CARLA MARIA CARNEIRO ALVES

LÓGICA
E
ÁLGEBRAS BOOLEANAS

DISSERTAÇÃO DE MESTRADO
EM MATEMÁTICA

Tese apresentada à Universidade Lusíada – Lisboa como requisito parcial para a obtenção do grau de Mestre em Matemática.

Universidade Lusíada
Lisboa, 2002

Índice

Índice de Figuras

Resumo

O principal objectivo deste trabalho consistiu em investigar e aprofundar os conhecimentos na área da Lógica clássica "booleana" e suas álgebras. Nesse sentido desenvolveu-se um trabalho organizado em capítulos, designados por:

- capítulo I - Lógica proposicional;
- capítulo II - Álgebras booleanas;
- capítulo III - Conclusões e considerações finais.

No primeiro capítulo desenvolveu-se a Lógica proposicional, essencialmente do ponto de vista semântico. Fez-se ainda uma breve revisão dos conteúdos considerados mais pertinentes para a investigação. Os principais tópicos desenvolvidos, neste capítulo, foram: a sintaxe, a semântica, as formas normais, os conjuntos completos de conectivos, o lema de interpolação e o teorema da compacidade e algumas suas aplicações.

No segundo capítulo desenvolveram-se as Álgebras booleanas. Deu-se particular ênfase aos conceitos de álgebra e de topologia, relacionados com as álgebras booleanas. Também neste capítulo foi feita uma revisão prévia acerca de alguns conteúdos considerados relevantes para o estudo. Para além de algumas definições e propriedades das álgebras booleanas, foram também abordados os seguintes subtemas: átomos, homomorfismos de álgebras booleanas, ideais e filtros e ainda o espaço de Stone. Os principais tópicos desenvolvidos foram: uma parte da álgebra e da topologia (alguns conteúdos necessários para o estudo), algumas definições de álgebras booleanas, átomos nas álgebras booleanas, homomorfismos, isomorfismos, subálgebras, ideais, filtros, teorema de Stone.

O terceiro capítulo constitui uma síntese do trabalho e uma reflexão sobre o modo como decorreu a investigação bem como sugestões e possíveis implicações para investigações futuras.

Palavras-chave: Lógica, Cálculo proposicional, Álgebras booleanas.

Abstract

The main objective of this work was to investigate and deepen our knowledge about Logic classical “boolean” and its algebras. For that, we considered two chapters of Logic, Propositional Logical and Boolean Algebras.

For that purpose, we developed a work that was organized in the following chapters:

- chapter I - Propositional Logic;
- chapter II – Boolean Algebras;
- chapter III – conclusions and final considerations.

The first chapter is about Propositional Logic, essentially from the semantical point of view. The main developed topics were, in this chapter, syntax, semantics, normal forms, connective full groups, interpolation lemma and the compactness theorem and some applications.

The second chapter is about Boolean Algebras. We emphasized algebra and topology concepts, which are related to Boolean algebras. In this chapter we also made a previous survey about some concepts that were relevant for this study. Besides some definitions and properties of Boolean algebras, the following subthemes were also considered: atoms, homomorphisms of Boolean algebras, ideals and filters and also Stone’s space. The main topics developed were: a part of algebra and of topology (some contents that were necessary for the study), some Boolean algebra definitions, atoms in Boolean algebras, homomorphisms, isomorphisms, subalgebras, ideals, filters, and Stone’s theorem.

The third chapter consists on a synthesis of the work and a reflexion about the way the investigation was taken and also on some suggestions and possible implications for future investigations.

Key words: Logic, Propositional Calculus, Boolean Algebras.

Ao Filipe, ao José e a meus Pais

Agradecimentos

Agradeço a todas as pessoas e Instituições que possibilitaram a realização deste trabalho, nomeadamente:

- ao Prof. Doutor Franco de Oliveira, pelo permanente apoio e competência com que me orientou;

- ao Prof. Doutor Carlos Mesquita Morais, pela colaboração, entusiasmo e disponibilidade na elaboração do meu trabalho;

- à colega Mestre Alexandra Soares Rodrigues pela disponibilidade, confiança e apoio que me transmitiu;

- ao Instituto Politécnico de Bragança e de forma particular à Escola Superior de Educação pelo apoio proporcionado;

- à professora Vanda Santos pelo apoio e simpatia que me transmitiu;

- a todos os professores que, com ensinamentos, críticas e opiniões, colaboraram neste trabalho.

Introdução

Foi objectivo deste trabalho aprofundar e investigar os conhecimentos numa componente da matemática pura, mais concretamente em Lógica. Nesse sentido desenvolveu-se um trabalho organizado em capítulos. Assim,

- no capítulo I abordamos a Lógica proposicional;
- no capítulo II tratamos as Álgebras booleanas;
- no capítulo III apresentaremos algumas conclusões e considerações finais assim como um breve resumo de todo o trabalho e algumas críticas sobre o mesmo.

As diferentes áreas em lógica surgem como resultado de dificuldades e novas descobertas numa história complicada.

Segundo Crossley (1990), a história associada à lógica pode ser vista a partir de dois fluxos diferentes ambos muito longos: um é a história da dedução formal que é anterior a Aristóteles e Euclides e outros daquela Era, e o outro é a história da análise matemática que pode ser datada antes de Arquimedes na mesma Era. Estes dois fluxos desenvolveram-se separadamente durante um longo tempo – até por volta de 1600-1700. De seguida temos Leibnitz que para além de pioneiro do cálculo infinitesimal, teve a ideia, que não chegou a realizar, de uma língua universal para as ciências.

Conclui-se, então, que há muito tempo que se considera a lógica como uma filial da matemática, mas com um estatuto um pouco especial que a distingue de todas as outras (Cori & Lascar, 2000: 1). Curiosamente, tanto os adversários mais fortes desta ideia como alguns dos seus discípulos mais entusiásticos concordam com a concepção que coloca a lógica perto da margem da matemática, na sua fronteira, ou até mesmo fora dela. Para os primeiros, a lógica não pertence à matemática real; outros, pelo contrário, vêem-na como uma disciplina reinando dentro da matemática, uma que transcende todas as outras, que suporta a estrutura principal.

Para quem quiser ter uma introdução para a lógica matemática, o primeiro conselho que daríamos é adoptar um ponto de vista radicalmente diferente do anterior. O tipo de mente a ser adoptado deve ser o mesmo que quando consultamos um tratado de álgebra ou de cálculo diferencial. É um texto matemático que estamos a apresentar aqui; nisto, estamos a fazer matemática, e não qualquer outra coisa. Parece-nos que esta é uma pré-condição essencial para um adequado entendimento formal dos conceitos que serão apresentados.

Isto não significa que a pergunta do lugar da lógica na matemática seja sem interesse. Pelo contrário, mas concerne um problema externo para a matemática. Qualquer matemático pode (e diremos até mesmo deve) até certo ponto reflectir no seu trabalho, e transformar-se ele próprio num epistemólogo, num filósofo, ou historiador de ciência; assim, ele deve cessar temporariamente a sua actividade matemática. Além disso, geralmente não há ambiguidade: quando lê um texto de análise, o que o estudante de matemática espera encontrar são: definições, teoremas, e demonstrações para estes teoremas.

O principal objectivo aparece quando é necessário aceitar simultaneamente as duas ideias seguintes:

(1) a lógica é uma filial da matemática;

(2) o objectivo da lógica é estudar matemática.

Confrontados com este aparente paradoxo, existem três possíveis atitudes. Primeiro, cada um pode considerar isto tão sério que ao empreender o estudo da lógica é logo condenado; segundo, cada um pode julgar que a suposta incompatibilidade entre (1) e (2) simplesmente compele a negação de (1), ou pelo menos a sua modificação, o que conduz à convicção de que realmente não se está a fazer matemática quando se estuda lógica; finalmente, a terceira atitude, consiste em desmantelar o paradoxo, considerado como nenhum, e situar a lógica matemática no seu lugar formal, dentro do coração de matemática.

No entanto, segundo Oliveira (1996: 228), a lógica matemática tem vindo progressivamente a supor o cariz de uma disciplina matemática à qual não são estranhas, portanto, as técnicas abstractas da matemática dos nossos dias, sendo talvez mais próximo da verdade dizer que a lógica matemática é mais uma matemática da lógica do que a lógica da matemática. Melhor dizendo, estes dois aspectos complementam-se e enriquecem-se constantemente. Acontece assim porque as investigações lógicas, desde finais do século passado, inicialmente motivadas por questões de fundamentos, levaram à concepção de novos tipos de “estrutura”, as chamadas linguagens formais, que como objectos de estudo despertaram a curiosidade dos matemáticos e permitiram, até, dar à matemática tradicional uma nova dimensão.

Vamos agora começar a estudar a lógica matemática. Para isso não se pede que esqueçamos tudo aquilo o que já aprendemos e para reconstruir tudo do nada. É o oposto que pretendemos. Desejamos explorar o fundo comum: familiaridade com os processos de racionalidade matemática, entre outros, indução, demonstração através da

contradição, com objectos matemáticos quotidianos dos quais conjuntos, relações, funções, números inteiros, números reais, polinómios, funções contínuas, e com alguns conceitos que podem não ser tão conhecidos dos quais anel, espaço vectorial, espaço topológico. Isto é o que é feito em qualquer curso de matemática: assim, fazemos uso do nosso conhecimento anterior na aquisição de novos conhecimentos. Procederemos precisamente deste modo e aprenderemos sobre novos objectos, possivelmente sobre novas técnicas de demonstração (mas atenção: a racionalidade matemática que habitualmente empregamos nunca será posta em causa; pelo contrário, esta é a única aqui contemplada).

Se simplificarmos um pouco, a abordagem da matemática é quase sempre a mesma se o assunto em estudo é teoria, espaço vectorial, conjuntos ordenados, ou qualquer outra área da chamada matemática clássica. Consiste em examinar estruturas, ou seja, conjuntos nos quais foram definidos relações e funções, e correspondências entre estas estruturas. Mas, para cada uma destas áreas clássicas, existe uma motivação particular que deu isto à luz e que nutriu o seu desenvolvimento. O objectivo era promover um modelo matemático de situações concretas, responder a um grande desejo que surge do mundo fora da matemática, para fornecer uma ferramenta útil à matemática.

A lógica matemática segue também esta mesma aproximação; a sua particularidade é que faz tentativas para descrever a realidade, não fora do mundo da matemática, mas a realidade na própria matemática.

Isto não deveria ser difícil, contanto que permanecemos atentos ao que está envolvido. Nenhum estudante de matemática confunde o seu ambiente físico com um segmento orientado tridimensional euclidiano, mas o conhecimento deste ambiente ajuda a intuição quando se vem a provar alguma propriedade desta estrutura matemática. O mesmo se aplica à lógica: de certo modo, estamos a fabricar uma cópia, um protótipo, ousamos mesmo dizer um modelo reduzido do universo da matemática, com o qual já estamos relativamente familiarizados. Mais precisamente, construiremos uma colecção inteira de modelos, mais ou menos prósperos. Adicionando um espécime que é verdadeiramente semelhante ao original, teremos criado outros, frequentemente bastante diferentes dos que imaginamos no início. O estudo desta colecção ensina-nos muitas lições; notavelmente, permite que esses que empreendem este estudo se possam questionar sobre algumas perguntas interessantes das suas percepções e das suas intuições do mundo matemático. Seja como for, temos de entender que é essencial não

confundir o original que nos inspirou com a cópia ou cópias. Mas o original é indispensável para a produção da cópia: a nossa familiaridade com o mundo da matemática guia-nos para fabricarmos a representação do que provaremos. Mas ao mesmo tempo, o nosso empreendimento é a matemática, é dentro deste universo que estamos a tentar compreender melhor.

Não existe nenhum ciclo vicioso. No lugar de um ciclo, imagine-se uma hélice, um tipo de escadaria em espiral: estamos no topo no *n*-ésimo andar, onde o nosso universo matemático está localizado; chame-se a este nível o nível intuitivo. O nosso trabalho leva-nos a um nível abaixo, ao nível (n - 1), onde encontramos o protótipo, o modelo reduzido; estamos então no nível formal e a nossa passagem de um nível para o outro será chamada "formalização".

Note-se que não há primeiro nem último nível. De facto, se o nosso modelo for bem construído, se na reprodução do universo matemático não se omitiu qualquer detalhe, então, também conterá uma parte do nosso próprio trabalho em formalização; isto exige-nos que consideremos o nível (n – 2), e assim por diante.

Vamos tão longe para dizer que, para qualquer valor de n, o *n*-ésimo nível na nossa escadaria é intuitivo relativamente ao nível (n – 1) e é formal relativamente ao nível (n + 1). À medida que progredimos na nossa formalização, poderíamos parar em qualquer momento e ter a oportunidade para verificar que o modelo formal, ou pelo menos o que podemos ver dele, concorda com o original intuitivo. Esta fase seguinte concerne ao meta-intuitivo, ou seja, ao nível (n + 1).

A teoria dos conjuntos, dando legitimidade a uma infinidade de objectos e permitindo manipulá-los como objectos reais (por exemplo, os inteiros), com as mesmas regras lógicas, criou uma certa resistência entre certos matemáticos; ainda mais porque as tentativas iniciais se mostraram contraditórias. O mundo matemático foi então dividido em dois clãs. Por um lado, havia os que não podiam resistir à liberdade que a teoria de conjuntos permitia, o Paraíso Cantoriano, como sugeriu Hilbert. Por outro lado, havia os que para quem só os objectos finitos tinham qualquer significado e que, como consequência, negavam a validade das demonstrações que faziam uso da teoria de conjuntos.

Segundo Hilbert (1950), para reconciliar estes pontos de vista, imaginou-se a seguinte estratégia: primeiro, as demonstrações seriam consideradas como sequências finitas de símbolos, consequentemente, como objectos finitos; segundo, um algoritmo

teria de ser encontrado e transformaria uma demonstração que usava a teoria de conjuntos numa demonstração finitária.

Capítulo I. Lógica Proposicional

Sumário

Neste capítulo vamos abordar inicialmente a parte da sintaxe, da semântica, as formas normais e conjuntos completos de conectivos, o lema de interpolação e o teorema da compacidade, tudo referente à Lógica proposicional.

Vamos discutir teoria de conjuntos. Provavelmente todos têm alguma ideia do que é um conjunto: uma colecção de coisas, mais concretamente, conjuntos são colecções de objectos matemáticos. Começaremos por fazer referência ao cálculo proposicional que é o estudo dos conectivos proposicionais; estes são operadores em frases (declarativas) ou em fórmulas. Em primeiro lugar há a negação que denotamos pelo símbolo $\neg$ que é colocado à frente de uma fórmula. Os outros conectivos são colocados entre duas fórmulas: consideraremos a conjunção ("*e*", representada por $\wedge$), a disjunção ("*ou*", representada por $\vee$), a implicação ($\Rightarrow$), e a equivalência ($\Leftrightarrow$). Por exemplo, com duas declarações A e B, é possível formar a conjunção (A $\wedge$ B): esta é outra declaração que é verdadeira se e só se A é verdadeira e B é verdadeira.

A primeira coisa que fazemos é construir objectos puramente formais a que chamaremos fórmulas proposicionais, ou, mais simplesmente, fórmulas. Ao construirmos blocos usaremos variáveis proposicionais que intuitivamente representam proposições elementares, e que juntamos usando os conectivos já mencionados. Inicialmente, as fórmulas aparecem como sucessões adequadamente combinadas com

símbolos. Apresentaremos regras precisas para a sua construção e meios para recuperar o método pelo qual uma determinada fórmula foi construída, o que permite que a fórmula seja lida. Todas estas considerações formais constituem o que chamamos de sintaxe.

Esta construção formal não é obviamente arbitrária, pois teremos que dar significado a estas fórmulas subsequentemente. Este é outro propósito. Se, para cada proposição elementar que aparece numa fórmula F, sabemos se é verdadeira ou não (falamos do valor de verdade da proposição), devemos saber decidir se o próprio F é verdadeiro ou não. Por exemplo, diremos que $A \Rightarrow B$ é verdadeiro em três dos quatro casos possíveis: quando A e B são ambos verdadeiros, quando A e B são ambos falsos, e quando A é falso e B é verdadeiro. Note-se a diferença entre a prática geral: por exemplo, no idioma quotidiano e até mesmo em textos de matemática, a frase "A implica B" sugere uma relação causal que, no nosso contexto, não existe necessariamente.

Assim chegamos às noções importantes: o conceito de tautologia e a noção de equivalência lógica.

Veremos que uma fórmula é sempre logicamente equivalente a uma outra fórmula que pode ser escrita duma forma muito particular (forma disjuntiva ou forma conjuntiva), outra secção é dedicada ao lema de interpolação e ao teorema de definibilidade cuja importância será apreciada quando estes teoremas forem generalizados ao cálculo de predicados. Na última secção, o teorema da compacidade é particularmente importante e também será generalizado. Aí se afirma que se cada parte finita de X tem um modelo, então X tem um modelo.

1.1 Sintaxe

1.1.1 Fórmulas proposicionais

Consideremos um conjunto P não vazio, finito ou infinito, a que chamaremos o conjunto de variáveis proposicionais. Os elementos de P são normalmente representados por letras do alfabeto latino possivelmente com índices.

Além disso, permitiremos os seguintes cinco símbolos:

$$\neg \quad \vee \quad \wedge \quad \Leftrightarrow \quad \Rightarrow$$

que leremos respectivamente como: "*não*", "*ou*", "*e*", "*é equivalente a*" e "*implica*" e os quais chamaremos de símbolos para conectivos proposicionais. Assumimos que não são elementos do conjunto P.

Os símbolos $\neg$, $\vee$, $\wedge$, $\Leftrightarrow$, $\Rightarrow$ são chamados respectivamente: negação, disjunção, conjunção, equivalência e implicação.

Devido às regras que lhes serão atribuídas, dizemos que o símbolo $\neg$ é unário e que os outros quatro símbolos para conectivos são binários.

Finalmente, consideraremos os seguintes dois símbolos:

$$) \qquad ($$

respectivamente chamados *o parêntese final* e *o parêntese de abertura*, distintos dos símbolos para os conectivos e também não pertencentes a P.

Certas sucessões finitas compostas de variáveis proposicionais, símbolos para conectivos proposicionais, e os parênteses serão chamados de **fórmulas proposicionais** (ou **proposições**). Fórmulas proposicionais são assim palavras formadas com o seguinte alfabeto:

$$A = \mathrm{P} \cup \{ \neg, \vee, \wedge, \Rightarrow, \Leftrightarrow\} \cup \{), (\} .$$

Convencionalmente, identificaremos os elementos de *A* com as correspondentes palavras de comprimento 1 em *W(A)* (o conjunto dos elementos de *A* que verificam a propriedade *W*). Em particular, P será considerado um subconjunto de *A*. Segue-se então a seguinte definição:

Definição 1.1 O **conjunto *F*** de fórmulas proposicionais construído a partir de P é o menor subconjunto de *W(A)* o qual

- inclui P;
- sempre que contém F, também contém $\neg$ F;
- sempre que contém F e G, também contém

$$(\mathrm{F} \wedge \mathrm{G}), (\mathrm{F} \vee \mathrm{G}), (\mathrm{F} \Rightarrow \mathrm{G}) \text{ e } (\mathrm{F} \Leftrightarrow \mathrm{G}).$$

Por outras palavras, *F* é o menor subconjunto de *W*(*A*) que inclui P e que é fechado para as seguintes operações:

$$\mathrm{F} \mapsto \neg \mathrm{F}$$

$$(F, G) \mapsto (F \wedge G)$$

$$(F, G) \mapsto (F \vee G)$$

$$(F, G) \mapsto (F \Rightarrow G)$$

$$(F, G) \mapsto (F \Leftrightarrow G).$$

Observe-se que há pelo menos um subconjunto de $W(A)$ que tem estas propriedades, nomeadamente o próprio $W(A)$. O conjunto F é a intersecção de todos os subconjuntos de $W(A)$ que gozam destas propriedades.

Consideremos agora alguns exemplos de fórmulas onde A, B e C são elementos de P:

$$A$$

$$(A \Rightarrow (B \Leftrightarrow A))$$

$$(\neg A \Rightarrow A)$$

$$\neg(A \Rightarrow A)$$

$$(((A \wedge (\neg B \Rightarrow \neg A)) \wedge (\neg B \vee \neg C)) \Rightarrow (C \Rightarrow \neg A)).$$

Consideremos também exemplos de algumas expressões que são palavras mas que não são fórmulas:

$$A \wedge B$$

$$\neg(A)$$

$$(A \Rightarrow B \vee C)$$

$$A \Rightarrow B, C$$

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

$$\forall A(A \vee \neg A)$$

$$((A \wedge (B \Rightarrow C)) \vee (\neg A \Rightarrow (B \wedge C)) \wedge (\neg A \vee B)).$$

Muitas vezes por abuso de linguagem na escrita de fórmulas escreveremos $A \wedge B$ com o intuito de representar a fórmula $(A \wedge B)$.

É possível dar uma descrição mais explícita do conjunto F: para isso, definiremos, através de indução, uma sucessão $(F_n)_{n\in\mathbb{N}}$ de subconjuntos de $W(A)$. Assim, fixamos

$$F_0 = P$$

e, para cada *n*,

$$F_{n+1} = F_n \bigcup \{\neg \mathrm{F} : \mathrm{F} \in F_n\} \bigcup \{(\mathrm{F}\, \alpha\, \mathrm{G}) : \mathrm{F}, \mathrm{G} \in F_n, \alpha \in \{\vee, \wedge, \Rightarrow, \Leftrightarrow\}\}$$

Observe-se que a sucessão $(F_n)_{n\in\mathbb{N}}$ é crescente (para $n \leq m$, temos que $F_n \subseteq F_m$).

De seguida iremos provar que

Teorema 1.2 $F = \bigcup_{n\in\mathbb{N}} F_n$

Demonstração: É claro que a união dos F_n , $n\in\mathbb{N}$ inclui P e é fechada para todas as operações a seguir indicadas, se duas palavras F e G pertencem a F_n para um dado inteiro *n*, então

$$\neg \mathrm{F},\ (\mathrm{F} \wedge \mathrm{G}),\ (\mathrm{F} \vee \mathrm{G}),\ (\mathrm{F} \Rightarrow \mathrm{G}) \text{ e } (\mathrm{F} \Leftrightarrow \mathrm{G})$$

pertencem a F_{n+1}. Segue-se que $\bigcup_{n\in\mathbb{N}} F_n$ inclui o menor de todos os conjuntos que gozam destas propriedades, ou seja, o próprio *F*.

Para provarmos a inclusão contrária, mostraremos por indução que para cada inteiro *n*, teremos que $F_n \subseteq F$ que é verdadeiro por definição se $n = 0$, e se supormos que $F_k \subseteq F$, também teremos que $F_{k+1} \subseteq F$ que preserva a definição de F_{k+1} e pelo facto de *F* ser fechado para todas as propriedades.

Temos duas definições equivalentes no conjunto de fórmulas proposicionais. Assim falamos de "**definição de cima para baixo**" no primeiro caso e "**definição de baixo para cima**" no caso que a seguir se segue. Este tipo de definição é chamada "indutiva" ou "por indução". Em cada caso o objectivo é definir o menor subconjunto de um conjunto E que inclui um subconjunto dado e que é fechado para certas operações definidas em E. Temos também uma definição equivalente à "definição de baixo para cima" que consiste em construir um conjunto qualquer para definir um nível de cada vez; o subconjunto dado inicialmente é do mais baixo nível e os elementos do nível $n + 1$ são definidos de forma a serem as imagens de determinadas operações dos elementos dos mais baixos níveis. O conjunto a ser definido é então a união de uma sucessão de subconjuntos, indexada pelo conjunto de números naturais. Em todas as

instâncias de conjuntos definidas por indução, que mais tarde conheceremos, bem como no método de demonstração por indução, a seguir descrito, encontraremos a noção de cota.

⍰ Como poderemos então definir cota?

Podemos definir cota de uma fórmula F $\in$ *F* como:

Definição 1.3 Cota de uma fórmula F $\in$ *F* é o menor inteiro *n* tal que F $\in F_n$ e que é representado por **h[F]**.

Por exemplo, dadas A e B variáveis proposicionais, temos que

$$h[A] = 0$$

$$h[(A \wedge B)] = 1$$

$$h[((A \vee B) \Rightarrow (\neg A))] = 2$$

$$h[\neg\neg\neg B] = 3$$

Observe-se que F_n é o conjunto de fórmulas com cota menor ou igual a *n* (ou seja, h[F_n] $\leq$ *n*) e que $F_{n+1} - F_n$ é o conjunto de fórmulas com cota *n* + 1 (isto é, h[$F_{n+1} - F_n$] = *n* + 1).

Segue-se também, da definição, que para todas as fórmulas F e G $\in$ *F*, temos que:

$$h[\neg F] \leq h[F] + 1 \qquad \text{e} \qquad h[(F\ \alpha\ G)] \leq \sup(h[F], h[G]) + 1,$$

onde α é um símbolo arbitrário, que representa um conectivo binário.

1.1.2 Demonstrações por indução num conjunto de fórmulas

Suponhamos que desejamos mostrar que uma certa propriedade *X*(F) é satisfeita por toda a fórmula F $\in$ *F*. Para isso podemos usar um argumento através de indução da cota de F: assim seríamos conduzidos a mostrar primeiro que *X*(F) é verdadeiro para

toda a fórmula F $\in F_0$, e que se X(F) é verdadeiro para todo F $\in F_n$, então também é verdadeiro para todo F $\in F_{n+1}$ (e assim, para qualquer n).

Este tipo de argumento é associado à definição "de cima para baixo" do conjunto de fórmulas.

É mais prático e mais natural, porém, tomar a primeira definição como ponto de partida. O passo inicial é o mesmo: mostramos que X(F) é satisfeito para todas as fórmulas que pertencem a P (ou seja, a F_0); o passo de indução consiste em provar que, se a fórmula F satisfaz a propriedade X, então também a fórmula $\neg$F satisfaz, e por outro lado, que se F e G satisfazem X, então também as fórmulas (F $\wedge$ G), (F $\vee$ G), (F $\Rightarrow$ G) e (F $\Leftrightarrow$ G) satisfazem.

Por outro lado, podemos ainda concluir que,

Teorema 1.4 A cota de uma fórmula é sempre estritamente menor que o seu comprimento, assumido como o número de caracteres não brancos, (simbolicamente, h[F] < lg[F]).

Demonstração: Neste caso temos que a propriedade X(F) é: h[F] < lg[F].

Assim, se F for uma variável proposicional vem que

$$h[F] = 0 \text{ e } lg[F] = 1$$

logo verifica-se a desigualdade. Continuemos agora com o passo de indução. Assim, suponhamos que a fórmula F satisfaz a desigualdade, h[F] < lg[F]. Então temos que

$$h[\neg F] \leq h[F] + 1 < lg[F] + 1 = lg[\neg F],$$

o que mostra que X($\neg$F) é verdadeiro. Suponhamos agora que F e G são fórmulas que verificam a desigualdade: h[F] < lg[F] e h[G] < lg[G]; então, e com α um símbolo de um conectivo binário, temos que

$$h[(F\ \alpha\ G)] \leq \sup(h[F], h[G]) + 1 < \sup(lg[F], lg[G]) + 1$$
$$< lg[F] + lg[G] + 3 = lg[(F\ \alpha\ G)],$$

o que significa que X(F α G) se verifica, e assim terminando a demonstração.

Como consequência desta propriedade, observa-se que não há nenhuma fórmula de comprimento 0 e que as únicas fórmulas de comprimento 1 são as variáveis proposicionais.

Consideremos uma propriedade $Y(W)$ de uma palavra arbitrária $W \in W(A)$ (não necessariamente uma fórmula).

Lema 1.5 Suponhamos que $Y(W)$ é verdadeira para toda a palavra $W \in P$ e que para quaisquer palavras W e V, se $Y(W)$ e $Y(V)$ são verdadeiras, então,

$$Y(\neg F),\ Y(F \wedge G),\ Y(F \vee G),\ Y(F \Rightarrow G),\ \text{e}\ Y(F \Leftrightarrow G)$$

também são verdadeiras. Então, $Y(F)$ é verdadeira para toda a fórmula F.

Demonstração: Seja Z um conjunto de palavras que verificam a propriedade Y, simbolicamente

$$Z = \{W \in W(A): Y(W)\}.$$

Por hipótese, $Z \supset P$, ou seja, $P \subset Z$ e é fechado para as operações:

$$W \mapsto \neg W,\ (W, V) \mapsto (W \wedge V),\ (W, V) \mapsto (W \vee V).$$

$$(W, V) \mapsto (W \Rightarrow V),\ (W, V) \mapsto (W \Leftrightarrow V).$$

Segue-se que, da definição do conjunto F, que $F \subset Z$, isto é, todos os elementos de F verificam a propriedade Y.

Consideremos agora o caso onde temos uma propriedade $X(F)$ só definida para fórmulas e não para palavras arbitrárias. Assim,

Lema 1.6 Suponhamos que $X(F)$ é verdadeira para toda a fórmula $F \in P$ e que, para todas as fórmulas F e G, se $X(F)$ e $X(G)$ são verdadeiras, então

$$X(\neg F),\ X(F \wedge G),\ X(F \vee G),\ X(F \Rightarrow G),\ \text{e}\ X(F \Leftrightarrow G)$$

também são verdadeiras. Então, $X(F)$ é verdadeira para toda a fórmula F.

Demonstração: Basta considerar a propriedade $Y(W)$: "$W \in F$ e $X(W)$", definida para toda a palavra $W \in W(A)$. Como F inclui P e é fechado para as operações

$$W \mapsto \neg W,\ (W, V) \mapsto (W \wedge V),\ (W, V) \mapsto (W \vee V),$$

$$(W, V) \mapsto (W \Rightarrow V)\ \text{e}\ (W, V) \mapsto (W \Leftrightarrow V)$$

vemos imediatamente que se a propriedade X satisfaz as hipóteses apresentadas, então a propriedade Y satisfaz o lema precedente. Concluímos que $Y(F)$ é verdadeira para toda a fórmula F e consequentemente o mesmo se verifica para $X(F)$.

1.1.3 Decomposição em árvore de uma fórmula

Vejamos que a seguinte palavra W:

$$(((A \wedge (\neg B \Rightarrow \neg A)) \wedge (\neg B \vee \neg C)) \Rightarrow (C \Rightarrow \neg A))$$

é realmente uma fórmula.

Assim, fixando

$$W_0 = ((A \wedge (\neg B \Rightarrow \neg A)) \wedge (\neg B \vee \neg C))$$

e

$$W_1 = (C \Rightarrow \neg A),$$

Observamos que W pode ser escrita como $(W_0 \Rightarrow W_1)$.

Então, depois de fixar

$$W_{00} = (A \wedge (\neg B \Rightarrow \neg A)),$$

$$W_{01} = (\neg B \vee \neg C),$$

$$W_{10} = C,$$

$$W_{11} = \neg A,$$

podemos escrever

$$W_0 = (W_{00} \wedge W_{01}) \text{ e}$$

$$W_1 = (W_{10} \Rightarrow W_{11}).$$

Da mesma forma, seremos conduzidos, sucessivamente, a fixar

$W_{000} = A$ $\qquad$ $W_{001} = (\neg B \Rightarrow \neg A)$

$W_{010} = \neg B$ $\qquad$ $W_{011} = \neg C$

$W_{110} = A$ $\qquad$ $W_{0010} = \neg B$

$W_{0011} = \neg A$ $\qquad$ $W_{0100} = B$

$W_{0110} = C$ $\qquad$ $W_{00100} = B$

$W_{00110} = A$

de tal maneira que

$W_{00} = (W_{000} \wedge W_{001})$, $\qquad$ $W_{01} = (W_{010} \vee W_{011})$,

$W_{11} = \neg W_{110}$, $\qquad$ $W_{001} = (W_{0010} \Rightarrow W_{0011})$,

$W_{010} = \neg W_{0100}$, $\qquad$ $W_{011} = \neg W_{0110}$,

$W_{0010} = \neg W_{00100}$ $\qquad$ e $\qquad$ $W_{0011} = \neg W_{00110}$.

Isto mostra-nos que a palavra W é obtida começando por variáveis proposicionais e aplicando, um número finito de vezes, operações permitidas na definição do conjunto de fórmulas. Segue-se que W é uma fórmula.

Podemos representar o processo de decomposição na forma de árvore. Assim, temos na Figura 1

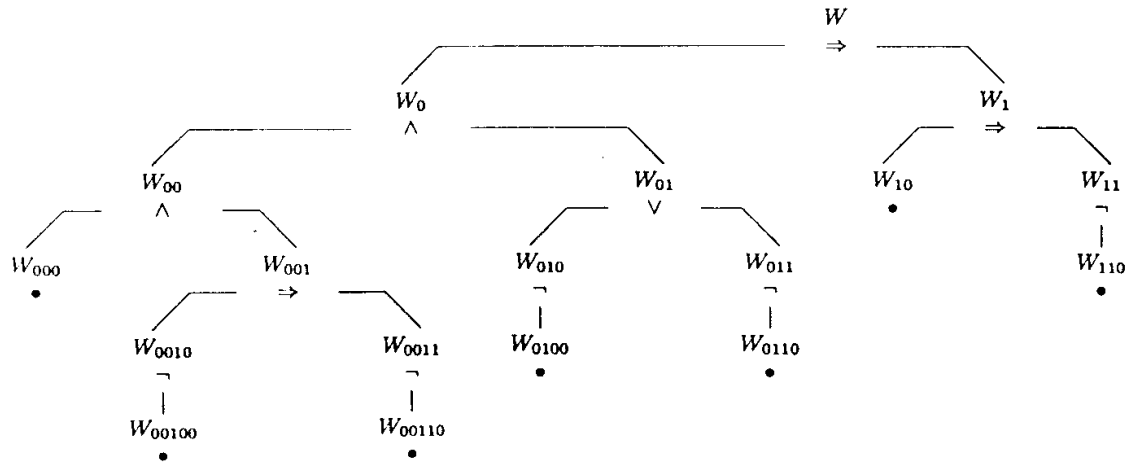

Fig. 1: Decomposição, da fórmula W, em árvore

(adaptada de Cori & Lascar (2000: 14)

Assim, teremos a raiz da árvore (a fórmula W) que estará no topo e os ramos crescem para o fundo. Cada nó da árvore é uma palavra V (que é sempre uma fórmula se a palavra de raiz da árvore é uma fórmula). Daqui três casos podem surgir:

- V é uma variável proposicional e, neste caso, será uma extremidade da árvore;
- V pode ser escrito como ¬V' no caso onde é um único ramo a partir de V e terminando imediatamente no nível abaixo ao nó V';
- V pode ser escrito como (V' α V") - onde α representa um símbolo de um conectivo binário, e neste caso há dois ramos a partir de V e terminando imediatamente no nível abaixo aos dois nós V e V" (neste caso o símbolo apropriado para um conectivo binário será colocado na figura entre os dois ramos).

A decomposição que escolhemos para a fórmula W do exemplo anterior mostra-nos que a sua cota é então menor ou igual a 5. No entanto, neste momento, nada nos permite constatar que a sua cota é exactamente 5.

⍰ Será possível imaginar um segundo modo de decompor esta fórmula de forma a obter uma árvore menor?

Tudo o que podemos dizer, em virtude do teorema 1.2, é que para toda a fórmula $F \in F$, há pelo menos uma decomposição do tipo acima exibido.

1.1.4 Teorema da representação única

Para cada palavra W $\in$ $W(A)$, iremos representar através de **a[W]** (respectivamente **f[W]**) **o número de parênteses de abertura** (respectivamente **o número de parênteses de fecho**) que ocorrem em W.

◈ Poderemos considerar que o número de parênteses abertura é igual ao número de parênteses de fecho?

De facto,

Lema 1.7 Em qualquer fórmula, o número de parênteses de abertura é igual ao número de parênteses de fecho.

Demonstração: Provaremos, por indução, na fórmula F.

- Se a fórmula F pertence ao conjunto P, então temos que
$$a[F] = f[F] = 0.$$
- Se a fórmula F pertence ao conjunto F tal que a[F] = f[F], pois a[F] = a[¬F] e f[F] = f[¬F], então temos que
$$a[\neg F] = f[\neg F].$$
- Para todas as fórmulas F, G $\in$ F tais que: a[F] = f[F] e a[G] = f[G], e com α um símbolo arbitrário de um conectivo binário, temos que
$$a[(F\ \alpha\ G)] = a[F] + a[G] + 1 = f[(F\ \alpha\ G)].$$

Então, a[F] = f[F] para qualquer fórmula proposicional F.

◈ Será que o mesmo se passa se W for um segmento inicial de uma fórmula?

Não. Pois

Lema 1.8 Para qualquer fórmula F $\in$ F e qualquer palavra W $\in$ $W(A)$, se W é um segmento inicial de F, então a[W] ≥ f[W].

Demonstração: A indução é sobre a fórmula F.

- Se F $\in$ P, então para todo o segmento inicial W de F, temos que a[W] = f[W] = 0, consequentemente a[W] ≥ f[W].
- Seja F uma fórmula tal que para todo o segmento inicial W de F, temos que a[W] ≥ f[W]. Consideremos um segmento inicial V de ¬F: se V é uma palavra vazia, então a[V] = f[V] = 0; se V é uma palavra não vazia,

então existe um segmento inicial W de F tal que V = ¬W; temos que a[V] = a[W] e f[V] = f[W], e uma vez que a[W] ≥ f[W] (por hipótese de indução); concluímos que a[V] ≥ f[V].

