Aurélien Bargeaud   ETH Zürich
Selim Gatti

Das Auswahlaxiom A.8

Sprache: Englisch

Definition: A Boolean algebra is an algebraic structure $(B, +, \cdot, -, 0, 1)$ where B is a non-empty set, "+" and "·" are two binary operations (called Boolean sum and product), "–" is a unary operation (called complement), and $0, 1$ are two constants.

For all $u, v, w \in B$, the Boolean operations satisfy the following axioms:

1) Commutativity

$u + v = v + u \qquad u \cdot v = v \cdot u$

2) Associativity

$u + (v + w) = (u + v) + w \qquad u \cdot (v \cdot w) = (u \cdot v) \cdot w$

3) Distributivity

$u \cdot (v + w) = (u \cdot v) + (u \cdot w) \qquad u + (v \cdot w) = (u + v)(u + w)$

4) Absorption

$u(u + v) = u \qquad u + (u \cdot v) = u$

5) Complementation

$u + (-u) = 1 \qquad u \cdot (-u) = 0$

Definition: An algebra of sets is a collection $\mathcal{S}$ of subsets of a given set S s.t.

- $S \in \mathcal{S}$
- $\forall X, Y \in \mathcal{S}: S \setminus (X \cap Y) \in \mathcal{S}$

The last condition means that $\mathcal{S}$ is closed under unions, intersections and complements

Example:

An algebra of sets $\mathcal{S} \subseteq \mathcal{P}(S)$, for a given set S, is a Boolean algebra with:

Boolean sum: $\cup$

Boolean product: $\cap$

Complement: $S \setminus \cdot$ (or $(\cdot)^c$)

$0 := \emptyset$, $1 := S$

In particular, for any set S,

$(\mathcal{P}(S), \cup, \cap, (\cdot)^c, \emptyset, S)$ is a Boolean algebra

Excursus: From the axioms of a Boolean algebra, we can derive (in green, the meaning for our example)

i) $u + u = u \cdot u = -(-u) = u$

$A \cup A = A \cap A = (A^c)^c = A$

ii) $u + 0 = u$

$A \cup \emptyset = A$

iii) $u \cdot 0 = 0$

$A \cap \emptyset = \emptyset$

iv) $u + 1 = 1$

$A \cup S = S$

v) $u \cdot 1 = u$

$A \cap S = A$

Proposition:

1) The complement of an element $u \in B$ is unique

2) $-0 = 1$ $\quad (\emptyset^c = S)$

Proof:

1) Assume not, i.e. $\exists -u \neq v \in B$ for $u \in B$ s.t.

$u + (-u) = 1 \qquad u \cdot (-u) = 0$

$u + v = 1 \qquad u \cdot v = 0$

Then,

$$
\begin{aligned}
v &= v \; 1 \\
&= v \cdot (u + (-u)) \\
&\overset{3)+}{=} (v \cdot u) + (v \cdot (-u)) \\
&= 0 + (v \cdot (-u)) \\
&= (u \cdot (-u)) + (v \cdot (-u)) \\
&\overset{3)+}{=} -u \cdot (u + v) \\
&= -u \cdot 1 \\
&= -u
\end{aligned}
$$

2) Using 1), it suffices to show:

- $0 + 1 = 1$, which is true by iv)
- $0 \cdot (-1) = 0$, which is true by iii)

Proposition: Furthermore, we can show the De Morgan laws. Let $u, v \in B$, then:

1) $-(u+v) = (-u)\cdot(-v)$ $\quad\left((A \cup B)^c = A^c \cap B^c\right)$

2) $-(u \cdot v) = (-u)+(-v)$ $\quad\left((A \cap B)^c = A^c \cup B^c\right)$

Proof:

