Heyting Algebra and Subobject Classifier

Prepared by CanaanZhou ;)

April 13

1 Heyting Algebra

Here we quickly introduce the concept of Heyting Algebra.

Definition 1.1 (Lattice)

A lattice $(L, \leq, \wedge, \vee)$ *is a poset with binary product* $\wedge$ *and binary coproduct* $\vee$*. They are called* join *and* meet *respectively. A* bounded lattice *is a lattice with all* finite *product and* finite *coproduct. In particular, it has a minimum* 0 *and a maximum* 1*.*

Definition 1.2 (Heyting Algebra)

A Heyting algebra $(A, \leq, \wedge, \vee, 0, 1, \Rightarrow)$ *is a bounded lattice that is a ccc:*

$$x \wedge y \leq z \textit{ iff } x \leq y \Rightarrow z.$$

where $\Rightarrow$ *is called* Heyting implication *operator.*

In other words, $y \Rightarrow z$ is the largest x such that $x \wedge y \leq z$.[1]

A Heyting algebra is often seen as an algebraic model of *intuitionistic propositional logic*. It's just like classical propositional logic (whose algebraic model is *Boolean algebra* as we will see later) except that *law of excluded middle* (LEM) $P \vee \neg P$, *double negation elimination* (DNE) $\neg\neg P \to P$ and everything equivalent is not available. These logical rules become algebraic rules in Heyting algebra.

Exercise 1.3

Fix a Heyting algebra A. Show the following equations are always valid. Can you recognize where they come from?

- $x \Rightarrow (y \Rightarrow x) = 1.$

[1]This fact is a corollary of our theorem of category of elements last week.

- $(x \Rightarrow (y \Rightarrow z)) \Rightarrow (x \Rightarrow y) \Rightarrow (x \Rightarrow z) = 1$.
- $x \wedge (x \Rightarrow y) \leq y$.
- $(x \Rightarrow z) \wedge (y \Rightarrow z) \leq (x \vee y) \Rightarrow z$.
- $(x \wedge y) \Rightarrow z = x \Rightarrow (y \Rightarrow z)$.

Hint: A is a ccc, so you can use our λ-calculus system.

The prototypical example of a Heyting algebra is $O(X)$, the poset of open sets in X, for a fixed topological space X. $\leq = \subseteq, 0 = \varnothing, 1 = X, \wedge = \cap, \vee = \cup$. For any opens U, V,

$$U \Rightarrow V = \bigcup \{W \in O(X) \mid W \cap U \subseteq V\}.$$

We have a concrete and easy-to-compute example. It can also be a good counterexample against many propositions.

Example 1.4 (Sierpiǹski space)

The Sierpiǹski space Σ *has two points* $0, 1$. *Opens are* $\varnothing, \{1\}, \Sigma$. *Thus* $O(\Sigma)$ *is a Heyting algebra with three elements.*

In fact, $O(X)$ is always a *complete* Heyting algebra. It has all limits and colimits.

Suppose a lattice L has arbitrary join. It's *infinitely distributive* if the following equation always holds.

$$x \wedge \left(\bigvee_i y_i \right) = \bigvee_i (x \wedge y_i).$$

Note that for any topological space X, $O(X)$ has arbitrary join (union) and is infinitely distributive:

$$U \wedge \left(\bigcup_i V_i \right) = \bigcup_i (U \cap V_i)$$

since $x \in U \wedge (\bigcup_i V_i)$ iff $x \in U$ and x is in some V_i iff x is in some $U \cap V_i$.

Proposition 1.5

Any lattice that has arbitrary join and is infinitely distributive is a complete Heyting algebra and vice versa.

Proof.

$\Leftarrow$ Suppose L is a complete Heyting algebra. We need to show that it's infinitely distributive:

$$x \wedge \left(\bigvee_i y_i \right) = \bigvee_i (x \wedge y_i).$$

This is simply because $x \wedge -$ is left adjoint to $x \Rightarrow -$, $\bigvee_i y_i$ is the colimit of y_i, and left adjoint preserves colimits.

