Model Theory and Non-Classical Logic

Cambridge University Mathematical Tripos: Part III

17th May 2024

Contents

1 Substructures

1.1 Notation

The interpretation of a function symbol f in a model $\mathcal{M}$ is denoted by $f^{\mathcal{M}}$, and similarly the interpretation of a relation symbol R in $\mathcal{M}$ is denoted by $R^{\mathcal{M}}$. If $\mathcal{M}$ is an $\mathcal{L}$-structure, and $A \subseteq \mathcal{M}$ is a subset, we will write $\mathcal{L}_A$ for the language obtained by adding a new constant symbol a to the signature of $\mathcal{L}$ for each element a of A. Then $\mathcal{M}$ is naturally an $\mathcal{L}_A$-structure by interpreting the constants in the obvious way. We will allow for the empty set to be an $\mathcal{L}$-structure.

1.2 Homomorphisms and substructures

Definition. Let $\mathcal{M}$ and $\mathcal{N}$ be $\mathcal{L}$-structures. An $\mathcal{L}$-*homomorphism* is a map $\eta : \mathcal{M} \to \mathcal{N}$ that preserves the interpretations of the symbols in the language: given $\mathbf{a} = (a_1, \dots, a_n) \in \mathcal{M}^n$,

(i) for all function symbols f of arity n, we have that

$$\eta(f^{\mathcal{M}}(\mathbf{a})) = f^{\mathcal{N}}(\eta(\mathbf{a}))$$

(ii) for all relation symbols r of arity n, we have that

$$\mathbf{a} \in R^{\mathcal{M}} \iff \eta(\mathbf{a}) \in R^{\mathcal{N}}$$

An injective $\mathcal{L}$-homomorphism is called an $\mathcal{L}$-*embedding*. An invertible $\mathcal{L}$-homomorphism is called an $\mathcal{L}$-*isomorphism*.

Definition. If $\mathcal{M} \subseteq \mathcal{N}$ and the inclusion map is an $\mathcal{L}$-homomorphism, we say that $\mathcal{M}$ is a *substructure* of $\mathcal{N}$, and that $\mathcal{N}$ is an *extension* of $\mathcal{M}$. We will typically use the notation $\mathcal{M} \subseteq \mathcal{N}$ to indicate that $\mathcal{M}$ is a substructure of $\mathcal{N}$ when both are $\mathcal{L}$-structures, not just that it is a subset.

Example. (i) Let $\mathcal{L}$ be the language of groups. Then $(\mathbb{N}, +, 0)$ is a substructure of $(\mathbb{Z}, +, 0)$, but it is not a subgroup.

(ii) If $\mathcal{M}$ is an $\mathcal{L}$-structure, X is the domain of a substructure of $\mathcal{M}$ if and only if it is closed under the interpretations of all function symbols. The forward implication is clear. If f is a function symbol of arity n and X is closed under $f^{\mathcal{M}}$, $f^{\mathcal{M}}|_{X^n}$ is a function $X^n \to X$ interpreting f on the domain X, as required. In particular, any substructure should also contain all of the constants in the language.

(iii) The substructure *generated by* a subset $X \subseteq \mathcal{M}$ is given by the smallest set that contains X and is closed under the interpretations of all function symbols in $\mathcal{M}$. This is denoted $\langle X \rangle_{\mathcal{M}}$, and one can check that for infinite $\mathcal{L}$ (but not necessarily infinite signature),

$$|\langle X \rangle_{\mathcal{M}}| \leq |X| + |\mathcal{L}|$$

We prove this by iteratively closing up X by applying interpretations of function symbols to elements of X, and then taking the union of the resulting sets. At each stage, for each function symbol f of arity n, we add at most $|X|^n \leq |X| \cdot \aleph_0$ new elements. So in a single stage, we add at most $|X| \cdot \aleph_0 \cdot |\mathcal{L}| = |X| \cdot |\mathcal{L}|$ new elements to X. Repeating this ω times, the final set has size at most

$$\begin{aligned}|X| + |X| \cdot |\mathcal{L}| + |X| \cdot |\mathcal{L}|^2 + \cdots &= |X|(1 + |\mathcal{L}| + |\mathcal{L}|^2 + \cdots) \\ &\leq |X|(|\mathcal{L}| + |\mathcal{L}| + |\mathcal{L}| + \cdots) \\ &= |X| \cdot |\mathcal{L}| \cdot \aleph_0 \\ &= |X| \cdot |\mathcal{L}|\end{aligned}$$