1)
$$
\begin{aligned}
&(u+v) + ((-u) \cdot (-v)) \\
&\overset{3)}{=} ((u+v) + (-u)) \cdot ((u+v) + (-v)) \\
&= (u + v + (-u)) \cdot (u + v + (-v)) \\
&\overset{1)+5)}{=} (1 + v) \cdot (u + 1) \\
&\overset{iv)}{=} 1 \; 1 \\
&\overset{v)}{=} 1 \qquad (1)
\end{aligned}
$$

$$
\begin{aligned}
&(u+v) \cdot ((-u) \cdot (-v)) \\
&\overset{3)}{=} u((-u) \cdot (-v)) + v \cdot ((-u)(-v)) \\
&\overset{1)+2)}{=} (u \cdot (-u)) \cdot (-v) + (v \cdot (-v)) \cdot (-u) \\
&\overset{5)}{=} 0 \cdot (-v) + 0 \cdot (-u) \\
&\overset{ii)+iii)}{=} 0 \qquad (2)
\end{aligned}
$$

By (1) and (2) and the fact that the complement is unique, we obtain:

$$-(u+v) = (-u)\cdot(-v)$$

2) Left to the reader

$\boxtimes$

Definition: Let $\mathcal{L}$ be a first-order language and let S be the set of all $\mathcal{L}$-sentences. We define an equivalence relation "$\sim$" on S by:

$\varphi \sim \psi \iff \vdash \varphi \leftrightarrow \psi$, i.e.

$\varphi \sim \psi$ if, and only if, φ is equivalent to ψ (in the logic sense)

The Lindebaum algebra is the set $B := S/\sim$ of all equivalence classes $[\varphi]$ with:

- $[\varphi] + [\psi] := [\varphi \vee \psi]$ · $0 := [\varphi \wedge \neg\varphi]$
- $[\varphi] \cdot [\psi] := [\varphi \wedge \psi]$ · $1 := [\varphi \vee \neg\varphi]$
- $-[\varphi] := [\neg\varphi]$

Define now

$$u \leq v \iff u\cdot(-v) = 0$$

The "$\leq$" is then a partial ordering on B and we have:

$$u \leq v \iff u+v = v \iff u\cdot v = u$$

Note: $[\varphi] \leq [\psi] \iff \vdash \varphi \to \psi$

Remarks:

- W.r.t "$\leq$", 1 is the greatest element of B, 0 is the least element
- For $u, v \in B$

  $u+v$ is the least upper bound of $\{u,v\}$

  $u\cdot v$ is the greatest lower bound of $\{u,v\}$

- We can define an additional operation "$\oplus$" on B:

$$u \oplus v = (u \cdot (-v)) + (v \cdot (-u))$$

Then,

$$u \oplus u = (u \cdot (-u)) + (u \cdot (-u)) \overset{i)}{=} u \cdot (-u) \overset{5)}{=} 0$$

So, every u is its own (and unique) inverse w.r.t. $\oplus$

- $(B, \oplus, \cdot, 0, 1)$ is a ring (proof left to the reader)

Let $(B, +, \cdot, -, 0, 1)$ be a Boolean algebra.

Def: An ideal I in B is a non-empty proper subset of B with the following properties:

- $0 \in I$ but $1 \notin I$
- If $u \in I$ and $v \in I$, then $u + v \in I$
- For all $w \in B$ and all $u \in I$, $w \cdot u \in I$

Remark: The third condition is equivalent to $w \in B, u \in I, w \leq u \Rightarrow w \in I$

Proof: Since $w \leq u$, $w = w \cdot u \in I$ $\square$

We consider the Boolean algebra $(\mathcal{P}(\omega), \cup, \cap, -, \emptyset, \omega)$.

Claim: The set of all finite subsets of ω, denoted by I_0, is an ideal

Proof:
- $\emptyset \in I_0$, $\omega \notin I_0$
- Let u, v be finite subsets of ω. Then $u \cup v$ is also finite
- Let $w \in \mathcal{P}(\omega)$, $u \in I_0$. Then $w \cap u \subseteq u$ and is thus finite $\square$

Def: We call this ideal the Fréchet ideal

Def: A filter F in B is a non-empty proper subset of B with the following properties:

- $0 \notin F$ but $1 \in F$
- If $u \in F$ and $v \in F$, then $u \cdot v \in F$
- For all $w \in B$ and all $u \in F$, $w + u \in F$

Remark: The last condition is equivalent to $w \in B, u \in F, w \geq u \Rightarrow w \in F$

Proof: Since $u \leq w$, $w = u + w \in F$ $\square$

Remark: Note that the notion of filter is the dual notion of the one of ideal.