$\Rightarrow$ Suppose L has arbitrary join and is infinitely distributive. Its minimum is $\bigvee \varnothing$ since the colimit of an empty diagram is the terminal. Its maximum is $\bigvee L$, the join of the whole lattice. It works here because L is a po*set*, so it's small.

We define Heyting implication as follows.

$$x \Rightarrow y := \bigvee \{z \mid z \wedge x \leq y\}.$$

To see the cc property: if $x \wedge y \leq z$, then $x \leq y \Rightarrow z$ by definition. For the other direction:

$$\begin{aligned} & x \leq y \Rightarrow z \\ \implies & x \leq \bigvee \{w \mid w \wedge y \leq z\} \\ \implies & x \wedge y \leq \bigvee \{w \wedge y \mid w \wedge y \leq z\} \leq z \end{aligned}$$

We still need to define infinite meet.

$$\bigwedge_i x_i := \bigvee \{y \mid \forall i. y \leq x_i\}.$$

Now we show the universal property. For each j, $\bigwedge_i x_i \leq x_j$, since for each y such that $\forall i. y \leq x_i$, it follows that $y \leq x_j$.

Suppose for each j, $x < x_j$ for some fixed x. Then trivially $x \leq \bigvee \{y \mid \forall i. y \leq x_i\}$, since x is a member of that set. □

From now on, fix a heyting algebra A.

Definition 1.6 (Negation)

The negation *operator* $\neg : A^{\mathrm{op}} \to A$ *is defined to be* $\neg x = x \Rightarrow 0$.

Suppose $A = O(X)$ for a topological space X, $U \subseteq X$ is an open set. By definition,

$$\neg U = U \Rightarrow \varnothing = \bigcup \{V \mid U \cap V = \varnothing\}$$

This is the interior of the complement of U.

Suppose $X = \mathbb{R}$ with standard topology. In $O(\mathbb{R})$, neither LEM nor DNE works.

- Suppose $U = (-\infty, 0)$, then $\neg U = (0, \infty)$, so $U \cup \neg U \subsetneq \mathbb{R}$.
- Suppose $U = (-\infty, 0) \cup (0, \infty)$, then $\neg U = \varnothing$, $\neg\neg U = \mathbb{R}$, so $U \subsetneq \neg\neg U$.

However, these are valid in any A:

Exercise 1.7

Show the following equations are always valid.

- $x \le \neg\neg x$.
- $\neg\neg\neg x = \neg x$.
- $x \wedge \neg x = 0$.
- $\neg(x \vee y) = \neg x \wedge \neg y$. *Hint: use* Exercise 1.3.
- $\neg x \vee \neg y \le \neg(x \wedge y)$.
- $\neg(x \wedge y) = x \Rightarrow (\neg y)$.

So *double negation* operator $\neg\neg : A \to A$ is a *closure operator*[2], in the sense that it's a idempotent functor (on poset, so it's in fact a *monad*).

Definition 1.8 (Boolean Algebra)

A Boolean algebra A is a Heyting algebra such that for any $x \in A$, $\neg\neg x = x$.

In most textbooks, a Boolean algebra is defined to be a bounded distributive lattice with a negation operator $\neg$ satisfying de Morgan's law and many other axioms, and Heyting implication is *defined* as $x \Rightarrow y := \neg x \vee y$. This is of course equivalent to our definition. However the internal logic of a topos is usually intuitionistic, and being Boolean is a very special property. Our treatment of Boolean algebra being a Heyting algebra with some special properties matches this phenomenon. Moreover, dealing with Heyting algebra provides more *intuition*.[3]

Exercise 1.9

Show that in any Boolean algebra A, the following equations always hold.

