *Sean α una fórmula, s_1 y s_2 dos avv en una estructura $\mathfrak{A}$. Si s_1 y s_2 coinciden en todas las variables que aparecen libres en α entonces $\mathfrak{A} \models \alpha[s_1]$ sí y sólo sí $\mathfrak{A} \models \alpha[s_2]$.*

DEMOSTRACIÓN. Inducción sobre la formación de α.

- Si α atómica entonces todas las variables que contiene aparecen libremente, así que por 3.1, para cualquier término t que aparezca en α, sucede que $I_{s_1}(t) = I_{s_2}(t)$. El resto del argumento se queda como ejercicio para el lector.
- Si α es de la forma $\beta \wedge \gamma$ entonces las variables libres de β y las variables libres de γ están contenidas en las variables libres de α y por tanto s_1 y s_2 coinciden en todas ellas, así que por hipótesis de inducción, tenemos que $\mathfrak{A} \models \beta[s_1]$ si y sólo si $\mathfrak{A} \models \beta[s_2]$ y $\mathfrak{A} \models \gamma[s_1]$ si y sólo si $\mathfrak{A} \models \gamma[s_2]$. Por tanto $\mathfrak{A} \models \alpha[s_1]$ si y sólo si $\mathfrak{A} \models \alpha[s_2]$. Con el resto de los conectivos el razonamiento es el mismo.
- Si α de la forma $\exists x\beta$, tenemos dos situaciones posibles
  (1) Si x no aparece libre en β , entonces las variables libres de β son las mismas que las de $\exists x\beta$ y por tanto $\mathfrak{A} \models \exists x\beta[s_1]$ sí y sólo sí existe a en A tal que $\mathfrak{A} \models \beta[s_1(x/a)]$. Pero $s_1(x/a)$ y $s_2(x/a)$ coinciden en todas las variables libres de β, por tanto, esta condición equivale a que exista a en A tal que $\mathfrak{A} \models \beta[s_2(x/a)]$, lo cual por Tarski equivale a $\mathfrak{A} \models \exists x\beta[s_2]$.
  (2) Si x aparece libre en β, entonces $\mathfrak{A} \models \exists x\beta[s_1]$ sí y sólo sí existe a en A tal que $\mathfrak{A} \models \beta[s_1(x/a)]$. Nuevamente, $s_1(x/a)$ y

$s_2(x/a)$ coinciden en todas las variables libres de β, pues estas son las de α, más la x, así que por hipótesis de inducción, $\mathfrak{A} \models \beta[s_2(x/a)]$ para alguna (la misma) a en A. Por Tarski, esto equivale a $\mathfrak{A} \models \exists\beta[s_2]$.

- El caso α de la forma $\forall x\beta$ es análogo al anterior y se deja como ejercicio para el lector.

□

Finalmente, queda establecido que una fórmula sin variables libres se satisface en una estructura independientemente de las avv. Llamaremos *enunciado* una fórmula que no tiene variables libres y diremos que una fórmula α es *verdadera en* $\mathfrak{A}$ si para toda avv s, $\mathfrak{A} \models \alpha[s]$. Denotaremos por $\mathfrak{A} \models \alpha$ el hecho de que α es verdadera en $\mathfrak{A}$. Todavía un poco más allá tenemos las fórmulas que son verdaderas incluso independientemente del universo donde se les interpreta. Decimos que α es *universalmente verdadera* si $\mathfrak{A} \models \alpha$ para toda estructura $\mathfrak{A}$ del mismo tipo que α. Por el contrario, una fórmula α es *falsa en* $\mathfrak{A}$ si hay no hay una avv s tal que $\mathfrak{A} \models \alpha[s]$, y se dice que α es *universalmente falsa* si no hay estructura ni avv que la satisfagan.

Ejercicios 15.

1. Demuestre la observación 3.1.
2. Escribir los detalles faltantes de la demostración de 3.8.
3. ¿Será exagerado haber pedido que los lenguajes de primer orden contengan una infinidad de variables? ¿de algún modo limita los lenguajes de primer orden el hecho de que sólo disponen de una cantidad numerable de variables?
4. Demuestra que si $\mathfrak{A} \models \alpha$ entonces $\mathfrak{A} \models \forall x\alpha$ y $\mathfrak{A} \models \exists x\alpha$, para cualquier variable x.
5. Medite unos segundos y como acto de fe acepte que todas las instancias de tautología (fórmulas de predicados que tienen el esquema de tautologías) son universalmente verdaderas. Si se niega a aceptarlo, demuéstrelo formalmente.
6. Demuestre que las fórmulas $x = x$, $x = y \to y = x$ y $(x = y \wedge y = z \to x = z$ son universalmente verdaderas.
7. Demuestre que la ley del borracho es universalmente verdadera. La ley del borracho es la fórmula:

$$\exists x(B(x) \to \forall y B(y)),$$

y adquiere su nombre al interpretar el predicado $B(x)$ como "x es borracho.