- Sejam F e G duas fórmulas cujos segmentos iniciais têm pelo menos tantos parênteses de abertura como parênteses de fecho, e seja α um símbolo de um conectivo binário. Seja H = (F α G). Seja V um segmento inicial de H. Quatro casos podem surgir:

  * ou V = ∅: neste caso, a[V] = f[V] = 0;

  * ou V = (W (onde W é um segmento inicial de F):

  então a[V] = a[W] + 1 e f[V] = f[W], e uma vez que a[W] ≥ f[W] (por hipótese de indução), concluímos que a[V] ≥ f[V];

  * ou V = (F α K (onde K é um segmento inicial de G):

  então a[V] = a[F] + a[K] + 1 e f[V] = f[F] + f[K]; mas a[F] = f[F] (pelo lema 1.7) e a[K] ≥ f[K] (por hipótese de indução), o que nos permite concluir uma vez mais que a[V] ≥ f[V];

  * ou V = H: e neste caso a[V] ≥ f[V] (pelo lema 1.7).

Vemos assim que em todos os casos, a[V] ≥ f[V].

◈ E o que se passará se a palavra W for um segmento inicial próprio de F?

Lema 1.9 Para qualquer fórmula F ∈ *F* cujo primeiro símbolo é um parêntese de abertura e para toda a palavra W ∈ *W*(*A*) que é um segmento inicial próprio de F, temos que a[W] > f[W], chamada desigualdade estrita.

Demonstração: Para provarmos a desigualdade estrita consideremos uma fórmula F tal que:

F = (G α H)

onde G e H são fórmulas arbitrárias e α é um símbolo de um conectivo binário. Seja W um segmento inicial próprio de F. Existem então dois casos possíveis:

- Ou W = K, onde K é um segmento inicial de G; neste caso temos que a[W] = a[K] + 1 e f[W] = f[K], e pois a[K] ≥ f[K], (pelo lema 1.8), concluímos que a[W] > f[W];

- Ou W = G α L, onde L é um segmento inicial de H; neste caso temos que a[W] = a[G] + a[L] + 1 e f[W] = f[G] + f[L]; mas a[G] = f[G] (pelo lema 1.7)e a[L] ≥ f[L], (pelo lema 1.8), o que nos leva a que a[W] > f[W].

◈ Será que se verifica sempre que se W for uma palavra então W é uma fórmula?

Não. Pois,

Lema 1.10 Para qualquer fórmula F ∈ *F* e para qualquer palavra W ∈ *W*(*A*), se W é um segmento inicial formal de F então W não é uma fórmula.

Demonstração: Vamos provar por indução sobre a fórmula F.

- Uma variável proposicional não tem nenhum segmento inicial formal.
- Se F é uma fórmula nenhum dos seus segmentos iniciais formais é uma fórmula, e se V é um segmento inicial formal de ¬F, então ou V = ¬ e neste caso não é uma fórmula (as únicas fórmulas de comprimento 1 são os elementos de P), ou então V = ¬W onde W é um segmento inicial formal de F; neste caso W não é uma fórmula (por hipótese de indução) e também não o é V = ¬W. Observe-se que, ao contrário do que estávamos à espera, o facto de que

  "se W não é uma fórmula, então também não o é ¬W"

  não é uma aplicação trivial da definição do conjunto de fórmulas, mas requer uma demonstração. Vamos então fazer a sua demonstração: se ¬W é uma fórmula, e examinando os seus símbolos concluímos que nem é uma variável proposicional nem uma fórmula do tipo (H α K); então, pelo teorema 1.2, existe pelo menos uma fórmula G tal que ¬W = ¬G; se as palavras ¬W e ¬G são idênticas, então também são as palavras W e G o que prova que W é uma fórmula.
- Sejam F e G duas fórmulas arbitrárias, α um símbolo para um conectivo binário, e V um segmento inicial formal de (F α G). Temos que a[V] > f[V] (pelo lema 1.9). Concluímos que V não é uma fórmula (pelo lema 1.7). Note-se que não era necessário, nesta parte do argumento por indução, supor que os segmentos iniciais formais de F e G não eram fórmulas.

◈ O que poderemos dizer acerca da decomposição, será ela única?

De facto a decomposição é única. Assim,

Teorema 1.11 Para qualquer fórmula F $\in$ *F*, um e só um dos três casos seguintes pode surgir:

- Caso l: F $\in$ P.
- Caso 2: existe uma única fórmula G tal que F = ¬G.
- Caso 3: existe um único símbolo para um conectivo binário α e um único par de fórmulas (G, H) $\in$ F^2 tal que F = (G α H).

Demonstração: É óbvio que estes três casos são mutuamente exclusivos: estamos no caso 1, no caso 2 ou no caso 3 (o objectivo é provar a unicidade em cada um destes casos) que preserva o primeiro símbolo de F é um elemento de P, é o símbolo ¬, ou o símbolo ((estas são as únicas possibilidades, que preserva o teorema 1.2).

O que já sabemos (pelo teorema 1.2) é que: ou F $\in$ P, ou então existe pelo menos uma fórmula G tal que F = ¬G, ou então existe pelo menos um símbolo para um conectivo binário α e fórmulas G e H tais que F = (G α H).

Assim só permanece para provarmos a unicidade da decomposição nos casos 2 e 3.

Para o caso 2 é mais ou menos óbvio: se F = ¬G = ¬G', então G = G'.

Para o caso 3, suponhamos que existem fórmulas G, H, K, e L e símbolos para conectivos binários α e β tais que F = (G α H) = (K β L). Concluímos que as duas palavras G α H e K β L são iguais, o que nos mostra que uma das duas fórmulas G e K é um segmento inicial da outra. Por um resultado anterior (lema 1.10), este não pode ser um segmento inicial formal. Uma vez que a palavra vazia não é uma fórmula, concluímos que G = K. Daqui segue-se que as palavras α H e β L são iguais. Os símbolos α e β são então idênticos, assim como as fórmulas H e L.

Podemos também concluir que para todas as fórmulas F e G pertencentes a *F*, temos que

$$h\,[\neg F] = h[F] + 1 \text{ e } h[(F\ \alpha\ G)] = \sup(h[F], h[G]) + 1$$

para qualquer símbolo de um conectivo binário α.

Vamos, de seguida, demonstrar a segunda igualdade.

Seja H a fórmula (F α G). Pois H não seja um elemento de P, existe um e um só inteiro *n* tal que h[H] = *n* + 1. Isto significa que H $\in$ F_{n+1} e H $\notin$ F_n. Pela definição de

F_{n+1} e porque H começa com um parêntese de abertura, concluímos que existem duas fórmulas H_1 e $H_2 \in F_n$ e um símbolo para um conectivo binário β tal que $H = (H_1\ \beta\ H_2)$. Pelo teorema de decomposição única concluímos que $\beta = \alpha$, $H_1 = F$ e $H_2 = G$. Consequentemente, F e G pertencem F_n. Se existir algum inteiro $m < n$ tal que F e G pertençam a F_m, a fórmula $(F\ \alpha\ G)$ pertenceria a F_{m+1}, e consequentemente também a F_n, o que é falso. Segue-se que pelo menos uma das fórmulas F e G tem cota *n*, e assim: $h[(F\ \alpha\ G)] = \sup(h[F], h[G]) + 1$.

1.1.5 Definições por indução (ou recorrência) no conjunto de fórmulas

Tal como podemos fazer demonstrações por indução no conjunto de fórmulas, também podemos obter definições por indução ou recorrência de funções ou de relações cujo domínio é o conjunto de fórmulas. O princípio é o seguinte: dado um conjunto arbitrário E fixo, para definir uma função ϕ de *F* para E, é suficiente, em primeiro lugar, dar os valores de ϕ a P, e depois dar regras que nos permitam, para todas as fórmulas F e G, determinar os valores de

$$\phi(\neg F),\ \phi((F \wedge G)),\ \phi((F \vee G)),\ \phi((F \Rightarrow G))\ \text{e}\ \phi((F \Leftrightarrow G))$$

à custa dos valores de $\phi(F)$ e $\phi(G)$. Sejamos mais precisos:

Lema 1.12 Seja ϕ_0 uma função de P em E, *f* uma função de E em E, e *g*, *h*, *i*, e *j* quatro funções de E^2 em E. Então existe uma única função ϕ de *F* para E que satisfaz as seguintes condições:

- a restrição de ϕ a P é ϕ_0;
- para qualquer fórmula $F \in F$, $\phi(\neg F) = f(\phi(F))$;
- para todas as fórmulas F e $G \in F$;

$$\phi((F \wedge G)) = g(\phi(F), \phi(G)) \qquad \phi((F \vee G)) = h(\phi(F), \phi(G))$$
$$\phi((F \Rightarrow G)) = i(\phi(F), \phi(G)) \qquad \phi((F \Leftrightarrow G)) = j(\phi(F), \phi(G))$$

Demonstração: A unicidade de ϕ é provada facilmente através da indução no conjunto de fórmulas usando o teorema da representação única. A existência de ϕ, que é intuitivamente clara, é provada com um argumento elementar da teoria dos conjuntos.

⍰ Como será então uma definição por recorrência?

Consideremos o seguinte exemplo para o conceito de subfórmula de uma fórmula proposicional.

Definição 1.13 Para cada fórmula $F \in F$ associamos um subconjunto **sf(F)** de *F*, chamado o **conjunto de subfórmulas de F**, que é definido por indução que preserva as seguintes condições:

- se $F \in P$,
$$sf(F) = \{F\};$$
- se $F = \neg G$,
$$sf(F) = sf(G) \cup \{F\};$$
- se $F = (G\ \alpha\ H)$ onde $\alpha \in \{\vee, \wedge, \Rightarrow, \Leftrightarrow\}$,
$$sf(F) = sf(G) \cup sf(H) \cup \{F\}.$$

É fácil verificar que as subfórmulas de uma fórmula são exactamente as que aparecem como nós na sua decomposição em árvore.

1.1.6 Substituições numa fórmula proposicional

Seja F uma fórmula de *F* e sejam $A_1, A_2, ..., A_n$ variáveis proposicionais de P distintas duas a duas. Usaremos a notação de $F[A_1, A_2, ..., A_n]$ para F quando quisermos salientar os elementos de P que ocorrem pelo menos uma vez em F e que estejam entre $A_1, A_2, ..., A_n$. Por exemplo, a fórmula $F = (A \Rightarrow (B \vee A))$ pode ser escrita tanto como F[A, B], ou F[A, B, C, D] se for útil em determinado contexto.

Se tivermos uma fórmula $F[A_1, A_2, ..., A_n, B_1, B_2, ..., B_m]$ e *n* fórmulas de $G_1, G_2, ..., G_n$, considere-se a palavra obtida substituindo a variável A_1, (respectivamente: $A_2, ..., A_n$) pela fórmula G_1 (respectivamente: $G_2, ..., G_n$) em cada ocorrência destas em F. Esta palavra será representada por $F_{G_1/A_1, G_2/A_2, ..., G_n/A_n}$, mas também representamos isto por $F[G_1, G_2, ..., G_n, B_1, B_2, ..., B_m]$, apesar de que isto poderia causar alguns problemas.

Por exemplo, se F = F[A, B] é a fórmula (A $\Rightarrow$ (B $\vee$ A)) e G é a fórmula (B $\Rightarrow$ A), então $F_{G/A}$ é a palavra ((B $\Rightarrow$ A) $\Rightarrow$ (B $\vee$ (B $\Rightarrow$ A))), a qual podemos representar por F[G, B] ou igualmente por F[(B $\Rightarrow$ A), B]. Se consideramos uma variável proposicional C (distinta de A e B) e uma fórmula H = C, então $F_{H/A}$ é a palavra (C $\Rightarrow$ (B $\vee$ C)) que pode ser escrita, que preserva as nossas convenções, como F[C, B]. Surge então uma ambiguidade, uma vez que não é claro como determinar, das igualdades,

$$F[A, B] = (A \Rightarrow (B \vee A)) \quad \text{e} \quad F[C, B] = (C \Rightarrow (B \vee C))$$

qual destas duas fórmulas é a fórmula F.

Não obstante, a notação $F[G_1, G_2, ..., G_n, B_1, B_2, ..., B_m]$ é extremamente prática e, na maioria dos casos, perfeitamente clara. É por isso que usaremos esta, apesar do perigo; limitamos o seu uso a circunstâncias onde não haja nenhuma ambiguidade.

De facto, poderemos dar uma definição de $F_{G_1/A_1,G_2/A_2,...,G_n/A_n}$ por indução sobre a fórmula F (onde $G_1, G_2, ..., G_n \in F$ e $A_1, A_2, ..., A_n \in P$ permanecem fixos):

- se $F \in P$, então

$$F_{G_1/A_1,G_2/A_2,...,G_n/A_n} = \begin{cases} G_K & \text{se } F = A_K \ (1 \le K \le n); \\ F & \text{se } F \notin \{A_1, A_2, ..., A_n\}. \end{cases}$$

- se F = ¬G, então

$$F_{G_1/A_1,G_2/A_2,...,G_n/A_n} = \neg G_{G_1/A_1,G_2/A_2,...,G_n/A_n};$$

- se F = (G α H), então

$$F_{G_1/A_1,G_2/A_2,...,G_n/A_n} = (G_{G_1/A_1,G_2/A_2,...,G_n/A_n} \ \alpha \ H_{G_1/A_1,G_2/A_2,...,G_n/A_n})$$

para todas as fórmulas G e H e para o conectivo binário α.

Nos exemplos anteriores, pudemos observar que a palavra obtida depois de substituir variáveis proposicionais por fórmulas numa fórmula era, em todos os casos, ela mesma uma fórmula, o que não é nada surpreendente uma vez que

Teorema 1.14 Dados um inteiro *n*, fórmulas F, G_1, G_2, ..., G_n, e variáveis proposicionais A_1, A_2, ..., A_n, a palavra $F_{G_1/A_1,G_2/A_2,...,G_n/A_n}$ é uma fórmula.

Demonstração: Sejam $G_1, G_2, ..., G_n \in F$ e $A_l, A_2, ..., A_n \in P$ fixados, provaremos o teorema por indução sobre a fórmula F.

- Se $F \in P$, $F_{G_1/A_1,G_2/A_2,...,G_n/A_n}$ é igual a G_k se $F = A_k$ $(1 \leq k \leq n)$ e para F se $F \notin \{A_1, A_2, ..., A_n\}$; em ambos os casos F é uma fórmula.
- Se $F = \neg G$, e se suposermos que $G_{G_1/A_1,G_2/A_2,...,G_n/A_n}$ é uma fórmula, então $F_{G_1/A_1,G_2/A_2,...,G_n/A_n}$, que é a palavra $\neg G_{G_1/A_1,G_2/A_2,...,G_n/A_n}$, é novamente uma fórmula.
- Se $F = (G \alpha H)$ (onde α é um símbolo de um conectivo binário) e se suposermos que as palavras $G_{G_1/A_1,G_2/A_2,...,G_n/A_n}$ e $H_{G_1/A_1,G_2/A_2,...,G_n/A_n}$ são fórmulas, então $F_{G_1/A_1,G_2/A_2,...,G_n/A_n}$, que é a palavra $(G_{G_1/A_1,G_2/A_2,...,G_n/A_n} \alpha H_{G_1/A_1,G_2/A_2,...,G_n/A_n})$, é também uma fórmula.

Note-se que a fórmula

$$F_{G_1/A_1,G_2/A_2,...,G_n/A_n}$$

é o resultado de substituir simultaneamente as variáveis $A_1, A_2, ..., A_n$ pelas fórmulas $G_1, G_2, ..., G_n$ na fórmula F. Em princípio obteríamos uma fórmula diferente se executássemos estas substituições uma após a outra; além disso, o resultado que obteríamos poderia depender da ordem pela qual estas substituições eram executadas.

Tomemos um exemplo. Consideremos

$$F = (A_1 \wedge A_2), \quad G_1 = (A_1 \vee A_2) \quad \text{e} \quad G_2 = (A_1 \Rightarrow A_2)$$

Temos então:

$$F_{G_1/A_1,G_2/A_2} = ((A_1 \vee A_2) \wedge (A_1 \Rightarrow A_2));$$

considerando que

$$[F_{G_1/A_1}]_{G_2/A_2} = (A_1 \vee (A_1 \Rightarrow A_2)) \wedge (A_1 \Rightarrow A_2));$$

e

$$[F_{G_2/A_2}]_{G_1/A_1} = ((A_1 \vee A_2) \wedge ((A_1 \vee A_2) \Rightarrow A_2)).$$

Também podemos, numa dada fórmula F, substituir uma subfórmula H de F por uma fórmula G. A palavra que resulta desta operação é uma vez mais uma fórmula. Embora, na prática, este tipo de substituição seja muito frequente, não introduziremos uma notação especial e não entraremos em detalhes. Consideremos apenas um exemplo. Suponhamos que

$F = (((A \wedge B) \Rightarrow (\neg B \wedge (A \Rightarrow C))) \vee (B \Leftrightarrow (B \Rightarrow (A \vee C))))$,

$G = (A \Leftrightarrow (B \vee C))$ e

$H = (\neg B \wedge (A \Rightarrow C))$.

Então, substituindo a subfórmula H pela fórmula G na fórmula F, obtemos a fórmula

$$(((A \wedge B) \Rightarrow (A \Leftrightarrow (B \vee C))) \vee (B \Leftrightarrow (B \Rightarrow (A \vee C)))).$$

1.2 Semântica

1.2.1 Atribuição de valores lógicos e tabelas de verdade

Definição 1.15 Uma **atribuição de valores lógicos** para P é uma aplicação de P no conjunto {0,l}.

Em vez de "atribuição de valores lógicos", fala-se de uma "**valoração**", ou de uma "**valuação**", ou "**distribuição de valores de verdade**".

Uma atribuição de valores lógicos para P é então um elemento do conjunto $\{0,1\}^P$.

Uma atribuição de valores lógicos $\delta \in \{0,1\}^P$ atribui, a cada variável proposicional A, um valor $\delta(A)$ que é 0 ou 1 (intuitivamente, falso ou verdadeiro). Uma vez feito isto, veremos que é possível, de uma e uma só maneira, estender δ ao conjunto de todas as fórmulas proposicionais e respeitando as regras que conformam, mais ou menos, o significado intuitivo dos nomes dados aos vários símbolos para conectivos proposicionais.

⍰ Porquê "mais ou menos"?

Porque, embora seja duvidoso que alguém fique espantado com o facto de uma fórmula F receber o valor 1 se e só se a fórmula $\neg$F receber o valor 0, a decisão para atribuir o valor 1 à fórmula $(F \Rightarrow G)$ quando as fórmulas F e G têm ambas o valor 0 talvez dê lugar a uma maior intranquilidade (pelo menos no princípio). Um modo para dissipar esta intranquilidade é perguntarmo-nos a nós próprios sob que circunstâncias a fórmula $(F \Rightarrow G)$ pode ser considerada falsa. Provavelmente concordaríamos que isto só aconteceria no caso de F ser verdadeira e sem G ser também verdadeira, o que nos conduz a atribuir o valor 1 para $(F \Rightarrow G)$ nos outros três casos possíveis. A dificuldade surge sem dúvida do facto de, em argumentos matemáticos, termos a impressão de que

praticamente nunca temos que considerar situações do tipo “falso implica falso” ou “falso implica verdade”. Mas esta impressão está errada.

Existe outra dificuldade relativa à implicação, em que os matemáticos vêem uma noção de causalidade, que o cálculo proposicional não leva em conta. Se P_1 e P_2 são duas frases verdadeiras, a lógica proposicional impõe o valor verdade na frase “P_1 implica P_2”. Mas um matemático frequentemente recusará afirmar que “P_1 implica P_2”é verdade quando as frases P_1 e P_2 nada têm em comum uma com a outra.

Embora os conflitos entre intuição ou uso matemático e as definições que estamos prestes a dar surjam especialmente com a implicação, os outros conectivos também podem fazer uma modesta contribuição para isto (a disjunção é frequentemente interpretada como exclusiva (A ou B mas não ambos) mas que não será o nosso $\vee$).

No cálculo proposicional, não serão considerados estes tipos de questões. Estaremos contentes por executar operações muito simples com dois objectos: 0 e 1, e a nossa única referência será feita às definições destas operações, ou seja, o que chamaremos de tabelas de verdade.

Que seja perfeitamente claro que a intuição a que nos referimos é a intuição exclusivamente matemática. A nossa preocupação não é invocar “sempre” a lógica (o que é conhecido como “senso comum”). Os Matemáticos não fazem questão de possuir um modo universal de razão. É difícil resistir a aplicar a razão matemática em situações fora da matemática, uma vez que ficamos seduzidos pelo rigor desta razão, quando a descobrimos. Mas o resultado não é o que estávamos à espera: rapidamente enfrentamos o facto de que os problemas humanos não se conseguem resolver através da lógica matemática. Uma das virtudes pedagógicas é dar exemplos da “vida real”, mas eles são o oposto do que alguns esperam. No entanto, este tipo de aproximação não faz a aprendizagem das regras da lógica matemática mais fácil, mas é muito útil para ensinar prudência, e até mesmo humildade: para aprender a razão matemática, estudemos matemática. A aplicação da lógica matemática à “vida real” produziu uma colecção de hilariantes exemplos que alguns estudantes conhecem bem e que atingiram uma certa popularidade entre os lógicos. Vejamos um desses exemplos:

- o que pensamos acerca da equivalência entre: *“se tens fome, há alguma comida no frigorifico”* e a sua contrapositiva: *“se não existe comida no frigorifico, não tens fome”*?

Como podemos ver, tudo isto tem sem dúvida um lado divertido, mas não nos ajuda em nada a resolver exercícios de matemática em geral ou lógica matemática em particular.

Teorema 1.16 Para qualquer atribuição de valores lógicos $\delta \in \{0,1\}^P$, existe uma única aplicação $\bar{\delta}: F \Rightarrow \{0,1\}$ que satisfaz δ em P e que verifica as seguintes propriedades:

(1) para qualquer fórmula F,

$$\bar{\delta}(\neg F) = 1 \text{ se e só se } \bar{\delta}(F) = 0;$$

(2) para todas as fórmulas F e G,

$$\bar{\delta}(F \wedge G) = 1 \text{ se e só se } \bar{\delta}(F) = \bar{\delta}(G) = 1;$$

(3) para todas as fórmulas F e G,

$$\bar{\delta}(F \vee G) = 0 \text{ se e só se } \bar{\delta}(F) = \bar{\delta}(G) = 0;$$

(4) para todas as fórmulas F e G,

$$\bar{\delta}(F \Rightarrow G) = 0 \text{ se e só se } \bar{\delta}(F) = 1 \text{ e } \bar{\delta}(G) = 0;$$

(5) para todas as fórmulas F e G,

$$\bar{\delta}(F \Leftrightarrow G) = 1 \text{ se e só se } \bar{\delta}(F) = \bar{\delta}(G).$$

Demonstração: De forma a simplificar a notação, observemos desde já que as condições de (1) até (5) podem ser expressas usando as operações de adição e multiplicação no corpo de dois elementos $\mathbb{Z}/2\mathbb{Z}$, com o qual podemos identificar naturalmente o conjunto $\{0,1\}$. Estas condições ficam então equivalentes a:

para todas as fórmulas F e G:

(i') $\bar{\delta}(\neg F) = 1 + \bar{\delta}(F)$;

(ii') $\bar{\delta}((F \wedge G)) = \bar{\delta}(F)\bar{\delta}(G)$;

(iii') $\bar{\delta}((F \vee G)) = \bar{\delta}(F) + \bar{\delta}(G) + \bar{\delta}(F)\bar{\delta}(G)$;

(iv') $\bar{\delta}((F \Rightarrow G)) = 1 + \bar{\delta}(F) + \bar{\delta}(F)\bar{\delta}(G)$;

(v') $\bar{\delta}((F \Leftrightarrow G)) = 1 + \bar{\delta}(F) + \bar{\delta}(G)$.

(A demonstração é imediata.)

Vemos que a função $\bar{\delta}$ é definida por indução no conjunto de fórmulas, o que garante a sua existência e unicidade (lema 1.12); aqui, as funções *f*, *g*, *h*, *i*, e *j* são definidas em $\mathbb{Z}/2\mathbb{Z}$ por: para todo o *x* e todo o *y*,

$$f(x) = 1 + x,\ g(x, y) = xy,\ h(x, y) = x + y + xy,$$
$$i(x, y) = 1 + x + xy \text{ e } j(x, y) = 1 + x + y.$$

Identificando {0,1} com $\mathbb{Z}/2\mathbb{Z}$ é extremamente prático e será usado no que se segue.

De seguida apresentaremos, na figura 2, as tabelas de verdade para a negação, a conjunção, a disjunção, a implicação e a equivalência

F	$\neg F$
0	1
1	0

F	G	$(F \wedge G)$
0	0	0
0	1	0
1	0	0
1	1	1

F	G	$(F \vee G)$
0	0	0
0	1	1
1	0	1
1	1	1

F	G	$(F \Rightarrow G)$
0	0	1
0	1	1
1	0	0
1	1	1

F	G	$(F \Leftrightarrow G)$
0	0	1
0	1	0
1	0	0
1	1	1

Fig. 2: Tabelas de verdade para a negação, a conjunção, a disjunção, a implicação e a equivalência

(adaptada de Cori & Lascar (2000: 25)

Na prática, não iremos fazer a distinção entre uma atribuição de valores lógicos e a sua extensão ao conjunto de fórmulas. Assim, falaremos do "valor lógico da fórmula F sob a atribuição δ" e eventualmente esqueceremos a barra por cima do δ que nos indicaria que estávamos a trabalhar com uma extensão.

Se F é uma fórmula e δ uma atribuição de valores lógicos, dizemos que F é satisfeito por δ, ou que δ satisfaz F, quando $\bar{\delta}(F) = 1$.

Dada uma fórmula F e uma atribuição de valores lógicos δ, a definição da extensão $\bar{\delta}$ aponta claramente para um método para calcular $\bar{\delta}(F)$: este consiste em calcular os valores tomados por $\bar{\delta}$ nas várias subfórmulas de F, começando pelas subfórmulas de cota 1 (os valores para os de cota 0), e aplicando as tabelas seguintes tantas vezes quantas as necessárias. Por exemplo, se F é a fórmula

$$((A \Rightarrow B) \Rightarrow (B \vee (A \Leftrightarrow C)))$$

e se δ é uma atribuição de valores lógicos para qual

$$\delta(A) = \delta(B) = 0 \text{ e } \delta(C) = 1,$$

então temos sucessivamente:

$$\overline{\delta}((A \Rightarrow B)) = 1;\ \overline{\delta}((A \Leftrightarrow C)) = 0;\ \overline{\delta}((B \vee (A \Leftrightarrow C))) = 0 \text{ e } \overline{\delta}(F) = 0.$$

Pode também acontecer que o cálculo dos valores de $\overline{\delta}$ para todas as subfórmulas de F não seja necessário tal como podemos constatar com a seguinte fórmula,

$$G = (A \Rightarrow (((B \wedge \neg A) \vee (\neg C \wedge A)) \Leftrightarrow (A \vee (A \Rightarrow \neg B))))$$

e com λ uma atribuição de valores lógicos para a qual $\lambda(A) = 0$; podemos então desde já concluir que $\lambda(G) = 1$ sem nos preocuparmos com o valor lógico da subfórmula

$$(((B \wedge \neg A) \vee (\neg C \wedge A)) \Leftrightarrow (A \vee (A \Rightarrow \neg B)))$$

uma vez que temos como operação principal da fórmula G uma implicação em que o antecedente é falso ($\lambda(A) = 0$) logo a implicação tem sempre o valor lógico verdade.

Verificamos que, para calcular o valor lógico de uma fórmula, apenas usamos os valores tomados pela atribuição de valores lógicos sob consideração das variáveis que de facto aparecem na fórmula.

Lema 1.17 Para qualquer fórmula $F[A_1, A_2, ..., A_n]$ (não envolvendo nenhuma variável proposicional para além de $A_1, A_2, ..., A_n$) e quaisquer atribuições de valores lógicos λ e $\mu \in \{0,1\}^P$, se λ e μ estão de acordo no conjunto das variáveis proposicionais $A_1, A_2, ..., A_n$, então $\overline{\lambda}(F) = \overline{\mu}(F)$.

Demonstração: A demonstração não envolve nenhuma dificuldade e é feita por indução sobre as fórmulas.

Seja $G[A_1, A_2, ..., A_n]$ uma fórmula. Para encontrar o conjunto de valores lógicos de G, ou seja, o conjunto de todas as possíveis atribuições de G, vemos que é suficiente omitir momentaneamente as variáveis de P que não aparecem em G, e supor que o conjunto de variáveis proposicionais é apenas $\{A_1, A_2, ..., A_n\}$. Então existe um número finito de atribuição de valores lógicos a considerar: é o número de aplicação de $\{A_1, A_2, ..., A_n\}$ para $\{0,1\}$, denominado por 2^n. Podemos identificar cada aplicação δ de $\{A_1, A_2, ..., A_n\}$ para $\{0,1\}$ com o n-uplo ordenado $(\delta(A_1), \delta(A_2), ..., \delta(A_n)) \in \{0,1\}^n$ e colocar o conjunto de valores lógicos tomados por G num quadro no qual cada fila corresponde a cada um dos 2^n n-uplos ordenados e que contém o correspondente valor lógico de G. Tal quadro, que também poderia conter os valores lógicos das subfórmulas

de G, será chamado de tabela de verdade da fórmula G. Esta não é mais do que uma tabela de valores de uma certa aplicação de $\{0,1\}^n$ em $\{0,1\}$.

Consideremos novamente o exemplo anterior:

$$G = (A \Rightarrow (((B \wedge \neg A) \vee (\neg C \wedge A)) \Leftrightarrow (A \vee (A \Rightarrow \neg B))))$$

e sejam

$$H = (B \wedge \neg A), \qquad I = (\neg C \wedge A), \qquad J = (A \Rightarrow \neg B),$$

$$K = (H \vee I), \qquad L = (A \vee J), \qquad M = (K \Leftrightarrow L).$$

Então temos que $G = (A \Rightarrow M)$, onde a tabela de verdade de G , figura 3, é:

A	*B*	*C*	¬*A*	¬*B*	¬*C*	*H*	*I*	*J*	*K*	*L*	*M*	*G*
0	0	0	1	1	1	0	0	1	0	1	0	1
0	0	1	1	1	0	0	0	1	0	1	0	1
0	1	0	1	0	1	1	0	1	1	1	1	1
0	1	1	1	0	0	1	0	1	1	1	1	1
1	0	0	0	1	1	0	1	1	1	1	1	1
1	0	1	0	1	0	0	0	1	0	1	0	0
1	1	0	0	0	1	0	1	0	1	1	1	1
1	1	1	0	0	0	0	0	0	0	1	0	0

Fig. 3: Tabela de verdade da fórmula $G = (A \Rightarrow (((B \wedge \neg A) \vee (\neg C \wedge A)) \Leftrightarrow (A \vee (A \Rightarrow \neg B))))$ (adaptada de Cori & Lascar (2000: 27)

Devemos notar que não existe uma única tabela de verdade para uma fórmula (por exemplo, as primeiras quatro colunas da tabela poderiam ser consideradas como a tabela de verdade da fórmula ¬A). Há, no entanto, uma tabela "mínima" para cada fórmula, que envolve apenas as variáveis proposicionais que aparecem pelo menos uma vez na fórmula.

Porém, mesmo restringindo-nos a esta noção de tabela mínima, pode ainda haver, para a mesma fórmula, várias tabelas que diferem apenas na ordem pela qual os *n*-uplos ordenados de $\{0,1\}^n$ são apresentados.

É razoável escolher, de uma vez por todas, uma ordem particular (entre os $2^n!$ que são possíveis) e adoptá-la sistematicamente. Escolhemos a ordem lexicográfica: na tabela, o *n*-uplo ordenado $(a_1, a_2, ..., a_n)$ será colocado à frente de $(b_1, b_2, ..., b_n)$ se, para a primeira subscrição $j \in \{1, 2, .., n\}$ para a qual $a_j \neq b_j$, temos que $a_j < b_j$.

1.2.2 Tautologias e fórmulas logicamente equivalentes

Definição 1.18

- Uma **tautologia** é uma fórmula que assume o valor 1 em cada atribuição de valores lógicos.

  A notação para "**F é um tautologia**" é: $\models \mathbf{F}$;

  E onde $\not\models$ **F** significa: "**F não é uma tautologia**".

- Dadas duas fórmulas F e G, F é **logicamente equivalente** a G se e só se a fórmula $(F \Leftrightarrow G)$ é uma tautologia.

  A notação para "F é logicamente equivalente a G" é: $F \sim G$.

Com base nestas definições seguem-se duas propriedades:

- Para todas as fórmulas F e G, temos que $F \sim G$ se e só se para toda a atribuição de valores lógicos $\delta \in \{0,1\}^P$, $\overline{\delta}(F) = \overline{\delta}(G)$.
- A relação binária ~ é uma relação de equivalência em *F*.

A **classe de equivalência** da fórmula F para a relação ~ é representada por **cl(F)**.

Uma tautologia é então uma fórmula cuja tabela de verdade contém apenas 1's na última coluna, ou seja, uma fórmula que é "sempre verdadeira". Duas fórmulas logicamente equivalentes são duas fórmulas que são satisfeitas exactamente pelas mesmas atribuições de valores lógicos, e que têm as mesmas tabelas de verdade. Qualquer fórmula logicamente equivalente a uma tautologia é uma tautologia. Para além disso, as tautologias constituem uma das classes de equivalência da relação binária ~, representada por 1. As fórmulas cujas negações são tautologias (chamadas de **antilogias**, ou de **antitautologias**, ou **contradições**) constituem outra classe de equivalência, distinta de 1, e representada por 0: estas são as fórmulas que são "sempre falsas", ou seja, aquelas cujas tabelas de verdade contêm apenas 0's na última coluna.

Vamos agora analisar o efeito das substituições nos valores de verdade de fórmulas.

Teorema 1.19 Dada uma atribuição de valores lógicos, δ, um número natural, *n*, fórmulas F, G_1, G_2, ..., G_n, e variáveis proposicionais A_l, A_2, ..., A_n, distintas duas a duas e tomemos λ a atribuição de valores lógicos definida por

$$\text{para todo o } X \in P,\ \lambda(X) = \begin{cases} \delta(X) & \text{se } X \notin \{A_1, A_2, ..., A_n\}; \\ \bar{\delta}(G_i) & \text{se } X = A_i \quad (1 \leq i \leq n). \end{cases}$$

temos então que

$$\bar{\delta}(F_{G_1/A_1, G_2/A_2, ..., G_n/A_n}) = \bar{\lambda}(F).$$

Demonstração: Vamos provar por indução sobre a fórmula F:

- Se F é um elemento de P, então:

ou $F \notin \{A_1, A_2, ..., A_n\}$; e neste caso, $F_{G_1/A_1, G_2/A_2, ..., G_n/A_n} = F$ e $\bar{\delta}(F_{G_1/A_1, G_2/A_2, ..., G_n/A_n}) = \bar{\delta}(F) = \delta(F) = \lambda(F) = \bar{\lambda}(F)$;

ou $F = A_i$ $(1 \leq i \leq n)$; e neste caso, $F_{G_1/A_1, G_2/A_2, ..., G_n/A_n} = G_i$ e $\bar{\delta}(F_{G_1/A_1, G_2/A_2, ..., G_n/A_n}) = \bar{\delta}(G_i) = \lambda(A_i) = \lambda(F) = \bar{\lambda}(F)$ por definição de λ.

- Se $F = \neg G$, e se suposermos que $\bar{\delta}(G_{G_1/A_1, G_2/A_2, ..., G_n/A_n}) = \bar{\lambda}(G)$ (a hipótese de indução), então

$$\begin{aligned} \bar{\delta}(F_{G_1/A_1, G_2/A_2, ..., G_n/A_n}) &= \bar{\delta}(\neg G_{G_1/A_1, G_2/A_2, ..., G_n/A_n}) \\ &= 1 + \bar{\delta}(G_{G_1/A_1, G_2/A_2, ..., G_n/A_n}) \\ &= 1 + \bar{\lambda}(G) = \bar{\lambda}(\neg G) = \bar{\lambda}(F). \end{aligned}$$

- Se $F = (G \wedge H)$, e se suposermos (a hipótese de indução)

$\bar{\delta}(G_{G_1/A_1, G_2/A_2, ..., G_n/A_n}) = \bar{\lambda}(G)$ e $\bar{\delta}(H_{G_1/A_1, G_2/A_2, ..., G_n/A_n}) = \bar{\lambda}(H)$,

então

$$\begin{aligned} \bar{\delta}(F_{G_1/A_1, G_2/A_2, ..., G_n/A_n}) &= \bar{\delta}((G_{G_1/A_1, G_2/A_2, ..., G_n/A_n} \wedge H_{G_1/A_1, G_2/A_2, ..., G_n/A_n})) \\ &= \bar{\delta}(G_{G_1/A_1, G_2/A_2, ..., G_n/A_n}) \times \bar{\delta}(H_{G_1/A_1, G_2/A_2, ..., G_n/A_n}) \\ &= \bar{\lambda}(G)\bar{\lambda}(H) = \bar{\lambda}((G \wedge H)) = \bar{\lambda}(F). \end{aligned}$$

- Os casos $F = (G \vee H)$, $F = (G \Rightarrow H)$, e $F = (G \Leftrightarrow H)$ são tratados de uma forma semelhante sem dificuldade.