- *"Definition" of Heyting implication: $x \Rightarrow y = \neg x \vee y$. Hint: check the adjunction property.*
- *LEM: $x \vee \neg x = 1$. Hint: if you're stuck with this, look up a bit.*
- *de Morgan's law: $\neg(x \wedge y) = \neg x \vee \neg y$. Note that the other part of de Morgan's law has been proven to be valid in any* Heyting *algebra.*

[2] It has absolutely *nothing* to do with the notion of *closure* in topology!

[3] Get it? Is it funny? No? Alright :(

- *Pierce's law:* $((x \Rightarrow y) \Rightarrow x) = x$. *Hint: Use de Morgan's law and "definition" of Heyting implication to compute directly.*

Definition 1.10

A homomorphism $f : A \to B$ *between Heyting algebras* A, B *is a functor that preserves* $\wedge, \vee, \Rightarrow$ *and in particular* $0, 1$. *Thus we have a category of Heyting algebras* HeyAlg. *It has a full subcategory* $\mathsf{BoolAlg}$ *consisting of Boolean algebras.*

Lemma 1.11

For any Heyting algebra A*, let* B *be the image of* $\neg\neg : A \to A$*, then* B *is a subposet of* A. *The two functors* $\neg\neg : A \to B$ *and* $i : B \to A$ *form an adjunction pair* $\neg\neg \dashv i$.

Proof. After untangling all the concepts, the lemma simply says that for any $x, y \in A$ such that $y = \neg\neg y$, $x \leq y$ iff $\neg\neg x \leq y$.

- If $\neg\neg x \leq y$, then $x \leq \neg\neg x \leq y$.
- If $x \leq y$, then $\neg\neg x \leq \neg\neg y = y$.

□

If you're familiar with monad theory, the image of $\neg\neg$ is the same as $\{x \in A \mid \neg\neg x \leq x\}$, the Eilenberg-Moore category of the monad $\neg\neg$. The adjunction then follows directly.

Lemma 1.12

The subposet B *defined above is a Boolean algebra and* $\neg\neg : A \to B$ *is a Heyting algebra homomorphism.*

Proof. $0, 1 \in B$ and are preserved by both $\neg\neg$ and i.

We prove that $\neg\neg$ preserves $\wedge$. Since $x \wedge y \leq x$, $\neg\neg(x \wedge y) \leq x$, same for y, so $\neg\neg(x \wedge y) \leq \neg\neg x \wedge \neg\neg y$.

To show $\neg\neg x \wedge \neg\neg y \leq \neg\neg(x \wedge y)$, we only need to show that $(\neg\neg x) \wedge (\neg\neg y) \wedge \neg(x \wedge y) \leq 0$. Indeed,

$$\begin{aligned}
(\neg\neg x) \wedge (\neg\neg y) \wedge \neg(x \wedge y) &= (\neg\neg x) \wedge (\neg y \Rightarrow 0) \wedge (x \Rightarrow \neg y) \\
&\leq (\neg\neg x) \wedge (x \Rightarrow 0) \\
&= 0.
\end{aligned}$$

Next, $\neg\neg$ preserves $\vee$ is simply because $\neg\neg$ is left adjoint and $\vee$ is colimit.

Finally we need to show that $\neg\neg$ preserves $\Rightarrow$.

$$(\neg\neg x) \Rightarrow (\neg\neg y) = \neg(\neg\neg x \wedge \neg y).$$

We claim that $\neg\neg x \wedge \neg y = \neg(x \Rightarrow y)$ and the lemma follows.

$$0 \leq y \implies \neg x \leq x \Rightarrow y \implies \neg(x \Rightarrow y) \leq \neg\neg x,$$

$$y \wedge x \leq y \implies y \leq x \Rightarrow y \implies \neg(x \Rightarrow y) \leq \neg y.$$