Def: If I is an ideal in B, $I^* := \{-u : u \in I\}$ is called the dual filter of I.

Def: If F is a filter in B, then $F^* := \{-u : u \in F\}$ is called the dual ideal of F.

Def: The dual filter $I_0^* := \{x \subseteq \omega : \omega \setminus x \text{ is finite}\}$ of the Fréchet ideal I_0 on $\mathcal{P}(\omega)$ is called the Fréchet filter.

Definitions: Let I be an ideal in B and F a filter in B.

I is called:
- trivial if $I = \{0\}$
- principal if $\exists u \in B : I = \{v : v \leq u\}$
- prime if $\forall u \in B$, either $u \in I$ or $-u \in I$

F is called:
- trivial if $F = \{1\}$
- principal if $\exists u \in B : F = \{v : v \geq u\}$
- an ultrafilter if $\forall u \in B$, either $u \in F$ or $-u \in F$

Ideals and filters over ω:

We consider the Boolean algebra $(\mathcal{P}(\omega), \cup, \cap, \setminus, \emptyset, \omega)$. A set $I \subseteq \mathcal{P}(\omega)$ is an ideal over ω if $\forall x, y \subseteq \omega$:

- $\emptyset \in I$ and $\omega \notin I$
- $(x \in I \wedge y \in I) \Rightarrow x \cup y \in I$
- $(x \in I \vee y \in I) \Rightarrow x \cap y \in I$

A set F is a filter over ω if $\forall x, y \subseteq \omega$:

- $\emptyset \notin F$ and $\omega \in F$
- $(x \in F \wedge y \in F) \Rightarrow x \cap y \in F$
- $(x \in F \vee y \in F) \Rightarrow x \cup y \in F$

Remarks:
- The trivial ideal over ω is $\{\emptyset\}$ and the trivial filter over ω is $\{\omega\}$
- For any non-empty subset $x \subseteq \omega$, $F_x := \{y \in \mathcal{P}(\omega) : y \supseteq x\}$ is a principal filter and the dual ideal $I_{\omega \setminus x} := (F_x)^* = \{z \in \mathcal{P}(\omega) : \omega \setminus z \in F_x\} = \{z \in \mathcal{P}(\omega) : z \cap x = \emptyset\}$ is a principal ideal. In particular, if $x = \{a\}$ for some $a \in \omega$, then F_x is a principal ultrafilter and $I_{\omega \setminus x}$ is a principal prime ideal.

<u>Claim</u>: Every principal ultrafilter over ω is of the form

$F_{\{a\}} = \{ y \in \mathcal{P}(\omega) : \{a\} \in y \}$ for some $a \in \omega$

<u>Proof</u>: Let F be a principal ultrafilter over ω. Because it is principal $\exists\, u \subseteq \omega$ such that $F = \{ v : v \supseteq u \}$. Take $y \subsetneq u$. Because F is an ultrafilter either $y \in F$ or $\mathcal{P}(\omega) \setminus y \in F$. The first case is not possible, thus the second case must hold and then $y \subsetneq u \subseteq \mathcal{P}(\omega) \setminus y$ ↯. Thus, $y \supseteq u$ and consequently u consists of a singleton. □

<u>Remark</u>: We denote that the Fréchet filter is neither a principal filter nor a ultrafilter. Similarly, the Fréchet ideal is neither prime nor principal.

We consider now ultrafilters over arbitrary non-empty sets S.