Segue-se imediatamente deste teorema que:

Corolário 1.20 Para todas as fórmulas F, G_1, G_2, ..., G_n e todas as variáveis proposicionais A_1, A_2, ..., A_n distintas duas a duas, se F é uma tautologia, então também o é a fórmula:

$$F_{G_1/A_1,G_2/A_2,...,G_n/A_n}.$$

Demonstração: Para demonstrar este corolário consideremos uma qualquer atribuição de valores lógicos δ e definamos uma atribuição λ tal como no teorema anterior; então temos que

$$\bar{\delta}(F_{G_1/A_1,G_2/A_2,...,G_n/A_n}) = \bar{\lambda}(F) = 1,$$

pois F seja uma tautologia.

Outro tipo de substituição que também nos permite preservar a equivalência lógica de fórmulas é:

Teorema 1.21 Considere-se uma fórmula F, uma subfórmula G de F e uma fórmula H que é logicamente equivalente a G (H ~ G). Então a fórmula F′, obtida de F substituindo a subfórmula G pela fórmula H, é logicamente equivalente a F.

Demonstração: Vamos demonstrar o teorema por indução sobre a fórmula F.

- Se $F \in P$, então, necessariamente, G = F e F′ = H. Então temos de certeza que F′ ~ F.
- Se $F = \neg F_1$, então ou G = F, F′ = H, e temos que F′ ~ F, ou então G é uma subfórmula de F_1 e, por hipótese de indução, a fórmula F'_1, que resulta da substituição de G por H em F_1, é logicamente equivalente a F_1 pois, para qualquer atribuição de valores lógicos δ, temos que
$$\bar{\delta}(F') = 1 + \bar{\delta}(F_1') = 1 + \bar{\delta}(F_1) = \bar{\delta}(\neg F_1) = \bar{\delta}(F).$$
- Se $F = (F_1 \wedge F_2)$, então existem três possibilidades. Ou G = F, F′ = H, e temos que F′ ~ F. Ou então G é uma subfórmula de F_1, e, por hipótese de indução, a fórmula F'_1, que resulta da substituição de G por H em F_1, é logicamente equivalente a F_1. Então a fórmula F′ é a fórmula $(F'_1 \wedge F_2)$; esta é logicamente equivalente a F porque, para qualquer atribuição δ, temos que
$$\bar{\delta}(F') = \bar{\delta}(F_1')\bar{\delta}(F_2) = \bar{\delta}(F_1)\bar{\delta}(F_2) = \bar{\delta}((F_1 \wedge F_2)) = \bar{\delta}(F).$$

No terceiro caso, o argumento é estritamente similar, quando G é uma subfórmula de F_2.

Os casos $F = (F_1 \Leftrightarrow F_2)$, $F = (F_1 \vee F_2)$, e $F = (F_1 \Rightarrow F_2)$ são tratados de uma forma análoga, usando as relações de (3) a (5), do teorema 1.16

Na prática, para mostrar que uma fórmula é uma tautologia, ou que duas fórmulas são logicamente equivalentes, temos vários métodos disponíveis. Em primeiro lugar, poderemos usar tabelas de verdade, mas não é muito viável uma vez que o número de variáveis pode exceder 3 ou 4. Em certos casos, poderemos recorrer ao que se poderá chamar de "tabelas de verdade económicas": estas consistem em discutir os valores tomados por um número restringido de variáveis; de certo modo, estamos a tratar várias linhas da tabela de verdade num único passo. Consideremos um exemplo onde mostraremos que a seguinte fórmula F é uma tautologia:

$$((A \Rightarrow ((B \vee \neg C) \wedge \neg(A \Rightarrow D))) \vee ((D \wedge \neg E) \vee (A \vee C))).$$

Fixando

$$H = (A \Rightarrow ((B \vee \neg C) \wedge \neg(A \Rightarrow D))) \text{ e}$$

$$K = ((D \wedge \neg E) \vee (A \vee C)),$$

temos que $F = (H \vee K)$. De seguida, considere-se uma atribuição de valores lógicos δ. Se $\delta(A) = 0$, vemos que $\bar{\delta}(H) = 1$, assim como $\bar{\delta}(F) = 1$. Se $\delta(A) = 1$, então $\bar{\delta}(A \vee C) = 1$, e consequentemente $\bar{\delta}(K) = 1$ e $\bar{\delta}(F) = 1$.

Da mesma maneira, por exemplo, para mostrar que a fórmula

$$G = ((\neg A \vee B) \vee \neg(A \Rightarrow B))$$

é uma tautologia, usamos primeiro o facto de que as fórmulas $(\neg A \vee B)$ e $(A \Rightarrow B)$ são logicamente equivalentes, o que nos mostra que G é logicamente equivalente a $((A \Rightarrow B) \vee \neg(A \Rightarrow B)$, então observe-se que esta última fórmula é obtida por substituição da variável A pela fórmula $(A \Rightarrow B)$ na tautologia $(A \vee \neg A)$, que é ela própria uma tautologia.

1.2.3 Algumas tautologias

Consideremos a seguinte lista de algumas tautologias mais comuns:

(A, B e C representam variáveis proposicionais; $\top$ representa uma tautologia arbitrária e $\bot$ a negação de $\top$, o que é o mesmo que dizer que toma sempre o valor 0).

(1) $((A \wedge A) \Leftrightarrow A)$

(2) $((A \vee A) \Leftrightarrow A)$

(3) $((A \wedge B) \Leftrightarrow (B \wedge A))$

(4) $((A \vee B) \Leftrightarrow (B \vee A))$

(5) $((A \wedge (B \wedge C)) \Leftrightarrow ((A \wedge B) \wedge C))$

(6) $((A \vee (B \vee C)) \Leftrightarrow ((A \vee B) \vee C))$

(7) $((A \wedge (B \vee C)) \Leftrightarrow ((A \wedge B) \vee (A \wedge C)))$

(8) $((A \vee (B \wedge C)) \Leftrightarrow ((A \vee B) \wedge (A \vee C)))$

(9) $((A \wedge (A \vee B)) \Leftrightarrow A)$

(10) $((A \vee (A \wedge B)) \Leftrightarrow A)$

(11) $(\neg(A \vee B) \Leftrightarrow (\neg A \wedge \neg B))$

(12) $(\neg(A \wedge B) \Leftrightarrow (\neg A \vee \neg B))$

(13) $((A \wedge \top) \Leftrightarrow A)$

(14) $((A \vee \bot) \Leftrightarrow A)$

(15) $((A \wedge \bot) \Leftrightarrow \bot)$

(16) $((A \vee \top) \Leftrightarrow \top)$

(17) $((A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A))$.

Estas tautologias reflectem propriedades importantes. Os números (1) e (2) exprimem a idempotência da conjunção e disjunção, (3) e (4) a comutatividade, (5) e (6) a associatividade, (7) e (8) a distributividade de cada um. Mas atenção! Tudo isso está a acontecer na equivalência lógica (ou seja, que estas propriedades são realmente propriedades de operações do conjunto $F/\sim$ de classes de equivalência para a relação $\sim$ em F), mas não só, uma vez que também está a acontecer na própria linguagem proposicional entre fórmulas com as operações lógicas $\wedge$, $\vee$ entre outras. Os números (11) e (12) exprimem as leis de De Morgan. A tautologia (13) (respectivamente, (14)) exprime a classe de tautologias 1 (respectivamente, a classe de antitautologias 0) é o elemento identidade para a conjunção (respectivamente, para a disjunção). O número (15) (respectivamente, número (16)) exprime que a classe 0 (respectivamente, a classe 1) é o elemento zero da conjunção (respectivamente, da disjunção). A fórmula $(\neg B \Rightarrow \neg A)$ é chamada de contrapositiva de $(A \Rightarrow B)$ e a tautologia número (17) exprime que toda a fórmula de implicação é logicamente equivalente à sua contrapositiva. Vamos dar ainda uma outra lista, agora com tautologias comuns adicionais:

(18) $(A \vee \neg A)$

(19) $(A \Rightarrow A)$

(20) $(A \Leftrightarrow A)$

(21) $(\neg\neg A \Rightarrow A)$

(22) $(A \Rightarrow (A \vee B))$

(23) $((A \wedge B) \Rightarrow A)$

(24) $(((A \Rightarrow B) \wedge A) \Rightarrow B)$

(25) $(((A \Rightarrow B) \wedge \neg B) \Rightarrow \neg A)$

(26) $((\neg A \Rightarrow A) \Rightarrow A)$

(27) $((\neg A \Rightarrow A) \Leftrightarrow A)$

(28) $(\neg A \Rightarrow (A \Rightarrow B))$

(29) $(A \vee (A \Rightarrow B))$

(30) $(A \Rightarrow (B \Rightarrow A))$

(31) $(((A \Rightarrow B) \wedge (B \Rightarrow C)) \Rightarrow (A \Rightarrow C))$

(32) $((A \Rightarrow B) \vee (C \Rightarrow A))$

(33) $((A \Rightarrow B) \vee (\neg A \Rightarrow B))$

(34) $((A \Rightarrow B) \vee (A \Rightarrow \neg B))$

(35) $((A \Rightarrow B) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \Rightarrow C)))$

(36) $(\neg A \Rightarrow (\neg B \Leftrightarrow (B \Rightarrow A)))$

(37) $((A \Rightarrow B) \Rightarrow (((A \Rightarrow C) \Rightarrow B) \Rightarrow B))$.

Além disso, na lista que se segue, fórmulas que estão na mesma linha são logicamente equivalentes duas a duas.

(38) $(A \Rightarrow B)$, $(\neg A \vee B)$, $(\neg B \Rightarrow \neg A)$, $((A \wedge B) \Leftrightarrow A)$, $((A \vee B) \Leftrightarrow B)$

(39) $\neg(A \Rightarrow B)$, $(A \wedge \neg B)$

(40) $(A \Leftrightarrow B)$, $((A \wedge B) \vee (\neg A \wedge \neg B))$, $(\neg A \vee B) \wedge (\neg B \vee A))$

(41) $(A \Leftrightarrow B)$, $((A \Rightarrow B) \wedge (B \Rightarrow A))$, $(\neg A \Leftrightarrow \neg B)$, $(B \Leftrightarrow A)$

(42) $(A \Leftrightarrow B)$, $((A \vee B) \Rightarrow (A \wedge B))$

(43) $\neg(A \Leftrightarrow B)$, $(A \Leftrightarrow \neg B)$, $(\neg A \Leftrightarrow B)$

(44) A, $\neg\neg A$, $(A \wedge A)$, $(A \vee A)$, $(A \vee (A \wedge B))$, $(A \wedge (A \vee B))$

(45) A, $(\neg A \Rightarrow A)$, $((A \Rightarrow B) \Rightarrow A)$, $((B \Rightarrow A) \wedge (\neg B \Rightarrow A))$

(46) A, $(A \wedge \top)$, $(A \vee \top)$, $(A \Leftrightarrow \top)$, $(\top \Rightarrow A)$

(47) $\neg A$, $(A \Rightarrow \neg A)$, $((A \Rightarrow B) \wedge (A \Rightarrow \neg B))$

(48) $\neg A$, $(A \Rightarrow \bot)$, $(A \Leftrightarrow \bot)$

(49) $\bot$, $(A \wedge \bot)$, $(A \Leftrightarrow \neg A)$

(50) $\top$, $(A \vee \top)$, $(A \Rightarrow \top)$, $(\bot \Rightarrow A)$

(51) $(A \wedge B)$, $(B \wedge A)$, $(A \wedge (\neg A \vee B))$, $\neg(A \Rightarrow \neg B)$

(52) $(A \vee B)$, $(B \vee A)$, $(A \vee (\neg A \wedge B))$, $(\neg A \Rightarrow B)$, $((A \Rightarrow B) \Rightarrow B)$

(53) $(A \Rightarrow (B \Rightarrow C))$, $((A \wedge B) \Rightarrow C)$, $(B \Rightarrow (A \Rightarrow C))$, $((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$

(54) $(A \Rightarrow (B \wedge C))$, $((A \Rightarrow B) \wedge (A \Rightarrow C))$

(55) $(A \Rightarrow (B \vee C))$, $((A \Rightarrow B) \vee (A \Rightarrow C))$

(56) $((A \wedge B) \Rightarrow C)$, $((A \Rightarrow C) \vee (B \Rightarrow C))$

(57) $((A \vee B) \Rightarrow C)$, $((A \Rightarrow C) \wedge (B \Rightarrow C))$

(58) $(A \Leftrightarrow (B \Leftrightarrow C))$, $((A \Leftrightarrow B) \Leftrightarrow C)$.

Deveríamos ter em conta, da linha (54) à (57), que a implicação não é distributiva em relação à conjunção nem em relação à disjunção. Vemos porém que é distributiva da esquerda ((54) e (55)), ou seja quando $\wedge$ e $\vee$ aparecem à direita de $\Rightarrow$. No caso em que um ou outro está localizado à esquerda de $\Rightarrow$, temos um tipo de distributividade artificial, o $\wedge$ (respectivamente, o $\vee$) é transformado em $\vee$ (respectivamente, em $\wedge$) após a sua "distributividade" ((56) e (57)). Isto alerta-nos para sermos vigilantes em todos os casos quando manipulamos este tipo de fórmula.

De agora em diante, admitiremos o seguinte abuso de notação:

- Em geral, quando escrevermos uma fórmula, permitir-nos-emos omitir os parênteses externos. Esta convenção supõe que esses parênteses reapareçam automaticamente quando esta fórmula aparecer como uma subfórmula de outra fórmula: por exemplo, aceitaremos a fórmula $F = A \Rightarrow B$ e a fórmula $F \wedge \neg C$, mas posteriormente será escrito obviamente como $(A \Rightarrow B) \wedge \neg C$ e não como $A \Rightarrow B \wedge \neg C$.
- Para todas as fórmulas F, G, e H,

  - a fórmula $((F \wedge G) \wedge H)$ será escrita como $(F \wedge G \wedge H)$,

  - a fórmula $((F \vee G) \vee H)$ será escrita como $(F \vee G \vee H)$.

Também podemos, aplicando a convenção prévia relativa à omissão de parênteses, escrever $F \wedge G \wedge H$ ou $F \vee G \vee H$.

- Geralmente para qualquer número natural *k*, não nulo, se F_1, F_2, ..., F_k são fórmulas, representaremos a fórmula

$$((\ldots (F_1 \wedge F_2) \wedge F_3) \wedge \ldots \wedge F_k)$$

por

$$F_1 \wedge F_2 \wedge \ldots \wedge F_k$$

(que começa com k - 1 ocorrências do símbolo de parêntese aberto). Claro que fazemos a convenção análoga para a disjunção.

- Se $I = \{i_1, i_2, \ldots, i_k\}$ é um conjunto finito, não vazio, de índices e se $F_{i_1}, F_{i_2}, \ldots, F_{i_k}$ são fórmulas, a fórmula $F_{i_1} \wedge F_{i_2} \wedge \ldots \wedge F_{i_k}$, também será escrita como:

$$\bigwedge_{j \in I} F_j$$

(para ser lida como "a conjunção dos F_j para j pertence a I").

Notamos que com esta notação, há uma ambiguidade relativa à ordem dos índices no conjunto I, que precisa de ser fixada para que esta maneira de escrita possa ter um significado. No entanto, a escolha desta ordem não tem nenhuma importância pelo facto da conjunção ser comutativa e associativa.

Da mesma forma, a fórmula $F_{i_1} \vee F_{i_2} \vee \ldots \vee F_{i_k}$ será abreviada:

$$\bigvee_{j \in I} F_j$$

(para ser lida como "a disjunção dos F_j para j pertence a I").

Naturalmente, também teremos variantes, como $\bigvee_{1 \le k \le n} G_k$ ou $\bigwedge_{F \in X} F$ (onde X é um conjunto finito, não vazio, de fórmulas), cujo significado é claro.

Relativamente à supressão dos parênteses baseamo-nos na associatividade da conjunção e da disjunção (números (5) e (6) da Secção 1.2.3), obtendo então uma fórmula da mesma classe de equivalência.

1.3 Formas normais e conjuntos completos de conectivos

1.3.1 Operações em {0,1} e fórmulas

Suporemos que o conjunto P de variáveis proposicionais é um conjunto finito de n elementos:

$$P = \{A_1, A_2, \ldots, A_n\}.$$

Isto permite-nos considerar que toda a fórmula F ∈ *F* tem as suas variáveis entre $A_1, A_2, ..., A_n$ e escrever $F = F[A_1, A_2, ..., A_n]$.

Consideremos então a seguinte notação:

- Para todo o *n*-uplo ordenado $(\varepsilon_1, \varepsilon_2, ..., \varepsilon_n) \in \{0,1\}^n$, $\delta_{\varepsilon_1,\varepsilon_2,...,\varepsilon_n}$ representa a distribuição de valores lógicos definidos por $\delta_{\varepsilon_1,\varepsilon_2,...,\varepsilon_n}(A_i) = \varepsilon_i$ para cada $i \in \{1, 2, ..., n\}$.
- Para cada variável proposicional A e para cada elemento $\varepsilon \in \{0,1\}$ representamos por εA a fórmula que é igual a A se $\varepsilon = 1$, e por $\neg A$ se $\varepsilon = 0$.

Para cada fórmula F, representamos por **Δ(F)** o **conjunto de distribuições** de valores lógicos que satisfazem F:

$$\Delta(F) = \{\delta \in \{0,1\}^P : \overline{\delta}(F) = 1\}.$$

Para cada fórmula F, definimos uma aplicação φ_F de $\{0,1\}^P$ para $\{0,1\}$ por

$$\varphi_F(\varepsilon_1, \varepsilon_2, ..., \varepsilon_n) = \overline{\delta_{\varepsilon_1, \varepsilon_2, ..., \varepsilon_n}}(F).$$

A aplicação φ_F não é mais do que a aplicação definida pela tabela de verdade de F. Por um abuso de linguagem dizemos que φ_F é a tabela de verdade de F.

Note-se ainda que duas fórmulas F e G são logicamente equivalentes ($F \sim G$) se e só se $\varphi_F = \varphi_G$, ou seja, a aplicação de $F \mapsto \varphi_F$ (de *F* para $\{0,1\}^{(\{0,1\}^n)}$) é compatível com a relação ~. Vemos também que esta aplicação não é injectiva (por exemplo, para qualquer fórmula F, temos que: $\varphi_{\neg\neg F} = \varphi_F$, ou seja, a dois objectos diferentes corresponde a mesma imagem), mas que a aplicação induzida, de $F/\sim$ em $\{0,1\}^{(\{0,1\}^n)}$ (a aplicação $cl(F) \mapsto \varphi_F$) é injectiva (note-se que cl(F) representa a classe de equivalência da fórmula F da relação de equivalência ~). Isto mostra que o número de classes de equivalência para a relação ~ em *F* é no máximo igual ao número de aplicações de $\{0,1\}^n$ em $\{0,1\}$, ou seja 2^{2^n}.

⍰ Será a aplicação de $F \mapsto \varphi_F$ sobrejectiva? Poderá a tabela de uma aplicação arbitrária de $\{0,1\}^n$ em $\{0,1\}$ ser vista como a tabela de verdade de alguma fórmula?

A resposta é afirmativa, tal como veremos no Lema seguinte.

Lema 1.22 Para qualquer *n*-uplo ordenado $(\varepsilon_1, \varepsilon_2, ..., \varepsilon_n) \in \{0,1\}^n$, a fórmula

$$\bigwedge_{1 \le k \le n} \varepsilon_k A_k$$

é satisfeita pela distribuição de valores lógicos $\delta_{\varepsilon_1,\varepsilon_2,...,\varepsilon_n}$ e por nenhuma outra.

Na nossa notação, isto seria escrito: $\Delta(\bigwedge_{1\le k\le n} \varepsilon_k A_k) = \{\delta_{\varepsilon_1,\varepsilon_2,...,\varepsilon_n}\}$.

Demonstração: Para demonstrar este teorema consideremos que, para qualquer distribuição de valores lógicos λ, temos que $\bar{\lambda}(\wedge_{1\le k\le n}\varepsilon_k A_k) = 1$ se e só se para todo $k \in \{1, ..., n\}$, $\bar{\lambda}(\varepsilon_k A_k) = 1$, o que, que preserva a definição de $\delta_{\varepsilon_1,\varepsilon_2,...,\varepsilon_n}$, é equivalente a:

$$\text{para todo } k \in \{1, ..., n\},\ \lambda(A_k) = \delta_{\varepsilon_1,\varepsilon_2,...,\varepsilon_n}(A_k),$$

por outras palavras, para $\lambda = \delta_{\varepsilon_1,\varepsilon_2,...,\varepsilon_n}$.

Lema 1.23 Seja X um subconjunto não vazio de $\{0,1\}^n$ e seja F_X a fórmula

$$\bigvee_{(\varepsilon_1,\varepsilon_2,...,\varepsilon_n)\in X} \left(\bigwedge_{1\le i\le n} \varepsilon_i A_i\right).$$

Então a fórmula F_X é satisfeita por estas distribuições de valores lógicos $\delta_{\varepsilon_1,\varepsilon_2,...,\varepsilon_n}$ para as quais $(\varepsilon_1, \varepsilon_2, ..., \varepsilon_n) \in X$ e apenas por estas.

Na nossa notação, isto seria escrito como:

$$\Delta(\bigvee_{(\varepsilon_1,\varepsilon_2,...,\varepsilon_n)\in X} (\bigwedge_{1\le i\le n} \varepsilon_i A_i)) = \{\delta_{\varepsilon_1,\varepsilon_2,...,\varepsilon_n} : (\varepsilon_1, \varepsilon_2, ..., \varepsilon_n) \in X\}.$$

Demonstração: Para qualquer distribuição de valores lógicos λ, temos que $\lambda(F_X) = 1$ se e só se existe um *n*-uplo $(\varepsilon_1, \varepsilon_2, ..., \varepsilon_n) \in X$ tal que $\bar{\lambda}(\wedge_{1\le i\le n}\varepsilon_i A_i) = 1$, o que é equivalente a: existe um *n*-uplo $(\varepsilon_1, \varepsilon_2, ..., \varepsilon_n) \in X$ tal que $\lambda = \delta_{\varepsilon_1,\varepsilon_2,...,\varepsilon_n}$, ou equivalente a,

$$\lambda \in \{\delta_{\varepsilon_1,\varepsilon_2,...,\varepsilon_n} : (\varepsilon_1, \varepsilon_2, ..., \varepsilon_n) \in X\}.$$

Teorema 1.24 Para qualquer aplicação φ de $\{0,1\}^n$ em $\{0,1\}$, existe pelo menos uma fórmula F tal que $\varphi_F = \varphi$.

Por outras palavras, toda a aplicação de $\{0,1\}^n$ em $\{0,1\}$ é uma tabela de verdade.

Demonstração: Fixemos uma aplicação φ de $\{0,1\}^n$ em $\{0,1\}$.

- Se assume apenas o valor 0, então é uma tabela de verdade, por exemplo, da fórmula $F = (A_1 \wedge \neg A_1)$.
- No caso oposto, o conjunto

$$X = \varphi^{-1}(\{1\}) = \{(\varepsilon_1, \varepsilon_2, ..., \varepsilon_n) \in \{0,1\}^n : \varphi(\varepsilon_1, \varepsilon_2, ..., \varepsilon_n) = 1\}$$

é não vazio e a fórmula

$$F_X = \bigvee_{(\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_n)\in X} \left(\bigwedge_{1\le i\le n} \varepsilon_i A_i \right)$$

é satisfeita por estas distribuições de valores lógicos $\delta_{\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_n}$ para as quais $\varphi(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n) = 1$ e apenas para estas.

Por outras palavras, para cada *n*-uplo $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n) \in \{0,1\}^n$, temos que

$$\overline{\delta_{\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_n}}(F) = 1 \text{ se e só se } \varphi(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n) = 1.$$

Isto significa que φ é a função φ_{F_X}, a tabela de verdade da fórmula F.

Vemos então que há 2^{2^n} classes de equivalência de fórmulas no conjunto de *n* variáveis proposicionais, correspondentes às 2^{2^n} possíveis tabelas de verdade.

Aplicações de $\{0,1\}^n$ em $\{0,1\}$ são às vezes chamadas de ***n*-ários conectivos proposicionais**. Veremos que é inofensivo identificar tal como um objecto com a classe de fórmulas que são naturalmente associadas a estas.

As tabelas seguintes, figuras 4 e 5, representam todos os conectivos proposicionais unários e binários (de φ_1 até φ_{16} e de Ψ_1 até Ψ_4). As primeiras colunas dão os valores de cada aplicação de cada ponto de $\{0,1\}^2$ ou de $\{0,1\}$. A coluna que se segue dá uma fórmula que pertence à classe de equivalência correspondente. Finalmente, a última coluna exibe o símbolo usado em comum, se algum representa o conectivo ou seu nome habitual.

Values of φ_i					Example of a formula whose truth table is φ_i	Usual denotation for φ_i	
ϵ_1	0	0	1	1			
ϵ_2	0	1	0	1		Symbol	Name
$\varphi_1(\epsilon_1, \epsilon_2)$	0	0	0	0	$(A_1 \wedge \neg A_1)$	0	FALSE
$\varphi_2(\epsilon_1, \epsilon_2)$	0	0	0	1	$(A_1 \wedge A_2)$	$\wedge$	AND
$\varphi_3(\epsilon_1, \epsilon_2)$	0	0	1	0	$\neg(A_1 \Rightarrow A_2)$	$\not\Rightarrow$	DOES NOT IMPLY
$\varphi_4(\epsilon_1, \epsilon_2)$	0	0	1	1	A_1		
$\varphi_5(\epsilon_1, \epsilon_2)$	0	1	0	0	$\neg(A_2 \Rightarrow A_1)$	$\not\Leftarrow$	
$\varphi_6(\epsilon_1, \epsilon_2)$	0	1	0	1	A_2		
$\varphi_7(\epsilon_1, \epsilon_2)$	0	1	1	0	$\neg(A_1 \Leftrightarrow A_2)$	$\not\Leftrightarrow$	NOT EQUIVALENT
$\varphi_8(\epsilon_1, \epsilon_2)$	0	1	1	1	$(A_1 \vee A_2)$	$\vee$	OR
$\varphi_9(\epsilon_1, \epsilon_2)$	1	0	0	0	$\neg(A_1 \vee A_2)$	$\downarrow$	SHEFFER'S 'OR'
$\varphi_{10}(\epsilon_1, \epsilon_2)$	1	0	0	1	$(A_1 \Leftrightarrow A_2)$	$\Leftrightarrow$	IS EQUIVALENT TO
$\varphi_{11}(\epsilon_1, \epsilon_2)$	1	0	1	0	$\neg A_2$		
$\varphi_{12}(\epsilon_1, \epsilon_2)$	1	0	1	1	$(A_2 \Rightarrow A_1)$	$\Leftarrow$	
$\varphi_{13}(\epsilon_1, \epsilon_2)$	1	1	0	0	$\neg A_1$		
$\varphi_{14}(\epsilon_1, \epsilon_2)$	1	1	0	1	$(A_1 \Rightarrow A_2)$	$\Rightarrow$	IMPLIES
$\varphi_{15}(\epsilon_1, \epsilon_2)$	1	1	1	0	$\neg(A_1 \wedge A_2)$	$\uparrow$	SHEFFER'S 'AND'
$\varphi_{16}(\epsilon_1, \epsilon_2)$	1	1	1	1	$(A_1 \vee \neg A_1)$	1	TRUE

Fig. 4: Tabela de conectivos proposicionais binários

(adaptada de Cori & Lascar (2000: 37)

Values of ψ_i			Example of a formula whose truth table is ψ_i	Usual designation of ψ_i
ϵ_1	**0**	**1**		
$\psi_1(\epsilon_1)$	**0**	**0**	$(A_1 \wedge \neg A_1)$	**0** (FALSE)
$\psi_2(\epsilon_1)$	**0**	**1**	A_1	IDENTITY
$\psi_3(\epsilon_1)$	**1**	**0**	$\neg A_1$	$\neg$ (NOT)
$\psi_4(\epsilon_1)$	**1**	**1**	$(A_1 \vee \neg A_1)$	**1** (TRUE)

Fig. 5: Tabela de conectivos proposicionais unários

(adaptada de Cori & Lascar (2000: 37)

1.3.2 Formas normais

Consideremos agora algumas definições:

Definição 1.25

(1) Uma fórmula F está na **forma normal disjuntiva** (**DNF**) se e só se

(a) existe um inteiro $m \geq 1$,

(b) existem inteiros $k_1, k_2, ..., k_n \geq 1$,

(c) para todo $i \in \{1, 2, ..., m\}$, existem k_i variáveis proposicionais $B_{il}, B_{i2}, ..., B_{ik_i}$ e k_i elementos $\varepsilon_{i1}, \varepsilon_{i2}, ..., \varepsilon_{ik_i}$ em $\{0,1\}$, tais que

$$F = \bigvee_{1 \leq i \leq m} \left(\varepsilon_{i1} B_{i1} \wedge \varepsilon_{i2} B_{i2} \wedge ... \wedge \varepsilon_{ik_i} B_{ik_i} \right).$$

(2) Uma fórmula F está na **forma normal disjuntiva canónica** (**CDNF**) se e só se existe um subconjunto não vazio X de $\{0,1\}^n$ tal que

$$F = \bigvee_{(\varepsilon_1, \varepsilon_2, ..., \varepsilon_n) \in X} \left(\bigwedge_{1 \leq i \leq n} \varepsilon_i A_i \right).$$

(3) Trocando os símbolos para a disjunção e a conjunção nas partes (1) e (2), obtemos respectivamente as definições de uma fórmula que está na **forma normal conjuntiva** (**CNF**) e uma fórmula que está na **forma normal conjuntiva canónica** (**CCNF**).

Podemos ver que, quando uma fórmula está na forma normal disjuntiva canónica, é um caso especial da forma normal disjuntiva (o caso onde cada k_i é igual a n, onde para cada $i \in \{1, 2, ..., n\}$ e $j \in \{1, 2, ..., m\}$, $B_{ij} = A_j$ e onde *os* m e n-uplos ordenados $\varepsilon_{i1}, \varepsilon_{i2}, ..., \varepsilon_{ik_i}$ são distintos dois a dois; note-se que isto força m a ser no máximo igual a 2^n).

Além disso observamos que, dada uma aplicação φ de $\{0,1\}^n$ em $\{0,1\}$ distinta da aplicação zero, existe uma fórmula F na forma normal disjuntiva canónica tal que $\varphi_F = \varphi$. (A fórmula F_X que temos considerado está certamente na forma normal disjuntiva canónica.) Como tal, podemos concluir um tipo de unicidade para formas normais disjuntivas (ou conjuntivas) canónicas, no sentido em que duas formas normais disjuntivas (ou conjuntivas) canónicas são logicamente equivalentes se diferirem apenas na "ordem dos factores". Mais precisamente, se as fórmulas:

$$\bigvee_{(\varepsilon_1,\varepsilon_2,...,\varepsilon_n)\in X} \left(\bigwedge_{1\le i\le n} \varepsilon_i A_i \right) \text{ e } \bigvee_{(\eta_1,\eta_2,...,\eta_n)\in Y} \left(\bigwedge_{1\le i\le n} \eta_i A_i \right)$$

são logicamente equivalentes, então os subconjuntos X e Y de $\{0,1\}^n$ são idênticos. O facto análogo para formas normais conjuntivas é obviamente verdadeiro.

Estas observações conduzem-nos ao seguinte teorema da forma normal:

Teorema 1.26 Toda a fórmula é logicamente equivalente a pelo menos uma fórmula na forma normal disjuntiva e a pelo menos uma fórmula na forma normal conjuntiva. Qualquer fórmula que não pertença à classe 0 é logicamente equivalente a uma única fórmula na forma normal disjuntiva canónica; toda a fórmula que não pertença à classe 1 é logicamente equivalente a uma única fórmula na forma normal conjuntiva canónica, onde a unicidade é entendida como sendo a menos da ordem dos factores.

Demonstração: Para demonstrar o teorema comecemos por considerar uma fórmula F.

- Se F é uma tautologia, é logicamente equivalente a $A_1 \vee \neg A_1$, que são ambas formas normais disjuntivas e formas normais conjuntivas.
- Se $\neg$F é uma tautologia, F é logicamente equivalente a $A_1 \wedge \neg A_1$, que é uma forma normal disjuntiva e uma forma normal conjuntiva.
- Nos outros casos, observamos que F é logicamente equivalente a uma fórmula na forma normal disjuntiva canónica. Mas isto também é verdade para $\neg$F, o que quer dizer que existe um subconjunto não vazio X de $\{0,1\}^n$ tal que

$$\neg F \quad \sim \quad \bigvee_{(\varepsilon_1,\varepsilon_2,...,\varepsilon_n)\in X} \left(\bigwedge_{1\le i\le n} \varepsilon_i A_i \right).$$

Além disso temos também que

$$\begin{aligned} F &\sim \neg\neg F \\ &\sim \neg\left(\bigvee_{(\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_n)\in X}\left(\bigwedge_{1\le i\le n}\varepsilon_i A_i\right)\right) \\ &\sim \left(\bigwedge_{(\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_n)\in X}\left(\bigvee_{1\le i\le n}\neg\varepsilon_i A_i\right)\right) \end{aligned}$$

pelas leis de De Morgan. Na última fórmula, se retirarmos a dupla negação, fica na forma normal conjuntiva canónica.

A segunda parte do teorema segue-se da primeira e das notas anteriores.

Podemos então falar da "CDNF" (forma normal disjuntiva canónica) de uma fórmula (contanto que não é uma antologia) e da "CCNF" (forma normal conjuntiva canónica) de uma fórmula (contanto que não é uma tautologia).

O teorema da forma normal também nos fornece um método prático para obter a CDNF e a CCNF de uma fórmula (quando elas existem), pois saibamos a sua tabela de verdade. Assim, por exemplo, a fórmula

$$G = (A \Rightarrow (((B \wedge \neg A) \vee (\neg C \wedge A)) \Leftrightarrow (A \vee (A \Rightarrow \neg B)))),$$

cuja tabela de verdade, apresentada na página 36, é satisfeita pelas distribuições

(0, 0, 0), (0, 0, 1), (0, 1, 0), (0, 1, 1), (1, 0, 0), e (1, 1, 0)

enquanto $\neg G$ é satisfeita apenas pelas distribuições (1, 0, 1) e (1, 1, 1). Daqui concluímos que a forma CDNF de G é

$$(\neg A \wedge \neg B \wedge \neg C) \vee (\neg A \wedge \neg B \wedge C) \vee (\neg A \wedge B \wedge \neg C) \vee (\neg A \wedge B \wedge C) \vee$$
$$\vee (A \wedge \neg B \wedge \neg C) \vee (A \wedge B \wedge \neg C),$$

e a forma CDNF de $\neg G$ é

$$(A \wedge \neg B \wedge C) \vee (A \wedge B \wedge C),$$

e finalmente, a forma CCNF de G é

$$(\neg A \vee B \vee \neg C) \wedge (\neg A \vee \neg B \vee \neg C).$$

Note-se que deveríamos mencionar que as fórmulas do tipo $\varepsilon_i A_i$ são por vezes chamadas de literais, estas fórmulas do tipo $\bigvee_{k\in J}\eta_k B_k$ (ou seja, disjunções de literais) são chamadas frequentemente **cláusulas** e aquelas formas normais conjuntivas (CNF) são chamadas **formas clausuais**.

1.3.3 Conjuntos completos de conectivos

Numa fórmula que está na forma normal disjuntiva (DNF), os únicos símbolos que podem aparecer para conectivos são: $\neg$, $\wedge$ e $\vee$. Então podemos concluir, pelo que já foi dito atrás, que toda a fórmula na forma normal disjuntiva é equivalente a pelo menos uma fórmula contendo apenas estes conectivos.

Esta propriedade pode ser redeclarada em termos de conectivos proposicionais, ou seja, em termos de operações em $\{0,1\}$. Segue-se então o seguinte lema:

Lema 1.27 Para todo o inteiro $m \geq 1$, toda a aplicação de $\{0,1\}^m$ em $\{0,1\}$ pode ser obtida por composição das aplicações $\neg$ (de $\{0,1\}$ em $\{0,1\}$), juntamente com $\wedge$ e $\vee$ (de $\{0,1\}^2$ em $\{0,1\}$).

Demonstração: Para demonstrar o lema, consideremos m um número natural não nulo e φ uma aplicação de $\{0,1\}^m$ em $\{0,1\}$. Escolhamos uma fórmula F que tenha φ como tabela de verdade e que seja escrita apenas com os símbolos para conectivos $\neg$, $\wedge$, $\vee$ (por exemplo uma fórmula em DNF). A decomposição em árvore da fórmula F dá-nos então uma composição de aplicações, tomando apenas as aplicações $\neg$, $\wedge$, $\vee$ que coincidem com a função φ. Sem entrar em muitos detalhes consideremos apenas um exemplo.