8. Demuestre que las siguientes fórmulas son universalmente verdaderas:
   a) $\neg\forall x\alpha \leftrightarrow \exists x\neg\alpha$,
   b) $\neg\exists x\alpha \leftrightarrow \forall x\neg\alpha$,
   c) $\exists x(\alpha \wedge \beta) \rightarrow \exists x\alpha \wedge \exists x\beta$
   d) $\forall x(\alpha \wedge \beta) \leftrightarrow \forall x\alpha \wedge \forall x\beta$,
   e) $\exists x(\alpha \vee \beta) \leftrightarrow \forall x\alpha \vee \forall x\beta$,
   f) $(\forall x\alpha \vee \forall x\beta) \rightarrow \forall x(\alpha \vee \beta)$,
   g) $\forall x(\alpha \rightarrow \beta) \rightarrow (\forall x\alpha \rightarrow \forall x\beta)$,
   h) $\exists x(\alpha \rightarrow \beta) \rightarrow (\exists x\neg\alpha \vee \exists x\beta)$,
   i) $\forall x\forall y\alpha \leftrightarrow \forall y\forall x\alpha$,
   j) $\exists x\exists y\alpha \leftrightarrow \exists y\exists x\alpha$,
   k) $\exists x\forall y\alpha \rightarrow \forall y\exists x\alpha$.

   Demuestra que las recíprocas de c,f,g,h y k no son universalmente verdaderas.

3.3. Implicación lógica y reglas de deducción. En la sección anterior hemos cumplido una de las tareas básicas de todo sistema lógico, para la lógica de predicados. Hemos definido las fórmulas distinguidas de la lógica de predicados, las universalmente verdaderas. Ahora cumpliremos con la segunda aspiración y definiremos la relación de consecuencia lógica.

Definición 3.9. Sean Γ un conjunto de fórmulas y α una fórmula, todos de un mismo tipo, digamos ρ. Decimos que α *es consecuencia lógica de* Γ si para cada estructura de tipo ρ en la que todas las fórmulas de Γ son verdaderas, también α lo es.

Es indispensable remarcar de manera muy enfática que la definición anterior dice *verdaderas*, y no que simplemente sean satisfechas por alguna avv particular. En general, los libros de texto definen la relación de consecuencia entre conjuntos de enunciados y enunciados, pero esta versión es equivalente, un poco más amplia y útil. En ambos casos, la intención es liberarnos del pesado lastre que significa arrastrar con las avv que pueden ser caprichosas con una fórmula.

Denotaremos por $\Gamma \models \alpha$ el hecho de que α es consecuencia lógica de Γ, lo cual será sinónimo de "Γ implica lógicamente a α". Usaremos las convenciones que acordamos para la consecuencia lógica en la sección de lógica proposicional. Diremos que α y β son *lógicamente equivalentes* si $\alpha \models \beta$ y $\beta \models \alpha$.

Cuando la relación de consecuencia se da entre algún conjunto finito de fórmulas, podemos establecer *reglas de deducción* que tendremos por seguro que nos permiten inferir verdades partiendo de verdades. Un ejemplo es el siguiente. La regla de Modus Ponens afirma que se

puede establecer la verdad de β cuando se ha establecido previamente la verdad de $\alpha \to \beta$ y de α. Esto es así porque $\{\alpha \to \beta, \alpha\} \models \beta$. Otro ejemplo relevante y fácil de demostrar, aunque probablemente contraintuitivo es la *regla de generalización*, que dice que se infiere $\forall x\alpha$ de α. El lector tendrá la oportunidad de demostrar este hecho a la manera de un ejercicio. Note que la demostración de que $\alpha \models \forall x\alpha$ se basa fuertemente en la suposición de que α es verdadera. Del mundo de las tautologías podemos rescatar muchas reglas, por ejemplo, el tercero excluído, la doble negación, etc, pero otras son netamente de predicados, analizaremos algunas de ellas en las posteriores subsecciones.