<u>Fact</u>: Let $\mathcal{U}$ be an ultrafilter over S.

a) If $\{x_0, \dots, x_{n-1}\} \subseteq \mathcal{P}(S)$ for some $n \in \omega$ such that $x_0 \cup \dots \cup x_{n-1} \in \mathcal{U}$ and for any distinct $i, j \in n$, we have $x_i \cap x_j \notin \mathcal{U}$, then there is a unique $k \in n$ such that $x_k \in \mathcal{U}$.

b) If $x \in \mathcal{U}$ and $|x| \geq 2$, then there is a proper subset $y \subsetneq x$ such that $y \in \mathcal{U}$

c) If $\mathcal{U}$ contains a finite set, then $\mathcal{U}$ is principal

<u>Proof</u>: a) Existence: Assume $x_k \notin \mathcal{U}\ \forall k \in n$. Then, $-x_k \in \mathcal{U}\ \forall k \in n$, which implies that $-x_0 \cap \dots \cap -x_{n-1} = -(x_0 \cup \dots \cup x_{n-1}) \in \mathcal{U} \Rightarrow x_0 \cup \dots \cup x_{n-1} \notin \mathcal{U}$ ↯

Uniqueness: Consider $i, j \in n$ distinct. Assume $x_i \in \mathcal{U}$ and $x_j \in \mathcal{U}$. Then $x_i \cap x_j \in \mathcal{U}$ ↯

b) If for any proper subset of x, $y \subsetneq x$, we have $y \notin \mathcal{U}$. Then $-y \in \mathcal{U} \Rightarrow \bigcap_{y \subsetneq x} -y = -\bigcup_{y \subsetneq x} y \underset{\text{since } |x| \geq 2}{=} -x \in \mathcal{U} \Rightarrow x \notin \mathcal{U}$ ↯ Since $|x| \geq 2$, the existence of proper subsets in $\mathcal{U}$ is ensured.

c) Let $A = \{a_1, \dots, a_n\}$ be a finite set in $\mathcal{U}$. By fact 1, we have that $\exists!\, k$ such that $\{a_k\} \in \mathcal{U}$. $F_{\{a_k\}} \subseteq \mathcal{U}$: Take $y \in F_{\{a_k\}}$. Then $y \cup \{a_k\} = y \in \mathcal{U}$ by the third property of a filter. Since $\mathcal{U}$ is a ultrafilter, each $x \in -F_{\{a_k\}}$ does not belong to $\mathcal{U}$. Thus, $\mathcal{U} = F_{\{a_k\}}$ and $\mathcal{U}$ is principal.

Theorem: (Prime ideal theorem)

If I is an ideal in a Boolean algebra, then I can be extended to a prime ideal

Recall of A.S (26.03):

Definition: A family $\mathcal{F}$ of sets is said to have finite character if for each set x:

$x \in \mathcal{F} \iff \text{fin}(x) \subseteq \mathcal{F}$, i.e. every finite subset of x belongs to $\mathcal{F}$

Teichmüller's principle:

Let $\mathcal{F}$ be a non-empty family of sets.

If $\mathcal{F}$ has finite character, then $\mathcal{F}$ has a maximal element (with respect to inclusion "$\subseteq$")

Theorem 6.1:

Axiom of Choice $\iff$ Teichmüller's principle

Proposition 6.6:

Axiom of Choice $\Rightarrow$ Principle ideal theorem

Proof:

- By Theorem 6.1, it suffices to prove:

  Teichmüller's principle $\Rightarrow$ Principle ideal theorem
- Let $(B, +, \cdot, -, 0, 1)$ be a Boolean algebra, let $I_0 \subsetneq B$ be an ideal
- Let $\mathcal{F}$ be the family of all sets $X \subseteq B \setminus I_0$ s.t. for every finite subset $\{u_0, \ldots, u_n\} \subseteq X \cup I_0$, we have

$$u_0 + \ldots + u_n \neq 1$$

- Take $X \in \mathcal{F}$, and $S \in \text{fin}(X)$, we know that

$$\forall \underset{\{u_0, \ldots, u_n\}}{A} \in \text{fin}(X \cup I_0): u_0 + \ldots + u_n \neq 1$$

Since $\text{fin}(S \cup I_0) \subseteq \text{fin}(X \cup I_0)$, it's clear that:

$\forall A \in \text{fin}(S \cup I_0) : u_0 + \_\_ + u_n \neq 1$

$\Rightarrow S \in \mathcal{F}$.