A aplicação φ de $\{0,1\}^3$ em $\{0,1\}$ que assume o valor 0 para (1, 0, 1) e (1, 1, 1) e o valor 1 para os restantes seis triplos é a tabela de verdade da fórmula

$$(\neg A \vee B \vee \neg C) \wedge (\neg A \vee \neg B \vee \neg C).$$

(Escolhemos uma fórmula na forma normal conjuntiva canónica (CCNF) porque é mais pequena e é também escrita usando apenas os símbolos $\neg$, $\wedge$, $\vee$).

A forma correcta de escrever esta fórmula é

$$(((\neg A \vee B) \vee \neg C) \wedge ((\neg A \vee \neg B) \vee \neg C)).$$

Concluímos que para quaisquer elementos x, y e z de $\{0,1\}$, temos que

$$\varphi(x, y, z) = \wedge(\vee(\vee(\neg x, y), \neg z), \vee(\vee(\neg x, \neg y), \neg z)).$$

(Nesta expressão os símbolos $\neg$, $\wedge$, $\vee$ representam operações em $\{0,1\}$).

Vemos que as operações $\neg$, $\wedge$, $\vee$ geram todas as possíveis operações em $\{0,1\}$.

Traduzimos a propriedade exibida dizendo que $\{\neg, \wedge, \vee\}$ é um conjunto completo de conectivos.

Definição 1.28 Um conjunto de conectivos define-se como **completo** se gera, através de composições, o conjunto de todos os conectivos proposicionais. Um conjunto completo de conectivos define-se como **minimal** quando nenhum subconjunto formal é um conjunto completo de conectivos.

O conjunto $\{\neg, \wedge, \vee\}$ não é um conjunto minimal completo. De facto, para toda a fórmula F que não possui outros conectivos para além de $\neg$, $\wedge$ e $\vee$ podemos associar uma fórmula logicamente equivalente que envolve apenas os símbolos para conectivos $\neg$ e $\vee$: basta substituir, para cada subfórmula de F da forma $(H \wedge K)$, a fórmula logicamente equivalente $\neg(\neg H \vee \neg K)$, repetindo a operação tantas vezes quantas as necessárias para eliminar todos os $\wedge$. Isto mostra que $\{\neg, \vee\}$ é um conjunto completo de conectivos que é um subconjunto formal de $\{\neg, \wedge, \vee\}$, logo o conjunto $\{\neg, \wedge, \vee\}$ não é um conjunto minimal completo, pela definição 1.28.

O conjunto $\{\neg, \vee\}$ é um conjunto minimal completo. Para ter a certeza, basta mostrar que $\{\neg\}$ e $\{\vee\}$ não são conjuntos completos.

Fórmulas nas quais não aparece outro símbolo para um conectivo diferente de $\neg$ são fórmulas do tipo $\neg\neg...\neg A$ (ou seja, uma variável proposicional precedida por um número finito, também possível zero, de ocorrências do símbolo $\neg$). Uma fórmula deste tipo ou é logicamente equivalente a A ou a $\neg A$, e é claro que há fórmulas, por exemplo $(A \vee B)$, que não são logicamente equivalentes a qualquer fórmula deste tipo. Então $\{\neg\}$ não é completo. Quanto ao conjunto $\{\vee\}$, note-se que uma fórmula na qual o único símbolo para um conectivo que aparece é $\vee$ é satisfeita pela distribuição de valores de verdade δ_1 definida por $\delta_1(X) = 1$ para toda a variável proposicional X. Podemos concluir que a fórmula $\neg A_1$, que toma o valor 0 para δ_1, não pode ser logicamente equivalente a qualquer fórmula que contenha apenas $\vee$ como símbolo para um conectivo. Então $\{\vee\}$ não é completo.

Suponhamos que queremos mostrar, por indução, que uma certa propriedade X(F) é verdadeira para toda a fórmula $F \in F$, e suponhamos que esta propriedade é compatível com a relação $\sim$ (ou seja, que qualquer fórmula que seja logicamente equivalente a uma fórmula com a propriedade X também tem essa propriedade).

Podemos explorar o facto de que $\{\neg, \vee\}$ é um conjunto completo. Assim, se provarmos que X(F) é verdadeira quando F é um elemento de P, e que, sempre que X(F) e X(G) sejam verdadeiras, então $X(\neg F)$ e $X((F \vee G))$ também sejam verdadeiras, estará garantido que a propriedade X é verdadeira para todas as fórmulas nas quais apenas apareçam os símbolos para conectivos $\neg$ e $\vee$. Seja H uma fórmula arbitrária de F. Uma vez que $\{\neg, \vee\}$ é completo, H é logicamente equivalente a pelo menos uma fórmula K que pode ser escrita usando apenas estes conectivos. Então X(K) é verdadeira, e pois X seja compatível com $\sim$, X(H) é também verdadeira. Note-se que esta observação se aplica da mesma maneira a qualquer outro conjunto completo de conectivos.

1.4 Lema de Interpolação

1.4.1 Lema de interpolação

Lema 1.29 Sejam F e G duas fórmulas que não têm nenhuma variável proposicional em comum. Então as seguinte duas propriedades são equivalentes:

(1) a fórmula $(F \Rightarrow G)$ é uma tautologia;

(2) pelo menos uma das fórmulas $\neg F$ ou G é uma tautologia.

Demonstração: É claro que a segunda propriedade implica a primeira: para qualquer distribuição de valores lógicos δ, temos que $\delta(G) = 1$ se G é uma tautologia e $\delta(F) = 0$ se $\neg F$ é uma tautologia. Em ambos os casos $\delta((F \Rightarrow G)) = 1$.

Suponhamos agora que a propriedade (2) é falsa. Então podemos escolher uma distribuição de valores lógicos λ tal que $\lambda(\neg F) = 0$, ou seja que $\lambda(F) = 1$, e uma distribuição de valores lógicos μ tal que $\mu(G) = 0$. De seguida definamos uma distribuição de valores lógicos δ fixando, para cada variável proposicional X,

$$\delta(X) = \begin{cases} \lambda(X) & \text{se X aparece pelo menos uma vez em F;} \\ \mu(X) & \text{se X não aparece em F.} \end{cases}$$

Pois, por hipótese, qualquer variável que apareça em G não possa aparecer em F, vemos que δ coincide com λ no conjunto de variáveis de F e com μ no conjunto de variáveis de G. Concluímos que $\delta(F) = \lambda(F) = 1$ e que $\delta(G) = \mu(G) = 0$, e, consequentemente, que $\delta((F \Rightarrow G)) = 0$. Então a propriedade (1) falha.

O resultado seguinte é conhecido como lema de interpolação:

Teorema 1.30 Seja n um inteiro não nulo, A_1, A_2, ..., A_n variáveis proposicionais distintas duas a duas, e F e G duas fórmulas que tenham (no máximo) as variáveis proposicionais A_1, A_2, ..., A_n em comum. Então as duas propriedades seguintes são equivalentes:

(1) a fórmula $(F \Rightarrow G)$ é uma tautologia;

(2) existe pelo menos uma fórmula H, contendo apenas as variáveis proposicionais A_1, A_2, ..., A_n, tal que as fórmulas

$$(F \Rightarrow H) \text{ e } (H \Rightarrow G)$$

são tautologias.

Tal fórmula H é chamada um interpolante entre F e G.

Demonstração: Suponhamos que $\models (F \Rightarrow H)$ e que $\models (H \Rightarrow G)$ e consideremos uma distribuição arbitrária de valores lógicos δ. Se $\delta(H) = 0$, então $\delta(F) = 0$, porque $\delta((F \Rightarrow H)) = 1$; se $\delta(H) = 1$, então $\delta(G) = 1$, porque $\delta((H \Rightarrow G)) = 1$. Em ambos os casos, $\delta((F \Rightarrow G)) = 1$, o que prova a propriedade (1).

Para mostrar a implicação contrária, suporemos que $\models (F \Rightarrow G)$ e argumentaremos por indução sobre o número de variáveis proposicionais que apareçam pelo menos uma vez em F mas que não apareçam em G.

- Se este número for zero, então fixando H = F obtemos claramente uma fórmula que não contenha outras variáveis proposicionais para além de A_1, A_2, ..., A_n e tal que $\models (F \Rightarrow H)$ e $\models (H \Rightarrow G)$.
- Suponhamos, hipótese de indução, que a propriedade (2) é verdadeira para as fórmulas F que contenham no máximo m variáveis que não apareçam em G e examinemos o caso em que há m+1 variáveis. Sejam B_1, B_2, ..., B_m, B_{m+1} as representantes das variáveis de F que não aparecem em G. Que preserva a nossa convenção, temos então que $F = F[A_1, A_2, ..., A_n, B_1, B_2, ..., B_m, B_{m+1}]$. Sejam

$$F_1 = F[A_1, A_2, ..., A_n, B_1, B_2, ..., B_m, A_1] = F_{A_1 / B_{m+1}}$$

$$F_0 = F[A_1, A_2, ..., A_n, B_1, B_2, ..., B_m, \neg A_1] = F_{\neg A_1 / B_{m+1}} .$$

Repare-se que por B_{m+1} não aparecer em G, o resultado da substituição da variável B_{m+1} pela fórmula A_1 na fórmula $(F \Rightarrow G)$ é a fórmula $(F_1 \Rightarrow G)$, e o resultado da substituição da variável B_{m+1} pela fórmula $\neg A_1$ na fórmula $(F \Rightarrow G)$ é a fórmula

($F_0 \Rightarrow G$). Por um corolário anterior (1.20) e por hipótese, concluímos que ($F_1 \Rightarrow G$) e ($F_0 \Rightarrow G$) são tautologias, tal como o são as fórmulas

$$((F_1 \Rightarrow G) \wedge (F_0 \Rightarrow G)) \text{ e } ((F_1 \vee F_0) \Rightarrow G)$$

(ver na secção 1.2.3 o número (57) da lista).

As variáveis na fórmula ($F_1 \vee F_0$) estão entre A_1, A_2, ..., A_n, B_1, B_2, ..., B_m. Então podemos usar a nossa hipótese de indução e encontrar uma fórmula H que seja um interpolante entre ($F_1 \vee F_0$) e G, ou seja que as suas variáveis estejam entre A_1, A_2, ..., A_n e tais que

$$\models ((F_1 \vee F_0) \Rightarrow H) \text{ e } \models (H \Rightarrow G).$$

Mostraremos que $\models (F \Rightarrow (F_1 \vee F_0))$. Conclui-se então a demonstração uma vez que $\models (F \Rightarrow H)$, o que faz com que H seja um interpolante entre F e G.

Seja então δ uma atribuição de valores lógicos que satisfaz F. Temos então que:

- ou $\delta(A_1) = \delta(B_{m+1})$, e neste caso $\delta(F_1) = \delta(F) = 1$,
- ou então $\delta(A_1) \neq \delta(B_{m+1})$, e então $\delta(F_0) = \delta(F) = 1$.

Em qualquer caso, $\delta((F_1 \vee F_0)) = 1$. E então $\models (F \Rightarrow (F_1 \vee F_0))$.

1.4.2 Teorema da definibilidade

Consideremos, agora, um corolário do lema de interpolação, o chamado teorema de definibilidade:

Teorema 1.31 Sejam A, B, A_1, A_2, ..., A_k variáveis proposicionais distintas duas a duas e seja $F = F[A, A_1, A_2, ..., A_k]$ uma fórmula (cujas variáveis estão entre A, A_1, A_2, ..., A_k). Assumimos que a fórmula

$$((F[A, A_1, A_2, ..., A_k] \wedge F[B, A_1, A_2, ..., A_k]) \Rightarrow (A \Leftrightarrow B))$$

é uma tautologia. Então existe uma fórmula $G = G[A_1, A_2, ..., A_k]$, cujas únicas variáveis estão entre A_1, A_2, ..., A_k e tais que a fórmula

$$(F[A, A_1, A_2, ..., A_k] \Rightarrow (A \Leftrightarrow G[A_1, A_2, ..., A_k]))$$

é uma tautologia.

Demonstração: Que preserva o que foi apresentado na secção 1.2.3, a hipótese do teorema conduz-nos às seguintes tautologias:

$\models ((F[A, A_1, A_2, ..., A_k] \wedge F[B, A_1, A_2, ..., A_k]) \Rightarrow (A \Rightarrow B))$,

$\models (((F[A, A_1, A_2, ..., A_k] \wedge F[B, A_1, A_2, ..., A_k]) \wedge A) \Rightarrow B)$,

$\models (((F[A, A_1, A_2, ..., A_k] \wedge A) \wedge F[B, A_1, A_2, ..., A_k]) \Rightarrow B)$,

$\models ((F[A, A_1, A_2, ..., A_k] \wedge A) \Rightarrow (F[B, A_1, A_2, ..., A_k] \Rightarrow B))$.

O lema de interpolação garante-nos a existência de um interpolante

$G[A_1, A_2, ..., A_k]$ entre $(F[A, A_1, A_2, ..., A_k] \wedge A)$ e $(F[B, A_1, A_2, ..., A_k]) \Rightarrow B)$. Então, em particular,

$$\models ((F[A, A_1, A_2, ..., A_k] \wedge A) \Rightarrow G)$$

e também

$$\models (F[A, A_1, A_2, ..., A_k] \Rightarrow (A \Rightarrow G)). \qquad (*)$$

Por outro lado,

$$\models (G \Rightarrow (F[B, A_1, A_2, ..., A_k] \Rightarrow B)),$$

e também

$$\models (G \wedge F[B, A_1, A_2, ..., A_k]) \Rightarrow B)$$

$$\models ((F[B, A_1, A_2, ..., A_k]) \wedge G) \Rightarrow B),$$

$$\models (F[B, A_1, A_2, ..., A_k] \Rightarrow (G \Rightarrow B)).$$

O resultado da substituição de B por A nesta última fórmula é novamente uma tautologia:

$$\models (F[A, A_1, A_2, ..., A_k] \Rightarrow (G \Rightarrow A)). \qquad (**)$$

As propriedades (*) e (**) juntamente com algumas tautologias da secção 1.2.3 dão-nos finalmente

$$\models (F[A, A_1, A_2, ..., A_k] \Rightarrow (A \Leftrightarrow G)).$$

Intuitivamente, a hipótese diz-nos que a fórmula $F[A, A_1, A_2, ..., A_k]$ determina o valor de A como uma função de valores de A_1, A_2, ..., A_k, no sentido de que distribuições de valores de verdade que satisfazem F e que assumam o mesmo valor para A_1, A_2, ..., A_k também têm de supor o mesmo valor para A; a conclusão é que o valor tomado por A é o valor tomado por uma certa fórmula $G[A_1, A_2, ..., A_k]$ que não depende de A e que pode ser chamado de "**definição de A módulo F**".

1.5 (Meta)Teorema da Compacidade

1.5.1 Satisfação de um conjunto de fórmulas

Definição 1.32 Sejam *A* e *B* dois conjuntos de fórmulas do cálculo proposicional no conjunto de variáveis proposicionais P, seja G uma fórmula e seja δ uma distribuição de valores lógicos em P.

- *A* é **satisfeito** por δ (ou δ **satisfaz** *A*) se e só se δ satisfaz todas as fórmulas pertencentes a *A*.

- *A* é **satisfazível** (ou **compatível**) se e só se existe pelo menos uma distribuição de valores lógicos que satisfaz *A*.

- *A* é **finitamente satisfazível** se e só se todo o subconjunto finito de *A* é satisfazível.

- *A* é **contraditório** ou **incompatível** se e só se não é satisfazível.

- G é uma **consequência** de *A* (o qual denotamos por: $A \models G$) se e só se toda a distribuição de valores de verdade que satisfazem *A* satisfaz G.
  (A notação para "G **não é uma consequência** de *A*" é: $A \not\models G$).

- *A* e *B* são **equivalentes** se e só se toda a fórmula de *A* é uma consequência de *B* e toda a fórmula de *B* é uma consequência de *A*.

Por exemplo, consideremos as variáveis proposicionais A, B, A_1, A_2, ..., A_m, ... distintas duas a duas: o conjunto $\{A, B, (\neg A \vee B)\}$ é satisfazível; $\{A, \neg B, (A \Rightarrow B)\}$ é contraditório; o conjunto vazio é satisfeito por qualquer distribuição de valores lógicos (se não fosse verdade, poderíamos encontrar uma distribuição de valores lógicos δ e uma fórmula $F \in \varnothing$ tal que $\delta(F) = 0$; mas tal facto é claramente impossível...). Assim, temos que

$$\{A, B\} \models (A \wedge B) \text{ e } \{A, (A \Rightarrow B)\} \models B.$$

Os conjuntos $\{A, B\}$ e $\{(A \wedge B)\}$ são equivalentes, tal como são os conjuntos

$$\{A_1, A_2, ..., A_m, ...\} \text{ e } \{A_1, A_1 \wedge A_2, ..., A_1 \wedge A_2 \wedge ... \wedge A_m, ...\}.$$

A partir destas definições podemos deduzir a seguinte lista de propriedades. Quase todas elas são consequências imediatas.

Lema 1.33 Para todos os conjuntos de fórmulas A e B, inteiros m e $p \geq 1$, e fórmulas G, H, F_1, F_2, ..., F_m e G_1, G_2, ..., G_p, verificam-se as seguintes propriedades:

- $A \models G$ (G é uma consequência de A) se e só se $A \cup \{\neg G\}$ é contraditório.

Demonstração:

Provemos a primeira implicação. Assim, suponhamos que $A \cup \{\neg G\}$ é satisfazível. Então, por definição, existe pelo menos uma distribuição de valores lógicos, δ, que satisfaz $A \cup \{\neg G\}$, ou seja, δ satisfaz A e δ satisfaz $\neg G$, logo não satisfaz G o que é impossível uma vez que por hipótese existe uma distribuição de valores lógicos que satisfaz A e satisfaz G. Concluímos então que se $A \models G$ então $A \cup \{\neg G\}$ é contraditório.

Para provarmos a implicação contrária tomemos a hipótese de $A \cup \{\neg G\}$ ser contraditório, então, por definição, não existe uma distribuição de valores lógicos que satisfaça $A \cup \{\neg G\}$, ou seja, não existe uma distribuição de valores lógicos que satisfaça simultaneamente A e $\neg G$. Então existe uma distribuição de valores lógicos que satisfaz A e que satisfaz G, ou seja, G é uma consequência de A ($A \models G$).

- Se A é satisfazível e se $B \subseteq A$, então B é satisfazível.

- Se A é satisfazível, então A é finitamente satisfazível.

- Se A é contraditório e se $A \subseteq B$, então B é contraditório.

- Se $A \models G$ e se $A \subseteq B$, então $B \models G$.

- $A \cup \{G\} \models H$ se e só se $A \models (G \Rightarrow H)$.

- $A \models (G \wedge H)$ se e só se $A \models G$ e $A \models H$.

- $\{F_1, F_2, ..., F_m\} \models G$ se e só se $\models ((F_1 \wedge F_2 \wedge ... \wedge F_m) \Rightarrow G)$.

- G é uma tautologia ($\models$ G) se e só se G é uma consequência do conjunto vazio ($\varnothing \models$ G).

Demonstração: $\models$ G se e só se $\varnothing \models$ G: porque o conjunto vazio é satisfeito por toda a distribuição de valores lógicos, G é uma consequência do conjunto vazio se e só se toda a distribuição de valores lógicos satisfaz G, por outras palavras: se e só se G é uma tautologia. Como resultado, observe-se que, a notação $\models$ G para "G é uma tautologia" aparece naturalmente.

- G é uma tautologia se e só se G é uma consequência de qualquer conjunto de fórmulas.

- *A* é contraditório se e só se $A \models (G \wedge \neg G)$.

- *A* é contraditório se e só se toda a fórmula é uma consequência de *A*.

- *A* é contraditório se e só se toda a antilogia é uma consequência de *A*.

- *A* é contraditório se e só se existe pelo menos uma antilogia que é uma consequência de *A*.

- $\{F_1, F_2, ..., F_m\}$ é contraditório se e só se $(\neg F_1 \vee \neg F_2 \vee ... \vee \neg F_m)$ é uma tautologia.

- *A* e *B* são equivalentes ($A \sim B$) se e só se são satisfeitos pelas mesmas tabelas de valores lógicos.

- Quando substituímos cada fórmula de *A* por uma fórmula logicamente equivalente, obtemos um conjunto que é equivalente a *A*.

- Se *A* é contraditório, então *B* é equivalente a *A* se e só se *B* é contraditório.

- *A* é equivalente ao conjunto vazio se e só se toda a fórmula pertencente a *A* for uma tautologia.

Demonstração: *A* é equivalente ao ∅ se e só se todo o elemento de *A* for uma tautologia: é claro, em primeiro lugar, que toda a fórmula que pertence ao ∅ é uma consequência de *A*, e isto verifica-se para qualquer conjunto *A* (caso contrário, existiria uma fórmula pertence ao ∅ que não seria uma consequência de *A*, o que é claramente impossível); assim o que temos de provar é que toda a fórmula de *A* é uma consequência do ∅ se e só se toda a fórmula de *A* for uma tautologia; mas esta é justamente a propriedade anterior.

- O conjunto vazio é satisfazível.

- O conjunto *F* de todas as fórmulas é contraditório.

- Os conjuntos {G} e {H} são equivalentes se e só se as fórmulas G e H são logicamente equivalentes.

- Os conjuntos $\{F_1, F_2, ..., F_m\}$ e $\{G_1, G_2, ..., G_p\}$ são equivalentes se e só se a fórmula $((F_1 \wedge F_2 \wedge ... \wedge F_m) \Leftrightarrow (G_1 \wedge G_2 \wedge ... \wedge G_p))$ é uma tautologia.

- Todo o conjunto finito de fórmulas é equivalente a um conjunto contendo apenas uma única fórmula.

- Quando o conjunto P é infinito, e apenas neste caso, existem conjuntos de fórmulas que não são equivalentes a nenhum conjunto finito de fórmulas.

Demonstração: P é infinito se e só se existe um conjunto de fórmulas que não são equivalentes a nenhum conjunto finito: se P é finito e tem *n* elementos, existem 2^{2^n} classes de fórmulas logicamente equivalentes; escolhamos um representante de cada classe. Podemos então, dado um conjunto arbitrário de fórmulas *X*, substituir cada fórmula de *X* pelo representante escolhido da sua classe de equivalência; o conjunto resultante é equivalente a *X* e é finito uma vez que pode conter no máximo 2^{2^n} elementos. Se P é infinito, consideremos o conjunto infinito de fórmulas $Y = \{A_1, A_2, ..., A_m, ...\}$ (onde os A_i são variáveis proposicionais distintas duas a duas); se *Y* for equivalente a um conjunto finito de fórmulas *Z*, então *Z* será satisfeito, tal como *Y*, pela distribuição constante $\delta_1 = 1$, e podemos escolher pelo menos um inteiro *k* tal que a

variável A_k não ocorra em nenhuma das fórmulas de *Z* (que é finito em número); então a distribuição λ que toma sempre o valor 1 excepto em A_k, onde o seu valor é 0, continua a satisfazer *Z* (pelo lema 1.17) mas que obviamente não satisfaz *Y*, gerando então uma contradição: temos então um conjunto *Y* que não é equivalente a nenhum conjunto de fórmulas.

- A relação binária "é equivalente a" é uma relação de equivalência no conjunto dos subconjuntos de *F*.

1.5.2 O (meta)teorema da compacidade para o cálculo proposicional

Consideremos, de seguida, algumas versões equivalentes do chamado Teorema da Compacidade. Assim, temos:

O (meta)Teorema da Compacidade, versão 1:
Teorema 1.34 Para qualquer conjunto *A* de fórmulas do cálculo proposicional, *A* é satisfazível se e só se *A* é finitamente satisfazível.

O (meta)Teorema da Compacidade, versão 2:
Teorema 1.35 Para qualquer conjunto *A* de fórmulas do cálculo proposicional, *A* é contraditório se e só se pelo menos um subconjunto finito de *A* é contraditório.
Demonstração: A demonstração deste teorema encontra-se mais adiante na página 83.

O (meta)Teorema da Compacidade, versão 3:
Teorema 1.36 Para qualquer conjunto *A* de fórmulas do cálculo proposicional e para qualquer fórmula F, F é uma consequência de *A* se e só se F é uma consequência de pelo menos um subconjunto finito de *A*.

Demonstração: A demonstração da equivalência destas três versões do teorema da Compacidade faz-se usando as propriedades elementares do lema 1.33. Observamos também que a implicação "$\Leftarrow$" da versão 1 e as implicações "$\Rightarrow$" das versões 2 e 3 são facilmente justificáveis.

Começaremos por provar a implicação "$\Rightarrow$", da versão 1.

Comecemos por ver uma primeira prova que é válida para o caso em que o conjunto de variáveis proposicionais, P, é infinito numerável:

$$P = \{A_0, A_1, A_2, ..., A_m, ...\}.$$

(Para o caso de P ser finito, o teorema é mais óbvio (existe apenas um número finito de classes de equivalência de fórmulas), no entanto podemos sempre invocar a situação da presente demonstração estendendo P a um conjunto numerável.)

Assim consideremos um conjunto *A* de fórmulas que são finitamente compatíveis. Temos de provar a existência de uma distribuição de valores lógicos que satisfaz todas as fórmulas de *A*. Para isto, definiremos, por indução, uma sucessão $(\varepsilon_n)_{n\in\mathbb{N}}$ de elementos de {0,1} tais que a distribuição de valores lógicos δ_0 definida por:

$$\text{para todo } n \in \mathbb{N}\ , \delta_0(A_n) = \varepsilon_n,$$

satisfaz *A*.

Para definir ε_0, consideramos dois casos:

- Caso 0_0: para todo o subconjunto finito $B \subset A$, existe pelo menos uma distribuição de valores lógicos $\delta \in \{0,1\}^P$ que satisfaz *B* e é tal que $\delta(A_0) = 0$.
  Neste caso, fixamos que $\varepsilon_0 = 0$.
- Caso 1_0: este é o caso contrário: podemos escolher um subconjunto finito $B_0 \subseteq A$ tal que, para toda a distribuição de valores lógicos $\delta \in \{0,1\}^P$ que satisfaz B_0, temos que $\delta(A_0) = 1$.
  Neste caso, fixamos que $\varepsilon_0 = 1$.

No caso de 1_0, podemos afirmar que:

Para todo o subconjunto finito $B \subseteq A$, existe pelo menos uma distribuição de valores lógicos $\delta \in \{0,1\}^P$ que satisfaz *B* e é tal que $\delta(A_0) = 1$.

Para ver isto, dado um subconjunto finito $B \subseteq A$, note-se que $B \cup B_0$ é um subconjunto finito de *A* que é compatível que preserva a hipótese inicial. Escolhamos uma distribuição de valores lógicos δ que o satisfaça. Então δ satisfaz B_0 (que é um subconjunto de $B \cup B_0$!), e, pela forma como foi escolhido B_0, temos que $\delta(A_0) = 1$. Mas uma vez que δ também satisfaz *B*, verifica-se a afirmação.

Assim, da nossa definição de ε_0, podemos concluir a seguinte propriedade (R_0):

(R_0)	Para todo o subconjunto finito $B \subseteq A$, existe pelo menos uma atribuição de valores lógicos $\delta \in \{0,1\}^P$ que satisfaz B e é tal que $\delta(A_0) = \varepsilon_0$.

Suponhamos (por hipótese de indução) que ε_0, ε_l, ..., ε_n (elementos de {0,1}) foram definido de tal modo que a seguinte propriedade (R_n) fosse satisfeita:

(R_n)	Para todo o subconjunto finito $B \subseteq A$, existe pelo menos uma atribuição de valores lógicos $\delta \in \{0,1\}^P$ que satisfaz B e é tal que $\delta(A_0) = \varepsilon_0$, $\delta(A_1) = \varepsilon_1$, ..., $\delta(A_{n-1}) = \varepsilon_{n-1}$, e $\delta(A_n) = \varepsilon_n$.

Definimos então ε_{n+1} considerando dois casos:

- Caso 0_{n+1}: Para todo o subconjunto finito $B \subseteq A$, existe pelo menos uma distribuição de valores lógicos $\delta \in \{0,1\}^P$ que satisfaz B e tal que $\delta(A_0) = \varepsilon_0$, $\delta(A_1) = \varepsilon_1$, ..., $\delta(A_n) = \varepsilon_n$, e $\delta(A_{n+1}) = 0$.
  Neste caso fixamos que $\varepsilon_{n+1} = 0$.

- Caso 1_{n+1}: este é o caso contrário: podemos escolher um subconjunto finito $B_{n+1} \subseteq A$ tal que, para toda a distribuição de valores lógicos $\delta \in \{0,1\}^P$ satisfaz B_{n+1} e que é tal que $\delta(A_0) = \varepsilon_0$, $\delta(A_1) = \varepsilon_1$, ..., $\delta(A_n) = \varepsilon_n$, temos que $\delta(A_{n+1}) = 1$.
  Neste caso, fixamos $\varepsilon_{n+1} = 1$.

Mostremos agora que a propriedade (R_{n+1}) é então satisfeita. Isto equivale a provar, para o caso 1_{n+1}, que para todo o subconjunto finito $B \subseteq A$, existe pelo menos uma distribuição de valores lógicos $\delta \in \{0,1\}^P$ que satisfaz B e tal que $\delta(A_0) = \varepsilon_0$, $\delta(A_1) = \varepsilon_1$, ..., $\delta(A_n) = \varepsilon_n$, e $\delta(A_{n+1}) = 1$.

Assim consideremos um subconjunto finito $B \subseteq A$. Então $B \cup B_{n+1}$ é um subconjunto finito de A; e, que preserva a propriedade (R_n), podemos escolher uma distribuição de valores lógicos δ que o satisfaça e tal que $\delta(A_0) = \varepsilon_0$, $\delta(A_1) = \varepsilon_1$, ..., $\delta(A_n) = \varepsilon_n$. Assim δ satisfaz B_{n+1} e, pelo modo como este conjunto foi escolhido,

podemos concluir que $\delta(A_{n+1}) = 1$. Uma vez que δ satisfaz *B*, concluímos a nossa demonstração.

A sucessão $(\varepsilon_n)_{n\in\mathbb{N}}$ foi assim definida; e, para todo o inteiro *n*, a propriedade (R_n) é satisfeita.

Como já fizemos, fixemos $\delta_0(A_n) = \varepsilon_n$ para todo o *n*.

Seja F uma fórmula de *A*, e seja *k* um número natural tal que todas as variáveis proposicionais que ocorrem em F então entre $\{A_1, A_2, ..., A_k\}$ (sendo F um "cordel" finito de símbolos, de tal forma que exista necessariamente um inteiro). A propriedade (R_k) e o facto de que {F} é um subconjunto finito de *A* mostra-nos que podemos encontrar uma distribuição de valores lógicos $\delta \in \{0,1\}^P$ que satisfaça F e tal que $\delta(A_0) = \varepsilon_0$, $\delta(A_1) = \varepsilon_1$, ..., $\delta(A_k) = \varepsilon_k$. Vemos que δ e δ_0 satisfazem os elementos do conjunto $\{A_1, A_2, ..., A_k\}$ o que nos permite concluir (pelo lema 1.17) que $\delta_0(F) = \delta(F) = 1$.

Concluímos que δ_0 satisfaz todas as fórmulas de *A*.

Provemos o teorema no caso geral: não faremos mais nenhuma suposição sobre o conjunto P.

Temos no entanto que invocar o lema de Zorn: Todo o conjunto não vazio, parcialmente ordenado e indutivo, tem elementos maximais.

Demonstração: Consideremos um conjunto de fórmulas finitamente compatível, *A*.

Tomemos ξ para representar o conjunto de aplicações cujo domínio é um subconjunto de P, que toma valores em {0,1} e que, para todo o subconjunto finito $B \subset A$, tenha uma extensão de todo o P, que é uma distribuição de valores lógicos que satisfaz *B*.

Formalmente:

$$\xi = \left\{ \varphi \in \bigcup_{X\subseteq P} \{0,1\}^X : (\forall B \in \wp_F(A))(\exists \delta \in \{0,1\}^P)(\delta \mid X = \varphi \text{ e } (\forall F \in B)(\delta(F) = 1)) \right\}$$

Note-se que este conjunto é não vazio, porque contém a aplicação vazia. Podemos ver isto, uma vez que, por hipótese, existe uma distribuição de valores lógicos δ em P que satisfaz *B*. Como δ é obviamente uma extensão da aplicação vazia, segue-se que satisfaz a condição para os elementos de ξ.

Observa-se que este é o único ponto na demonstração onde se usa a hipótese de que *A* é finitamente compatível.

Definamos a relação binária $\leq$ em ξ por

$$\varphi \leq \psi \text{ se e só se } \psi \text{ é uma extensão de } \varphi$$

(por outras palavras, $\mathrm{dom}(\varphi) \subseteq \mathrm{dom}(\psi)$ e para todo o $A \in \mathrm{dom}(\varphi)$, $\varphi(A) = \psi(A)$).

Facilmente se prova que $\leq$ é uma relação de ordem em ξ.

Provaremos que o conjunto ordenado $(\xi, \leq)$ é indutivo, ou seja que todo o subconjunto de ξ que é totalmente ordenado por $\leq$ tem um ínfimo em ξ. Isto é o mesmo que mostrar que ξ é não vazio e que todo o subconjunto não vazio de ξ que é totalmente ordenado por $\leq$ tem um ínfimo em ξ. Isto permite-nos (pelo lema de Zorn) afirmar a existência de um elemento maximal em ξ para a ordem $\leq$.

Já observamos que ξ é não vazio. Consideremos um subconjunto não vazio $C \subseteq \xi$ que é totalmente ordenado por $\leq$. Definimos uma aplicação λ, como se segue:

- O domínio de λ é a união dos domínios dos elementos de C.
- Para todo o $A \in \mathrm{dom}(\lambda)$ e para todo o $\varphi \in C$, se $A \in \mathrm{dom}(\varphi)$, então $\lambda(A) = \varphi(A)$.

Esta definição faz sentido porque, se φ e ψ são elementos de ξ tais que $A \in \mathrm{dom}(\varphi)$ e $A \in \mathrm{dom}(\psi)$, então ou temos $\varphi \leq \psi$ ou $\psi \leq \varphi$, e em ambos os casos $\varphi(A) = \psi(A)$; assim o valor da aplicação λ no ponto A pode ser legitimamente definido como o valor em A tomado por uma aplicação arbitrária que pertence ao subconjunto C e é definido em A; assim λ é a extensão comum natural de todos os elementos de C.

Vamos mostrar que λ é um elemento de ξ. Para isto, dado um subconjunto finito $B \subseteq A$, temos de encontrar uma distribuição de valores lógicos $\mu \in \{0,1\}^{\mathrm{P}}$ que é uma extensão de λ e a qual satisfaz *B*. Uma vez que *B* é finito, existe no máximo um número finito de variáveis proposicionais que aparecem nas fórmulas de *B*.

Sejam $A_1, A_2, \ldots, A_n$ as variáveis proposicionais que ocorrem em pelo menos uma fórmula de *B* e que pertencem ao domínio de λ, ou seja, à união dos domínios dos elementos de C. Então existem em C elementos $\varphi_1, \varphi_2, \ldots, \varphi_n$ tais que $A_1 \in \mathrm{dom}(\varphi_1)$, $A_2 \in \mathrm{dom}(\varphi_2)$, ..., $A_n \in \mathrm{dom}(\varphi_n)$. Porque C é totalmente ordenado por $\leq$, um dos φ_i é uma extensão de todos os outros: chame-se φ_0. Assim temos $\varphi_0 \in C$ e

$\{A_1, A_2, ..., A_n\} \subseteq \mathrm{dom}(\varphi_0)$. Sendo um elemento de ξ, φ_0 tem uma extensão de ψ_0 a P que satisfaz *B*. Definamos a aplicação μ de P em $\{0,1\}$ da seguinte forma:

$$\mu(A) = \begin{cases} \lambda(A) & \text{se } A \in \mathrm{dom}(\lambda); \\ \psi_0(A) & \text{se } A \notin \mathrm{dom}(\lambda). \end{cases}$$

- μ é uma extensão de λ: o que é que preserva λ no $\mathrm{dom}(\lambda)$.
- μ satisfaz *B*: para isto, temos por um lado que para toda a variável $A \in \mathrm{dom}(\varphi_0)$,

  $$\mu(A) = \lambda(A) = \varphi_0(A) = \psi_0(A);$$

  concluímos disto que μ concorda com ψ_0 em $\{A_1, A_2, ..., A_n\}$; por outro lado, se A é uma variável que ocorre em algumas fórmulas de *B* sem pertencer ao conjunto $\{A_1, A_2, ..., A_n\}$, temos que $A \notin \mathrm{dom}(\lambda)$, então $\mu(A) = \psi_0(A)$; assim vemos que μ toma o mesmo valor que ψ_0 para todas as variáveis proposicionais do conjunto *B*; e uma vez que ψ_0 satisfaz *B*, então também satisfaz μ (pelo lema 1.17).

Assim encontramos uma distribuição de valores lógicos que é uma extensão de λ e que satisfaz *B*, assim $\lambda \in \xi$ e ξ é visto como um conjunto ordenado indutivo. O lema de Zorn permite-nos então escolher um elemento γ de ξ que é maximal para a ordem $\leq$.