We say that $\mathcal{M}$ is *finitely generated* if there exists a finite subset $X \subseteq \mathcal{M}$ such that $\mathcal{M} = \langle X \rangle_{\mathcal{M}}$.

(iv) Consider

$$(\mathbb{R}, \cdot, -1) \vDash \neg \exists x. (x^2 = -1)$$

But it has an extension $(\mathbb{C}, \cdot, -1)$ that does not model this sentence.

Proposition. Let $\varphi(\mathbf{x})$ be a quantifier-free $\mathcal{L}$-formula with n free variables. Let $\mathcal{M}$ be an $\mathcal{L}$-structure, and let $\mathbf{a}$ be an n-tuple in $\mathcal{M}$. Then for every extension $\mathcal{N}$ of $\mathcal{M}$,

$$\mathcal{M} \vDash \varphi(\mathbf{a}) \iff \mathcal{N} \vDash \varphi(\mathbf{a})$$

Proof. We proceed by induction on the structure of formulae. First, we show that if $t(\mathbf{x})$ is a term with k free variables, then

$$t^{\mathcal{M}}(\mathbf{b}) = t^{\mathcal{N}}(\mathbf{b})$$

for all $\mathbf{b} \in \mathcal{M}^k$. It is clearly the case if $t = x_i$ is a variable, as both structures interpret $t(\mathbf{b})$ as b_i. Suppose t is a term of the form $t = f(q_1, \dots, q_\ell)$ for f a function symbol of arity ℓ and the q_i are terms. By the inductive hypothesis we have

$$q_i^{\mathcal{M}}(\mathbf{b}) = q_i^{\mathcal{N}}(\mathbf{b})$$

Therefore,

$$\begin{aligned}t^{\mathcal{M}}(\mathbf{b}) &= f^{\mathcal{M}}(q_1^{\mathcal{M}}(\mathbf{b}), \dots, q_\ell^{\mathcal{M}}(\mathbf{b})) \\ &= f^{\mathcal{N}}(q_1^{\mathcal{M}}(\mathbf{b}), \dots, q_\ell^{\mathcal{M}}(\mathbf{b})) \\ &= f^{\mathcal{N}}(q_1^{\mathcal{N}}(\mathbf{b}), \dots, q_\ell^{\mathcal{N}}(\mathbf{b})) \\ &= t^{\mathcal{N}}(\mathbf{b})\end{aligned}$$

Thus terms are interpreted the same way in both models. For terms t_1, t_2 with the same free variables $\mathbf{x}$, then for any choice of $\mathbf{a}$,

$$\begin{aligned}\mathcal{M} \vDash (t_1(\mathbf{x}) = t_2(\mathbf{x})) &\iff t_1^{\mathcal{M}}(\mathbf{a}) = t_2^{\mathcal{M}}(\mathbf{a}) \\ &\iff t_1^{\mathcal{N}}(\mathbf{a}) = t_2^{\mathcal{M}}(\mathbf{b}) \\ &\iff \mathcal{N} \vDash (t_1(\mathbf{x}) = t_2(\mathbf{x}))\end{aligned}$$

Let R be a relation symbol of arity n, and let $t_1, \dots, t_n$ be terms with the same free variables $\mathbf{x}$.