Now, let $X \subseteq B$, assume that

$\forall S \in \text{fin}(X) : S \in \mathcal{F}$

Suppose now that $X \notin \mathcal{F}$, i.e.

1) $X \not\subseteq B \setminus I_0$ or 2) $\exists \{u_0, \_, u_n\} \subseteq X \cup I_0$ s.t. $u_0 + \_ + u_n \neq 1$

1) cannot hold because otherwise,

$\exists u \in X$ s.t. $u \notin X \Rightarrow \{u\} \notin \mathcal{F}$, but $\{u\} \in \text{fin}(X)$ ↯

2) Take $U' := \bigcup_{\substack{u_i \notin I_0 \\ 0 \le i \le n}} \{u_i\}$, then $U' \notin \mathcal{F}$ but $U' \in \text{fin}(X)$ ↯

So, 2) cannot hold and we have: $X \in \mathcal{F} \Leftrightarrow \text{fin}(X) \in \mathcal{F}$

$\Rightarrow \mathcal{F}$ has finite character

$\overset{\text{Teic Principle}}{\Rightarrow}$ $\mathcal{F}$ has a maximal element I_1

In particular, $I_1 \cap I_0 = \emptyset$

- Let $I := I_0 \cup I_1$, then for finitely many elements $\{u_0, \_, u_n\} \in I$, we have that

$$u_0 + \_\_ + u_n \neq 1 \quad (*)$$

- <u>Claim 1</u>: I is an ideal

▸ $0 \overset{\text{ideal}}{\in} I_0 \subseteq I$

$1 \notin I_0$ and $1 \notin I_1$, because otherwise, we would obtain a contradiction to $(*) \Rightarrow 1 \notin I$

▸ Let $u, v \in I$,

→ If $u, v \in I_0$, then $u + v \in I_0 \subseteq I$

→ If $u \in I_0$, $v \in I_1$,

take $X = \{u + v\}$, then $X \in \mathcal{F}$ because $X \notin \mathcal{F}$ would contradict that $v \in I_1$

So, $X \subseteq I_1$ by maximality of I_1

$\Rightarrow u + v \in I_1 \subseteq I$

→ If $u, v \in I_1$, again by maximality of I_1, we have that $u+v \in I_1 \subseteq I$

- Let $w \in B$, $u \in I$

→ If $u \in I_0$, then $w \cdot u \in I_0 \subseteq I$

→ If $u \in I_1$, by absorption 4)

$$u + (u \cdot w) = u \quad (**)$$

Suppose $u + w \notin I_1$,

$$\overset{\text{max.}}{\underset{\text{of } I_1}{\Rightarrow}} \exists \{u_0 + \dots + u_n\} \in I_0 \cup I_1 : (u+w) + u_0 + \dots + u_n = 1$$

By iv), this implies:

$$u + ((u+w) + u_0 + \dots + u_n) = 1$$

$$\overset{\text{dist.}}{\underset{(**)}{\Rightarrow}} \quad u + u_0 + \dots + u_n = 1 \Rightarrow u \notin I_1 \quad \lightning$$

Hence, I is an ideal

- <u>Claim 2:</u> I is prime

<u>Proof:</u>

By maximality of I_1,

$$\forall v \in B \setminus I \; \exists u \in I : u + v = 1$$

By uniqueness of the complement,

$$\forall v \in B \setminus I : -v \in I$$

So, for all u in B, either $u \in I$ or $-u \in I$

$\Rightarrow I$ is prime

- Hence, I is a prime ideal in B which extends I_0

$\boxtimes$

Ultrafilter theorem: If F is a filter over a set S, then F can be extended to an ultrafilter

We introduce the following definitions:

Def: Let S be a set and $\mathcal{B}$ a set of binary functions (i.e. with values 0 or 1) defined on finite subsets of S. We say that $\mathcal{B}$ is a binary mess on S if $\mathcal{B}$ satisfies:

a) For each finite $P \subseteq S$, there is a function $g \in \mathcal{B}$ such that $\operatorname{dom}(g) = P$, i.e. g is defined on P.

b) For each $g \in \mathcal{B}$ and each finite set $P \subseteq S$, $g|_P$ belongs to $\mathcal{B}$.