Suponhamos que o domínio de γ não são todos os elementos de P e consideremos uma variável proposicional A que não pertença ao domínio de γ. Definiremos uma extensão γ' de γ para o conjunto $\mathrm{dom}(\gamma) \cup \{A\}$ do seguinte modo:

- $\gamma'|_{\mathrm{dom}(\gamma)} = \gamma$;
- $\gamma'(A) = 0$ se para todo o subconjunto finito *B* de *A* existe uma distribuição de valores lógicos δ em P que satisfaz *B*, que é uma extensão de γ, e tal que $\delta(A) = 0$;
- $\gamma'(A) = 1$ caso contrário.

Podemos então fazer a seguinte observação: se $\gamma'(A) = 1$, então para todo o subconjunto finito $B \subseteq A$, existe uma distribuição de valores lógicos δ em P que satisfaz *B*, que é uma extensão de γ, e tal que $\delta(A) = 1$.

Para vermos isto, note-se que se $\gamma'(A) \neq 0$, podemos encontrar um subconjunto finito $B_0 \subseteq A$ tal que para toda a distribuição de valores lógicos δ que satisfaz B_0 e que é

uma extensão de γ, temos que δ(A) = 1. Seja *B* um subconjunto finito arbitrário de *A*. O conjunto $B \cup B_0$ é um subconjunto finito de *A* então existe (por definição do conjunto ξ ao qual γ pertence) uma distribuição de valores lógicos δ que é uma extensão de γ e que satisfaz $B \cup B_0$; δ satisfaz B_0 e é uma extensão de γ: assim δ(A) = 1. Encontramos então na realidade uma extensão de γ para P que satisfaz *B* (uma vez que: $B \subseteq B \cup B_0$) e que toma o valor 1 no ponto A.

Vimos que qualquer que seja o valor de γ'(A), existe, para todo o subconjunto finito *B* de *A*, uma extensão δ de γ para P que satisfaz *B* e tal que δ(A) = γ'(A). Isto simplesmente serve para dizer que δ é de facto uma extensão de γ'. Por conseguinte, para todo o subconjunto finito $B \subseteq A$, γ' pode ser uma extensão de uma distribuição de valores lógicos que satisfazem *B*. Isto significa que γ' pertence a ξ; assim γ' está em ξ e é estritamente maior que γ para a ordem ≤ ($\mathrm{dom}(\gamma) \subsetneq \mathrm{dom}(\gamma')$), o que contradiz o facto de que γ é um elemento maximal de ξ.

Assim a suposição que fizemos sobre o domínio de γ era absurda.

Segue-se que dom(γ) = P. Assim vemos que γ é uma distribuição de valores lógicos em P e que qualquer extensão de γ para P é igual a γ. Assim por definição de ξ, todo o subconjunto finito *B* de *A* é satisfeito por γ. Em particular, isto é verdade para todo o subconjunto com apenas um único elemento, o que significa que toda a fórmula $F \in A$ é satisfeita por γ. Assim *A* é satisfazível.

1.5.3 Algumas aplicações do (meta)teorema da Compacidade

Comecemos por analisar uma primeira aplicação.

Seja dado um conjunto **M** de rapazes e um conjunto **N** de raparigas suas namoradas. O *Problema do Casamento* é o problema de casar cada rapaz com uma das suas namoradas, sem bigamia. Sob certas condições, o problema é solúvel. O caso finito é contemplado no seguinte resultado.

"Lema do casamento": Se M é um conjunto finito de $m \geq 1$ rapazes tal que, para cada $k \leq m$, quaisquer k rapazes dispõem de, pelo menos, k namoradas, então o problema do casamento tem solução.

Trataremos agora do caso infinito, isto é, do caso em que o conjunto dos rapazes e o conjunto das raparigas são infinitos.

"Teorema do casamento": Se M é um conjunto infinito (numerável) de rapazes, cada rapaz tem um número finito de namoradas e, para cada inteiro positivo *k*, quaisquer *k* rapazes dispõem de, pelo menos, *k* namoradas, então o problema do casamento tem solução.

Demonstração: Seja $M = \{r_0, r_1, ...\}$ o conjunto dos rapazes, $N = \{s_0, s_1, ...\}$ o conjunto das raparigas, e consideremos

$$P = M \times N = \{(r_i, s_j): i \geq 0, j \geq 0\}.$$

Para tornar mais fácil a notação consideremos $p_{ij} = (r_i, s_j)$ para $i \geq 0, j \geq 0$. Consideremos os p_{ij} como variáveis proposicionais da linguagem proposicional sobre P e, nesta linguagem, os conjuntos das fórmulas

$\Gamma_1 = \{ p_{ii_1} \vee ... \vee p_{ii_n} : i \geq 0$ e, para cada i, $s_{i_1},...,s_{i_n}$ são as namoradas de $r_i\}$;

$\Gamma_2 = \{\neg(p_{ij} \wedge \neg p_{ik}) : i, j, k \geq 0, j \neq k\}$

$\Gamma_3 = \{\neg(p_{ik} \wedge p_{jk}) : i, j, k \geq 0, j \neq k\}$

O significado intuitivo das fórmulas que compõem estes conjuntos é claro, se encararmos p_{ij} como verdadeira se e só se o rapaz r_i casa com a rapariga s_j. Por exemplo, a fórmula

$$p_{22_1} \vee ... \vee p_{22_n}$$

exprime que o rapaz r_2 casa com uma das suas namoradas $s_{2_1},...,s_{2_n}$. As fórmulas de Γ_2 e Γ_3 exprimem que não há bigamia.

Para que o problema do casamento tenha solução basta, pois, que o conjunto $\Gamma = \Gamma_1 \cup \Gamma_2 \cup \Gamma_3$ seja compatível e, para isto acontecer, basta, pelo (meta)teorema da compacidade, que toda a parte finita de Γ seja compatível. É o que mostramos de seguida.

Seja Γ_0 uma parte finita qualquer de Γ. Em Γ_0 há apenas um número finito de fórmulas de Γ, nas quais ocorrem ao todo, pois, também um número finito de variáveis, as quais dizem respeito a um número finito de rapazes, digamos

$$r_{i_1},...,r_{i_m}.$$

Pelo “lema do casamento” (cujas hipóteses são as mesmas do “teorema do casamento”, excepto no número de rapazes), o problema do casamento tem solução para estes rapazes. Feito o casamento destes *m* rapazes com *m* raparigas, sem bigamia, definimos a valoração υ_0 pondo:

$\upsilon_0(p_{ij}) = 1$ se e só se o rapaz r_i casou com a rapariga s_j, para $i = i_1, ..., i_m$, $j = j_1, ..., j_m$, e $\upsilon_0(p_{ij}) = 0$ (este valor é, porém, irrelevante) para os p_{ij} que não ocorrem em fórmulas de Γ_0. Assim dito e feito, facilmente verificamos que todas as fórmulas de Γ_0 são satisfeitas por υ_0, isto é, que υ_0 é modelo de Γ_0. Portanto, Γ_0 é compatível.

Como se disse acima, Γ é compatível, por compacidade. Falta agora o final. Seja υ um modelo de Γ. Definimos o casamento da totalidade dos rapazes do seguinte modo:

Casamos r_i com s_j se e só se $\upsilon(p_{ij}) = 1$.

Por υ ser modelo de Γ, e atendendo ao que as fórmulas de Γ exprimem, vê-se que o problema do casamento tem solução e o teorema está demonstrado.

Vejamos de seguida uma outra aplicação do (meta)teorema da compacidade.

Chamemos mapa a um conjunto M de regiões fechadas (com interior não vazio) do plano euclidiano, duas a duas disjuntas ou adjacentes mas, neste último caso, a parte comum das fronteiras não se reduzindo a pontos isolados. O *Problema das quatro cores* é um problema clássico de coloração de mapas: colorir as regiões do mapa utilizando somente 4 cores, mas de tal modo que duas regiões adjacentes recebam cores diferentes. Digamos que uma tal coloração é *própria*. A *Conjectura de Guthrie*, ou *conjectura das quatro cores*, é a conjectura de que *todo* o mapa finito admite uma coloração própria. Foi formulada por um jovem licenciado da Universidade de Londres em 1852, Francis Guthrie, que a passou a seu irmão Frederick, estudante de Física, que por sua vez a passou ao seu mestre A. De Morgan. De Morgan mostrou facilmente que 3 cores não são suficientes, e também mostrou que não é possível 5 regiões de um mapa estarem numa posição tal que cada uma delas seja adjacente às outras quatro, mas quanto à conjectura ... passou-a aos seus discípulos e colegas. Arthur Cayley fez publicar a conjectura nos *Proceedings* da Sociedade Matemática de Londres em 1878 e, desde então, muitos matemáticos investiram na tentativa de resolver a conjectura. Finalmente, em 1976, após quatro anos de labor intenso e mais de 1200 horas de

cálculo num super-computador, dois jovens matemáticos da Universidade de Ilinnois, nos E.U.A., anunciaram ter demonstrado o

"Teorema das quatro cores (caso finito)": Todo o mapa finito admite uma coloração própria.

Pela primeira vez na história da matemática, partes substanciais e cruciais de uma demonstração (?) foram realizadas por um computador, utilizando ideias formuladas durante e como consequência do próprio decurso da computação. A validade e legitimidade da demonstração foram questionadas por alguns críticos, já que repousava ou parecia repousar na *crença* de que o programa utilizado fazia exactamente o que os seus autores haviam projectado. Assim, um novo tipo de argumentação matemática parece ter nascido: a análise da correcção de um programa computacional. Em todo o caso, e dando o teorema das quatro cores como provado, no caso finito, provaremos a versão infinita do mesmo:

"Teorema das quatro cores (caso infinito)": Todo o mapa infinito (numerável) $M = \{R_0, R_1, ...\}$ admite uma coloração própria.

Demonstração: Designemos as quatro cores por l, 2, 3 e 4 e consideremos a linguagem proposicional cujas variáveis proposicionais são

p_{ij}, para todo $i \geq 0$, $1 \leq j \leq 4$.

Pensemos nos conjuntos de fórmulas

$\Gamma_1 = \{ p_{i1} \vee p_{i2} \vee p_{i3} \vee p_{i4} : i \geq 0\}$,

$\Gamma_2 = \{p_{ij} \rightarrow \neg p_{ik} : i \geq 0,\ 1 \leq j \leq 4,\ 1 \leq k \leq 4,\ j \neq k\}$,

$\Gamma_3 = \{p_{ik} \rightarrow \neg p_{jk}$: $i, j \geq 0$, $1 \leq k \leq 4$, as regiões R_i e R_j são adjacentes$\}$.

Se interpretarmos intuitivamente p_{ij} como verdadeira se e só se a região R_i recebe a cor j, as fórmulas do conjunto $\Gamma = \Gamma_1 \cup \Gamma_2 \cup \Gamma_3$ exprimem que o mapa M admite uma coloração própria. Para demonstrar o teorema basta mostrar, pois, que o conjunto Γ é compatível e *definir a coloração* a partir de um modelo υ de Γ do seguinte modo:

R_i recebe a cor j se e só se $\upsilon(p_{ij}) = 1$.

Para mostrar que Γ é compatível basta mostrar que toda a parte finita de Γ é compatível e aplicar o (meta)teorema da compacidade. É o que fazemos de seguida.

Seja Γ_0 uma parte finita qualquer de Γ. Nas formulas de Γ_0 há não mais do que um número finito de variáveis p_{ij}, as quais dizem respeito a um número *finito* de regiões e formam, portanto, um mapa finito, digamos

$$M_0 = \{ R_{i_1}, ..., R_{i_m} \}.$$

Pelo teorema das quatro cores no caso finito, este mapa admite uma coloração própria. *Definimos a valoração* υ_0 pondo

$\upsilon_0(p_{ij}) = 1$ se e só se R_i recebeu a cor j, para $i = i_1, ..., i_m$, $1 \leq j \leq 4$,

e $\upsilon_0(p_{ij}) = 0$ nos outros casos (na realidade, estes outros valores de υ_0 são irrelevantes). Facilmente se pode concluir que υ_0 (ou melhor, a valoração booleana correspondente $\hat{\upsilon}_0$) satisfaz todas as fórmulas de Γ_0, logo este conjunto é compatível. Por exemplo, se a fórmula $p_{ij} \rightarrow \neg p_{ik}$ está em Γ_0, então a região R_i está em M_0; se esta região recebeu a cor j, então não recebeu nenhuma outra cor, logo $\upsilon_0(p_{ij}) = 1$ e $\upsilon_0(p_{ik}) = 0$ para todo $j \neq k$, donde $\hat{\upsilon}_0(p_{ij} \rightarrow \neg p_{ik}) = 1$.

Capítulo II. Álgebras booleanas

Sumário

Neste capítulo vamos abordar na perspectiva das álgebras booleanas uma parte da álgebra, uma parte da topologia, algumas definições de álgebras booleanas, átomos nas álgebras booleanas, homomorfismos, isomorfismos, subálgebras, ideais, filtros e o teorema de Stone.

Quando identificamos fórmulas logicamente equivalentes do cálculo proposicional, obtemos um conjunto no qual, de um modo natural, podemos definir uma operação unária e duas operações binárias que correspondem respectivamente à negação, à conjunção e à disjunção. A estrutura obtida deste modo é um exemplo de uma álgebra booleana. Outro exemplo de uma álgebra booleana é dado pelo conjunto de subconjuntos de um determinado conjunto com as operações de complementação, intersecção e união (que são chamadas, frequentemente, operações booleanas).

Existem várias maneiras de abordar álgebras booleanas. Inicialmente, começaremos com duas apresentações puramente algébricas e chegaremos à conclusão, no fim deste capítulo, de que podemos da mesma maneira adoptar um ponto de vista topológico: toda a álgebra booleana pode ser identificada com o conjunto destes subconjuntos compactos, o espaço zero dimensional, simultaneamente, aberto e fechado. A secção 2.1 conterá as revisões necessárias, tanto de álgebra como de topologia.

A secção 2.2 conterá as definições algébricas e correspondentes propriedades básicas. Considerou-se uma álgebra booleana como sendo um anel no qual todo o elemento é igual ao seu quadrado; mas esse anel é também distributivo, um reticulado complementado, ou seja, um conjunto ordenado no qual: (i) existe um mínimo e um máximo, (ii) todo o par de elementos tem um minorante e um majorante, cada uma destas operações é distributiva relativamente à outra, e, finalmente, (iii) todo o elemento tem um complementar.

A secção 2.3 será dedicada a átomos: elementos não nulos que são minimais relativamente à ordem da álgebra booleana.

Na secção 2.4 estudaremos homomorfismos de álgebras booleanas. Em álgebra, os núcleos destes homomorfismos (que neste contexto são ideais) desempenham um papel essencial. Quando consideramos uma álgebra booleana *A* como um reticulado, preferimos não estudar os ideais mas antes os filtros que são canonicamente associados a eles (obtemos um filtro tomando os complementares dos elementos de um ideal).

O objectivo da secção 2.5 é o estudo destes ideais e filtros. Particular atenção é prestada a filtros maximais ou ultrafiltros, para os quais correspondem ideais maximais, mas também correspondem a homomorfismos de *A* na álgebra booleana {0,1}. O conjunto destes homomorfismos é determinado pela topologia: isto é então o chamado espaço de Stone de *A*, que vai ser tratado na última secção, 2.6, deste capítulo. Também será analisado no âmbito do estudo deste espaço o teorema de compactação para o cálculo proposicional que está relacionado de uma forma natural com a compactação do espaço de Stone da álgebra de classes de equivalência e de fórmulas logicamente equivalentes.

2.1 Álgebra e Topologia

2.1.1 Álgebra

Consideremos um anel comutativo com identidade $A = \langle A, +, \times, 0, 1\rangle$.

Suporemos sempre em tal anel que $0 \neq 1$. Como é habitual, qualquer uma das notações $a \times b$ ou ab denotarão o produto de dois elementos a e b de *A*.

Temos então a seguinte definição:

Definição 2.1 Um **ideal** de *A* é um subconjunto *I* de A tal que

- $\langle I, +, 0\rangle$ é um subgrupo de $\langle \mathrm{A}, +, 0\rangle$;
- para todo o elemento *x* de *I* e para todo o elemento *y* de A, $x \times y \in I$.

O conjunto A satisfaz obviamente estas condições. Um ideal de *A* distinto de A define-se como um ideal formal. Um ideal *I* de *A* é um ideal formal se e só se $1 \notin I$. (Se $I = \mathrm{A}$, então $1 \in I$; se $1 \in I$, então para todo o elemento *y* de A, $1 \times y = y \in I$, pois A = *I*).

Aqui apenas consideraremos ideais formais. Assim, um ideal de *A* será um subconjunto *I* de A, o qual, para além de satisfazer as duas condições anteriores, satisfaz a seguinte propriedade:

- $1 \notin I$.

No entanto, adoptar este ponto de vista pode, às vezes, ter inconvenientes: por exemplo, dados dois ideais *I* e *J* de *A*, pode não existir um ideal menor contendo ambos *I* e *J* por causa da soma de dois ideais *I* e *J*, ou seja, o conjunto

$$I + J = \{ x \in \mathrm{A}: (\exists_{y \in I})(\exists_{z \in J})(x = y + z) \}$$

que normalmente goza desta propriedade, pode não ser um ideal formal. Por exemplo, no anel dos inteiros $\mathbb{Z}$, a soma dos ideais $2\mathbb{Z}$ (o conjunto dos múltiplos de 2) e $3\mathbb{Z}$ (o conjunto dos múltiplos de 3) são o anel inteiro $\mathbb{Z}$.

De seguida, enunciaremos o chamado teorema de Krull.

Teorema 2.2 Todo o ideal num anel comutativo com identidade está incluído em pelo menos um ideal maximal.

(Um **ideal é maximal** se não está estritamente incluído em qualquer outro ideal.)

Demonstração: Para provarmos este teorema vamos usar o lema de Zorn. Seja *I* um ideal no anel *A*. Seja ξ representante do conjunto de ideais em *A* que incluem *I*;

$$\xi = \{J \in \wp(\mathrm{A}): J \text{ é um ideal e } I \subseteq J\}.$$

O teorema ficará provado se conseguirmos estabelecer a existência de pelo menos um elemento maximal no conjunto ordenado $\langle \xi, \subseteq \rangle$. Para tal é suficiente, pelo lema de Zorn, mostrar que este conjunto parcialmente ordenado é não vazio, o que é claro uma vez que *I* é um elemento de ξ, e que todo o subconjunto não vazio totalmente ordenado de ξ

tem um majorante em ξ. Então consideremos um subconjunto X de ξ que é totalmente ordenado com a relação de inclusão; assumimos que X é não vazio. Seja I_0 a união dos elementos de X: $I_0 = \bigcup_{J \in X} J$. Como X é não vazio e como cada elemento de X inclui *I*, *I* está incluído em I_0, então $0 \in I_0$. Se *x* e *y* são elementos de I_0, existem dois ideais *J* e *K* em X tais que $x \in J$ e $y \in K$. Como X é totalmente ordenado, temos que ou $J \subseteq K$ ou $K \subseteq J$. Se estivermos perante a primeira situação, então $x \in K$ e $y \in K$, logo $x - y \in K$ e $x - y \in I_0$. Segue-se que $\langle I_0, +, 0\rangle$ é um subgrupo de $\langle A, +, 0\rangle$. De igual forma, se $x \in I_0$ e $y \in A$, então pelo menos para um ideal $J \in X$, temos que $x \in J$, e também $xy \in J$ e $xy \in I_0$. Finalmente, temos que $1 \notin I_0$, no caso oposto, 1 pertenceria a um dos elementos de X, o que é absurdo. Estabelecemos que I_0 é um ideal de *A* que inclui *I*, ou seja, é um elemento de ξ. Para cada *J* em X, $J \subseteq I_0$: segue-se que I_0 é, em ξ, um majorante do conjunto X.

Seja *I* um ideal no anel *A*. Definimos uma relação de equivalência em A chamada **congruência modulo *I*** e representada por $\equiv_I$:

para todos os elementos x e y de A, $x \equiv_I y$ se e só se $x - y \in I$.

O facto de que a relação $\equiv_I$ é uma relação de equivalência é facilmente demonstrado. Seja $\bar{a}$ o representante da classe de equivalência do elemento $a \in A$. Temos $\bar{0} = I$. A relação de congruência modulo *I* é compatível com as operações + e × do anel: isto significa que se *a*, *b*, *c* e *d* são elementos de A, se $a \equiv_I c$ e $b \equiv_I d$, então $a + b \equiv_I c + d$ e $a \times b \equiv_I c \times d$. Isto permite-nos definir duas operações no conjunto $A/\equiv_I$ de classes de equivalência, as quais continuaremos a representar por + e ×, definidas por: para todos os elementos *x* e *y* de A, $\bar{x} + \bar{y} = \overline{x + y}$ e $\bar{x} \times \bar{y} = \overline{x \times y}$. Estas duas operações no conjunto $A/\equiv_I$ dão-lhe a estrutura de um anel comutativo com unidade (o elemento zero é *I*, o elemento unidade é $\bar{1}$) chamado o anel quociente de *A* pelo ideal *I* e representado por *A*/*I* em lugar de $A/\equiv_I$. O exemplo mais famoso do que descrevemos é dado pelos anéis $\mathbb{Z}/n\mathbb{Z}$ (onde *n* é um número natural maior ou igual que 2).

Teorema 2.3 O anel quociente *A*/*I* é um corpo se e só se o ideal *I* é maximal.

Demonstração: Se suposermos que *I* não é maximal, podemos escolher um ideal *J* de *A* tal que $I \subsetneq J$ (inclusão estrita). Seja *a* um elemento de *J* que não pertence a *I*. Temos

que $\bar{a} \neq I$, consequentemente $\bar{a}$ é um elemento não nulo do anel quociente. Se este elemento fosse invertível, haveria um elemento $b \in$ A tal que $\bar{a} \times \bar{b} = \bar{1}$, ou seja que $ab \equiv_I 1$ ou equivalentemente $ab - 1 \in I$, e também $ab - 1 \in J$. Porque $a \in J$ e J é um ideal, $ab \in J$. Assim a diferença $ab - (ab - 1) = 1$ pertenceria a J, o que é impossível. Segue-se que existe pelo menos um elemento não nulo, não invertível no anel A/I: não é então um corpo.

Agora suponhamos que I é maximal. Seja a um elemento de A tal que $\bar{a} \neq \bar{0}$ (ou equivalentemente, $a \notin I$). O nosso objectivo é mostrar que $\bar{a}$ é um elemento invertível do anel quociente A/I. Consideremos o seguinte conjunto:

$$K = \{x \in \text{A}: (\exists_{y \in \text{A}}) (\exists_{z \in \text{I}}) (x = ay + z)\}.$$

É fácil verificar que $\langle \text{K}, +, 0 \rangle$ é um subgrupo de $\langle \text{A}, +, 0 \rangle$: em primeiro lugar, $0 \in K$ pois $0 = (a \times 0) + 0$; também, se $x_1 \in K$ e $x_2 \in K$, então podemos encontrar elementos y_1 e y_2 em A, e z_1 e z_2 em I, tais que $x_1 = ay_1 + z_1$ e $x_2 = ay_2 + z_2$; concluímos que

$$x_1 - x_2 = a(y_1 - y_2) + z_1 - z_2,$$

que $y_1 - y_2 \in$ A, e que $z_1 - z_2 \in I$, assim $x_1 - x_2 \in K$. Por outro lado, se $x \in K$ e $t \in$ A, então $xt \in K$: de facto, existem elementos $y \in$ A e $z \in I$ tais que $x = ay + z$, e $xt = a(ty) + tz$; mas $ty \in$ A e $tz \in I$, então $xt \in K$. Isto mostra que as duas primeiras condições na definição de um ideal são satisfeitas por K. Se a terceira destas condições também for satisfeita (assim se $1 \notin K$), K será um ideal em A. Mas o conjunto K inclui estritamente o conjunto I: de facto, todo o elemento x de I pode ser escrito como $x = (a \times 0) + x$, e assim também pertence a K; e o elemento a que pode ser escrito como $(a \times 1) + 0$, pertence a K mas não a I. Como I é um ideal maximal, K pode então não ser um ideal em A. Concluímos que $1 \in K$. Assim podemos então encontrar dois elementos $y \in$ A e $z \in I$ tais que

$$ay + z = 1.$$

Então temos que $1 - ay = z \in I$, ou equivalentemente, passando às classes de equivalência para a relação $\equiv_I$, $\overline{1 - ay} = \bar{0}$ que se traduz como $\bar{a} \times \bar{y} = \bar{1}$. Então o elemento $\bar{a}$ tem um inverso no anel quociente A/I.

Mostramos assim que todo o elemento não nulo deste anel é invertível: A/I é então um corpo.

2.1.2 Topologia

Comecemos por dar algumas definições.

Uma **topologia** num conjunto X é uma colecção $\Im$ de subconjuntos de X com as seguintes propriedades:

(1) $\varnothing$ e X pertencem a $\Im$.

(2) A união dos elementos de qualquer subcolecção de $\Im$ está em $\Im$.

(3) A intersecção dos elementos de qualquer subcolecção finita de $\Im$ está em $\Im$.

Um conjunto X para o qual foi especificada uma topologia $\Im$ define-se como um **espaço topológico**.

Falando correctamente, um espaço topológico é um par ordenado (X, $\Im$) que consiste num conjunto X e numa topologia $\Im$ em X, no entanto omitiremos frequentemente a menção específica de $\Im$ se não houver confusão.

Seja X um espaço topológico e Y um subconjunto de X. Consideramos Y uma topologia, chamada **topologia induzida** em Y por X, tomando como conjuntos abertos desta topologia as intersecções com Y de subconjuntos abertos de X. Por outras palavras, para o subconjunto $\Omega \subseteq$ Y ser aberto na topologia induzida, é necessário e suficiente que exista um conjunto aberto O na topologia de X tal que Ω = O $\cap$ Y. Vemos imediatamente que os conjuntos fechados para a topologia induzida em Y são as intersecções com Y dos subconjuntos fechados de X. Quando falamos de um **subespaço** de um espaço topológico X, referimo-nos a um subconjunto com a topologia induzida.

Uma **base** para os conjuntos abertos de um espaço topológico X é uma família $(O_i)_{i \in I}$ de conjuntos abertos na topologia tal que todo o conjunto aberto é uma união de conjuntos abertos desta família; por outras palavras, para todo o conjunto aberto G, existe pelo menos um subconjunto $J \subseteq I$ tal que G = $\cup_{j \in J} O_j$. Quando uma base para os conjuntos abertos de um espaço topológico é escolhida, os elementos desta base são chamados **conjuntos abertos básicos**. Os complementares em X dos conjuntos abertos

básicos são chamados **conjuntos fechados básicos** e é claro que todo o conjunto fechado é uma intersecção de conjuntos fechados básicos. Para a topologia habitual no conjunto $\mathbb{R}$ de números reais, os intervalos abertos limitados (ou seja, os conjuntos da forma $]a, b[$ onde $a \in \mathbb{R}$, $b \in \mathbb{R}$ e $a < b$) constituem uma base para os conjuntos abertos. Além disso, é óbvio que em qualquer espaço topológico, a família de todos os conjuntos abertos é uma base dos conjuntos abertos. Segue-se a propriedade:

Lema 2.4 Se $(O_i)_{i \in I}$ é uma base para os conjuntos abertos do espaço topológico X e se Y é um subconjunto de X, então a família $(O_i \cap Y)_{i \in I}$ é uma base para a topologia em Y induzida por X.

Isto significa que as intersecções com Y dos subconjuntos abertos básicos de X são subconjuntos abertos básicos de Y.

Sejam X e Y dois espaços topológicos. Uma **aplicação** *f* de X em Y é chamada **contínua** se e só se a imagem inversa por *f* de todo o subconjunto aberto de Y é um subconjunto aberto de X. Por outras palavras, *f* é contínua se e só se, para todo o subconjunto aberto Ω de Y, o conjunto $f^{-1}[\Omega] = \{x \in X : f(x) \in \Omega\}$ é um subconjunto aberto de X.

Lema 2.5 Seja $(\Omega_i)_{i \in I}$ uma base para os subconjuntos abertos de um espaço topológico Y e seja *f* uma aplicação de X em Y. Para *f* ser contínua, é necessário e suficiente que para todo o índice $i \in I$, $f^{-1}[\Omega_i]$ seja um subconjunto aberto de X.

Demonstração: Este lema é necessário devido à definição de continuidade (algo que serve para todos os subconjuntos abertos de Y tem de servir em particular para os subconjuntos abertos básicos). O lema é suficiente uma vez que, se Ω é um qualquer subconjunto aberto de Y, então existe um subconjunto $J \subseteq I$ tal que $\Omega = \bigcup_{j \in J} O_j$, e consequentemente $f^{-1}[\Omega] = \bigcup_{j \in J} f^{-1}[O_j]$ (este último facto é uma propriedade bem conhecida de imagens inversas); se todos os $f^{-1}[O_i]$ são subconjuntos abertos de X, $f^{-1}[\Omega]$ será uma união de subconjuntos abertos, e consequentemente um subconjunto aberto de X.

Definição 2.6 Um **homeomorfismo** de um espaço topológico X num espaço topológico Y é uma aplicação bijectiva, contínua de X em Y cuja inversa é uma aplicação contínua de Y em X. (Neste contexto falamos de uma aplicação bijectiva bicontínua).

Definição 2.7 Um **espaço topológico** X define-se como **Hausdorff** (ou **separado**) se e só se para todo o par de elementos distintos x e y de X existem conjuntos abertos disjuntos G e H tais que $x \in G$ e $y \in H$. É imediato que todo o subespaço de um espaço de Hausdorff é de Hausdorff.

Lema 2.8 Seja X um espaço topológico de Hausdorff e seja Y um subconjunto de X. Então a topologia induzida em Y por X faz de Y um espaço de Hausdorff.
Demonstração: Se x e y forem pontos distintos de Y, a intersecção com Y de dois subconjuntos abertos disjuntos de X que contêm x e y respectivamente serão dois subconjuntos abertos disjuntos de Y que contêm x e y respectivamente.

Definição 2.9 Uma **cobertura** de um espaço topológico X é uma família $(E_i)_{i\in I}$ de subconjuntos de X tais que $X = \bigcup_{i\in I} E_i$. Se todos os E_i forem conjuntos abertos, falamos de uma cobertura aberta. Uma **subcobertura** de uma cobertura $(E_i)_{i\in I}$ é uma subfamília $(E_j)_{j\in J}$ $(J \subseteq I)$ que é uma cobertura de X. Falaremos de uma **cobertura finita** (ou **subcobertura**) quando o conjunto correspondente de índices for finito.

Definição 2.10 Um **espaço topológico** define-se como **compacto** se e só se

1. for de Hausdorff
2. de toda a cobertura aberta de X podermos extrair uma subcobertura finita.

Lema 2.11 Seja X um espaço de Hausdorff. Para X ser compacto, é necessário e suficiente que toda a família de subconjuntos fechados de X e cuja intersecção é vazia tenha uma subfamília finita cuja intersecção é vazia.
Demonstração: É suficiente observar que se $(F_i)_{i\in I}$ é uma família de subconjuntos fechados de X e se, para cada $i \in I$, representarmos o complementar de F_i em X por O_i (que é um conjunto aberto), então $\cap_{i\in I} F_i = \varnothing$ se e só se $\cup_{i\in I} O_i = X$. Assim, para cada

família de subconjuntos fechados de X cuja intersecção é vazia, corresponde, por complementação, uma coberta aberta de X, e vice-versa.

Lema 2.12 Seja $(\Omega_i)_{i\in I}$ uma base para os conjuntos abertos do espaço de Hausdorff X. Para X ser compacto, é necessário e suficiente que de toda a cobertura X de conjuntos abertos básicos possamos extrair uma subcobertura finita.

Demonstração: A condição é obviamente necessária. Assumindo que é satisfeita e que $(G_k)_{k\in K}$ é uma cobertura de X de conjuntos abertos arbitrários, temos que $X = \bigcup_{k\in K} G_k$. Mas uma vez que cada G_k é uma união de conjuntos abertos básicos, temos uma cobertura de X de uma família de conjuntos abertos básicos $(\Omega_j)_{j\in J}$ ($J \subseteq I$), com cada Ω_j incluído em pelo menos um dos conjuntos abertos G_k. Assim, com a nossa suposição, podemos extrair desta cobertura uma subcobertura finita e teremos, por exemplo, $X = \Omega_{j_1} \cup \Omega_{j_2} \cup ... \cup \Omega_{j_n}$. Agora é suficiente escolher conjuntos abertos $G_{k_1}, G_{k_2}, ..., G_{k_n}$ da família $(G_k)_{k\in K}$ que incluem $\Omega_{j_1}, \Omega_{j_2}, ..., \Omega_{j_n}$ respectivamente; teremos então uma subcobertura finita de $(G_k)_{k\in K}$ donde $X = G_{k_1} \cup G_{k_2} \cup ... \cup G_{k_n}$. Isto prova que X é compacto.

Naturalmente, a propriedade anterior pode ser reformulada em termos de conjuntos fechados:

Lema 2.13 Seja X um espaço de Hausdorff com uma determinada base para os conjuntos abertos. Para X ser compacto, é necessário e suficiente que de toda a família de conjuntos fechados básicos cuja intersecção é vazia, possamos extrair um subfamília finita cuja intersecção é ainda vazia.

Definição 2.14 Um subconjunto de um espaço topológico X que é simultaneamente aberto e fechado (ou seja, um subconjunto aberto em X cujo complementar é também aberto) será chamado **aberto e fechado**.

Definição 2.15 Um espaço topológico que tem uma base consistindo de conjuntos abertos e fechados define-se como **zero-dimensional**. Por exemplo, no espaço $\mathbb{Q}$ de números racionais, os intervalos limitados abertos cujos pontos externos são irracionais

constituem uma base de conjuntos abertos e fechados para a topologia habitual: assim $\mathbb{Q}$ é um espaço topológico zero-dimensional.

Lema 2.16 Para um espaço topológico ser zero-dimensional, é necessário e suficiente que a família de subconjuntos abertos e fechados seja uma base dos conjuntos abertos.
Demonstração: É óbvio que qualquer família de conjuntos abertos que inclua uma base para os subconjuntos abertos de X é ela própria uma base para os subconjuntos abertos de X. Assim, se X é zero-dimensional, então a família de todos os seus subconjuntos, simultaneamente, abertos e fechados é uma base dos conjuntos abertos. A implicação contrária é imediata.

Lema 2.17 Todo o subespaço Y de um espaço topológico zero-dimensional X é zero--dimensional.
Demonstração: Seja $(O_i)_{i\in I}$ uma base para os subconjuntos abertos de X que consiste em conjuntos simultaneamente abertos e fechados. A família $(O_i \cap Y)_{i\in I}$ é uma base para os subconjuntos abertos de Y (lema 2.4) mas estes conjuntos abertos são também subconjuntos fechados de Y uma vez que eles são as intersecções com Y de subconjuntos fechados de X.

Definição 2.18 Um espaço topológico zero-dimensional compacto define-se como um **espaço booleano**.

Definição 2.19 Seja $(X_i)_{i\in I}$ uma família de espaços topológicos. No produto $\prod_{i\in I} X_i$ desta família, podemos definir uma **topologia** tomando como conjuntos abertos básicos todos os subconjuntos da forma $\prod_{i\in I} O_i$ onde, para cada índice $i \in I$, O_i é um subconjunto aberto de X_i, e onde para todos excepto um número finito de índices, temos $O_i = X_i$. É fácil verificar que a colecção consistindo de uniões de conjuntos deste tipo é fechada para as intersecções e as uniões arbitrárias. É esta colecção de conjuntos que tomamos como a família de conjuntos abertos para a topologia em $\prod_{i\in I} X_i$. A topologia definida desta forma é chamada **topologia produto**.

O teorema de Tychonoff afirma que:

Teorema 2.20 O produto de qualquer família de espaços topológicos compactos é um espaço topológico compacto.

A demonstração deste teorema faz uso do lema de Zorn e pode ser encontrada, por exemplo, no livro de J.L. Kelley (*General Topology*, Van Nostrand, 1955, reproduzido por Springer-Verlag, Graduate Texts in Mathematics, 1991) (no entanto, tem a desvantagem de usar a noção de filtro que só será estudada mais à frente, neste capítulo).

Consideremos agora o caso especial que nos interessa neste capítulo (Secção 2.6): o caso em que cada X_i da família de espaços $(X_i)_{i\in I}$ é o conjunto $\{0,1\}$ com a topologia discreta (na qual todos os subconjuntos são abertos).

Neste caso, o produto $\prod_{i\in I} X_i$ é o conjunto $\{0,1\}^I$ de aplicações de I em $\{0,1\}$.