Y como en el caso de la lógica proposicional, tenemos una definición del concepto de ser satisfacible: Una fórmula α es *satisfacible* si es verdadera en alguna estructura del mismo tipo que la fórmula.

Ejercicios 16.

1. Demuestra que si $\alpha \to \beta$ es universalmente verdadera entonces $\alpha \models \beta$. ¿será cierto también el regreso? Demuestra que sí lo es cuando α es un enunciado.
2. Demuestra que $\alpha \models \forall x\alpha$, donde x es cualquier variable.
3. Demuestra que si α es un enunciado y $\mathfrak{A}$ una estructura del mismo tipo, entonces $\mathfrak{A} \models \alpha$ o $\mathfrak{A} \models \neg\alpha$.
4. Demuestra que un enunciado α es universalmente falso si y sólo si no es satisfacible. ¿es esto cierto en general para todas las fórmulas?
5. Demuestra que $\Gamma \models \alpha$ si y sólo si $\Gamma \cup \{\neg\alpha\}$ no es sastisfacible.
6. Demuestre que si $\alpha,\ \alpha',\ \beta$ y β' son fórmulas tales que $\models \alpha \leftrightarrow \alpha'$ y $\models \beta \leftrightarrow \beta'$, entonces $\neg\alpha \leftrightarrow \alpha'$, $(\alpha \wedge \beta) \leftrightarrow (\alpha' \wedge \beta')$, $(\alpha \vee \beta) \leftrightarrow (\alpha' \vee \beta')$, $(\alpha \to \beta) \leftrightarrow (\alpha' \to \beta')$ son universalmente verdaderas.
7. Demuestra que si $\alpha,\ \alpha',\ \beta$ y β' son enunciados tales que α y α' son lógicamente equivalentes, y β y β' también lo son, entonces $\neg\alpha$ y $\neg\alpha'$, $(\alpha \wedge \beta)$ y $(\alpha' \wedge \beta')$, $(\alpha \vee \beta)$ y $(\alpha' \vee \beta')$, $(\alpha \to \beta)$ y $(\alpha' \to \beta')$ son pares de fórmulas lógicamente equivalentes.

3.3.1. Regla de Particularización. Particularizar significa pasar del conocimiento general al específico. Si todos tienen una cierta propiedad entonces cada caso particular la tiene. Esto aparenta la verdad universal de las fórmulas de la forma $\forall x\alpha \to \alpha(x/t)$, donde $\alpha(x/t)$ se obtiene al reemplazar las apariciones de la variable x por un término t en α. La idea es correcta pero induce a engaño en algunos casos.

EJEMPLO 3.10. La fórmula $\forall x \exists y\ (x \neq y)$ vale en todo universo que tenga más de un elemento. Particularizando ingenuamente (reemplazando x por y) deducimos la fórmula $\exists y(y \neq y)$. Sin embargo esta es universalmente falsa.

El error en el que se incurre al particularizar ingenuamente es que el término que hemos cambiado por la variable x incluye una variable que queda cuantificada al hacer la sustitución.

Reemplazar una variable que está cuantificada por un término puede no producir de nuevo una fórmula, así que las apariciones de reemplazo de una variable siempre deberá ser libres. A cuntinuación la definición formal de $\alpha(x/t)$.

DEFINICIÓN 3.11. Sea t un término de algún tipo, digamos ρ. Se define recursivamente la fórmula $\alpha(x/t)$ para cada ρ-fórmula α.

- Si α es de la forma $t_1 = t_2$ entonces $\alpha(x/t)$ es $t_1(x/t) = t{-}2(x/t)$ (ver Definición 3.3). Si α es $P(t_1, \ldots, t_n)$ entonces $\alpha(x/t)$ es $P(t_1(x/t), \ldots, t_n(x/t)$, (aquí P es una letra predicativa n-aria y $t-1, \ldots, t_n$ términos.
- Si α es $\beta \circ \gamma$ entonces $\alpha(x/t)$ es $\beta(x/t) \circ \gamma(x/t)$, para cualquier conectivo $\circ$.
- Si α es de la $\forall z\beta$ o de la forma $\exists z\beta$ entonces $\alpha(x/t)$ es la misma $\alpha(x/t)$ si z es x, y es respectivamente $\forall z\beta(x/t)$ o $\exists z\beta(x/t)$, si z no es x.

El lector puede verificar por sí mismo que esta definición recursiva corresponde con lo deseado, es decir, $\alpha(x/t)$ se obtiene de α al reemplazar todas las apariciones libres de x por t. De modo recursivo también se define la situación en la que una variable de un término puede quedar indeseablemente acotada al realizar una sustitución.