Def: Let f be a binary function on S and let $\mathcal{B}$ be a binary mess on S. We say that f is consistent with $\mathcal{B}$ if for every finite set $P \subseteq S$, we have $f|_P \in \mathcal{B}$

We can now state the following:

Consistency Principle: For every binary mess $\mathcal{B}$ on a set S, there exists a binary function f on S which is consistent with $\mathcal{B}$.

We introduce now some terminology from Propositional Logic.

The alphabet of propositional logic consists of an arbitrarily large but fixed set $\mathcal{P} := \{p_\lambda : \lambda \in \Lambda\}$ of so-called propositional variables, as well as of the logic operators "$\neg$", "$\wedge$" and "$\vee$".

Definition: The formulae of propositional logic are defined recursively as follows:

- A single propositional variable $p \in \mathcal{P}$ by itself is a formula.
- If φ and ψ are formulae, then so are $\neg\varphi$, $\varphi \wedge \psi$ and $\varphi \vee \psi$

Definition: A realisation of propositional logic is a map of $\mathcal{P}$, the set of propositional variables to the two element Boolean algebra $(\{0,1\}, +, \cdot, -, 0, 1)$

Definition: Let φ be any formula. If a realisation f maps φ to 1, then we say that f satisfies φ. A set Σ of formulae of propositional logic is satisfiable if there is a realisation which simultaneously satisfies all the formulae in Σ.

Compactness theorem for propositional logic: Let Σ be a set of formulae of propositional logic. If every finite subset of Σ is satisfiable, then Σ is also satisfiable.

We can now state the following theorem:

Theorem: The following statements are equivalent:

a) Prime ideal theorem

b) Ultrafilter theorem

c) Consistency principle

d) Compactness theorem for propositional logic

e) Every Boolean algebra has a prime ideal

Proof: "a) $\Rightarrow$ b)" The ultrafilter theorem is an immediate consequence of the dual form of the prime ideal theorem

"b) $\Rightarrow$ c)" Let $\mathcal{B}$ be a binary mess on a non-empty set S. We have to show that there is a binary function f on S which is consistent with $\mathcal{B}$, assuming that the ultrafilter theorem holds.

Let $fin(S)$ be the set of all finite subsets of S. For each $P \in fin(S)$, define $\mathcal{X}_P := \{ g \in {}^S 2 : g|_P \in \mathcal{B} \}$. Since $\mathcal{B}$ is a binary mess, we have that for each $g \in \mathcal{B}$ and

(${}^S 2$: set of binary functions over S)

for each finite set P $g \in \mathcal{X}_P$. Thus, the intersection of finitely many $\mathcal{X}_P$ is non-empty.

We can notice that the family $\mathcal{F}$ of all supersets of intersections of finitely many sets $\mathcal{X}_P$ is a filter over ${}^S 2$. Indeed,

- $\emptyset \notin \mathcal{F}$ and ${}^S 2 \in \mathcal{F}$,
- Take two supersets of intersections of finitely many $\mathcal{X}_P$. Their intersection is also a superset of intersections of finitely many $\mathcal{X}_P$.
- Take $A \in {}^S 2$ and $B \in \mathcal{F}$. Then, $A \cup B \in \mathcal{F}$ because it is a superset of B, which is itself a superset of intersections of finitely many $\mathcal{X}_P$.