$$\begin{aligned}\mathcal{M} \vDash R(t_1(\mathbf{x}), \dots, t_n(\mathbf{x})) &\iff (t_1^{\mathcal{M}}(\mathbf{a}), \dots, t_n^{\mathcal{M}}(\mathbf{a})) \in R^{\mathcal{M}} \\ &\iff (t_1^{\mathcal{M}}(\mathbf{a}), \dots, t_n^{\mathcal{M}}(\mathbf{a})) \in R^{\mathcal{N}} \\ &\iff (t_1^{\mathcal{N}}(\mathbf{a}), \dots, t_n^{\mathcal{N}}(\mathbf{a})) \in R^{\mathcal{N}} \\ &\iff \mathcal{N} \vDash R(t_1(\mathbf{x}), \dots, t_n(\mathbf{x}))\end{aligned}$$

So the result holds for all atomic formulae. For connectives, note that

$$\begin{aligned} \mathcal{M} \vDash \neg\varphi &\iff \mathcal{M} \nvDash \varphi \\ &\iff \mathcal{N} \nvDash \varphi \\ &\iff \mathcal{N} \vDash \neg\varphi \end{aligned}$$

and

$$\begin{aligned} \mathcal{M} \vDash \varphi \wedge \psi &\iff (\mathcal{M} \vDash \varphi) \wedge (\mathcal{M} \vDash \psi) \\ &\iff (\mathcal{N} \vDash \varphi) \wedge (\mathcal{N} \vDash \psi) \\ &\iff \mathcal{N} \vDash \varphi \wedge \psi \end{aligned}$$

As quantifier-free formulae can be built out of atomic formulae, negation, and conjunction, we have completed the proof. □

1.3 Elementary equivalence

Definition. Structures $\mathcal{M}, \mathcal{N}$ are called *elementarily equivalent* if for every $\mathcal{L}$-sentence,

$$\mathcal{M} \vDash \varphi \iff \mathcal{N} \vDash \varphi$$

A map $f : \mathcal{M} \to \mathcal{N}$ is an *elementary embedding* if it is injective, and for all $\mathcal{L}$-formulae $\varphi(x_1, \dots, x_n)$ and elements $m_1, \dots, m_n \in \mathcal{M}$, we have

$$\mathcal{M} \vDash \varphi(m_1, \dots, m_n) \iff \mathcal{N} \vDash \varphi(f(m_1), \dots, f(m_n))$$

If there is an elementary embedding between two structures, they are elementarily equivalent. If $\mathcal{M}$ and $\mathcal{N}$ are elementarily equivalent, we write $\mathcal{M} \equiv \mathcal{N}$.

Remark. If $\mathcal{M}$ and $\mathcal{N}$ are $\mathcal{L}$-structures, and $\mathbf{m} \in \mathcal{M}, \mathbf{n} \in \mathcal{N}$ are ordered tuples of the same length k, then by

$$(\mathcal{M}, \mathbf{m}) \equiv (\mathcal{N}, \mathbf{n})$$

we view $(\mathcal{M}, \mathbf{m})$ and $(\mathcal{N}, \mathbf{n})$ as structures over $\mathcal{L}$ with k additional constants, interpreting these new constants as the elements of $\mathbf{m}$ and $\mathbf{n}$ respectively.

Proposition. If $\mathcal{M} \cong \mathcal{N}$, then $\mathcal{M} \equiv \mathcal{N}$.

This can be easily shown by induction. The converse is generally not true, for example if the structures are infinite.

Definition. A substructure $\mathcal{M} \subseteq \mathcal{N}$ is an *elementary substructure* if the inclusion map is an elementary embedding. In this case, we also say that $\mathcal{N}$ is an *elementary extension* of $\mathcal{M}$. We write $\mathcal{M} \preceq \mathcal{N}$.

1.4 Categorical and complete theories

Recall that a theory $\mathcal{T}$ is *complete* if either $\mathcal{T} \vdash \varphi$ or $\mathcal{T} \vdash \neg\varphi$ for all sentences φ. Then any two models of a complete theory are elementarily equivalent, but they may have different cardinalities.