DEFINICIÓN 3.12. Sean α una fórmula, x una variable y t un término, todos del mismo tipo. Diremos que t *es libre para* x *en* α si:

- α es atómica,
- α es combinación booleana de β y γ y t es libre para x en β y en γ.
- α es de la forma $\forall z\beta$ o $\exists z\beta$, t es libre para x en β y la variable z no aparece en t.

La anterior definición recursiva expresa el hecho de que si osamos reemplazar las apariciones de x por t en α, nunca tendremos una de las variables de t quedando acotada por un cuantificador. Este hecho se puede demostrar por inducción sobre la construcción de α, y el lector tendrá la oportunidad de hacerlo a la manera de un ejercicio. El

teorema relevante de esta sección afirma que el único obstáculo para una particularización adecuada es la no-libertad del término para la variable en la fórmula, y para demostrarlo empecemos por el siguiente resultado técnico

LEMA 3.13. *Si t es un término libre para x en α y s es una avv en $\mathfrak{A}$ entonces $\mathfrak{A} \models \alpha(x/t)[s]$ si y sólo si $\mathfrak{A} \models \alpha[s(x/I_s(t))]$.*

DEMOSTRACIÓN. Procederemos por inducción sobre la formación de α.

Si α es de la forma $t_1 = t_2$ con t_1 y t_2 términos, entonces $\mathfrak{A} \models (t_1 = t_2)(x/t)[s]$ si y sólo si $\mathfrak{A} \models t_1(x/t) = t_2(x/t)[s]$, lo que por Tarski equivale a que $I_s(t_1(x/t))$ sea igual a $I_s(t_2(x/t))$, pero estos son iguales respectivamente a $I_{s(x/I_s(t))}(t_1)$ y $I_{s(x/I_s(t))}(t_2)$ (esto por Proposición 3.5), por lo que estos valores son iguales entre sí y por tanto tenemos que $\mathfrak{A} \models t_1 = t_2[s(x/I_s(t))]$. El mismo argumento funciona para el caso en el que α es una letra predicativa aplicada a términos. Si α es combinación booleana fórmulas, el resultado se sigue directamente de la hipótesis de inducción. Supongamos ahora que α es de la forma $\forall z\beta$. Como t es libre para x en α, tenemos que t es libre para x en β y z no aparece en t. Así pues,

$$\begin{aligned}
\mathfrak{A} \models \alpha(x/t)[s] &\Leftrightarrow & \mathfrak{A} &\models \forall z(\beta(x/t))[s] \\
&\Leftrightarrow & \mathfrak{A} &\models \beta(x/t)[s(z/a)] \text{ para cualquier } a \text{ en } A \\
&\Leftrightarrow & \mathfrak{A} &\models \beta[s(z/a)(x/I_{s(z/a)}(t))] \text{ para cualquier } a \text{ en } A \\
&\Leftrightarrow & \mathfrak{A} &\models \beta[s(z/a)(x/I_s(t))] \text{ para cualquier } a \text{ en } A \\
&\Leftrightarrow & \mathfrak{A} &\models \forall z\beta[s(x/I_s(t))].
\end{aligned}$$

El paso del tercer al cuarto renglón merece destacar que vale porque las sucesiones s y $s(z/a)$ coinciden en todas las variables que aparecen en t. El caso α de la forma $\exists z\beta$ se obtiene de modo análogo.

□

TEOREMA 3.14 (Regla de particularización). *Si t es libre para x en α entonces $\forall x\alpha \models \alpha(x/t)$.*

DEMOSTRACIÓN. Supongamos que $\alpha(x/t)$ no es verdadera en $\mathfrak{A}$. Entonces existe una avv, digamos s, tal que $\mathfrak{A} \not\models \alpha(x/t)[s]$, lo cual, por el lema anterior, equivale a que $\mathfrak{A} \not\models \alpha[s(x/I_s(t))]$, así que para $a = I_s(t)$, ocurre que $\mathfrak{A} \not\models \alpha[s(x/a)]$, de donde se deduce que $\mathfrak{A} \not\models \forall x\alpha[s]$ y por tanto $\forall x\alpha$ no es verdadera en $\mathfrak{A}$. □

La regla de particularización tiene una versión dual, la *regla existencial*. Dada la presencia de un testigo, se infiere el existencial, es decir,

de la verdad de $\alpha(x/t)$ (el término t es quien la hace de testigo) se infiere $\exists x\alpha$. Nuevamente el requisito es que t sea libre para x en α. Quede como ejercicio al lector demostrar la validez de la regla existencial.