Para construir um conjunto aberto básico Ω na topologia de produto, devemos tomar um número finito de índices, $i_1, i_2, ..., i_k$ em I e conjuntos abertos $O_{i_1}, O_{i_2}, ..., O_{i_k}$ de $\{0,1\}$, os quais, neste caso, são subconjuntos arbitrários de $\{0,1\}$. Fixamos então

$$\Omega = O_{i_1} \times O_{i_2} \times ... \times O_{i_k} \times \{0,1\}^{I-\{i_1, i_2, ..., i_k\}},$$

ou alternativamente

$$\Omega = \{f \in \{0,1\}^I : f(i_1) \in O_{i_1} \text{ e } f(i_2) \in O_{i_2} \text{ e ... e } f(i_k) \in O_{i_k}\}.$$

É natural pensar que só estamos realmente interessados nesses índices i_j para os quais o correspondente conjunto aberto é algo diferente do conjunto $\{0,1\}$. Também é insensato considerar casos nos quais cada um dos O_{i_j} é o conjunto vazio, para os quais teríamos $\Omega = \varnothing$. Temos então apenas duas possíveis escolhas para os O_{i_j}: $O_{i_j} = \{0\}$ ou $O_{i_j} = \{1\}$.

Assim vemos que para construirmos um conjunto básico aberto Ω na topologia de produto em $\{0,1\}$, devemos tomar um número finito de índices, $i_1, i_2, ..., i_k$ em I e o mesmo número de elementos $\varepsilon_1, \varepsilon_2, ..., \varepsilon_k$ em $\{0,1\}$ e então fixar

$$\Omega = \{f \in \{0,1\}^I : f(i_1) = \varepsilon_1 \text{ e } f(i_2) = \varepsilon_2 \text{ e ... e } f(i_k) = \varepsilon_k\}.$$

Um conjunto aberto básico é, então, o conjunto de todas as aplicações de I em $\{0,1\}$ que assumem determinados valores de um número finito de determinados pontos.

Observe-se que o complementar em $\{0,1\}^I$ do conjunto Ω que há pouco consideramos é o seguinte conjunto:

$$\bigcup_{1\leq j\leq k}\left\{f\in\{0,1\}^I : f\left(i_j\right)=1-\varepsilon_j\right\}.$$

Assim é a união de *k* conjuntos abertos básicos que é obviamente um conjunto aberto. Concluímos que **Ω** é um conjunto fechado.

Os conjuntos abertos básicos na topologia em $\{0,1\}^I$ são então conjuntos simultaneamente abertos e fechados. Por conseguinte, demonstramos que:

Lema 2.21 O espaço topológico $\{0,1\}^I$ é zero-dimensional.

Pois o espaço discreto {0,1} seja claramente compacto, podemos concluir, usando o teorema de Tychonoff, que:

Lema 2.22 O espaço $\{0,1\}^I$ é um espaço topológico booleano.

Demonstração:

Dizer que $\{0,1\}^I$ é um espaço topológico booleano é o mesmo que dizer que $\{0,1\}^I$ é um espaço topológico zero-dimensional compacto. Uma vez que já foi provado que $\{0,1\}^I$ é um espaço topológico zero-dimensional (lema 2.21), falta ver que é compacto. Pelo teorema de Tychonoff basta apenas provarmos que o espaço {0,1} é compacto, mais concretamente, que o espaço {0,1} é separado. Assim, para todo o par de elementos distintos *x* e *y* de {0,1} existem conjuntos abertos disjuntos G e H tais que $x \in$ G e $y \in$ H, por exemplo: G =]-∞;0,1[e H =]0,1;+∞[. Conclui-se então que $\{0,1\}^I$ é um espaço topológico booleano.

2.1.3 Uma aplicação ao cálculo proposicional

O teorema de Tychonoff permite-nos fazer uma demonstração rápida do (meta)teorema da compacidade, versão 2, para o cálculo proposicional. Assim,

Teorema 1.35 Para qualquer conjunto *A* de fórmulas do cálculo proposicional, *A* é contraditório se e só se pelo menos um subconjunto finito de *A* é contraditório.

Demonstração:

Seja P um conjunto de variáveis proposicionais e seja *F* o conjunto associado de fórmulas. Para cada F$\in$ *F*, seja Δ(F) o conjunto de atribuições de valores lógicos que o satisfazem:

$$\Delta(F) = \{\delta \in \{0,1\}^P: \bar{\delta}(F) = 1\}.$$

Se A_1, A_2, ..., A_n são as variáveis que aparecem na fórmula F, vemos que o conjunto Δ(F) é a união de conjuntos da forma

$$\{\delta \in \{0,1\}^I: \delta(A_1) = \varepsilon_1 \text{ e } \delta(A_2) = \varepsilon_2 \text{ e ... e } \delta(A_k) = \varepsilon_k\},$$

onde os ε_i são elementos de $\{0,1\}$.

De facto, a satisfação da fórmula F por uma atribuição δ não depende dos valores que δ assume fora do conjunto $\{A_1, A_2, ..., A_n\}$.

Assim, o conjunto Δ(F) é a união de conjuntos abertos básicos no espaço topológico $\{0,1\}^P$. Esta é uma união finita: envolve no máximo 2^n conjuntos. Então concluímos que Δ(F) é um conjunto simultaneamente aberto e fechado.

Agora consideremos um conjunto de fórmulas T $\subseteq$ *F* que não é satisfazível. Isto significa, justamente, que a intersecção, $\bigcap_{F\in T}\Delta(F)$, é o conjunto vazio. Assim, a família $(\Delta(F))_{F\in T}$ é, no espaço compacto $\{0,1\}^P$, uma família de conjuntos fechados cuja intersecção é vazia. Assim é possível extrair uma subfamília finita cuja intersecção é vazia; assim existe um subconjunto finito $T_0 \subseteq$ T tal que $\bigcap_{F\in T_0}\Delta(F) = \phi$. Isto significa que existe algum subconjunto finito de T que não é satisfazível. Isto prova o (meta)teorema da compacidade (versão 2) para o cálculo proposicional.

2.2 Algumas definições de Álgebras booleanas

Definição 2.23 Segundo Yaglom (1983), uma **álgebra booleana** coincide com um reticulado (distributivo) complementado, também chamado de reticulado booleano.

Definição 2.24 Segundo Cori & Lascar (2000), uma **álgebra booleana** (às vezes chamada **anel booleano**) é um anel $\langle A, +, \times, 0, 1\rangle$ em que cada elemento é um idempotente para a multiplicação (ou seja, é igual ao seu quadrado).

Vejamos agora alguns exemplos de anéis booleanos:

- O anel $\langle \mathbb{Z}/2\mathbb{Z}, +, \times, 0, 1\rangle$.
- A álgebra de Boole $\langle \wp(E), \Delta, \cap, \varnothing, E\rangle$, onde E é um conjunto arbitrário não vazio, Δ e $\cap$ são respectivamente as operações de diferença simétrica e intersecção no conjunto $\wp(E)$ de todos os subconjuntos de E.
- Outro exemplo interessante é fornecido através do cálculo proposicional.

Considere-se um conjunto de variáveis proposicionais e o correspondente conjunto *F* de fórmulas. Como já vimos, o conjunto $F / \sim$ de classes de equivalência de fórmulas logicamente equivalentes com as operações de não equivalente e $\wedge$ tem a estrutura de uma álgebra booleana (estas operações podem ser definidas neste conjunto porque a relação $\sim$ é compatível com os conectivos proposicionais - ou seja, que qualquer fórmula que seja logicamente equivalente a uma fórmula com os conectivos proposicionais também tem esses conectivos). A classe 0 de antilogias e a classe 1 de tautologias são, respectivamente, os elementos identidade para as operações não equivalente e $\wedge$.

2.2.1 Propriedades das álgebras booleanas, relações de ordem

Vejamos, agora o seguinte lema:

Lema 2.25

- em qualquer álgebra booleana, todo o elemento é o seu próprio inverso aditivo;
- toda a álgebra booleana é comutativa.

Demonstração: Seja $\langle A, +, \times, 0, 1\rangle$ uma álgebra booleana e sejam *x* e *y* elementos de A. Da definição, temos que $x^2 = x$, $y^2 = y$, e $(x + y)^2 = x + y$, além disso, como em qualquer anel, temos que

$$(x + y)^2 = x^2 + xy + yx + y^2.$$

Assim podemos concluir, pela idempotência, que

$$x + y = x + xy + yx + y,$$

ou depois da simplificação, $xy + yx = 0$. Tomando $y = 1$, obtemos em particular que $x + x = 0$ ou $x = -x$, o que prova o primeiro ponto. Então, para *x* e *y* arbitrários, *xy* é o

inverso de xy, mas uma vez que $xy + yx = 0$, também xy é o inverso de yx. Concluímos então que $xy = yx$ e que a álgebra é comutativa.

O anel booleano $\langle \mathbb{Z}/2\mathbb{Z}, +, \times, 0, 1 \rangle$ é o único anel booleano que é um corpo, e até mesmo o único anel booleano que é um domínio de integridade: de facto, a relação $x^2 = x$, que é equivalente a $x(x-1) = 0$, requer, num domínio de integridade, que $x = 0$ ou $x = 1$.

Seja $\langle A, +, \times, 0, 1 \rangle$ uma álgebra booleana. Definimos uma **relação binária** $\leq$ em A da seguinte forma: para todos os elementos x e y de A, $x \leq y$ se e só se $xy = x$.

Verificaremos de seguida que esta é realmente uma **relação de ordem parcial**. Para todos os elementos x, y e z de A, temos que:

- $x \leq x$, pois $x^2 = x$ por definição;
- se $x \leq y$ e $y \leq z$, então $xy = x$ e $yz = y$; e também, $xz = (xy)z = x(yz) = xy = x$, então $x \leq z$;
- se $x \leq y$ e $y \leq x$, então $xy = x$ e $yx = y$, assim $x = y$ por comutatividade.

  Assim a relação $\leq$ é reflexiva, transitiva e anti-simétrica.

Teorema 2.26 Principais propriedades da relação de ordem, $\leq$:

(1) 0 é o menor elemento e 1 é o maior elemento da relação $\leq$;

Demonstração: De facto, para todo o x, $0 \times x = 0$ e $1 \times x = x$, consequentemente $0 \leq x$ e $x \leq 1$.

(2) Quaisquer dois elementos x e y de A têm um ínfimo (ou seja, um minorante comum que é maior do que qualquer outro minorante comum), representado por $x \cap y$: ou seja, o seu produto xy.

Demonstração: Temos que

$$(xy)x = x^2y = xy \text{ e } (xy)y = xy^2 = xy,$$

assim xy é um minorante tanto para x como para y. Além disso, se z é um minorante comum para x e y, temos que $zx = z$ e $zy = z$, e consequentemente $z(xy) = (zx)y = zy = z$, o que significa que $z \leq xy$; assim xy é o ínfimo comum a x e y.

(3) Quaisquer dois elementos x e y de A têm um supremo (ou seja, um majorante comum que é menor do que qualquer outro majorante comum), representado por $x \cup y$: ou seja, o elemento $x + y + xy$.

Demonstração: De facto,

$$x(x + y + xy) = x^2 + xy + x^2y = x + xy + xy = x + 0 = x,$$

e de forma análoga, $y(x + y + xy) = y$. Assim temos que $x \leq x + y + xy$ e $y \leq x + y + xy$. Por outro lado, se z é um elemento de A tal que $x \leq z$ e $y \leq z$, ou seja que $xz = x$ e $yz = y$, então,

$$(x + y + xy)z = xz + yz + xyz = x + y + xy,$$

assim $x + y + xy \leq z$; assim $x + y + xy$ é o supremo comum a x e y.

(4) As operações $\cap$ e $\cup$ assim definidas em A são associativas e comutativas.

Demonstração: Isto é verdade em qualquer conjunto parcialmente ordenado que satisfaz as propriedades (2) e (3).

(5) 0 é um elemento identidade para a operação $\cup$ e um elemento absorvente para a operação $\cap$; enquanto 1 é um elemento identidade para a operação $\cap$ e um elemento absorvente para a operação $\cup$.

Demonstração: Traduzindo por outras palavras, para todo o elemento x de A, temos que $x \cup 0 = x$, $x \cap 0 = 0$, $x \cap 1 = x$ e $x \cup 1 = 1$. Isto é verdade em qualquer conjunto ordenado que satisfaz as propriedades (1), (2), e (3). É trivial verificar isto.

(6) Todo o subconjunto não vazio finito $\{x_1, x_2, ..., x_k\}$ de A ($k \in \mathbb{N}$ *) tem um ínfimo igual a $x_1 \cap x_2 \cap ... \cap x_k$ e um supremo igual a $x_1 \cup x_2 \cup ... \cup x_k$.

Demonstração: Com excepção do caso óbvio no qual $k = 1$, esta é uma simples generalização das propriedades (2) e (3), as quais obtemos naturalmente através da indução sobre k.

Desejamos chamar a atenção para o seguinte facto: a expressão $x_1 \cap x_2 \cap ... \cap x_k$ não é uma notação nova que pretende representar alguns objectos recentemente introduzidos. Representa um elemento de A que é legitimamente definido (através de indução) tal como a operação $\cap$ foi definida (é o elemento que devemos representar por

$$((\ldots((x_1 \cap x_2) \cap x_3) \cap \ldots \cap x_{k-1}) \cap x_k),$$

uma expressão que contém k - 1 pares de parênteses, os quais suprimimos devido à associatividade. Relativamente à operação $\cap$, a propriedade (6) afirma dois factos distintos: primeiro, que os elementos $x_1, x_2, \ldots, x_k$ têm um ínfimo comum; e segundo que este ínfimo comum é

$$x_1 \cap x_2 \cap \ldots \cap x_k .$$

(7) Cada uma das operações $\cap$ e $\cup$ é distributiva relativamente à outra.

Demonstração: Por um lado,

$$x \cap (y \cup z) = x(y + z + yz) = xy + xz + xyz$$
$$= xy + xz + xy.\, xz = (x \cap y) \cup (x \cap z)$$

para quaisquer elementos x, y, e z de A os quais garantem que $\cap$ é distributiva relativamente a $\cup$.

Por outro lado, com x, y, e z ainda elementos arbitrários de A,

$$(x \cup y) \cap (x \cup z) = (x + y + xy)(x + z + xz)$$
$$= x^2 + xz + x^2z + yx + yz + yxz + x^2y + xyz + x^2yz$$
$$= x + yz + xyz$$

depois de várias simplificações.

Mas $x + yz + xyz = x \cup (yz) = x \cup (y \cap z)$, consequentemente da outra propriedade distributiva.

(8) Para todo o elemento x de A, existe um elemento x' de A chamado o complementar de x, tal que $x \cup x' = 1$, e $x \cap x' = 0$.

Demonstração: Se existe um elemento x', que satisfaz $xx' = 0$ e $x + x' + xx' = 1$, e também consequentemente $x + x' = 1$, ou novamente $x' = 1 + x$, é fácil de verificar por outro lado que $x \cup (1 + x) = 1$ e $x \cap (1 + x) = 0$.

Estabelecemos assim não só a existência mas também a singularidade do complementar de x: que é $1 + x$.

(9) A aplicação $x \mapsto 1 + x$ de A em A é uma bijecção que inverte a ordem.

Demonstração: Esta aplicação é até mesmo uma involução (uma bijecção que é a sua própria inversa) pois, para todo o x, $1 + (1 + x) = x$. Por outro lado, para quaisquer elementos x e y, temos que

$$(1 + x)(1 + y) = 1 + x + y + xy.$$

Este elemento é igual a $1 + x$ se e só se $y + xy = 0$, ou novamente $xy = y$. Vemos desta forma que $1 + x \leq 1 + y$ se e só se $y \leq x$.

A relação de ordem numa álgebra booleana é compatível com a multiplicação: isto significa que se os elementos a, b, c e d satisfazem $a \leq b$ e $c \leq d$, então $a \times c \leq b \times d$ (se $a \times b = a$ e $c \times d = c$, então $a \times c \times b \times d = a \times c$). O facto importante que interessa reter é que esta ordem não é compatível com a adição: por exemplo, temos $0 \leq 1$, mas não temos $0 + 1 \leq 1 + 1$.

Segue-se uma propriedade que usaremos frequentemente:

Lema 2.27 Para quaisquer elementos x e y de A, temos que $x \leq 1 + y$ se e só se $xy = 0$.

Demonstração: De facto, $x \leq 1 + y$ quer dizer por definição que $x(1 + y) = x$, ou novamente $x + xy = x$, que é certamente equivalente a $xy = 0$.

2.2.2 Álgebras booleanas como conjuntos parcialmente ordenados

De facto, as propriedades (1), (2), (3), (7), e (8) do Teorema 2.26 caracterizam as álgebras booleanas, como mostra o seguinte teorema; este também nos fornece um segundo método para definir álgebras booleanas.

Teorema 2.28 Seja $\langle A, \leq \rangle$ um conjunto parcialmente ordenado com as seguintes propriedades:

(a) existe um elemento menor (representado por 0) e um elemento maior (representado por 1);

(b) quaisquer dois elementos x e y têm um supremo (representado por $x \cup y$) e um ínfimo (representado por $x \cap y$);

(c) cada uma das operações $\cap$ e $\cup$ é distributiva relativamente à outra;

(d) para todo o elemento x em A, existe pelo menos um elemento x' em A tal que $x \cup x' = 1$ e $x \cap x' = 0$.

Então A pode ter a estrutura de uma álgebra booleana $\langle A, +, \times, 0, 1\rangle$ de tal modo que a ordem dada $\leq$ em A coincida com a ordem que é associada à sua estrutura de álgebra booleana (ou seja, teremos $x \leq y$ se e só se $xy = x$).

Vejamos algumas observações preliminares:

♦ Um conjunto ordenado que tem as propriedades (a) e (b) do teorema define-se como **reticulado**. Se também tiver a propriedade (c), define-se como um **reticulado distributivo**. Se as propriedades (a), (b), e (d) são satisfeitas, falamos de um **reticulado complementado** onde o complementar de um elemento x é o único elemento x' para o qual $x \cup x' = 1$ e $x \cap x' = 0$. A unicidade é fácil de provar:

Demonstração: Suponhamos que x' e x'' são ambos complementares de x e consideremos o elemento $y = (x \cap x') \cup x''$. Por um lado, y é igual a $0 \cup x''$, ou seja a x''. Por outro lado, a distributividade leva-nos a

$$y = (x \cup x'') \cap (x' \cup x'') = 1 \cap (x' \cup x'') = x' \cup x''.$$

Então temos que $x'' = x' \cup x''$, o que significa que $x' \leq x''$. Trocando os papéis de x' e x'' neste argumento, obtemos naturalmente $x'' \leq x'$, e, no fim, $x' = x''$.

♦ O **complementar** do elemento x será representado por $\boldsymbol{x^C}$. Temos obviamente que $1^C = 0$ e $0^C = 1$. Observe-se que como consequência da singularidade do complementar a aplicação $x \mapsto x^C$ de A para A é uma bijecção que é igual à sua inversa (para todo x, $(x^C)^C = x$).

Note-se que, na adição como já observámos, quando as hipóteses (a), (b), (c), e (d) são satisfeitas, também são as propriedades (4), (5), e (6) do Teorema 2.26 que refere as propriedades da relação de ordem.

De seguida estabeleceremos o que é geralmente conhecido como as leis de De Morgan:

Lema 2.29 Para quaisquer elementos x e y de A,

$$(x \cap y)^C = x^C \cup y^C \text{ e} \qquad (*)$$
$$(x \cup y)^C = x^C \cap y^C$$

Demonstração: A segunda lei segue-se da primeira substituindo x por x^C e y por y^C e depois usar as propriedades de complementação.

Para provar a primeira lei, mostramos que $(x^C \cup y^C) \cup (x \cap y) = 1$ e que $(x^C \cup y^C) \cap (x \cap y) = 0$: para isto, usamos a distributividade das operações $\cup$ e $\cap$ bem como a associatividade e a comutatividade:

$$(x^C \cup y^C) \cup (x \cap y) = (x^C \cup y^C \cup x) \cap (x^C \cup y^C \cup y)$$
$$= (1 \cup y^C) \cap (x^C \cup 1) = 1 \cap 1 = 1;$$
$$(x^C \cup y^C) \cap (x \cap y) = (x^C \cap x \cap y) \cup (y^C \cap x \cap y)$$
$$= (0 \cap y) \cup (0 \cap x) = 0 \cup 0 = 0.$$

Através de indução, as leis de De Morgan generalizam imediatamente, como se segue, que:

Lema 2.30 Para qualquer inteiro $k \geq 1$ e elementos $x_1, x_2, ..., x_k$ de A,

$$(x_1 \cap x_2 \cap ... \cap x_k)^C = x_1^C \cup x_2^C \cup ... \cup x_k^C \text{ e}$$
$$(x_1 \cup x_2 \cup ... \cup x_k)^C = x_1^C \cap x_2^C \cap ... \cap x_k^C .$$

Definiremos agora uma adição + e uma multiplicação $\times$ no conjunto A: para todo x e y, fixamos que

$$x \times y = x \cap y \text{ e}$$
$$x + y = (x \cap y^C) \cup (x^C \cap y)$$

Podemos obter outra expressão para $x + y$, usando o facto de que $\cup$ é distributiva sobre $\cap$:

$$x + y = (x \cup x^C) \cap (x \cup y) \cap (y^C \cup x^C) \cap (y^C \cup y)$$
$$= 1 \cap (x \cup y) \cap (x^C \cup y^C) \cap 1, \text{ consequentemente,}$$
$$x + y = (x \cup y) \cap (x^C \cup y^C).$$

Provaremos de seguida que $\langle A, +, \times, 0, 1 \rangle$ é um anel booleano.

Demonstração:

- A propriedade "para todo o x, $x^2 = x$" é imediata ($x \cap x = x$);
- $\langle A, +, 0 \rangle$ é um grupo comutativo:

  * a comutatividade segue-se imediatamente de $\cap$ e de $\cup$.

  * 0 é um elemento identidade para a adição: para todo o x em A,

$$x + 0 = (x \cap 0^C) \cup (x^C \cap 0) = (x \cap 1) \cup 0 = x \cup 0 = x.$$

* todo o elemento x de A tem um inverso: nomeadamente, ele próprio:

$$x + x = (x \cap x^C) \cup (x^C \cap x) = 0 \cup 0 = 0.$$

* A adição é associativa: se x, y, e z são elementos de A, temos que

$$(x + y) + z = ([x + y] \cap z^C) \cup ([x + y]^C \cap z)$$

(usando a definição de +)

$$= ([(x \cap y^C) \cup (x^C \cap y)] \cap z^C) \cup ([x + y]^C \cap z)$$

(usando a definição de +)

$$= ([(x \cap y^C) \cup (x^C \cap y)] \cap z^C) \cup ([(x \cup y) \cap (x^C \cup y^C)]^C \cap z)$$

(usando (*))

$$= ([(x \cap y^C) \cup (x^C \cap y)] \cap z^C) \cup ([(x \cup y)^C \cup (x^C \cup y^C)^C] \cap z)$$

(através das leis de De Morgan)

$$= ([(x \cap y^C) \cup (x^C \cap y)] \cap z^C) \cup ([(x^C \cap y^C) \cup (x \cap y)] \cap z)$$

(através das leis de De Morgan)

$$= [(x \cap y^C \cap z^C) \cup (x^C \cap y \cap z^C)] \cup [(x^C \cap y^C \cap z) \cup$$
$$\cup (x \cap y \cap z)]$$

(distributividade de $\cap$ sobre $\cup$).

Finalmente, e usando a associatividade de $\cup$, obtemos que

$$(x + y) + z = (x \cap y^C \cap z^C) \cup (x^C \cap y \cap z^C) \cup (x^C \cap y^C \cap z) \cup (x \cap y \cap z).$$

A comutatividade de $\cup$ e $\cap$ implica que todas as permutações em x, y, e z produzam o mesmo resultado. Em particular, $(x + y) + z = (y + z) + x$, mas uma vez que a operação adição é comutativa, temos também

$$(x + y) + z = x + (y + z).$$

- A multiplicação $\times$ é associativa e tem 1 como um elemento identidade: estas são obviamente propriedades da operação $\cap$.
- A multiplicação é distributiva relativamente à adição: para provarmos isto, invocamos novamente a associatividade e a comutatividade de $\cup$ e $\cap$, a distributividade da $\cap$ relativamente à $\cup$, juntamente com as leis de De Morgan. Omitiremos as justificações de cada passo no cálculo.

  Sejam x, y, e z elementos de A. Temos que

  $$xy + xz = (x \cap y) + (x \cap z)$$
  $$= [(x \cap y) \cap (x \cap z)^C] \cup [(x \cap y)^C \cap (x \cap z)]$$
  $$= [(x \cap y) \cap (x^C \cup z^C)] \cup [(x^C \cup y^C) \cap (x \cap z)]$$

$$= [(x \cap y \cap x^C) \cup (x \cap y \cap z^C)] \cup [(x^C \cap x \cap z) \cup (y^C \cap x \cap z)]$$
$$= (x \cap y \cap z^C) \cup (x \cap y^C \cap z)$$
$$= x \cap [(y \cap z^C) \cup (y^C \cap z)]$$
$$= x \cap [y + z]$$
$$= x\,(y + z).$$

Isto completa a demonstração de que $\langle A, +, \times, 0, 1\rangle$ é uma álgebra booleana.

Seja $<<$ a ordem associada a esta estrutura. Para quaisquer elementos x e y de A, $x << y$ se e só se $xy = x$, ou novamente, $x \cap y = x$, mas esta última igualdade significa precisamente que x é menor ou igual a y para a ordem $\leq$ dada inicialmente em A. Segue-se que estas duas ordens coincidem.

Então, uma álgebra booleana é, opcionalmente, um anel no qual todo o elemento é igual ao seu quadrado, ou um conjunto ordenado que tem a estrutura de um reticulado complementar distributivo.

Sem fazer disto uma regra rígida, tenderemos a adoptar o segundo ponto de vista no resto do capítulo.

No que se segue, apesar do ponto de vista adoptado, iremos permitir-nos usar, simultaneamente, a relação de ordem $\leq$, multiplicação e adição, e as operações $\cup$ e $\cap$.

2.3 Átomos nas álgebras booleanas

Definição 2.31 Um elemento A numa álgebra booleana $\langle A, \leq, \cup, \cap, 0, 1\rangle$ define-se como um **átomo** se e só se é não nulo e não tem nenhum minorante não nulo.

Por outras palavras, a é um átomo se e só se $a \neq 0$ e, para todo elemento b em A, se $b \leq a$, então ou $b = a$ ou $b = 0$.

Vejamos, agora, alguns exemplos de átomos.

↳ Na álgebra booleana $\wp(E)$ de subconjuntos do conjunto E, os átomos são os conjuntos singulares (ou seja, subconjuntos contendo um só elemento).

↳ Existem álgebras booleanas sem átomos: é o caso da álgebra booleana *F*/~ de classes de equivalência de fórmulas do cálculo proposicional quando o conjunto P de variáveis proposicionais é infinito.

Demonstração: A relação de ordem nesta álgebra booleana é a seguinte:

se F e G são fórmulas,

então cl(F) ≤ cl(G) se e só se a fórmula (F ⇒ G) é uma tautologia.

Para provarmos que não existem átomos em *F*/~, mostraremos que todo o elemento não nulo tem um minorante estrito para além de 0. Assim consideremos a fórmula F tal que cl(F) ≠ 0, ou seja tal que ¬F não seja uma tautologia, ou equivalentemente que existe pelo menos uma distribuição de valores lógicos de P que satisfazem F. Escolhamos tal distribuição e representemo-la por δ. Escolhamos também uma variável proposicional X que não apareça na fórmula F. Isto é possível porque P é infinito. Representemos por G a fórmula (F ∧ X). Temos obviamente que ⊨ ((F ∧ X) ⇒ F), consequentemente cl(G) ≤ cl(F). A distribuição de valores lógicos λ, definida por,

$$\text{para todo o } Y \in P, \quad \lambda(Y) = \begin{cases} \delta(Y) & \text{se } Y \neq X \\ 1 & \text{se } Y = X \end{cases}$$

satisfaz F (pois X não apareça em F) e satisfaz X, assim satisfaz G. Segue-se que cl(G) ≠ 0. Por outro lado, a distribuição de valores lógicos μ definida por

$$\text{para todo o } Y \in P, \quad \mu(Y) = \begin{cases} \delta(Y) & \text{se } Y \neq X \\ 0 & \text{se } Y = X \end{cases}$$

satisfaz F (pela mesma razão que λ satisfaz) mas não satisfaz G, e também não satisfaz a fórmula (F ⇒ G). Assim não temos que cl(F) ≤ cl(G), o que nos mostra que cl(G) é um minorante estrito para cl(F); assim é um minorante estrito não nulo.

Segue-se a seguinte definição:

Definição 2.32 Uma álgebra booleana é **atómica** se e só se todo o elemento não nulo é maior ou igual a pelo menos um átomo.

Esta é a situação, por exemplo, da álgebra booleana de todos os subconjuntos de um dado conjunto (todo o conjunto não vazio contém pelo menos um conjunto singular).

Seguem-se os seguintes teoremas:

Teorema 2.33 Toda a álgebra booleana finita é atómica.

Demonstração: Seja $\langle A, \leq, \cup, \cap, 0, 1\rangle$ uma álgebra booleana finita e seja x um elemento não nulo de A. Representemos por $m(x)$ o conjunto de minorantes estritos não nulos de x em A. Se $m(x)$ for vazio, então x é um átomo. Se $m(x)$ for não vazio, então porque é finito, pelo menos um dos seus elementos é minimal na ordem $\leq$, ou seja, nenhum elemento de $m(x)$ está estritamente abaixo dele. Facilmente se vê que tal elemento minimal é um átomo de A abaixo de x.

Teorema 2.34 Seja $\langle A, +, \times, 0, 1\rangle$ uma álgebra booleana (finita ou não). Então para todo o elemento a não nulo de A e para todo o inteiro $k \geq 2$, as seguintes propriedades são equivalentes:

(1) a é um átomo;

(2) para todo o elemento x de A, temos $a \leq x$ ou $a \leq 1 + x$;

(3) para todos os elementos $x_1, x_2, ..., x_k$ de A, se $a \leq x_1 \cup x_2 \cup ... \cup x_k$, então $a \leq x_1$ ou $a \leq x_2$ ou $... a \leq x_k$.

Demonstração: Observemos primeiro que em virtude de um lema anterior (2.27) e da definição da ordem $\leq$, (2) é equivalente a

(2 ') para todo o elemento x em A, temos que $ax = a$ ou $ax = 0$.

Provemos agora o teorema.

Seja a um elemento não nulo de A e k um número natural maior ou igual que 2.

- (1) $\Rightarrow$ (2'): para todo o elemento x em A temos que $ax \leq a$, consequentemente, pois a seja um átomo, $ax = a$ ou $ax = 0$.
- (2) $\Rightarrow$ (3): assumamos (2) e escolhamos elementos x_1, x_2, ..., x_k em A tais que $a \leq x_1 \cup x_2 \cup ... \cup x_k$. Se nenhum dos $a \leq x_1$, $a \leq x_2$, ..., $a \leq x_k$ for verdadeiro, então concluímos, de (2), que $a \leq 1 + x_1$, e $a \leq 1 + x_2$, e ... e $a \leq 1 + x_k$; assim a seria um minorante comum para $1 + x_1$, $1 + x_2$, ..., $1 + x_k$, e consequentemente seria menor ou igual ao seu maior minorante $1 + (x_1 \cup x_2 \cup ... \cup x_k)$ (De Morgan). O elemento a seria então simultaneamente menor ou igual a ambos $x_1 \cup x_2 \cup ... \cup x_k$ e ao seu complementar, o que é impossível uma vez que a é não nulo. Assim (3) está demonstrado.
- (3) $\Rightarrow$ (1): assumamos (3) e seja b um minorante de a. É óbvio que $a \leq b \cup (1 + b) = 1$. Tomando $x_1 = b$ e $x_2 = x_3 = ... = x_k = 1 + b$ em (3),

deduzimos que $a \leq b$ ou $a \leq 1 + b$. No primeiro caso, obtemos $b = a$ e no segundo caso, $b = ab = 0$ (lema 2.27). Demonstramos assim que a é um átomo.

2.4 Homomorfismos, isomorfismos, subálgebras

2.4.1 Homomorfismos e isomorfismos

Geralmente referimo-nos a um homomorfismo de anéis com unidade (ou seja, uma aplicação que preserva a adição e a multiplicação bem como os seus elementos identidade) como um homomorfismo de álgebras booleanas. Daremos definições, exemplos, contra-exemplos e caracterizações em termos de conjuntos ordenados.

Definição 2.35 Sejam $A = \langle A, +, \times, 0, 1\rangle$ e $A' = \langle A', +, \times, 0, 1\rangle$ álgebras booleanas e h uma aplicação de A em A'. Dizemos que h é um **homomorfismo de álgebras booleanas** de A em A' se e só se para todos os elementos x e y de A, tivermos que

$$h(x + y) = h(x) + h(y);$$
$$h(x \times y) = h(x) \times h(y);$$
$$h(1) = 1.$$

A condição $h(0) = 0$ não é parte da definição, uma vez que pode ser deduzida imediatamente a partir da primeira condição (basta fixar $x = y = 0$).

A situação é diferente para o elemento identidade da multiplicação: a terceira relação não é uma consequência da segunda, como mostra o seguinte exemplo: tomemos $A = \wp(\mathbb{N})$ e $A' = \wp(\mathbb{Z})$ com a sua estrutura natural de álgebra booleana e tomemos h para ser a aplicação identidade de A em A (a qual podemos considerar como uma aplicação de A em A' pois $A \subseteq A'$); é muito fácil verificar que as primeiras duas relações acima são satisfeitas, mas a terceira não é uma vez que o elemento identidade da multiplicação em A é $\mathbb{N}$ enquanto em A' é $\mathbb{Z}$.

A noção de homomorfismo aqui definida é nada mais do que a noção geral de homomorfismo para anéis com unidade, especialmente o caso de anéis booleanos. (Deveríamos notar que podem existir homomorfismos de anéis com unidade numa álgebra booleana e um anel com unidade que não é uma álgebra booleana.) Propriedades que estão de acordo para homomorfismos arbitrários de anéis com unidade continuam de acordo, obviamente, para álgebras booleanas: por exemplo, a composição de dois homomorfismos de álgebras booleanas é um homomorfismo de álgebras booleanas.

Lema 2.36 Sejam $A = \langle A, +, \times, 0, 1\rangle$ e $A' = \langle A', +, \times, 0, 1\rangle$ duas álgebras booleanas e h um homomorfismo de álgebras booleanas de A em A'. Então temos:

Para todos os elementos x e y de A,

$$h(x \cap y) = h(x) \cap h(y);$$
$$h(x^C) = (h(x))^C;$$
$$h(x \cup y) = h(x) \cup h(y);$$
$$\text{se } x \leq y, \text{ então } h(x) \leq h(y).$$

Demonstração: Porque as operações $\times$ e $\cap$ são idênticas, a primeira relação é já uma consequência da definição de homomorfismo. A segunda pode ser reescrita como $h(1 + x) = 1 + h(x)$, que é uma consequência imediata de $h(1) = 1$ e da aditividade de h. A terceira relação segue-se das duas primeiras através das leis de De Morgan. Finalmente, a última relação pode ser reescrita como: se $xy = x$, então $h(x)h(y) = h(x)$; e o posterior é verdadeiro pois $h(xy) = h(x)h(y)$.

Teorema 2.37 Sejam $A = \langle A, +, \times, 0, 1\rangle$ e $A' = \langle A', +, \times, 0, 1\rangle$ duas álgebras booleanas e h uma aplicação de A em A'. Para h ser um homomorfismo de álgebras booleanas, é necessário e suficiente que para todos os elementos x e y de A tenhamos que

$$h(x \cap y) = h(x) \cap h(y),$$
$$h(x^C) = (h(x))^C.$$

Demonstração: Que preserva o lema anterior 2.36, a condição é necessária. Suponhamos que é satisfeita e sejam x e y elementos de A. Temos então que:

$$h(xy) = h(x \cap y) = h(x) \cap h(y) = h(x)h(y),$$
$$h(x + y) = h((x \cap y^C) \cup (x^C \cap y)) = h(((x \cap y^C)^C \cap (x^C \cap y)^C)^C)$$
$$= (h((x \cap y^C)^C \cap (x^C \cap y)^C))^C = (h((x \cap y)^C)^C \cap h((x^C \cap y)^C))^C$$

$$= ((h(x \cap y^C))^C \cap (h(x^C \cap y))^C)^C = h(x \cap y^C) \cup h(x^C \cap y)$$
$$= (h(x) \cap h(y^C)) \cup (h(x^C) \cap h(y))$$
$$= (h\,(x) \cap (h(y))^C) \cup ((h(x))^C \cap h\,(y))$$
$$= h(x) + h(y)$$

Segue-se que $h(0) = 0$ e consequentemente que

$$h(1) = h(0^C) = (h(0)\,)^C = 0^C = 1$$

O que mostra que h é um homomorfismo.

É claro que, no teorema anterior, podemos substituir a operação $\cap$ pela operação $\cup$ em todos os lugares.

Definição 2.38 Um **isomorfismo de álgebras booleanas** é um homomorfismo de álgebras booleanas que é bijectivo.

Teorema 2.39 Sejam $A = \langle A, +, \times, 0, 1\rangle$ e $A' = \langle A', +, \times, 0, 1\rangle$ duas álgebras booleanas e h uma aplicação sobrejectiva de A sobre A'. Para h ser um isomorfismo de álgebras booleanas, é necessário e suficiente que

(*) para todos os elementos x e y de A, $x \leq y$ se e só se $h(x) \leq h(y)$.