Definition. A theory $\mathcal{T}$ is *model-complete* if every embedding between models of $\mathcal{T}$ is elementary.

Definition. Let κ be an infinite cardinal. A theory $\mathcal{T}$ is *κ-categorical* if all models of $\mathcal{T}$ of cardinality κ are isomorphic.

It turns out that if theory on a countable language is categorical for some uncountable cardinal, then it is categorical for all infinite cardinals.

Proposition (Vaught's test)**.** Let $\mathcal{T}$ be a consistent $\mathcal{L}$-theory that has no finite models. If $\mathcal{T}$ is κ-categorical for some infinite $\kappa \geq |\mathcal{L}|$, then $\mathcal{T}$ is complete.

Proof. Suppose there is some φ such that $\mathcal{T} \nvDash \varphi$ and $\mathcal{T} \nvDash \neg\varphi$. Then $\mathcal{T} \cup \{\varphi\}$ and $\mathcal{T} \cup \{\neg\varphi\}$ are consistent theories, so have models. As $\mathcal{T}$ has no finite models, these two models are infinite. In fact, by the Löwenheim–Skolem theorem, the models can be forced to have size κ. But these models are in particular models of $\mathcal{T}$, so they must be isomorphic. Since they are isomorphic, they are elementarily equivalent. But the models disagree on the truth value of φ, giving a contradiction. $\square$

Example. (i) Any two countable dense linear orders are isomorphic, so the theory of dense linear orders without endpoints is $\aleph_0$-categorical. Thus, by Vaught's test, the theory DLO of dense linear orders without endpoints is complete.

(ii) Let F be a field. The theory of infinite (not infinite-dimensional) F-vector spaces is κ-categorical for $\kappa > |F|$. Hence, the theory is complete.

1.5 Tarski–Vaught test

Proposition. Let $\mathcal{N}$ be an $\mathcal{L}$-structure, and let $M \subseteq \mathcal{N}$. Then M is the domain of an elementary substructure if and only if for any formula $\varphi(x, \mathbf{t})$ and tuple $\mathbf{m} \in M$, if there exists a witness $n \in \mathcal{N}$ such that $\mathcal{N} \vDash \varphi(n, \mathbf{m})$, then there is a witness $\hat{n} \in M$ such that $\mathcal{N} \vDash \varphi(\hat{n}, \mathbf{m})$.

Proof. If M is the domain of an elementary substructure $\mathcal{M}$, then $\mathcal{N} \vDash \exists x.\, \varphi(x, \mathbf{m})$ implies that $\mathcal{M} \vDash \exists x.\, \varphi(x, \mathbf{m})$. Thus $\mathcal{M} \vDash \varphi(\hat{m}, \mathbf{m})$ for some $\hat{m} \in \mathcal{M}$. But then $\mathcal{N} \vDash \varphi(\hat{m}, \mathbf{m})$, as required.

For the other implication, if $M \subseteq \mathcal{N}$ has the stated property, we first show that M is closed under the interpretation of function symbols. Consider the formulae $\varphi_f(x, \mathbf{t}) = (x = f(\mathbf{t}))$ for each function symbol f in $\mathcal{L}$. Then for any $\mathbf{m} \in M$, there exists $n \in \mathcal{N}$ such that $\mathcal{N} \vDash n = f(\mathbf{m})$, but then by hypothesis, there exists $\hat{m} \in M$ such that $\mathcal{N} \vDash \hat{m} = f(\mathbf{m})$. Thus $f(\mathbf{m}) = \hat{m} \in M$. Interpreting relation symbols on M in the obvious way, we turn M into an $\mathcal{L}$-structure $\mathcal{M}$, which is clearly a substructure of $\mathcal{N}$.