Ejercicios 17.

1. Pruebe que si t es un término constante (es decir, no incluye variables), o la variable x, o una variable que no aparece en α entonces t es libre para x en α.
2. Demuestre la regla existencial, es decir, $\alpha(x/t) \models \exists x\alpha$, donde t es libre para x en α.
3. Sea α una fórmula y y una variable que no aparece en α. Demuestre que $\forall x\alpha$ es lógicamente equivalente a $\forall y\alpha(x/y)$. Pruebe que lo mismo vale con cuantificadores existenciales.

3.3.2. Igualdad y sustitución.

De una igualdad entre términos $t = r$ se infiere inmediatamente que las verdades que cumple t las cumple r y viceversa. Leibnitz pensaba que lo inverso es también cierto, y lo es cuando se dispone de un lenguaje suficientemente poderoso, más que los de primer orden. En esta sección estableceremos la validez de la regla de sustitución de iguales por iguales, con la salvedad de que nuevamente, la sustitución de una variable por un término sólo es válida cuando el término es libre para tal variable en la tal fórmula. Un detalle adicional es que en este caso, la sustitución no tiene por qué ocurrir en todas las apariciones de x, sino que puede ser sólo en algunas de ellas.

Teorema 3.15. *Sean α una fórmula, x una variable y t un término. Si t es libre para x en α entonces $x = t \to (\alpha \leftrightarrow \alpha')$ es universalmente válida, donde α' es cualquier fórmula que se obtiene de α al sustituir algunas, todas o ninguna de las apariciones libres de x por t.*

Demostración. Sea $\mathfrak{A}$ una estructura y s una avv en A tales que $\mathfrak{A} \models x = t[s]$, lo cual quiere decir que $I_s(t) = I_s(x) = s(x)$. Imitando la demostración del Lema 3.5, salvo que en lugar de $t(x/r)$ consideremos cualquier término t' que se obtiene sustituyendo algunas de las apariciones de x en t por r (no necesariamente todas), podemos concluir que $I_s(t') = I_{s(x/I_s(r))}(t) = I_s(t)$, la última igualdad como consecuencia de que $\mathfrak{A} \models x = t[s]$. Esta igualdad nos garantiza que si α es atómica y $\mathfrak{A} \models \alpha[s]$ entonces $\mathfrak{A} \models \alpha'[s]$. El caso de los conectivos booleanos se sigue inmediatamente de la hipótesis de inducción y el ejercicio 16. Supongamos que α es de la forma $\forall z\beta$. Si z fuera la misma variable que x, entonces no hay nada qué sustituir, y por tanto α' es

α y el resultado es inmediato. Supongamos que x aparece libre en α y por tanto z no es x. Como t es libre para x en α, tenemos que z no aparece en t, y por tanto, $I_{s(z/a)}(t) = I_s(t) = s(x) = s(z/a)(x)$, (i. e. $\mathfrak{A} \models x = t[s(z/a)]$) para todo a en A. Así pues, $\mathfrak{A} \models \forall z\beta[s]$ si y sólo si $\mathfrak{A} \models \beta[s(z/a)]$ para todo a en A, lo cual a su vez, por hipótesis de inducción, equivale a $\mathfrak{A} \models \beta'[s(z/a)]$, y finalmente, esto equivale a $\mathfrak{A} \models \forall z\beta[s]$. □

Como consecuencia de esta propiedad de sustitución de iguales por iguales, se pueden probar, junto con otras reglas ya demostradas o dejadas como ejercicio y la verdad universal de $x = x$, todas las reglas usuales de la igualdad, como la simetría y la transitividad.

Ejercicios 18.

1. Establece las propiedades de simetría y transitividad de la igualdad, argumentando las reglas vistas sobre sustitución de iguales por iguales.

A partir de este momento, nos enfocaremos en el estudio de enunciados, más que de fórmulas en general. Recordemos que un enunciado es una fórmula que no tiene variables libres, y por tanto su verdad ya no depende de las avv, es decir, un enunciado siempre es verdadero o falso en una estructura. En la sección anterior definimos los conceptos de consecuencia lógica y satisfacibilidad para fórmulas en general, ahora haremos unas cuantas observaciones sobre estos conceptos en el caso especial de los enunciados.