Since $\mathcal{F}$ is a filter, we can extend it by the ultrafilter theorem to an ultrafilter $\mathcal{U} \subseteq \mathcal{P}({}^S2)$. Since $\mathcal{U}$ is an ultrafilter, for each $x \in S$, either $\{g \in {}^S2 : g(x) = 0\}$ or $\{g \in {}^S2 : g(x) = 1\}$ belongs to $\mathcal{U}$. Define $f \in {}^S2$ by stipulating that $\mathcal{X}_{\{x\}} := \{g \in {}^S2 : g(x) = f(x)\}$ belongs to $\mathcal{U}$. For any finite set $P = \{x_0, \dots, x_n\} \subseteq S$, we have that $\bigcap_{i \leq n} \mathcal{X}_{\{x_i\}} \in \mathcal{U}$, since $\mathcal{U}$ is a filter and thus $f|_P \in \mathcal{B}$, i.e. f is consistent with $\mathcal{B}$.

"c) ⇒ d)" Let Σ be a set of formulae of propositional logic and let $S \subseteq \mathcal{P}$ be the set of propositional variables which appear in formulae of Σ. Assume that every finite subset is satisfiable, i.e. for every finite subset $\Sigma_0 \subseteq \Sigma$ there is a realisation $g_{\Sigma_0} : S_{\Sigma_0} \longrightarrow \{0,1\}$ which satisfies Σ_0, where S_{Σ_0} denotes the set of propositional variables which appear in formulae of Σ_0.

Assuming the consistency principle, we have to show that Σ is also satisfiable.

Define $\mathcal{B}_\Sigma := \{ g_{\Sigma_0}|_P : \Sigma_0 \in fin(\Sigma) \wedge P \subseteq S_{\Sigma_0} \}$

We denote that: · For each $P \subseteq S$ finite, we have by assumption a g_{Σ_0} in $\mathcal{B}_\Sigma$ such that g_{Σ_0} is defined on P

· For each $g \in \mathcal{B}_\Sigma$ and each finite $P \subseteq S$, $g|_P \in \mathcal{B}_\Sigma$

Thus $\mathcal{B}_\Sigma$ is a binary mess. By the consistency principle, there exists a binary function f on S which is consistent with $\mathcal{B}_\Sigma$. By the definition of $\mathcal{B}_\Sigma$, it means that f is a realisation which satisfies Σ.

d) $\Rightarrow$ e):

- Let $(B, +, \cdot, -, 0, 1)$ be a Boolean algebra. Let $P := \{p_v \mid v \in B\}$, a set of propositional variables. Let Σ_B be the following set of formulae of Propositional Logic:

I) p_0, $\neg p_1$

II) $p_v \vee \neg p_v$ (for each $v \in B$)

III) $\neg(p_{v_1} \wedge \dots \wedge p_{v_n}) \vee p_{v_1 + \dots + v_n}$ (for each finite set $\{v_1, \dots, v_n\} \subseteq B$)

IV) $\neg(p_{v_1} \vee \dots \vee p_{v_n}) \vee p_{v_1 \cdots v_n}$ (for each finite set $\{v_1, \dots, v_n\} \subseteq B$)

- Every finite subset of B generates a finite subalgebra of B and every finite Boolean algebra has a prime ideal
- Every finite prime ideal in a finite subalgebra of B corresponds to a finite subset of Σ_B, and vice versa $\overset{d)}{\Rightarrow}$ Σ_B is satisfiable
- Let f be a realisation of Σ_B, define $I := \{v \in B \mid f(p_v) = 1\} \subseteq B$
- Claim 1: I is an ideal

Proof:

$\rightarrow$ $f(p_0) \overset{I)}{=} 1$ and $-f(p_1) = f(\neg p_1) \overset{I)}{=} 1 \overset{vi)}{\Rightarrow} f(p_1) = 0$