It now remains to show that the substructure $\mathcal{M}$ of $\mathcal{N}$ is elementary. This follows from induction over the number of quantifiers in formulae, noting that the truth values of quantifier-free formulae are always preserved under any extension. $\square$

1.6 Universal theories and the method of diagrams

Definition. A formula φ is *universal* if it is of the form $\forall \mathbf{x}.\, \psi(\mathbf{x}, \mathbf{y})$ where ψ is quantifier-free. A theory is *universal* if all its axioms are universal sentences.

Definition. Let $\mathcal{N}$ be an $\mathcal{L}$-structure. We define the *diagram* of $\mathcal{N}$ to be the set

$$\operatorname{Diag} \mathcal{N} = \{\varphi(n_1, \dots n_k) \mid \varphi \text{ is a quantifier-free } \mathcal{L}_{\mathcal{N}}\text{-formula}, \mathcal{N} \vDash \varphi(n_1, \dots, n_k)\}$$

The *elementary diagram* of $\mathcal{N}$ is

$$\operatorname{Diag}_{\mathrm{el}} \mathcal{N} = \{\varphi(n_1, \dots n_k) \mid \varphi \text{ is an } \mathcal{L}_{\mathcal{N}}\text{-formula}, \mathcal{N} \vDash \varphi(n_1, \dots, n_k)\}$$

The diagram of a group is a slight generalisation of its multiplication table. Note that a model of a diagram is the same as an extension, and a model of an elementary diagram is the same as an elementary extension.

Lemma. Let $\mathcal{T}$ be a consistent theory, and let $\mathcal{T}_\forall$ be the theory of universal sentences proven by $\mathcal{T}$. If $\mathcal{N}$ is a model of $\mathcal{T}_\forall$, then $\mathcal{T} \cup \operatorname{Diag} \mathcal{N}$ is consistent.

Proof. Suppose $\mathcal{T} \cup \operatorname{Diag} \mathcal{N}$ is inconsistent. As $\mathcal{T}$ is consistent, by compactness there must be a finite number of sentences in the diagram $\operatorname{Diag} \mathcal{N}$ that are inconsistent with $\mathcal{T}$. Taking the conjunction, we can reduce to the case where there is a single sentence $\varphi(\mathbf{n})$ that is inconsistent with $\mathcal{T}$. Then as $\mathcal{T} \cup \{\varphi(\mathbf{n})\}$ is inconsistent, $\mathcal{T} \vdash \neg\varphi(\mathbf{n})$. Since $\mathcal{T}$ has nothing to say about the new constants $\mathbf{n}$, we must in fact have $\mathcal{T} \vdash \forall \mathbf{x}.\, \neg\varphi(\mathbf{x})$. This is a universal consequence of $\mathcal{T}$, so by assumption $\mathcal{N}$ models it, giving a contradiction. □

Corollary (Tarski, Łoś)**.** An $\mathcal{L}$-theory $\mathcal{T}$ has a universal axiomatisation if and only if it is preserved under substructures. That is, if $\mathcal{M} \subseteq \mathcal{N}$ are substructures and $\mathcal{M} \vDash \mathcal{T}$ then $\mathcal{N} \vDash \mathcal{T}$. Dually, a theory has an existential axiomatisation if and only if it is preserved under extensions.

Proof. One direction is clear. Suppose $\mathcal{T}$ is preserved under taking substructures. If $\mathcal{N} \vDash \mathcal{T}$, then $\mathcal{N} \vDash \mathcal{T}_\forall$; we show that the converse also holds. By the previous proposition, $\mathcal{T} \cup \operatorname{Diag} \mathcal{N}$ is consistent. Let $\mathcal{N}^\star$ be a model of this theory. So $\mathcal{N}^\star$ is an extension of $\mathcal{N}$, and also models $\mathcal{T}$. But as $\mathcal{T}$ is preserved under substructures, $\mathcal{N}$ must model $\mathcal{T}$. □

We can show much more with the same method.