∗ Observaciones: Sean α y β enunciados. Entonces

1. $\beta \models \alpha$ si y sólo si $\beta \to \alpha$ es universalmente verdadera.
2. β es satisfacible si y sólo si β no es universalmente falsa si y sólo si $\neg\beta$ no es universalmente verdadera.
3. $\Gamma \not\models \beta$ si y sólo si $\Gamma \cup \{\neg\beta\}$ es satisfacible.
4. Si $\Gamma \subseteq \Sigma$ y Σ es satisfacible, entonces Γ es satisfacible.

4. Aritmética de Peano de primer orden

Entraremos de lleno en un ejemplo de teoría formal de primer orden analizando la aritmética de Peano, la cual es la más popular versión de la aritmética de los números naturales. Giuseppe Peano propuso en 1885 una axiomatización para los números naturales, que en una versión moderna, consta de cinco postulados:

1. 0 es un número natural.
2. Todo número natural n tiene un único sucesor n'.

3. 0 no es sucesor de ningún número natural.
4. Si $n' = m'$ entonces $n = m$.
5. Si A es un conjunto de números naturales tal que 0 es elemento de A y cada que un natural n pertenezca a A, ocurra que n' también pertenezca a A, entonces todos los números naturales pertenecen a A.

Además, Peano definió las operaciones de suma y multiplicación de manera recursiva, usando la operación sucesor, mediante los siguientes axiomas:

1. $n + 0 = n$
2. $n + m' = (n + m)'$
3. $n \cdot 0 = 0$
4. $n \cdot m' = n \cdot m + n$.

En el contexto que nos concierne, para formalizar la aritmética de Peano precisamos un tipo de semejanza que conste de un símbolo constante, una letra funcional unitaria y dos letras funcionales binarias. Sea entonces $\rho_{AP} = \{0, ', +, \cdot\}$ el tipo de la aritmética de Peano, e interpretemos del modo usual. Es innecesario postular los dos primeros axiomas, pues la constante 0 se interpreta como un elemento del universo (en este caso, los números naturales) y la letra $'$ como una función unitaria. El resto de los axiomas (excepto inducción) escritos en primer orden quedan así:

1. $\forall v_0(\neg 0 = v_0')$
2. $\forall v_0 \forall v_1\, (v_0' = v_1' \to v_0 = v_1)$
3. $\forall v_0(v_0 + 0 = v_0)$
4. $\forall v_0 \forall v_1(v_0 + v_1' = (v0 + v_1)')$
5. $\forall v_0(v_0 \cdot 0 = 0)$
6. $\forall v_0 \forall v_1(v_0 \cdot v_1' = (v_0 \cdot v_1) + v_0)$.

En los términos en los que está escrito, claramente el axioma de inducción no es de primer orden, pues cuantifica sobre todos los subconjuntos del universo. El truco usual para tratar con enunciados de segundo orden como éste, es cambiar el axioma de segundo orden por un *esquema de axiomas*, es decir, muchos axiomas que digan lo mismo, sólo que en instancias de conjuntos particulares, mínimamente aquellos que pueden emularse con fórmulas. Observe que si φ tiene una variable libre x, dada una avv s que tome valores en $\mathbb{N}$, podemos considerar al conjunto $\{n : \mathbb{N} \models \varphi[s(x/n)\}$. Emulando todos los conjuntos de este tipo mediante todas las posibles fórmulas φ con al menos una variable libre x, enunciamos el principio de inducción para esta φ:

$AP_\varphi \quad (\varphi(x/0) \wedge \forall x\varphi \to \varphi(x/x')) \to \forall x\varphi$.

Denotaremos por AP al conjunto formado por $AP1 - AP6$ y todos los AP_φ, y lo primero que quisiéramos saber es qué tan bien simulado ha quedado el axioma de inducción.

En primer lugar, es sencillo ver que la aritmética de Peano de segundo orden es *categórica*, es decir, cualesquiera dos modelos de ella son isomorfos (ver ejercicios de la sección). Veamos que AP tiene modelos que no son isomorfos a $\mathbb{N}$. Esto se logra encontrando un modelo en el que haya un elemento que no esté en la *órbita* del 0 bajo la operación sucesor, es decir, alguien que no es alcanzable desde el cero, aplicando la operación sucesor una cantidad finita de veces. Para esto, enriquecemos el lenguaje de AP con un símbolo de constante c más los siguientes axiomas:

$$C = \{c \neq 0, c \neq 0', c \neq 0'', \ldots, c \neq 0^{(n)}, \ldots\}$$

que en términos llanos dicen (entre todos, no individualmente) que c no es interpretable como ninguno de los números naturales estándar. Nótese que si $AP \cup C$ tuviese un modelo, éste sería obviamente uno de AP que no podría ser isomorfo $\mathbb{N}$, pues en este último (sabemos que) todos sus elementos están en la órbita del 0 bajo sucesor, mientras que c necesariamente se interpreta como alguien que no está en la órbita de 0 bajo sucesor. ¿Cómo podemos ver que $AP \cup C$ tiene modelo? Usemos el teorema de compacidad.