Thus $\neg(x \Rightarrow y) \leq \neg\neg x \wedge \neg y$. For the other direction, note that

$$\neg\neg x \wedge \neg y \leq \neg(x \Rightarrow y) \Leftrightarrow \neg\neg x \wedge \neg y \wedge (x \Rightarrow y) \leq 0$$

however one can "compose" $\neg y \wedge (x \Rightarrow y)$:

$$\neg\neg x \wedge \neg y \wedge (x \Rightarrow y) \leq \neg\neg x \wedge \neg x = 0.$$

□

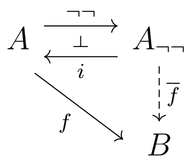
Note that the inclusion functor $i : B \to A$ is usually *not* a homomorphism, since it might not preserve join. For example, let $A = O(\mathbb{R}), U = (-\infty, 0), V = (0, \infty)$. $U \cup V \neq \neg\neg(U \cup V)$, so $U \cup V \notin B$. B still has a join operator $\vee$, it just doesn't coincide with $\cup$ in A.

Proposition 1.13

Our construction of B from A above is a functor $\neg\neg$: $\mathsf{HeyAlg} \to \mathsf{BoolAlg}$, called Booleanization. *Moreover, it's the left adjoint of the inclusion functor i : $\mathsf{BoolAlg} \to \mathsf{HeyAlg}$.*[4]

Proof. To avoid confusion, for any $A \in \mathsf{HeyAlg}$, let's write $A_{\neg\neg}$ for $\neg\neg(A) \in \mathsf{BoolAlg}$. We check the universal property of $(A_{\neg\neg}, \neg\neg : A \to A_{\neg\neg})$.

Suppose we have a homomorphism $f : A \to B$, we need to show that there uniquely exists a $\overline{f} : A_{\neg\neg} \to B$.



Define $\overline{f} : A_{\neg\neg} \to B$ to be $f \circ i$. The diagram commutes because for any $a \in A$,

$$\overline{f} \circ \neg\neg a = f(\neg\neg a) = \neg\neg f(a) = f(a).$$

[4] I'm aware that I use $\neg\neg \dashv i$ for both adjunction between $A, A_{\neg\neg}$ and between $\mathsf{HeyAlg}, \mathsf{BoolAlg}$. It should be clear from context, but sorry if it causes confusion.

Now suppose there's a $g : A_{\neg\neg} \to B$ such that the diagram commutes, meaning for every $a \in A$, $g \circ \neg\neg a = f(a)$. Since $\neg\neg : A \to A_{\neg\neg}$ is by definition epic ($A_{\neg\neg}$ is literally defined to be the image of $\neg\neg$), $\overline{f} \circ \neg\neg = g \circ \neg\neg$ implies $\overline{f} = g$. □

We have met some good examples of *reflective subcategory.*

Definition 1.14 (Reflective Subcategory)

Suppose $i : \mathsf{C} \to \mathsf{D}$ *is fully faithful, so* C *is a full subcategory of* D.

- C *is a* reflective subcategory *if* i *has a left adjoint.*
- *Dually,* C *is a* coreflective subcategory *if* i *has a right adjoint.*

By definition, $\mathsf{BoolAlg}$ is a full subcategory of HeyAlg, and we have shown that $\mathsf{BoolAlg}$ is in fact a reflective subcategory. For every Heyting algebra A, its Booleanization $A_{\neg\neg}$ is a reflective subcategory of A. I've actually written a pretty in-depth note on this topic.

2 Subobject Classifier

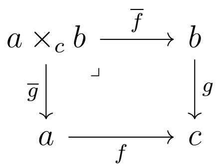
2.1 Pullback

We need to develop some calculus about pullback. Recall the definition:

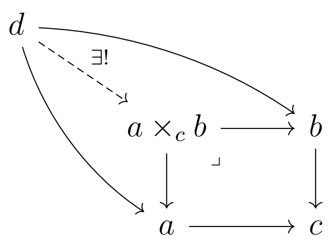
Definition 2.1 (Pullback)

The limit of a $\bullet \to \bullet \leftarrow \bullet$ *diagram is called a pullback.*

Let's expand the definition. For simplicity, let's work in a category C with finite limits. Given two morphisms $f : a \to c, g : b \to c$, the pullback cone forms a commutative square:



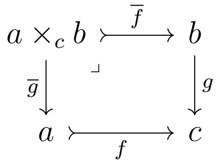
such that for any object d with $h : d \to a$ and $k : d \to b$ such that $fh = gk$, there is a unique $d \to a \times_c b$ such that everything commutes.