Demonstração: Primeiro suponhamos que h é um isomorfismo e sejam x e y elementos de A. Se $x \leq y$, então por um lema anterior 2.36, $h(x) \leq h(y)$. Se $h(x) \leq h(y)$, então por definição de $\leq$ e porque h é um homomorfismo, $h(x) = h(x)h(y) = h(xy)$. Mas uma vez que h é injectiva, leva-nos a que $x = xy$ ou seja que $x \leq y$. Assim (*) é satisfeito.

Para provar o inverso, suponhamos (*) e u e v dois elementos de A tais que $h(u) = h(v)$. Temos que $h(u) \leq h(v)$ e $h(v) \leq h(u)$, assim, por (*), $u \leq v$, e $v \leq u$, logo $u = v$. Assim, h é injectiva. De seguida, sejam x e y elementos arbitrários de A. Seja $t = h(x) \cap h(y)$. Uma vez que h é uma bijecção, existe um único elemento z em A tal que $t = h(z)$. Temos $h(z) \leq h(x)$ e $h(z) \leq h(y)$, consequentemente, usando (*), $z \leq x$, e $z \leq y$, e assim $z \leq x \cap y$. Mas uma vez que $x \cap y \leq x$ e $x \cap y \leq y$, temos, e sempre usando (*), que $h(x \cap y) \leq h(x)$ e $h(x \cap y) \leq h(y)$, o que implica que

$$h(x \cap y) \leq h(x) \cap h(y) = h(z).$$

Usando (*) uma vez mais, obtemos $x \cap y \leq z$, e reunindo tudo, $z = x \cap y$, o que prova

$$h(x \cap y) = h(x) \cap h(y).$$

Quando substituímos $\cap$ por $\cup$ e $\leq$ por $\geq$ no argumento anterior, obtemos

$$h(x \cup y) = h(x) \cup h(y).$$

Seja u um elemento arbitrário de A' e seja t a sua única pré-imagem em A sobre h. Em A, temos que $0 \leq t$ e $t \leq 1$. Segue-se, e usando (*), que, em A', $h(0) \leq u$, e $u \leq h(1)$. Isto mostra-nos que $h(0)$ e $h(1)$ são, respectivamente, o menor e o maior elementos de A', ou por outras palavras, que $h(0) = 0$ e $h(1) = 1$.

Assim para todo o elemento x em A, temos que

$$h(x^C) \cap h(x) = h(x^C \cap x) = h(0) = 0 \text{ e}$$

$$h(x^C) \cup h(x) = h(x^C \cup x) = h\,(1) = 1.$$

Além disso $h(x^C)$ é o complementar de $h(x)$, ou por outras palavras,

$$(h(x))^C = h(x^C).$$

Concluímos, usando um teorema anterior 2.37, que h é um homomorfismo de álgebras booleanas.

Corolário 2.40 A composição de dois isomorfismos de álgebras booleanas, tal como o inverso de um isomorfismo de álgebras booleanas, são isomorfismos de álgebras booleanas.

Demonstração: Sejam $A = \langle A, +, \times, 0, 1\rangle$, $B = \langle B, +, \times, 0, 1\rangle$ e $C = \langle C, +, \times, 0, 1\rangle$ álgebras booleanas, seja ϕ um isomorfismo de álgebras booleanas de A sobre B e ψ um isomorfismo de álgebras booleanas de B sobre C. As aplicações ϕ^{-1} e ψ o ϕ são obviamente sobrejectivas. Para todos os elementos u e v de B, $\phi^{-1}(u) \leq \phi^{-1}(v)$ é equivalente a $\phi(\phi^{-1}(u)) \leq \phi(\phi^{-1}(v))$, ou seja para $u \leq v$. Por outro lado, para todos os elementos x e y de A, temos que $x \leq y$ se e só se $\phi(x) \leq \phi(y)$, e $\phi(x) \leq \phi(y)$ se e só se $\psi(\phi(x)) \leq \psi(\phi(y))$. Com o teorema anterior 2.39, concluímos que ϕ^{-1} e ψ o ϕ são isomorfismos de álgebras booleanas, de B sobre A e de A sobre C respectivamente.

Teorema 2.41 Toda a álgebra booleana finita é isomórfica à álgebra booleana de subconjuntos de algum conjunto.

Demonstração: Seja $A = \langle A, +, \times, 0, 1\rangle$ uma álgebra booleana finita e seja E o conjunto dos seus átomos. Note-se que E é não vazio uma vez que existe pelo menos um átomo que é menor ou igual ao elemento não nulo1 (teorema 2.33). Mostraremos que A é isomorfo à álgebra de subconjuntos de E.

Para isto, consideremos a aplicação h de A em $\wp$(E), a qual, a cada elemento x de A, associa o conjunto de átomos que estão abaixo de x:

para cada $x \in$ A, $h(x) = \{a \in$ E: a é um átomo e $a \leq x\}$.

- h é sobrejectiva: realmente, em primeiro lugar temos $h(0) = \varnothing$ (não existe nenhum átomo abaixo de 0); como tal, seja X = $\{a_1, a_2, ..., a_k\}$ um subconjunto não vazio de E e seja $M_X = a_1 \cup a_2 \cup ... \cup a_k$; assumimos que $h(M_X) = X$: a inclusão $X \subseteq h(M_X)$ segue-se imediatamente conforme a definição de h (todo o elemento de X é um átomo que está abaixo de M_X); a inclusão inversa é provada usando um teorema anterior 2.34: se a é um elemento de $h(M_X)$, ou seja, um átomo que está abaixo de $M_X = a_1 \cup a_2 \cup ... \cup a_k$, então temos que $a \leq a_i$; para pelo menos um índice i (isto é claro se $k = 1$ e esta é a cláusula (3) do teorema se $k \geq 2$), mas uma vez que a e a_i são átomos, requer que $a = a_i$, e assim $a \in$ X.
- Para todos os elementos x e y de A, se $x \leq y$, então $h(x) \leq h(y)$: de facto, se $x \leq y$, todo o átomo que está abaixo de x é um átomo que está abaixo de y.
- Para todos os elementos x e y de A, se $h(x) \subseteq h(y)$, então $x \leq y$: de facto, se x não é menor ou igual que y, então $x(1 + y) \neq 0$ (pelo lema 2.27). Como A é finito, é atómico (teorema 2.33), assim podemos encontrar um átomo $a \in$ E tal que $a \leq x(1 + y)$. O átomo a está assim abaixo de x e $1 + y$; não pode estar abaixo de y uma vez que é não nulo. Então temos que $a \in h(x)$ e $a \notin h(y)$, o que nos mostra que $h(x)$ não está incluído em $h(y)$.

Podemos concluir agora, pelo teorema 2.39, que h é um isomorfismo de Álgebras booleanas de A sobre $\wp$(E).

Corolário 2.42 A cardinalidade de qualquer álgebra booleana finita é uma potência de 2.

Demonstração: Se o conjunto finito E tem cardinalidade n, então o conjunto dos seus subconjuntos, $\wp$(E), tem cardinalidade 2^n.

2.4.2 Subálgebras booleanas

Definição 2.43 Seja $A = \langle$A, +, ×, 0, 1$\rangle$ uma álgebra booleana. Um subconjunto B de A constitui uma **subálgebra booleana** de A se e só se B contém os elementos 0 e 1 e é

fechado para as operações + e × (por outras palavras, $0 \in$ B, $1 \in$ B, e se $x \in$ B e $y \in$ B, então $x + y \in$ B e $xy \in$ B).

Uma subálgebra booleana de *A* é assim um subanel de *A* que contém o elemento 1. Esta distinção é essencial: num anel com unidade, um subanel pode ser um anel com unidade sem conter o elemento unidade de todo o anel: neste caso, o papel do elemento identidade para a multiplicação é representado por outros elementos. Reexaminemos o anel $(\wp(\mathbb{Z}), \Delta, \cap, \varnothing, \mathbb{Z})$: $\wp(\mathbb{N})$ é um subconjunto que é fechado para as operações Δ e $\cap$ e contém o $\varnothing$; é então um subanel de $\wp(\mathbb{Z})$. Obviamente, $\mathbb{Z} \notin \wp(\mathbb{N})$. Todavia, $\mathbb{N}$ é o elemento identidade para o anel $\wp(\mathbb{N})$. Assim o anel booleano $\wp(\mathbb{N})$ é um anel com unidade e é um subanel de $\wp(\mathbb{Z})$, mas não é uma subestrutura de $\wp(\mathbb{Z})$ um anel com unidade: não é então uma subálgebra booleana de $\wp(\mathbb{Z})$.

Teorema 2.44 Seja $A = \langle A, +, \times, 0, 1\rangle$ uma álgebra booleana e seja B um subconjunto de A. Para B ser uma subálgebra de *A*, é necessário e suficiente que exista uma álgebra booleana $A' = \langle A', +', \times', 0', 1'\rangle$ e um homomorfismo de álgebras booleanas, *h*, de *A*' em *A* tal que a imagem da aplicação *h* é o subconjunto B.

Demonstração:

- É necessário: tomemos A' = B, +' = +, ×' = ×, 0' = 0, 1' = 1, e *h* = a aplicação identidade de B em A. É imediato verificar que *h* é um homomorfismo de álgebras booleanas cuja imagem é B.
- É suficiente: escolhamos *A*' e *h* como indicado. Temos que $h(0') = 0$, consequentemente $0 \in$ B, e $h(1') = 1$, assim $1 \in$ B. Além disso, se *x* e *y* são elementos de B, então podemos escolher elementos *x*' e *y*' em A' tais que $x = h(x')$ e $y = h(y')$. Temos então que

  $x + y = h(x') + h(y') = h(x' + y')$, consequentemente $x + y \in \mathrm{Im}(h) =$ B; e

  $xy = h(x')h(y') = h(x'y')$, consequentemente $xy \in \mathrm{Im}(h) =$ B.

  Assim B é uma subálgebra booleana de *A*.

Teorema 2.45 Numa álgebra booleana $A = \langle A, +, \times, 0, 1\rangle$, para um subconjunto B ser uma subálgebra booleana, é necessário e suficiente que B contenha 0 e seja fechado para as operações $x \mapsto x^C$ e $(x, y) \mapsto x \cap y$.

Demonstração:

- É necessário: uma vez que $x^C = 1 + x$ e $x \cap y = xy$, e pois B contenha 0 e 1 e seja fechado para + e ×, o resultado é imediato.
- É suficiente: para todo x e y em A temos que $x \cup y = (x^C \cap y^C)^C$. Assim, o facto de B ser fechado para a complementação e ∩ garante o seu fecho para ∪. Além disso, $1^C = 0$ deve pertencer a B. Uma vez que as operações + e × podem ser definidas exclusivamente em termos de ∩, ∪, e complementação, concluímos que B é fechado para as operações + e × e que $\langle B, +, \times, 0, 1\rangle$ é uma subálgebra booleana de *A*.

Vejamos, agora, dois exemplos.

1) Seja E um conjunto infinito, seja A = $\wp$(E) o conjunto de todos os seus subconjuntos, e seja B o subconjunto de A consistindo desses subconjuntos de E que são finitos ou cujos complementares são finitos. Mostra-se, usando o teorema precedente, que B é uma subálgebra booleana da álgebra booleana de subconjuntos de E.

Demonstração: Um subconjunto de E cujo complementar seja finito será chamado cofinito. O conjunto vazio que é um subconjunto finito de E pertence a B. É claro que B é fechado para a complementação: o complementar de um subconjunto finito de E é um subconjunto cofinito e o complementar de um conjunto cofinito é finito. Também, B é fechado para ∩: de facto, a intersecção de um subconjunto finito de E com qualquer subconjunto de E é um subconjunto finito de E; como para a intersecção de dois subconjuntos cofinitos de E, este também é um subconjunto cofinito de E: para ver isto, suponhamos que U ⊆ E e V ⊆ E são cofinitos; isto significa que E – U e E – V são finitos e consequentemente, assim é a sua união (E – U) ∪ (E – V) que é simplesmente E – (U ∩ V); segue-se que U ∩ V é cofinito.

2) Seja X um espaço topológico e seja *B*(X) o subconjunto de $\wp$(X) consistindo de subconjuntos de X que são ambos abertos e fechados na topologia em X. Este conjunto *B*(X) é uma subálgebra booleana da álgebra booleana de subconjuntos de X.

Demonstração: Em primeiro lugar, o conjunto vazio (0) e todo o espaço X (1) são eles próprios abertos e fechados. Logo, o complementar de um conjunto aberto e fechado é aberto e fechado e a intersecção de dois conjuntos abertos e fechados é aberta e fechada. Por um teorema anterior, 2.45, chegamos à conclusão pretendida.

Pode acontecer que a álgebra booleana $B(X)$ aqui considerada seja reduzida a $\{0,1\}$ (é o caso, por exemplo, quando X é o espaço $\mathbb{R}$ com a sua topologia habitual: $\varnothing$ e $\mathbb{R}$ são os únicos subconjuntos que são simultaneamente abertos e fechados); $B(X)$ também pode coincidir com $\wp(X)$ (quando a topologia em X é a topologia discreta - a topologia na qual todos os subconjuntos são abertos - e, obviamente, só neste caso).

Consideremos agora dois exemplos de homomorfismos de álgebras booleanas.
1) Consideremos a álgebra booleana $F/\sim$ de classes de equivalência de fórmulas logicamente equivalentes do cálculo proposicional construídas a partir de um conjunto de variáveis P. Escolhamos uma atribuição δ de valores lógicos em P e como sempre seja $\bar{\delta}$ representando a extensão de δ no conjunto F de todas as fórmulas. Podemos então definir uma aplicação h_δ de $F/\sim$ em $\{0,1\}$ fixando, para todas as fórmulas F,

$$h_\delta(\mathrm{cl}(F)) = \bar{\delta}(F).$$

Esta definição é legítima visto que $\bar{\delta}(F)$ assume o mesmo valor em todas as fórmulas numa dada classe de equivalência.

Esta aplicação, h_δ, é um homomorfismo de álgebras booleanas de $F/\sim$ em $\{0,1\}$. Em virtude de um Teorema anterior, 2.37, e das definições das operações para a álgebra booleana $F/\sim$, é suficiente que para todas as fórmulas F e G em F, temos que

$$h_\delta(\mathrm{cl}(F \wedge G)) = h_\delta(\mathrm{cl}(F)\ )\ h_\delta(\mathrm{cl}(G)) \text{ e}$$

$$h_\delta(\mathrm{cl}(\neg F)) = 1 - h_\delta(\mathrm{cl}(F)).$$

Agora estas relações são equivalentes a

$$\bar{\delta}(F \wedge G) = \bar{\delta}(F)\ \bar{\delta}(G) \text{ e}$$

$$\bar{\delta}(\neg F) = 1 - \bar{\delta}(F),$$

que são verdadeiras por definição de $\bar{\delta}$.

2) Seja $A = \langle A, +, \times, 0, 1\rangle$ uma álgebra booleana e seja a um átomo nesta álgebra (estamos a supor que existe). Definamos uma aplicação h_a de A em {0,1} por

$$h_a(x) = \begin{cases} 1 \text{ se } x \in A \text{ e } a \leq x \\ 0 \text{ se } x \in A \text{ e } a \leq 1 + x \end{cases}$$

(estes dois casos são mutuamente exclusivos pois $a \neq 0$, e não existem outros casos pois a seja um átomo).

Teorema 2.46 h_a é um homomorfismo de álgebras booleanas de A em $\{0,1\}$.

Demonstração: Para provar isto, usaremos um Teorema anterior (2.37): sejam x e y dois elementos de A. Temos que $h_a(x \cap y) = 1$ se e só se $a \leq x \cap y$, mas isto é equivalente, pela definição de ínfimo, a $a \leq x$ e $a \leq y$, e consequentemente a $h_a(x) = 1$ e $h_a(y) = 1$, o que é necessário e suficiente para $h_a(x) \cap h_a(y) = 1$. Segue-se que

$$h_a(x \cap y) = h_a(x) \cap h_a(y).$$

Também, $h_a(x^C) = 1$ se e só se $a \leq x^C$, ou seja que $a \leq 1 + x$, o que é equivalente a $h_a(x) = 0$. Uma vez que h_a apenas assume os valores 0 ou 1, isto significa que

$$h_a(x^C) = (h_a(x))^C.$$

2.5 Ideais e filtros

2.5.1 Propriedades dos ideais

Teorema 2.47 Seja $A = \langle A, \leq, 0, 1\rangle$ uma álgebra booleana e I um subconjunto de A. Para I ser um ideal, é necessário e suficiente que as seguintes três condições sejam satisfeitas:

(i) $0 \in I$ e $1 \notin I$;

(ii) para todos os elementos x e y de I, $x \cup y \in I$;

(iii) para todo o $x \in I$ e para todo o $y \in A$, se $y \leq x$, então $y \in I$.

Demonstração: Suponhamos que I é um ideal. Então, em particular, é um subgrupo do grupo $\langle A, +, 0\rangle$, então $0 \in I$. Se 1 estivesse em I, então I seria todo o anel e excluímos este caso; assim (i) é verificado. Se x e y estão em I, então também está o seu produto xy e, por conseguinte, a soma $x + y + xy = x \cup y$, o que prova (ii). Finalmente,

verifiquemos (iii): se $x \in I$ e $y \in$ A, então $xy \in I$ e se $y \leq x$, então $xy = y$ e, consequentemente, $y \in I$.

Reciprocamente, suponhamos que (i), (ii), e (iii) são satisfeitos. Temos que mostrar que I é um ideal de A. Se $x \in I$ e $y \in I$, então $x \cup y \in I$ por (ii), mas uma vez que $x + y \leq x \cup y$ e uma vez que $x + y = x - y$ (estamos numa álgebra booleana), concluímos usando (iii) que $x - y \in I$. Como $0 \in I$, temos tudo o que precisamos para $\langle I , +, 0\rangle$ ser um subgrupo de $\langle$A, +, 0$\rangle$. Além disso, se $x \in I$ e $y \in$ A, então uma vez que $xy \leq x$, podemos concluir de (iii) que $xy \in I$. O conjunto I é então um ideal em A ($I \neq$ A pois $1 \notin I$).

Corolário 2.48 Se I é um ideal numa álgebra booleana $\langle$A, +, ×, 0, 1$\rangle$, então não existe nenhum elemento x em A que possa satisfazer simultaneamente $x \in I$ e $1 + x \in I$.

Demonstração: Se o ideal I contém x e $1 + x$, também contém o elemento $x \cup (1 + x) = 1$ (invocando a propriedade (ii) do teorema 2.47). Mas isto não é possível uma vez que $1 \notin I$ (propriedade (i)).

Corolário 2.49 Seja $A = \langle$A, +, ×, 0, 1$\rangle$ um anel booleano e seja I um ideal em A. Para qualquer inteiro $k \geq 1$ e quaisquer elementos $x_1, x_2 ..., x_k$ em I, o supremo $x_1 \cup x_2 \cup ... \cup x_k$ pertence a I.

Demonstração: Esta é uma generalização da propriedade (ii) do teorema 2.47; a demonstração é imediata através de indução sobre o inteiro k (o caso $k = 1$ não necessita nenhum argumento).

Vejamos mais alguns exemplos:

(1) Se E é um conjunto infinito, o conjunto $\wp_f$(E) de subconjuntos finitos de E é um ideal na álgebra booleana $\wp$(E). São fáceis de verificar as condições (i), (ii), e (iii) do teorema: ∅ é um subconjunto finito de E enquanto o próprio E não é, a união de dois subconjuntos finitos de E é um subconjunto finito de E, e qualquer subconjunto de um subconjunto finito de E é um subconjunto finito de E.

(2) Seja $A = \langle$A, +, ×, 0, 1$\rangle$ uma álgebra booleana e seja a um elemento de A diferente de 1. O conjunto $I_a = \{x \in$ A: $x \leq a\}$ é um ideal em A. Também a verificação das propriedades (i), (ii), e (iii) é imediata: temos $0 \leq a$ e pois a seja diferente de 1, não

temos que $1 \leq a$; se $x \leq a$ e $y \leq a$, então $x \cup y \leq a$; finalmente, se $x \leq a$ e $y \leq x$, então $y \leq a$. I_a define-se como o ideal primo gerado por a. Isto está que preserva a definição habitual de um ideal primo num anel comutativo arbitrário pois, num anel booleano, o conjunto de elementos de um determinado elemento seja também o conjunto dos seus múltiplos.

(3) Em qualquer álgebra booleana, {0} é obviamente um ideal.

Lema 2.50 Para qualquer anel booleano $A = \langle A, +, \times, 0, 1\rangle$ e para qualquer ideal I em A, o anel quociente A/I é um anel booleano.

Demonstração: Para cada elemento x em A, seja $\bar{x}$ o representante da classe de equivalência de x modulo I. Já sabemos que A/I é um anel com unidade. Assim é suficiente mostrar que todo o elemento é um idempotente para a multiplicação. Mas esta é uma consequência imediata da definição de multiplicação em A/I e do facto de A ser uma álgebra booleana: se $x \in$ A, $\bar{x}^2 = \overline{x^2} = \bar{x}$.

Recorde-se que num anel comutativo arbitrário com unidade, os ideais são justamente os núcleos de homomorfismos de anéis com unidade definida no anel. O teorema que se segue traduz este resultado para anéis booleanos, com mais precisão: mostra-nos que os ideais num anel booleano são precisamente os núcleos de homomorfismos de álgebras booleanas definidas no anel.

Teorema 2.51 Seja $A = \langle A, +, \times, 0, 1\rangle$ um anel booleano e seja I um subconjunto de A. As seguintes propriedades são equivalentes:

(1) I é um ideal em A;

(2) existe um homomorfismo de álgebras booleanas, h, definido em A cujo núcleo é I (por outras palavras),

$$I = h^{-1}[\{0\}] = \{x \in A: h(x) = 0\};$$

(3) existe um homomorfismo de anéis comutativos com unidade definidos em A cujo núcleo é I.

Demonstração: A equivalência de (1) e (3) é um resultado da observação precedente; (2) $\Rightarrow$ (3) verifica-se uma vez que, por hipótese, $I = h^{-1}[\{0\}] = \{x \in A: h(x) = 0\}$, e como já foi dito acima, num anel comutativo arbitrário com unidade os ideais são os núcleos de homomorfismos de anéis com unidade, logo existe um homomorfismo de

anéis comutativos com unidade definidos em A. Provaremos todavia que (3) $\Rightarrow$ (1) e que (1) $\Rightarrow$ (2) que é, como observado acima, mais precisamente que (1) $\Rightarrow$ (3) (resulta da transitividade da implicação, uma vez que temos por hipótese (1) $\Rightarrow$ (2) e (2) $\Rightarrow$ (3) logo (1) $\Rightarrow$ (3)).

- (3) $\Rightarrow$ (1): suponhamos que existe um homomorfismo h de A num anel com unidade $B = \langle B, +, \times, 0, 1\rangle$ tal que $I = h^{-1}[\{0\}] = \{x \in A: h(x) = 0\}$. Verifiquemos que as propriedades (i), (ii), e (iii) do Teorema 2.47 são satisfeitas.

  Temos que $h(0) = 0$ e $h(1) = 1$, consequentemente $0 \in I$ e $1 \notin I$. Se $x \in I$ e $y \in I$, então $h(x) = 0$ e $h(y) = 0$, assim

$$h(x \cup y) = h\,(x + y + xy) = h(x) + h(y) + h(x)h(y) = 0$$

  e assim $x \cup y \in I$. Finalmente, se $x \in I$, $y \in A$, e $y \leq x$, então $h(x) = 0$ e $xy = y$, consequentemente $h(y) = h(x)h(y) = 0$, ou seja que $y \in I$.

  Assim, I é um ideal de A.

- (1) $\Rightarrow$ (2): suponhamos que I é um ideal em A e consideremos a aplicação h de A em A/I a qual, a cada elemento x, associa a sua classe de equivalência, $\bar{x}$, modulo I. h é um homomorfismo de álgebras booleanas: para vermos isto, invocamos um Teorema anterior, 2.37; se $x \in A$ e $y \in A$, então

$$h(x \cap y) = h(xy) = \overline{xy} = \bar{x} \times \bar{y} = h(x) \times h(y) = h(x) \cap h(y) \text{ e}$$

$$h(x^C) = h(1 + x) = \overline{1 + x} = \bar{1} + \bar{x} = \bar{1} + h(x) = (h(x))^C.$$

Também, é claro que $I = \bar{0} = \{x \in A: h(x) = \bar{0}\}$: I é o núcleo de h.

2.5.2 Ideais maximais

De seguida apresentamos uma colecção de formas para caracterizar ideais maximais numa álgebra booleana:

Teorema 2.52 Para todo o anel booleano $A = \langle A, +, \times, 0, 1\rangle$, para todo o ideal I em A, e para todo o inteiro $k \geq 2$, as seguintes propriedades são equivalentes:

(1) I é um ideal maximal;

(2) A/I é isomorfo à álgebra booleana {0,1};

(3) I é o núcleo de um homomorfismo de A em {0,1};

(4) para todo o elemento x em A, $x \in I$ ou $1 + x \in I$;

(5) para todos os elementos x e y de A, se $xy \in I$, então $x \in I$ ou $y \in I$;

(6) para todos os elementos $x_1, x_2 ..., x_k$ em A, se $x_1 x_2 ... x_k \in I$, então $x_1 \in I$ ou $x_2 \in I$ ou ... ou $x_k \in I$.

Demonstração:

- (1) $\Rightarrow$ (2): Na Secção 1, recordamos que se o ideal I é maximal, então o anel quociente A/I é um corpo. Mas observamos também que o único anel booleano que é um corpo é {0,1}. Assim, o resultado segue-se usando um Lema anterior, 2.50.
- (2) $\Rightarrow$ (3): Basta notar que I é sempre o núcleo de um homomorfismo canónico h de A em A/I. Se existir um isomorfismo ϕ de A/I sobre {0,1}, então I obviamente será o núcleo do homomorfismo ϕ o h de A em {0,1}.
- (3) $\Rightarrow$ (4): Consideremos um homomorfismo h de A em {0,1} cujo núcleo é I e seja x um elemento arbitrário de A. Temos que $h(x) = 0$ ou $h(x) = 1$. No primeiro caso, $x \in I$; no segundo caso, temos que $1 + h(x) = 0$, assim $h(1 + x) = 0$ e $1 + x \in I$.
- (4) $\Rightarrow$ (5): Sejam x e y elementos de A tais que $x \notin I$ e $y \notin I$. Se (4) se verificar, então $1 + x \in I$ e $1 + y \in I$, assim $(1 + x) \cup (1 + y) \in I$, propriedade (ii) do teorema 2.47. Mas

  $$(1 + x) \cup (\mathrm{l} + y) = 1 + (x \cap y) = \mathrm{l} + xy,$$

  assim, pelo corolário 2.48, $xy \notin I$, e assim (5) está provado.
- (5) $\Rightarrow$ (1): Suponhamos que I não é maximal. Seja J um ideal de A que inclui estritamente I e seja a um elemento de J que não pertence a I. Usando um Corolário anterior, 2.48, $1 + a \notin J$, e assim $1 + a \notin I$ uma vez que $I \subseteq J$. O ideal I nem contém a nem $1 + a$, mas contém obviamente o produto $a(1 + a) = 0$. Concluímos que (5) não é satisfeito.
- (5) $\Rightarrow$ (6): Assumimos que (5) é satisfeito e discutimos através de indução sobre o inteiro k. Para $k = 2$, (6) coincide com (5). Assumindo que (6) se verifica para k, provaremos que é satisfeito para $k + 1$. Sejam x_1, x_2, ..., x_k, x_{k+1} elementos de A tais que $x_1 x_2 ... x_k x_{k+1} \in I$. Por (5) temos que ter qualquer um $x_1 x_2 ... x_k \in I$ ou $x_{k+1} \in I$. Em primeiro lugar, pela hipótese de indução,

temos $x_1 \in I$ ou $x_2 \in I$ ou ... ou $x_k \in I$. Concluímos então que temos que ter $x_i \in I$ para pelo menos um índice i tal que $1 \leq i \leq k + 1$; isto prova (6) para $k + 1$.

- (6) $\Rightarrow$ (5): Sejam x e y dois elementos de A tais que $xy \in I$. Fixemos $x_1 = x$ e $x_2 = x_3 = ... = x_k = y$. Assim temos que $x_1x_2 ... x_k = xy \in I$. Assim se (6) é verdadeiro, temos que ter $x_i \in I$ para pelo menos um índice i entre l e k; então ou $x \in I$ ou $y \in I$ e (5) é verificado.

Num anel comutativo arbitrário, um ideal com a propriedade (5) do teorema anterior define-se como um **ideal primo**. Prova-se que os ideais principais são iguais aos ideais maximais. Mas há anéis para os quais isto não é verdade. O que é sempre verdade é que um ideal é principal se e só se o anel quociente associado é um domínio de integridade; daqui concluímos que um ideal maximal necessariamente tem de ser principal (basta considerar o anel quociente correspondente). No entanto, também pode falhar (por exemplo, no anel $\mathbb{R}$ [X, Y] de polinómios de duas variáveis com coeficientes reais: o ideal gerado pelo polinómio X, ou seja, o conjunto {XP: P $\in$ $\mathbb{R}$ [X, Y]} é principal mas não é maximal uma vez que está estritamente incluído no ideal gerado pelos polinómios X e Y, ou seja, o conjunto {XP +YQ: P $\in$ $\mathbb{R}$ [X, Y], Q $\in$ $\mathbb{R}$ [X, Y]}).

Em particular, deveríamos tomar nota da equivalência entre as propriedades (1) e (3). Observe-se que se dois homomorfismos h e g de uma álgebra booleana $A = \langle A, +, \times, 0, 1\rangle$ em {0,1} têm o mesmo núcleo, I, então são iguais: porque para qualquer elemento x em A, ou $x \in I$ e $g(x) = h(x) = 0$ ou então $x \notin I$ e $g(x) = h(x) = 1$. Daqui podemos concluir que existe uma bijecção entre o conjunto de ideais maximais numa álgebra booleana e o conjunto de homomorfismos de álgebras booleanas desta álgebra para {0,1}.

2.5.3 Filtros

Introduziremos agora a noção de dual de um ideal numa álgebra booleana: definiremos então filtros.

Definição 2.53 Um **filtro numa álgebra booleana** $A = \langle A, +, \times, 0, 1\rangle$ é um subconjunto F de A tal que o conjunto

$$\{x \in A : x^C \in F\}$$

é um ideal em *A*.

Seja F um filtro numa álgebra booleana $A = \langle A, +, \times, 0, 1\rangle$. Seja *I* o ideal $\{x \in A: x^C \in F\}$. *I* é tomado como a imagem inversa de F para a operação de complementação: $x \mapsto x^C$. Mas, como esta operação é uma involução, ver teorema 2.26 (9), *I* é também a imagem directa de F desta operação: $I = \{x \in A: \exists_y (y \in F \text{ e } x = y^C)\}$. Por outras palavras, *I* é o conjunto dos complementares dos elementos de F e F é o conjunto dos complementares dos elementos de *I*. O ideal *I* define-se como o ideal dual do filtro F. É fácil ver que, dado um ideal arbitrário *J* em *A*, o conjunto $G = \{x \in A: x^C \in J\}$ é um filtro cujo ideal dual é precisamente *J*. Chamaremos a *G* o **filtro dual** do ideal *J*. Existe assim uma bijecção entre o conjunto de ideais e o conjunto de filtros numa álgebra booleana.

Teorema 2.54 Seja $A = \langle A, \leq, 0, 1\rangle$ uma álgebra booleana e F um subconjunto de A. Para F ser um filtro, é necessário e suficiente que as três condições seguintes sejam satisfeitas:

(f) $0 \notin F$ e $1 \in F$;

(ff) para todos os elementos *x* e *y* de F, $x \cap y \in F$;

(fff) para todo o $x \in F$ e para todo o $y \in A$, se $y \geq x$, então $y \in F$.

Demonstração: Seja $I = \{x \in A: x^C \in F\}$. Se F é um filtro, então *I* é o seu ideal dual e as condições (i), (ii), e (iii) de um Teorema anterior, 2.47, estão satisfeitas. Assim, temos que $0 \in I$, consequentemente $0^C = 1 \in F$, e $1 \notin I$, consequentemente $1^C = 0 \notin F$, o que prova (f). Se $x \in F$ e $y \in F$, então $x^C \in I$ e $y^C \in I$, então $x^C \cup y^C \in I$ (por (ii)), e, como $x^C \cup y^C = (x \cap y)^C$, concluímos que $x \cap y \in F$ e que (ff) é satisfeito. Finalmente,

se $x \in$ F, $y \in$ A, e $y \geq x$, então $x^C \in I$ e $y^C \leq x^C$, assim, (por (iii)) $y^C \in I$ e $y \in$ F, consequentemente (fff).

Reciprocamente, de uma forma estritamente análoga, (i) segue-se de (f), (ii) de (ff) e (iii) de (fff).

Corolário 2.55 Seja $A = \langle A, \leq, 0, 1\rangle$ uma álgebra booleana e F um subconjunto de A. Para qualquer inteiro $k \geq 1$ e quaisquer elementos $x_1, x_2 ..., x_k$ em F, o ínfimo $x_1 \cap x_2 \cap ... \cap x_k$ pertence a F.

2.5.4 Ultrafiltros

Definição 2.56 Numa álgebra booleana, um **ultrafiltro** é um filtro maximal, ou seja, um filtro que não está estritamente incluído em qualquer outro filtro.

É claro que, devido à dualidade explicada anteriormente, os ultrafiltros correspondem a ideais maximais. Por outras palavras, o filtro dual de um ideal maximal é um ultrafiltro e o ideal dual de um ultrafiltro é um ideal maximal.

Teorema 2.57 Para todo o anel booleano $A = \langle A, +, \times, 0, 1\rangle$, para todo o ideal F em *A*, e para todo o inteiro $k \geq 2$, as seguintes propriedades são equivalentes:

(1') F é um ultrafiltro;

(3') existe um homomorfismo *h* de *A* em {0,1} tal que

$$F = \{x \in A : h(x) = 1\};$$

(4') para todo o elemento *x* em A, $x \in$ F ou $1 + x \in$ F;

(5') para todos os elementos *x* e *y* de A, se $x \cup y \in$ F, então $x \in$ F ou $y \in$ F;

(6') para todos os elementos $x_1, x_2 ..., x_k$ em A, se $x_1 \cup x_2 \cup ... \cup x_k \in$ F, então $x_1 \in$ F ou $x_2 \in$ F ou ... ou $x_k \in$ F.

Demonstração: Dada a álgebra *A*, o filtro F e o inteiro *k*, seja *I* o representante do ideal dual de F. É elementar verificar que as propriedades (1'), (3'), (4'), (5') e (6') para o filtro F são respectivamente equivalentes às propriedades (1), (3), (4), (5), e (6) do Teorema de ideais maximais para o ideal *I*.

O “ou” da propriedade (4) do Teorema de ideais maximais, 2.52, bem como a alínea (4') das propriedades anteriores, é de facto um “ou exclusivo”, corolário 2.48. Isto significa que, se F é um ultrafiltro numa álgebra booleana $\langle A, +, \times, 0, 1\rangle$ e se *I* é o ideal maximal dual para F, então *I* e F constituem uma partição de A. Assim cada um dos conjuntos *I* e F é simultaneamente:

- o complementar do outro (vistos como subconjuntos de A),
- o conjunto de complementares dos elementos do outro (no sentido de complementação na álgebra booleana considerada).

A segunda destas propriedades aparece sempre que temos um ideal e um filtro que são dual um do outro, mas a primeira só aparece quando o ideal e o filtro em questão são maximais.

Podemos agora insistir no facto de que para uma álgebra booleana, *A*, existem correspondências de um para um canónicas sobre (i) o ideal maximal em *A*, (ii) os ultrafiltros em *A* e (iii) os homomorfismos de álgebras booleanas de *A* para {0,1}.

Para ter exemplos de filtros, basta obviamente referirmo-nos aos exemplos previamente descritos de ideais e transformá-los por dualidade. Assim,

(1) Se E é um conjunto infinito, o conjunto de todos os subconjuntos cofinitos de E é um filtro na álgebra booleana $\langle \wp(E), \subseteq, \varnothing, E\rangle$. Este filtro define-se como o filtro de Fréchet em E. Não é um ultrafiltro, uma vez que existem subconjuntos de E que são infinitos e cujos complementares são também infinitos, assim a condição (4') do Teorema dos ultrafiltros, 2.57, não é satisfeita.

(2) Se *a* é um elemento não nulo duma álgebra booleana $\langle A, \leq, 0, 1\rangle$, o conjunto $F_a = \{x \in A : x \geq a\}$ é um filtro chamado o filtro principal gerado por *a*. É o filtro dual do ideal gerado por 1 + *a*.

(3) O conjunto {1} é o filtro dual do ideal {0}.

Teorema 2.58 Seja $\langle A, \leq, 0, 1\rangle$ uma álgebra booleana e seja *a* um elemento não nulo de A. Para o filtro principal gerado por *a* ser um ultrafiltro, é necessário e suficiente que *a* seja um átomo.

Demonstração: Em virtude de um Teorema anterior, 2.34, e da definição do filtro F_a, a é um átomo se e só se para todo o elemento x de A, $x \in F_a$ ou $1 + x \in F_a$; mas para isto acontecer, é necessário e suficiente que F_a seja um ultrafiltro, teorema 2.57.