$\Rightarrow$ $p_0 \in I$, $p_1 \notin I$

$\rightarrow$ If $f(p_{v_1}) = f(p_{v_2}) = 1$, then

$$
\begin{aligned}
1 &\overset{III)}{=} f(\neg(p_{v_1} \wedge p_{v_2}) \vee p_{v_1 + v_2}) \\
&= f(\neg(p_{v_1} \wedge p_{v_2})) + f(p_{v_1 + v_2}) \\
&= -f(p_{v_1} \wedge p_{v_2}) + f(p_{v_1 + v_2}) \\
&= -(f(p_{v_1}) \cdot f(p_{v_2})) + f(p_{v_1 + v_2}) \\
&\overset{\text{De Morgan}}{=} \underbrace{-f(p_{v_1})}_{=0} + \underbrace{-f(p_{v_2})}_{=0} + f(p_{v_1 + v_2})
\end{aligned}
$$

$= f(p_{v_1+v_2})$

$\Rightarrow \forall v_1, v_2 \in I,\ v_1+v_2 \in I$

$\rightarrow$ Analogously, let $v_1 \in I$, $v_2 \in B$

IV) $\Rightarrow f(p_{v_2 \cdot v_1}) = 1 \Rightarrow v_2 \cdot v_1 \in I$

- Claim 2: I is prime

Proof: Suppose $v \notin I$

By II),

$f(p_v) = 0 \Rightarrow p_v \notin \Sigma_B \overset{\text{II)}}{\Rightarrow} f(\neg p_v) = 1$

If $v \in I$,

$f(\neg p_v) = -f(p_v) = -1 = 0$

⊠

e) $\Rightarrow$ a).

- Let $(B, +, \cdot, -, 0, 1)$ be a Boolean algebra and $I \subseteq B$ be an ideal

Goal: Show that I is contained in some prime ideal in B

- Define an equivalence relation on B:

$$u \sim v \iff (u \cdot (-v)) + (v \cdot (-u)) \in I$$

Notice that this means:

$$u \sim v \iff u \oplus v \in I$$

(Quick check that this is indeed an equivalence relation:

$\rightarrow$ $u \sim u$ because $u \cdot (-u) = 0 \in I$

$\rightarrow$ $u \sim v \iff v \sim u$, clear by def.

$\rightarrow$ $u \sim v$, $v \sim z$, then

$u \oplus z = u \oplus \underbrace{v \oplus v}_{=0} \oplus z$

$= (\underbrace{u \oplus v}_{\in I} \cdot (-(v \oplus z)) + (-(u \oplus v)) \cdot \overbrace{(v \oplus z)}^{\in I}) \in I$)

- Let $C := B/\sim$, with on C.

$$[u]+[v] = [u+v]$$
$$[u]\cdot[v] = [u\cdot v]$$
$$-[u] = [-u]$$

Then, $(C,+,\cdot,-,[0],[1])$ is a Boolean algebra, called the quotient of B modulo I

- e) $\Rightarrow$ C has a prime ideal $J \subseteq C$
- <u>Claim.</u> $P := \{u \in B \mid [u] \in J\}$ is a prime ideal in B which extends I

<u>Part 1.</u> $I \subseteq P$

Let $u \in I$, then $u \sim 0$ because

$$(u\cdot(-0)) + (0\cdot(-u)) \overset{vi)+iii)}{=} u\cdot 1 + 0 \overset{v)}{=} u + 0 \overset{ii)}{=} u \in I$$

$[0] \in J$, $[0]=[u] \Rightarrow [u] \in J \Rightarrow u \in P$

<u>Part 2.</u> P is a prime ideal

$\rightarrow$ $0 \in P$ because $[0] \in J$

$1 \notin P$ because $[1] \notin J$

$\rightarrow$ Let $u,v \in P$, then

$[u+v] = [u]+[v] \in J \Rightarrow u+v \in P$

$\rightarrow$ Let $w \in B$, $u \in P$, then

$[w\cdot u] = [w]\cdot[u] \in J \Rightarrow w\cdot u \in P$

So actually,

J is an ideal $\Rightarrow$ P is an ideal

$\rightarrow$ Let $u \in B$,

if $u \notin P$, then $[u] \notin J$

J prime $\Rightarrow$ $-[u] = [-u] \in J \Rightarrow -u \in P$

Analogously, if $u \in P$, then $-u \notin P$

So we have.

J prime $\Rightarrow$ P prime $\blacksquare$