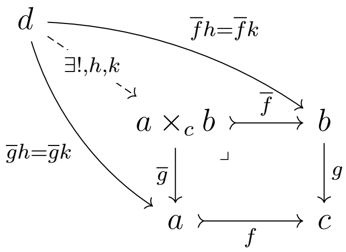
This diagram is super important, please keep it in mind.

Lemma 2.2 (Pullback preserves mono)

Suppose in the diagram above $f : a \to c$ is monic, then $\overline{f}$ is also monic.



Proof. Suppose we have $h, k : d \rightrightarrows a \times_c b$ such that $\overline{f}h = \overline{f}k$, then $g\overline{f}h = g\overline{f}k$. Since the square commutes, $f\overline{g}h = f\overline{g}k$. But since f is monic, $\overline{g}h = \overline{g}k$.



Then there exists a unique morphism $d \to a \times_c b$ such that everything commutes, but both h and k meet this condition, so we must have $h = k$. □

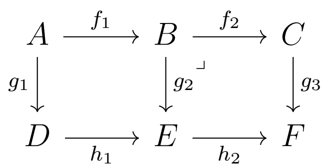
Exercise 2.3

- *Show that pullback preserves isomorphism.*

Pullback of an epimorphism is not necessarily an epimorphism. However it does in Set as well as any topos. For counterexample you can see here.

Lemma 2.4 (Pasting Lemma)

Suppose we have the following commutative diagram and the square on the right is a pullback square, then the one on the left is a pullback square iff the outer rectangle is.



Proof. Take any object U, we argue through U's generalized element.

Left square is pullback

$\Leftrightarrow \mathsf{C}(U, A) \cong \{(b : U \to B, d : U \to D) \mid g_2 b = h_1 d\}$

$\Leftrightarrow \mathsf{C}(U, A) \cong \{(e : U \to E, c : U \to C, d : U \to D) \mid g_3 c = h_2 e \wedge e = h_1 d\}$

$\Leftrightarrow \mathsf{C}(U, A) \cong \{(e : U \to E, d : U \to D) \mid g_3 c = h_2 h_1 d\}$

$\Leftrightarrow$ Out rectangle is pullback

□

2.2 Subobject Classifier

Fix a category C and an object c. Consider the collection (usually a class) of monomorphisms targetting at c. We define an equivalence relation: $f : a \rightarrowtail c$ and $g : b \rightarrowtail c$ are equivalent iff there's an isomorphism $\alpha : a \cong b$ such that the triangle commutes.

$$\begin{array}{ccc} a & \xrightarrow{\cong} & b \\ & {\scriptstyle f}\searrow \quad \swarrow{\scriptstyle g} & \\ & c & \end{array}$$

A *subobject* of c is an equivalence class of such monomorphisms. The collection of subobjects of c is denoted as $\mathrm{Sub}_{\mathsf{C}}(c)$ or simply $\mathrm{Sub}(c)$, when the category is clear from context.

A category is *well-powered* if for each object c, $\mathrm{Sub}(c)$ is small enough to be a set. All categories we care are well-powered. In fact, I don't think I've ever encountered a category that is not well-powered.

The prototypical example is again Set.

Example 2.5 (Subobjects in Set)
In Set, a subobject of a set X is an equivalence class of monomorphisms $m : S \rightarrowtail X$ targetting at X. Each equivalence class corresponds to a subset *of X, so* $\mathrm{Sub}_{\mathsf{Set}}(X) \cong \mathcal{P}(X) \cong 2^X$.