Quando o filtro principal F_a gerado por um elemento não nulo a de A é um ultrafiltro (ou seja, quando a é um átomo), dizemos que é um ultrafiltro trivial. O homomorfismo h_a com valores em $\{0,1\}$ que é associado também define-se como um homomorfismo trivial. É definido por: $h_a(x) = 1$ se $x \in F_a$ e $h_a(x) = 0$ se $x \notin F_a$, e como isto é obviamente equivalente a: $h_a(x) = 1$ se $a \leq x$ e $h_a(x) = 0$ se $a \leq 1 + x$, vemos que o que é envolvido é precisamente o homomorfismo já estudado num Exemplo anterior.

Lema 2.59 Seja A uma álgebra booleana e seja U um ultrafiltro em A. Para U ser trivial, é necessário e suficiente que contenha pelo menos um átomo.

Demonstração: Se U é trivial, é gerado por um átomo, a, e uma vez que $a \leq a$, $a \in U$.

Reciprocamente, se U contém um átomo, b, também contém todos os elementos maiores ou iguais que b, teorema 2.54 (fff). Segue-se que o filtro principal F_b gerado por b está incluído em U. Mas uma vez que b é um átomo, F_b é maximal e não pode estar estritamente incluído no filtro U. Consequentemente $U = F_b$ e U é um ultrafiltro trivial.

Lema 2.60 Seja E um conjunto infinito e seja U um ultrafiltro na álgebra booleana $\wp(E)$. Para U ser não trivial, é necessário e suficiente que inclua o filtro de Fréchet em E.

Demonstração: Os átomos de $\wp(E)$ são os conjuntos singulares (subconjuntos que consistem apenas de um único elemento): assim são conjuntos finitos. Se U inclui o filtro de Fréchet, todo subconjunto cofinito de E pertence a U, uma vez que nenhum subconjunto finito de E pode pertencer a U (U não pode conter simultaneamente um subconjunto de E e o seu complementar). Em particular, nenhum átomo pode pertencer a U. Segue-se, pelo lema precedente, 2.59, que U é não trivial.

Se U não inclui o filtro de Fréchet, podemos escolher um subconjunto cofinito X de E que não pertence a U, e consequentemente cujo complementar E − X pertence a U. Como E é o elemento identidade da álgebra booleana $\wp(E)$, $E \in U$; consequentemente

$X \neq E$. O complementar de X em E é assim um subconjunto finito não vazio de E: por exemplo, $E - X = \{\alpha_1, \alpha_2, ..., \alpha_n\}$ ($n \geq 1$). Assim temos que $(\alpha_1, \alpha_2, ..., \alpha_n) \in U$, que é também dizer:

$$\{\alpha_1\} \cup \{\alpha_2\} \cup ... \cup \{\alpha_n\} = \{\alpha_1\} \cup \{\alpha_2\} \cup ... \cup \{\alpha_n\} \in U.$$

Se $n = 1$, $\{\alpha_1\} \in U$. Se $n \geq 2$, então por uma propriedade anterior, teorema 2.57 (6′), temos que $\{\alpha_i\} \in U$ para pelo menos um índice i entre 1 e n. Vemos que em qualquer caso, U contém um conjunto singular, ou seja, um átomo. O lema precedente, 2.59, mostra-nos então que U é trivial.

2.5.5 Bases de filtros

Definição 2.61 Numa álgebra booleana $\langle A, \leq, 0, 1\rangle$, uma **base para um filtro** (base de filtro) é um subconjunto de A que tem a seguinte propriedade, conhecida como a propriedade da intersecção finita: todo o subconjunto não vazio finito de B tem ínfimo não nulo.

Por outras palavras, $B \subseteq A$ é uma base de filtro se e só se: para qualquer inteiro $k \geq 1$ e quaisquer elementos $x_1, x_2 ..., x_k$ de B, $x_1 \cap x_2 \cap ... \cap x_k \neq 0$.

Lema 2.62 Seja $\langle A, \leq, 0, 1\rangle$ uma álgebra booleana e seja X um subconjunto de A. Para a existência de um filtro em A que inclua X, é necessário e suficiente que X seja uma base de filtro.

Demonstração: Se X está incluído num filtro F, e se $x_1, x_2 ..., x_k$ são elementos de X, então o ínfimo $x_1 \cap x_2 \cap ... \cap x_k$ pertence a F, pelo corolário 2.55, e como $0 \notin$ F, este ínfimo é não nulo; assim X é uma base de filtro.

Agora suponha-se que X é uma base de filtro.

- Se $X = \varnothing$, $\{1\}$ é um filtro em A que inclui X.
- Se X não é vazio, consideremos

$$F_X = \{x \in A: (\exists k \in \mathbb{N}^*) (\exists x_1 \in X)(\exists x_2 \in X) ... (\exists x_k \in X) (x \geq x_1 \cap x_2 \cap ... \cap x_k)\}.$$

Assim F_X consiste dos elementos de A que são maiores ou iguais que os ínfimos de subconjuntos finitos não vazios de X assim como desses ínfimos. Em particular, cada elemento de X pertence a F_X, consequentemente F_X inclui X. É fácil mostrar que F_X é um filtro, no entanto vamos apenas restringir-nos a algumas observações:

(f) $0 \notin F_X$ (caso contrário a propriedade de intersecção finita não seria verdadeira para X) e $1 \in F_X$ (porque X é não vazio: pelo menos um elemento de X é menor ou igual a 1).

(ff) Se $x \geq x_1 \cap x_2 \cap ... \cap x_k$ e $y \geq y_1 \cap y_2 \cap ... \cap y_k$, então temos que

$$x \cap y \geq x_1 \cap x_2 \cap ... \cap x_k \cap y_1 \cap y_2 \cap ... \cap y_k .$$

(fff) Se $x \geq x_1 \cap x_2 \cap ... \cap x_k$ e $y \geq x$, então $y \geq x_1 \cap x_2 \cap ... \cap x_k$, Assim encontramos um filtro que inclui X.

No caso particular de álgebras Booleanas, podemos enunciar o teorema de Krull em termos de filtros. É então conhecido como o teorema dos ultrafiltros:

Teorema 2.63 Numa álgebra booleana, todo o filtro está incluído em pelo menos um ultrafiltro.

Demonstração: Dado um filtro F, o ideal dual de F está incluído em pelo menos um ideal maximal; o seu filtro dual é então um ultrafiltro que inclui F.

Claro que, para álgebras booleanas, a formulação em termos de filtros e a formulação em termos de ideais são equivalentes.

O teorema do ultrafiltro permite-nos dar uma forma ligeiramente diferente ao lema 2.62:

Lema 2.64 Seja $\langle A, \leq, 0, 1\rangle$ uma álgebra booleana e seja X um subconjunto de A. Para a existência de um ultrafiltro em *A* que inclua X, é necessário e suficiente que X seja uma base de filtro.

Demonstração: As propriedades de: existe um ultrafiltro em *A* que inclui X e existe um filtro em *A* que inclui X são equivalentes: a primeira implica claramente a segunda; a implicação inversa segue-se do teorema do ultrafiltro, 2.63. A conclusão segue-se então de um Lema anterior, 2.62.

2.6 Teorema de Stone

O primeiro exemplo de uma álgebra booleana é, sem dúvida, o da álgebra de subconjuntos de um determinado conjunto. Será toda a álgebra booleana igual (queremos realmente dizer "isomórfica a") a uma álgebra booleana de subconjuntos de algum conjunto?

A resposta é não, uma vez que já encontrámos álgebras booleanas sem átomos, num exemplo anterior, e sabemos que a álgebra de subconjuntos de um conjunto contém sempre átomos: os conjuntos singulares; e qualquer isomorfismo transforma átomos em átomos; uma álgebra booleana que não contém átomos não pode então ser isomórfica a uma álgebra que os contenha.

O teorema de Stone mostra que existe sempre uma ligação entre uma álgebra booleana e uma álgebra de subconjuntos de um conjunto. Mais precisamente, toda a álgebra booleana é isomórfica a uma subálgebra de uma álgebra booleana de subconjuntos de um conjunto.

2.6.1 O espaço de Stone numa álgebra booleana

Consideremos a álgebra booleana $A = \langle A, +, \times, 0, 1\rangle$.

Definição 2.65 O conjunto de homomorfismos de uma álgebra booleana A em $\{0,1\}$ é representado por $S(A)$ e define-se como o **espaço de Stone** de A.

Poderíamos ter escolhido o conjunto de ideais maximais ou o conjunto de ultrafiltros em A.

O conjunto $S(A)$ é um subconjunto de $\{0,1\}^A$, o conjunto de aplicações de A em $\{0,1\}$, o qual consideramos anteriormente como um espaço topológico tomando a topologia discreta em $\{0,1\}$ e dando a este espaço a topologia do produto. Assim podemos dar a $S(A)$ a topologia induzida por $\{0,1\}^A$. Os subconjuntos abertos de $S(A)$ são então as intersecções com $S(A)$ dos subconjuntos abertos de $\{0,1\}^A$.

Lema 2.66 O espaço topológico $S(A)$ é zero dimensional.

Demonstração: Vimos que $\{0,1\}^A$ é zero dimensional, lema 2.21. Assim, basta aplicar um lema anterior, 2.17.

Já exibimos uma base $(\Omega_i)_{i\in I}$ para o espaço $\{0,1\}^A$ consistindo de conjuntos simultaneamente abertos e fechados. Cada um dos Ω_i é o conjunto de todas as aplicações de A em $\{0,1\}$ que assumem valores específicos de um número finito de pontos. Se para cada *i*, fixarmos $\Gamma_i = \Omega_i \cap S(A)$, como no lema 2.17, então a família $(\Gamma_i)_{i\in I}$ é uma base para os conjuntos abertos em $S(A)$ consistindo de conjuntos simultaneamente abertos e fechados. Cada Γ_i é um conjunto de homomorfismos de álgebras booleanas de *A* em $\{0,1\}$ que assumem valores dados de um número finito de determinados pontos.

De agora em diante, apenas usaremos esta base para os conjuntos abertos que consideraremos para o espaço $S(A)$. Quando falamos de um conjunto aberto básico para o espaço de Stone de *A*, queremos dizer um dos conjuntos simultaneamente abertos e fechados na família $(\Gamma_i)_{i\in I}$.

Lema 2.67 Para um subconjunto Δ de $S(A)$ ser um conjunto aberto básico, é necessário e suficiente que exista um elemento *a* em A tal que

$$\Delta = \{h \in S(A): h(a) = 1\}.$$

Além disso, quando esta condição é verificada, tal elemento é único.

Demonstração:

- É suficiente: Suponhamos que $\Delta = \{h \in S(A): h(a) = 1\}$; Δ é o conjunto de homomorfismos de A em $\{0,1\}$ que assumem o valor 1 no ponto *a*: assim é um dos conjuntos abertos básicos em $S(A)$.
- É necessária: Suponhamos que Δ é um subconjunto aberto básico de $S(A)$.

  * Se $\Delta = \varnothing$, então $\Delta = \{h \in S(A): h(0) = 1\}$.

  * Se $\Delta \neq \varnothing$, então existe um inteiro $n \geq 1$, elementos $a_1, a_2, ..., a_n$ em A e elementos $\varepsilon_1, \varepsilon_2, ..., \varepsilon_n$ em $\{0,1\}$ tais que

$$\Delta = \{h \in S(A): h(a_1) = \varepsilon_1 \text{ e } h(a_2) = \varepsilon_2 \text{ e } ... \; h(a_n) = \varepsilon_n\}.$$

  Para todo o $k \in \{1, 2, ..., n\}$, consideremos

$$b_k = \begin{cases} a_k & \text{se } \varepsilon_k = 1; \\ 1 + a_k & \text{se } \varepsilon_k = 0. \end{cases}$$

  Para todo o homomorfismo $h \in S(A)$ e para todo o $k \in \{1, 2, ..., n\}$, temos que

$$h(b_k) = \begin{cases} h(a_k) & \text{se } \varepsilon_k = 1; \\ 1 + h(a_k) & \text{se } \varepsilon_k = 0. \end{cases}$$

Segue-se que para $h \in S(A)$, $h \in \Delta$ se e só se $h(b_k) = 1$ para todo o $k \in \{1, 2, ..., n\}$. Mas esta última condição é equivalente a

$$h(b_1) \cap h(b_2) \cap ... \cap h(b_n) = 1,$$

ou novamente, pois um homomorfismo esteja envolvido, para

$$h(b_1 \cap b_2 \cap ... \cap b_n) = 1.$$

Assim, vemos que, fixando $a = b_1 \cap b_2 \cap ... \cap b_n$, temos que

$$\Delta = \{h \in S(A): h(a) = 1\}.$$

Agora provemos a unicidade: se a e b são elementos distintos de A, então $a + b \neq 0$; assim podemos considerar o filtro principal gerado por $a + b$ e, pelo teorema do ultrafiltro, um ultrafiltro que inclui este filtro. Para tal ultrafiltro, existe um homomorfismo associado ϕ de A em $\{0,1\}$ que satisfaz $\phi(a + b) = 1$, ou novamente, $\phi(a) + \phi(b) = 1$, o que significa que um e só um dos dois elementos $\phi(a)$ e $\phi(b)$ é igual a 1. Isto prova que

$$\{h \in S(A): h(a) = 1\} \neq \{h \in S(A): h(b) = 1\}$$

uma vez que ϕ pertence a um destes dois conjuntos e não ao outro.

Corolário 2.68 O conjunto de subconjuntos fechados básicos de S(A) coincide com o conjunto dos seus subconjuntos abertos básicos.

Demonstração: Seja Γ um subconjunto fechado básico de S(A). Então $\Delta = S(A) - \Gamma$ é um subconjunto aberto básico; consequentemente (pelo lema precedente, 2.67) existe um elemento $a \in$ A tal que

$$\Delta = \{h \in S(A): h(a) = 1\}.$$

Consequentemente,

$$\begin{aligned} \Gamma &= \{h \in S(A): h(a) \neq 1\} \\ &= \{h \in S(A): h(a) = 0\} \\ &= \{h \in S(A): h(1 + a) = 1\}. \end{aligned}$$

Assim, vemos, graças novamente ao lema anterior, 2.67, que Γ é um subconjunto aberto básico. Da mesma forma, podemos mostrar que todo o conjunto aberto básico é um conjunto fechado básico.

Lema 2.69 O espaço topológico S(A) é compacto.

Demonstração: Em primeiro lugar, e uma vez que a topologia em $\{0,1\}^A$ é de Hausdorff, também é a topologia de S(A).

Então, temos de mostrar que, de qualquer família de subconjuntos fechados de S(A) cuja intersecção é vazia, podemos extrair uma subfamília finita cuja intersecção é também vazia. Mas já vimos que basta fazer isto para famílias de conjuntos fechados básicos, lema 2.13. Agora, como há pouco vimos, os conjuntos fechados básicos coincidem com os conjuntos abertos básicos. Assim, consideremos uma família infinita $(\Sigma_j)_{j\in J}$ de subconjuntos abertos básicos de S(A) tais que $\bigcap_{j\in J} \Sigma_j = \varnothing$. Pelo lema precedente2.67, existe, para cada $j \in$ J, um elemento único x_j em A tal que

$$\Sigma_j = \{h \in S(A): h(x_j) = 1\}.$$

Seja X = $\{x_j: j \in J\}$. Dizer que a intersecção da família $(\Sigma_j)_{j\in J}$ é vazia é dizer que não existe nenhum homomorfismo de álgebras booleanas de A em $\{0,1\}$ que toma o valor 1 para todos os elementos de X, ou novamente, que não existe nenhum ultrafiltro em A que contém X. Isto significa que X não é uma base de filtro, lema 2.64. Assim, existe um subconjunto finito $\{x_{j1}, x_{j2}, ..., x_{jk}\} \subseteq$ X cujo ínfimo é zero. Assim, nenhum ultrafiltro em A pode conter simultaneamente x_{j1}, x_{j2}, e ... e x_{jk}. Por outras palavras, nenhum homomorfismo de A em $\{0,1\}$ pode simultaneamente supor o valor 1 nos pontos x_{j1}, x_{j2}, e ... e x_{jk}. Isto quer dizer que

$$\Sigma_{j1} \cap \Sigma_{j2} \cap \ldots \cap \Sigma_{jk} = \varnothing.$$

Temos então uma subfamília finita da família $(\Sigma_j)_{j\in J}$ cuja intersecção é vazia.

Podemos dar uma demonstração diferente de que S(A) é compacto invocando o facto de que $\{0,1\}^A$ é ele próprio compacto, teorema 2.20. Bastaria então mostrar para isso que S(A) é fechado em $\{0,1\}^A$ (uma vez que todo o subconjunto fechado de um espaço compacto é compacto):

Para $a \in$ A e $b \in$ A, fixemos

$$\Omega(a, b) = \{f \in \{0,1\}^A: f(ab) = f(a) f(b) \text{ e } f(1 + a) = 1 + f(a)\}.$$

Temos ainda que, S(A) = $\bigcap_{\substack{a\in A \\ b\in A}} \Omega(a, b)$, teorema 2.37. Mas para todos os elementos a e b de A, podemos escrever:

$$\Omega(a, b) = \{f \in \{0,1\}^A: f(a) = 0 \text{ e } f(b) = 0 \text{ e } f(ab) = 0 \text{ e } f(1 + a) =1\} \cup$$
$$\cup \{f \in \{0,1\}^A: f(a) = 0 \text{ e } f(b) = 1 \text{ e } f(ab) = 0 \text{ e } f(1 + a) = 1\} \cup$$
$$\cup \{f \in \{0,1\}^A: f(a) = 1 \text{ e } f(b) = 0 \text{ e } f(ab) = 0 \text{ e } f(1 + a) = 0\} \cup$$

$\cup \{f \in \{0,1\}^A: f(a) = 1 \text{ e } f(b) = 1 \text{ e } f(ab) = 1 \text{ e } f(1 + a) = 0\}$.

Todos os quatro conjuntos do lado direito desta igualdade são subconjuntos abertos básicos de $\{0,1\}^A$, bem como conjuntos simultaneamente abertos e fechados. Em particular, a sua união é fechada. Assim a intersecção de todos os conjuntos da forma $\Omega(a, b)$, com a e b a variar em A, é um subconjunto fechado de $\{0,1\}^A$. E como já vimos, esta intersecção é S(A).

Corolário 2.70 O espaço de Stone de A é um espaço topológico booleano.
Demonstração: De facto, o espaço S(A) é compacto (lema 2.69) e é zero dimensional (lema 2.66).

Lema 2.71 O conjunto de subconjuntos simultaneamente abertos e fechados de S(A) coincide com o conjunto dos seus conjuntos abertos básicos.
Demonstração: Já sabemos que todos os conjuntos abertos básicos são simultaneamente abertos e fechados (lema 2.66).

Reciprocamente, seja Γ um subconjunto arbitrário simultaneamente aberto e fechado de S(A). Como Γ é aberto, é uma união de conjuntos abertos básicos: por exemplo, $\Gamma = \bigcup_{i \in J} \Gamma_i$ para algum subconjunto $J \subseteq I$. Mas uma vez que Γ é um subconjunto fechado do espaço compacto S(A), é ele próprio compacto. Assim da cobertura aberta $(\Gamma_i)_{i \in J}$ de Γ, podemos extrair uma subcobertura finita, por exemplo:
$\Gamma = \Gamma_{j1} \cup \Gamma_{j2} \cup ... \cup \Gamma_{jm}$. Já sabemos, lema 2.67, que podemos encontrar elementos x_1, x_2, ..., x_m em A tais que

para todo o $k \in \{1, 2, ..., m\}$, $\Gamma_{jk} = \{h \in S(A): h(x_k) = 1\}$.

Sejam $x = x_1 \cup x_2 \cup ... \cup x_k$ e seja $\Delta = \{h \in S(A): h(x) = 1\}$; mostraremos que $\Gamma = \Delta$. Todo o elemento de Γ é um homomorfismo que assume o valor 1 em pelo menos um dos pontos x_1, x_2, ..., x_m; assim também assume o valor 1 em x que é o seu supremo. Assim, $\Gamma \subseteq \Delta$. Por outro lado, qualquer homomorfismo que não está em Γ, e assim não assume o valor 1 em qualquer dos pontos x_1, x_2, ..., x_m, deve supor o valor 0 para cada um destes pontos, e então também para o ponto x que é o seu supremo; assim não pode pertencer a Δ. Isto prova que $\Delta \subseteq \Gamma$. Finalmente, $\Gamma = \Delta$, e como Δ é um conjunto aberto básico, lema 2.67, Γ deve ser um também.

2.6.2 Teorema de Stone

De seguida, apresentaremos o chamado Teorema de Stone

Teorema 2.72 Toda a álgebra booleana é isomórfica à álgebra booleana de subconjuntos simultaneamente abertos e fechados do seu espaço de Stone.

Demonstração: A álgebra booleana de subconjuntos simultaneamente abertos e fechados de S(A) é representada por B(S(A)).

Seja H representante da aplicação de A em $\wp$(S(A)), a qual, a cada elemento a em A, associa

$$H(a) = \{h \in S(A): h(a) = 1\}.$$

Vamos mostrar que H é um isomorfismo de álgebras booleanas de A sobre B(S(A)).

Que preserva alguns resultados anteriores, lemas 2.67 e 2.71, a aplicação H assume os seus valores em B(S(A)) e a sua imagem é o B(S(A)). Assim, H é uma aplicação sobrejectiva de A sobre B(S(A)).

Por um resultado anterior, teorema 2.39, para mostrar que H é um isomorfismo de álgebras booleanas, basta garantir que para todos os elementos x e y em A, $x \leq y$ se e só se H(x) $\subseteq$ H(y).

Assim sejam x e y dois elementos de A. Se $x \leq y$, então para qualquer homomorfismo h que satisfaz $h(x) = 1$, também temos que ter $h(y) = 1$ o que significa que H(x) é um subconjunto de H(y). Se x não é menor ou igual que y, então $x(1 + y) \neq 0$, lema 2.27. Assim podemos considerar o filtro principal gerado por $x(1 + y)$, um ultrafiltro que o inclui (pelo teorema do ultrafiltro) e o homomorfismo $h \in S(A)$ associado ao ultrafiltro. Temos que $h(x(1 + y)) = 1$, consequentemente $h(x) = 1$ e $h(1 + y) = 1 + h(y) = 1$, ou seja que $h(y) = 0$. Concluímos que $h \in H(x)$ e $h \notin H(y)$, e assim H(x) não está incluído em H(y).

Corolário 2.73 Toda a álgebra booleana finita é isomórfica a uma álgebra booleana de subconjuntos de algum conjunto.

Demonstração: Se o conjunto A é finito, então a topologia em $\{0,1\}^A$ é uma topologia discreta. Assim, este também é o caso para a topologia induzida no subconjunto S(A).

Todos os subconjuntos de S(A) são então simultaneamente abertos e fechados. Então a álgebra booleana B(S(A)) coincide com $\wp$(S(A)) e A é isomorfo a $\wp$(S(A)).

No caso de uma álgebra booleana arbitrária, o que o teorema de Stone mostra é que ela é isomórfica a uma subálgebra booleana da álgebra de subconjuntos de algum conjunto.

2.6.3 Espaços booleanos como espaços de Stone

A cada álgebra booleana associamos um espaço topológico booleano: o seu espaço de Stone S(A), e vimos que A é isomorfo à álgebra booleana de subconjuntos simultaneamente abertos e fechados deste espaço booleano. É então natural estudar o caso no qual A é dada como uma álgebra booleana de subconjuntos simultaneamente abertos e fechados de algum espaço topológico booleano X. O problema que então surge é comparar o espaço X com este outro espaço booleano que é o espaço de Stone de A, por outras palavras, comparar X e S(B(X)). O resultado desta comparação revelará que estes dois objectos se assemelham muito um ao outro.

Teorema 2.74 Todo o espaço topológico booleano X é homeomorfo ao espaço de Stone S(B(X)) da álgebra booleana de subconjuntos simultaneamente abertos e fechados de X.
Demonstração: Seja X um espaço booleano. Que preserva o estudado, lema 2.16, podemos tomar a álgebra booleana B(X) de subconjuntos simultaneamente abertos e fechados de X como uma base para os conjuntos abertos na topologia em X.

Para cada $x \in$ X, seja f_x o representante da aplicação de B(X) em {0,1} definida por

$$f_x(\Omega) = \begin{cases} 1 & \text{se } x \in \Omega; \\ 0 & \text{se } x \notin \Omega. \end{cases}$$

Mostraremos que a aplicação f que, a cada $x \in$ X, associa f_x, é um homeomorfismo do espaço topológico X sobre o espaço topológico S(B(X)).

Como f é, à priori, uma aplicação de X em $\{0,1\}^{B(X)}$, temos de mostrar, primeiro, que realmente toma valores em S(B(X)):

- Para cada $x \in X$, f_x é um homomorfismo de álgebras booleanas;

Demonstração: Para quaisquer subconjuntos simultaneamente abertos e fechados Ω e Δ de X, temos que $f_x(\Omega \cap \Delta) = 1$ se e só se $x \in \Omega \cap \Delta$, ou seja que, $x \in \Omega$ e $x \in \Delta$, o que é equivalente a $f_x(\Omega) = 1$ e $f_x(\Delta) = 1$, e consequentemente a $f_x(\Omega)f_x(\Delta) = 1$. Concluímos que

$$f_x(\Omega \cap \Delta) = f_x(\Omega)f_x(\Delta).$$

Por outro lado, $f_x(X - \Omega) = 1$ se e só se $x \in X - \Omega$, ou seja que $x \notin \Omega$, ou novamente, $f_x(\Omega) = 0$. Assim, $f_x(X - \Omega) = 1 + f_x(\Omega)$. Assim, f_x é realmente um homomorfismo, pelo teorema 2.37.

- A aplicação f é injectiva;

Demonstração: Sejam x e y elementos distintos de X. Como X é de Hausdorff, podemos encontrar um conjunto aberto O, tal que $x \in O$ e $y \notin O$ (por exemplo, poderíamos considerar $O = X - \{y\}$). Mas O é a união de conjuntos abertos básicos da base $B(X)$; então existe algum conjunto simultaneamente aberto e fechado $\Omega \in B(X)$ tal que $x \in \Omega$ e $y \notin \Omega$. Temos que $f_x(\Omega) = 1$ e $f_y(\Omega) = 0$, o que prova que f_x é diferente de f_y.

- A aplicação f é sobrejectiva sobre $S(B(X))$;

Demonstração: Seja h um elemento de $S(B(X))$, ou seja, um homomorfismo de $B(X)$ em $\{0,1\}$. O ultrafiltro em $B(X)$ associado a h é

$$U = \{\Omega \in B(X) : h(\Omega) = 1\} = h^{-1}[\{1\}].$$

Uma vez que U goza da propriedade de intersecção finita, lema 2.64, e como os elementos de U são fechados, e como o espaço topológico X é compacto, podemos afirmar que a intersecção de todos os elementos de U é não vazia. Seja x um elemento desta intersecção.

Para todo o conjunto simultaneamente aberto e fechado $\Omega \in B(X)$, temos que: ou $\Omega \in U$, e neste caso $f_x(\Omega) = 1$ e $h(\Omega) = 1$, ou então $\Omega \notin U$, e neste caso $X - \Omega \in U$, assim $f_x(\Omega) = 0$ e $h(\Omega) = 0$. Assim, para todo o $\Omega \in B(X)$, $f_x(\Omega) = h(\Omega)$. Segue-se que $h = f_x = f(x)$.

Podemos observar que o elemento x é uma pré-imagem de h pela aplicação f (como acabamos de mostrar), é o único elemento na intersecção de todos os conjuntos

simultaneamente abertos e fechados pertencentes a U. Para ver isto, note-se que qualquer elemento y nesta intersecção iria satisfazer $h = f(y)$, e pois f fosse injectiva, isto implicaria $x = y$. Esta observação permitir-nos-á descrever a bijecção inversa f^{-1}: é a aplicação de S(B(X)) em X que, para cada homomorfismo h de B(X) em {0,1}, associa o único elemento na intersecção de todos os conjuntos simultaneamente abertos e fechados pertencentes ao ultrafiltro $h^{-1}[\{1\}]$.

- A aplicação f é contínua.

Demonstração: Seja G um conjunto aberto que pertence à base de subconjuntos simultaneamente abertos e fechados de S(B(X)). Que preserva o estudado anteriormente, lema 2.67, existe um elemento Ω em B(X) tal que G = $\{h \in S(B(X)): h(\Omega) = 1\}$. A imagem inversa de G sobre a aplicação f é

$$\{x \in X: f_x \in G\} = \{x \in X: f_x(\Omega) = 1\} = \{x \in X: x \in \Omega\} = \Omega.$$

Assim é um subconjunto aberto de X.

- A aplicação inversa f^{-1} é contínua.

Demonstração: Seja Ω um conjunto aberto básico no espaço X (ou seja um elemento de B(X)). Uma vez que f é uma bijecção, a imagem inversa de Ω sobre f^{-1} é a sua imagem directa sobre f. Assim é o conjunto $f[\Omega] = \{f_x: x \in \Omega\}$. Temos que mostrar que este é um conjunto aberto no espaço S(B(X)).

Consideremos V = $\{h \in S(B(X)): h(\Omega) = 1\}$.

O conjunto V é aberto (é até mesmo um conjunto aberto básico) em S(B(X)), lema 2.67. Se mostramos que $f[\Omega]$ = V, isto completará a demonstração.

Para todo o $x \in \Omega$, temos que $f_x(\Omega) = 1$ por definição de f_x, assim $f_x \in$ V. Logo, $f[\Omega] \subseteq$ V.

Todo o $h \in$ V tem uma pré-imagem $y \in$ X sobre a bijecção f, ou seja $h = f_y$. Como $h \in$ V, temos que $h(\Omega) = f_y(\Omega) = 1$, assim $y \in \Omega$ e $f_y = h \in f[\Omega]$. Consequentemente, V está incluído em $f[\Omega]$.

Existe um famoso teorema de topologia que afirma que qualquer bijecção contínua de um espaço topológico compacto num espaço de Hausdorff é um homeomorfismo (a continuidade da bijecção inversa é garantida).

Definitivamente estabelecemos uma correspondência de um para um entre álgebras Booleanas e espaços topológicos Booleanos (um isomorfismo por um lado, um homeomorfismo por outro lado):

- toda a álgebra booleana é (isomórfica a) uma álgebra booleana de subconjuntos simultaneamente abertos e fechados de algum espaço topológico booleano;
- todo o espaço topológico booleano é (homeomórfico a) um espaço de Stone de alguma álgebra booleana.

Observemos que temos muito boas razões para chamar a espaços zero dimensional compactos “espaços booleanos”.

De um modo natural, temos as seguintes duas propriedades:

- para quaisquer duas álgebras booleanas serem isomórficas, é necessário e suficiente que os seus espaços de Stone sejam homeomorfos;
- para quaisquer dois espaços topológicos booleanos serem homomórficos, é necessário e suficiente que as álgebras booleanas que consistem nos seus respectivos subconjuntos simultaneamente abertos e fechados sejam isomorfos.

Capítulo III. Conclusões e considerações finais

Após a investigação realizada poderemos entre outras considerações apresentar as seguintes:

- ❖ no primeiro capítulo revestiu-se de maior importância o estudo da Lógica proposicional. Assim, neste âmbito foram abordados os seguintes conteúdos: a sintaxe, a semântica, as formas normais, os conjuntos completos de conectivos, o lema de interpolação e o teorema da compacidade.
- ❖ no segundo capítulo deu-se mais ênfase ao estudo das álgebras booleanas. Nesta perspectiva, abordaram-se os seguintes conteúdos: algumas definições e propriedades das álgebras booleanas, átomos, homomorfismos e isomorfismos de álgebras booleanas, subálgebras, ideais, filtros, o teorema de Stone e ainda o espaço de Stone.

Como implicações futuras destaca-se a necessidade de criar condições a nível do Ensino Superior e não Superior para o estudo da lógica, mais concretamente da lógica proposicional, das álgebras booleanas e também do cálculo de predicados. A razão de se defender a perspectiva de um maior destaque à lógica e suas aplicações prende-se com os seguintes aspectos:

- no Ensino Básico, que se divide em três grandes blocos, nomeadamente, números e operações, problemas e suportes de aprendizagem, as grandes finalidades do ensino da Matemática consistem em: desenvolver a

capacidade de raciocínio, desenvolver a capacidade de comunicação e desenvolver a capacidade de resolver problemas. Nesse sentido deve-se dar importância relevada aos seguintes itens, entre outros

- questões de linguagem;
- raciocínio e seus processos;
- relações de ordem;
- operações no conjunto das condições e das proposições, nomeadamente, disjunção, conjunção, negação, explorando tais operações de forma intuitiva e informal.

- no Ensino Superior com o aprofundamento da lógica, dando mais sentido às operações referidas, poderá assim existir uma base científica mais sólida nos diversos ramos do saber, nomeadamente, na Engenharia, na Engenharia de Sistemas com os operadores lógicos, na Economia, em Gestão e em todos os cursos cujo eixo regulador seja a Matemática, e mais actualmente na pesquisa de informação na Internet através dos diversos motores de pesquisa.

- no geral, a lógica é importante pois é utilizada no dia-a-dia, uma vez que os termos "*e*", "*ou*", "*existe*", "*qualquer*", "*se ... então*", "*é equivalente*" entre outros, são muitas vezes utilizados na linguagem corrente. Tal utilização da lógica evita equívocos e pode clarificar muitas situações, que sem o seu uso são extremamente ambíguas tais como:
  - O João comeu chocolates *e* bolachas ao lanche;
  - A Paula combinou ir ao cinema *ou* ao teatro;
  - Na turma 6º A *existe* um aluno que teve nível 5 a todas as disciplinas;
  - Na equipa de futebol masculino *qualquer* que seja o jogador escolhido é do sexo masculino;
  - *Se* for ao circo *então* vou ver os palhaços;
  - O preço de uma camisola *é equivalente* ao preço de umas calças.

Podemos dizer que a lógica matemática actua sob dois aspectos:

i. aspecto explicativo, segundo o qual a lógica é um sofisticado instrumento de análise que permite a formalização de fragmentos de discursos, em particular, na matemática, competindo deste modo, parcialmente, com a linguística geral;

ii. aspecto calculativo ou operativo, segundo o qual a lógica é considerada um instrumento de cálculo formal destinado a substituir a argumentação intuitiva e informal dos cientistas e matemáticos profissionais, e a responder a algumas questões, como por exemplo:

- Em que consiste a demonstração de um teorema a partir de uma determinada hipótese?

"Os ramos da lógica matemática organizam-se, por assim dizer, nas tentativas de responder a estas questões anteriores. Em síntese, diremos que a lógica matemática comporta quatro ou cinco grandes ramos, cada um com especificidade própria, mas todos eles interligados e interactuantes entre si e com outras disciplinas matemáticas. Assim, temos:

(a) Teoria da demonstração;
(b) Teoria dos modelos;
(c) Teoria da computabilidade;
(d) Teoria dos conjuntos;
(e) Lógica e matemática intuicionista/construtivista." (Oliveira (1996: 229)

Após a realização do trabalho, podemos ainda constatar que é com base no cálculo proposicional e quantificacional que se constrói a língua de um povo.

Bibliografia

Bell, John Lane & al. (1991). *A course in mathematical logic*. North-Holland: Elsevier.

Cori, René & al. (2000). *Mathematical logic.* Oxford: Oxford University Press.

Crossley, John N. & al. (1990). *What is Mathematical Logic?* New York: Dover Publications.

Departamento da Educação Básica (1998). *Organização Curricular e Programas Ensino Básico – 1.º Ciclo*. Mem Martins: Ministério da Educação.

Ebbinghaus, Heins-Dieter & al. (1996). *Mathematical logic.* New York: Springer.

Gödel, Kurt (1977). *O teorema de Gödel e a hipótese do contínuo.* Lisboa: Fundação Calouste Gulbenkian.

Kelley, J. L. (1991). *General Topology*. Springer-Verlag: Graduate Texts in Mathematics

Kelley, John L. (1995). *General topology.* New York: Springer (Graduate Texts in Mathematics).

Kneale, William C. & al. (1968). *O Desenvolvimento da Lógica (2ª edição).* Lisboa: Fundação Calouste Gulbenkian.

Mates, Benson (1987). *Logica matematica elemental.*

Mendelson, Elliott (1997). *Introduction to mathematical logic*. London: Chapman Hall.

Munkres, James R. (1975). *Topology: a first course.* New Jersey: Prentice Hall.

Oliveira, Augusto Franco (1996). *Lógica e Aritmética.* Lisboa: Gradiva – Publicações, L.da.

Rubin, Jean E. (1990). *Mathematical Logic : Applications and Theory.* Indiana: The Saunders Series.

Sikorski, Roman (1969). *Boolean algebras*. New York: Springer-Verlag.

Stolyar, Abram Aronovich (1983). *Introduction to elementary mathematical logic.* New York: Dover.

Suppes, Patrick & al. (1975). *Primer curso de lógica matemática.* Barcelona: Editorial Reverté.

Truss, John K. (1999). *Discrete Mathematics for computer scientists (Second Edition).* England: Addison-Wesley.

Yaglom, I. (1983). *Álgebras booleanas*. Moscovo: Editora Mir.