Ejercicios 19.

1. Sea $\langle M, *, +_M, \cdot_M, 0_M\rangle$ un modelo de la aritmética de Peano de segundo orden. Por recursión sobre los naturales se define una función f cuyo dominio es $\mathbb{N}$ y cuya imagen está contenida en M, de modo tal que $f(0) = 0_M$, y $f(n') = f(n)^*$ para toda n. Demuestra que:
   a) f es suprayectiva (utiliza que vale el principio de inducción de M),
   b) f es inyectiva (utiliza que vale el principio de inducción en $\mathbb{N}$),
   c) para todos $n, m \in \mathbb{N}$, $f(n+m) = f(n) +_M f(m)$ y $f(n \cdot m) = f(n) \cdot_M f(m)$.

   Con todo esto tenemos demostrado que M es isomorfo a $\mathbb{N}$.
2. Demuestra que la fórmula $\forall x(x = 0 \vee \exists y(x = y'))$ es consecuencia lógica de AP.
3. Enuncia y demuestra el Principio del Buen Orden en el lenguaje de AP.

4. Demuestra que de $AP1 - AP6$ más la fórmula $\forall x(x = 0 \vee \exists y(x = y'))$ más el Principio del Buen Orden, es consecuencia el Principio de Inducción.

5. Compacidad de la lógica de primer orden

La lógica de predicados de primer orden es compacta, en los mismos términos que la de proposiciones, es decir, el enunciado es idéntico, aunque el significado de cada concepto difiere, y por tanto la técnica para demostrarlo también es muy diferente.

TEOREMA 5.1. *Todo conjunto finitamente satisfacible de enunciados es satisfacible.*

DEMOSTRACIÓN. Esta demostración pasará por la prueba de varios lemas; por lo pronto se puede adelantar que los ladrillos con los que se va a construir el modelo que se enuncia saldrán de algunas construcciones basadas en el lenguaje del conjunto de enunciados con el que empezamos. Sea pues T un conjunto de enunciados en un lenguaje ρ_0. Al igual que en el caso proposicional, una teoría maximal finitamente satisfacible da luz sobre el modelo, pero aquí no basta eso. Además es preciso contar con *testigos* para las fórmulas existenciales, es decir, si en T tenemos una fórmula existencial, digamos $\exists x\alpha$, sería conveniente contar con un término cerrado (es decir, sin variables) de modo tal que el enunciado $\alpha(x/t)$ también se encuentre en T. Nuestro lenguaje ρ_0 puede ser insuficiente, en el sentido de que no posea suficientes constantes para tal efecto, sin embargo veremos que en un lenguaje más amplio, podremos conseguir todo a la vez, es decir , un conjunto S de enunciados en un lenguaje σ tales que σ contiene a ρ, S es maximal finitamente satisfacible, todos sus existenciales tienen testigos y contiene a T.

LEMA 5.2. *Si T es un conjunto de enunciados en un lenguaje ρ y es finitamente satisfacible entonces existe un conjunto de enunciados T' en el mismo lenguaje ρ que contiene a T y es maximal finitamente satisfacible.* □

Omitimos demostrar este lema pues se puede proceder de modo análogo al caso proposicional. El lector quedará invitado a comprobarlo.

LEMA 5.3. *Si T es un conjunto finitamente satisfacible de enunciados en un lenguaje ρ entonces existen un lenguaje ρ^* y un conjunto de enunciados T^* en el lenguaje ρ^* el cual es finitamente satisfacible, contiene a T y todos los enunciados existenciales de T tienen testigo en T^*.*