Regard $2 = \{\top, \bot\}$[5] as the set of *truth values* in Set, then 2^X is the set of *predicates* over X, while $\mathcal{P}(X)$, which we *identify* as $\mathrm{Sub}(X)$, is the set of subsets over X. The isomorphism $\mathcal{P}(X) \cong 2^X = \mathsf{Set}(X, 2)$ is given by identifying a subset $S \subseteq X$ as the *characterstic function* $\chi_S : X \to 2$ sending everything in S to $\top$ and everything else to $\bot$.

In other words, the following diagram is a *pullback*:

$$\begin{array}{ccc} S & \xrightarrow{!} & 1 \\ \downarrow & \lrcorner & \downarrow{\scriptstyle \top} \\ X & \xrightarrow[\chi_S]{} & 2 \end{array}$$

which simply expresses that

$$S = \chi_S^{-1}(\top).$$

[5] In logic, $\top$ means true and $\bot$ means false.

Now suppose we have a function $f : Y \to X$ and a subset $S \subseteq X$. One can pull $S \rightarrowtail X$ back along f:

$$\begin{array}{ccccc} f^{-1}(S) & \longrightarrow & S & \xrightarrow{!} & 1 \\ \downarrow & \lrcorner & \downarrow & \lrcorner & \downarrow \top \\ Y & \xrightarrow[f]{} & X & \xrightarrow[\chi_S]{} & 2 \end{array}$$

obtaining a subset $f^{-1}(S) \subseteq Y$. One can view $S \rightarrowtail X$ as any injection into X instead of a subset since they are categorically indistinguishable anyway. The pullback process still works because pullback preserves monomorphisms.

By pasting lemma, the outer rectangle above is also a pullback. The characterstic function $\chi_{f^{-1}(S)}$ of $f^{-1}(S) \rightarrowtail Y$ is the *composition* $Y \xrightarrow{f} X \xrightarrow{\chi_S} 2$. So $\mathrm{Sub}_{\mathsf{Set}}$ is in fact a functor $\mathrm{Sub}_{\mathsf{Set}} : \mathsf{Set}^{\mathrm{op}} \to \mathsf{Set}$, which is *naturally isomorphic* to $\mathsf{Set}(-, 2)$. For any function $f : Y \to X$, the induced function $f^* : \mathrm{Sub}_{\mathsf{Set}}(X) \to \mathrm{Sub}_{\mathsf{Set}}(Y)$ is given by "pulling back along f".

These observations motivate the definition of subobject classifier.

Definition 2.6 (Subobject Classifier)

Suppose C *has all finite limits. The subobject classifier of* C *consists of the following data:*

- *A special "truth value" object* Ω*,*
- *A "true" monomorphism* $\top : 1 \rightarrowtail \Omega$*, where* 1 *is the terminal.*
- *A natural isomorphism* $\mathrm{Sub}_{\mathsf{C}} \cong \mathsf{C}(-, \Omega) : \mathsf{C}^{\mathrm{op}} \to \mathsf{Set}$ *given by "pulling back along* $\top$*".*

We can finally define topos now.

Definition 2.7 (Elementary Topos)

A category $\mathcal{E}$ *is an* elementary topos*, or simply* topos*, if:*

- $\mathcal{E}$ *has all finite limits and colimits.*
- $\mathcal{E}$ *is Cartesian closed.*
- $\mathcal{E}$ *has a subobject classifier* $\top : 1 \to \Omega$*.*

Obviously Set is a topos as well as FinSet. Next time we will study presheaf category $\mathsf{Set}^{\mathsf{C}^{\mathrm{op}}}$ in detail and prove that they are also toposes.[6].

[6]The word topos comes from ancient Greek language. The plural form should be *topoi*, but people also say *toposes*. Personally I prefer toposes.