DEMOSTRACIÓN. Es suficiente con agregar a ρ una constante nueva para cada fórmula existencial de T, y agregar a T todas las fórmulas del tipo $\alpha(x/c)$ donde $\exists x\alpha$ es un enunciado de T y c es la constante nueva en ρ^* asociada a esta fórmula. Claramente, todos los enunciados existenciales de T tiene testigos en T^* y T está contenido en T^*. Sea T_0 cualquier subconjunto finito de T^*. Definamos $T_1 = (T_0 \cap T) \cup \{existsx\alpha : \alpha(x/c) \in T_0\}$, el cual claramente es un subconjunto finito de T. Por hipótesis, T tiene un modelo $\mathfrak{A}$, el cual por cierto satisface a las fórmulas $\exists x\alpha$ con $\alpha(x/c)$ en T_0. Interpretando cada constante nueva c como un elemento a de A tal que $\mathfrak{A} \models \alpha[(x/a)]$, tenemos un modelo del nuevo lenguaje, que hace verdaderos a todos los enunciados de T_0. □

LEMA 5.4. *Si T es un conjunto finitamente satisfacible de enunciados en un lenguaje ρ, entonces existen un lenguaje σ y un conjunto de enunciados S en el lenguaje sigma, el cual es maximal finitamente satisfacible y todo enunciado existencial en S tiene testigo en S.*

DEMOSTRACIÓN. Definamos recursivamente $T_0 = T$, $\rho_0 = \rho$, si n es par entonces $T_{n+1} = T'$ (como en el lema 5.2 y $\rho_{n+1} = \rho_n$; y si n es impar entonces $\rho_{n+1} = \rho_n^*$ y $T_{n+1} = T^*$ (como en el lema 5.3). Sean $S = \bigcup_n T_n$ y $\sigma = \bigcup_n \rho_n$. Dado que S es una unión creciente de conjuntos finitamente satisfacibles, S es también finitamente satisfacible. Sea α un enunciado en el lenguaje σ que no esté en S. Como α sólo contiene una cantidad finita de símbolos, α es un enunciado de tipo ρ_n para alguna n, considerémosla par. Como α no está en S, tampoco está en T_{n+1}, pero este conjunto es maximal finitamente satisfacible, por lo que existe un subconjunto finito R de T_{n+1} (y por tanto de S) tal que $R \cup \{\alpha\}$ no es satisfacible, y por tanto $S \cup \{\alpha\}$ no es finitamente satisfacible. Esto prueba que S es maximal finitamente satisfacible. Ahora supongamos qu la fórmula $\exists x\alpha$ está en T^*, y sea n tal que $\exists x\alpha$ está en T_n, podemos considerar n impar. Asṕues, $\exists x\alpha$ tendrá un testigo en T_{n+1} y por tanto en S. □

Supongamos que S es como en el lema 5.4, y empecemos a construir un modelo para S. Sobre la familia de todos los términos cerrados en el lenguaje σ, definamos la siguiente relación: $t \simeq t'$ si y sólo si la fórmula $t = t'$ está en S. El lector se encargará de probar que ésta es una relación de equivalencia, y el universo A de la estructura $\mathfrak{A}$ que nos interesa el precisamente la partición inducida por esta. Nuestro siguiente paso es interpretar las letras predicativas, funcionales y constantes de σ.

- Si P es una letra predicativa n-aria en σ, entonces una n-tupla de elementos de A, digamos $([t_1], \ldots, [t_n])$ está en la interpretación de P si y sólo si el enunciado $P(t_1, \ldots, t_n)$ está en S.
- Si f es una letra funcional n-aria en σ, entonces la intepretación de f asignará la clase $[f(t_1, \ldots, t_n)]$ a una n-tupla de clases $([t_1], \ldots, [t_n])$.
- Si c es una constante en σ entonces la intepretación de c, será precisamente la clase de c.

El lector queda invitado a demostrar que estas definiciones no dependen de representantes. Ya entrados en gastos, el lector también debería demostrar que para cada enunciado α en el lenguaje σ, $\mathfrak{A} \models \alpha$ si y sólo si α está en S. Es cierto que para nuestros fines basta demostrar el regreso, pero paradójicamente es más fácil demostrar el bicondicional, por inducción sobre la formación de α. Finalmente, nuestro conjunto de enunciados original T tiene un modelo que se puede obtener (1) extendiendo T a un conjunto S de enunciados en un lenguaje σ que es maximal finitamente satisfacible cuyos existenciales tienen testigos, y que por tanto tiene un modelo $\mathfrak{A}$. (2) Olvidando las interpretaciones en $\mathfrak{A}$ de los símbolos de σ que no están en ρ, nos queda una estructura de tipo ρ que hace verdaderas a todas las fórmulas de T, que era lo que buscábamos. □

Ejercicios 20.

1. Demuestre el Lema 5.2, imitando los pasos de 2.47.
2.