Theorem (elementary amalgamation theorem)**.** Let $\mathcal{M}, \mathcal{N}$ be $\mathcal{L}$-structures, and $\mathbf{m} \in \mathcal{M}, \mathbf{n} \in \mathcal{N}$ be tuples of the same size such that $(\mathcal{M}, \mathbf{m}) \equiv (\mathcal{N}, \mathbf{n})$. Then there is an elementary extension $\mathcal{K}$ of $\mathcal{M}$ and an elementary embedding $g : \mathcal{N} \rightarrowtail \mathcal{K}$ mapping each n_i to m_i.

Proof. Replacing $\mathcal{N}$ with an isomorphic copy if required, we can assume $\mathbf{m} = \mathbf{n}$, and that $\mathcal{M}$ and $\mathcal{N}$ have no other common elements. We show that the theory

$$\mathcal{T} = \operatorname{Diag}_{\mathrm{el}} \mathcal{M} \cup \operatorname{Diag}_{\mathrm{el}} \mathcal{N}$$

is consistent, using compactness. Suppose that Φ is a finite subset of sentences in $\mathcal{T}$, which of course includes only finitely many sentences in $\operatorname{Diag}_{\mathrm{el}} \mathcal{N}$. Let the conjunction of those sentences be written as $\varphi(\mathbf{m}, \mathbf{k})$, where $\varphi(\mathbf{x}, \mathbf{y})$ is an $\mathcal{L}_{\mathcal{N}}$-formula, and $\mathbf{k}$ are pairwise distinct elements of $\mathcal{N} \setminus \mathbf{m}$. If Φ is inconsistent, then

$$\operatorname{Diag}_{\mathrm{el}} \mathcal{M} \vdash \neg\varphi(\mathbf{m}, \mathbf{k})$$

Since the elements of $\mathbf{k}$ are distinct and not in $\mathcal{M}$, we in fact have

$$\operatorname{Diag}_{\mathrm{el}} \mathcal{M} \vdash \forall \mathbf{y}.\, \neg\varphi(\mathbf{m}, \mathbf{y})$$

In particular,

$$(\mathcal{M}, \mathbf{m}) \vDash \forall \mathbf{y}.\, \neg\varphi(\mathbf{m}, \mathbf{y})$$

By hypothesis,

$$(\mathcal{N}, \mathbf{n}) \vDash \forall \mathbf{y}.\, \neg\varphi(\mathbf{m}, \mathbf{y})$$

This is a contradiction, as $\varphi(\mathbf{m}, \mathbf{k}) \in \operatorname{Diag}_{\mathrm{el}} \mathcal{N}$. Hence $\mathcal{T}$ is consistent. Take $\mathcal{K}$ to be the $\mathcal{L}$-reduct of a model of $\mathcal{T}$. □

We can also use this technique to constrain the size of a model.

Theorem (Löwenheim–Skolem theorem)**.** Let $\mathcal{M}$ be an infinite $\mathcal{L}$-structure. Let $\kappa \geq |\mathcal{L}|$ be an infinite cardinal. Then,

(i) if $\kappa < |\mathcal{M}|$, there is an elementary substructure of $\mathcal{M}$ of size κ;
(ii) if $\kappa > |\mathcal{M}|$, there is an elementary extension of $\mathcal{M}$ of size κ.

We postpone the proof of part (i).

Proof. Expand the language $\mathcal{L}$ by adding constant symbols for each $m \in \mathcal{M}$ and $c \in \kappa$. Let

$$\mathcal{T} = \operatorname{Diag}_{\mathrm{el}} \mathcal{M} \cup \bigcup_{c \neq c' \in \kappa} \{\neg(c = c')\}$$

$\mathcal{T}$ has a model by compactness, and this model must be an elementary extension of $\mathcal{M}$ with size at least κ. We then apply the downward Löwenheim–Skolem theorem if necessary to obtain a model of size exactly κ. □

For example, if $\mathcal{L}$ is countable, every infinite $\mathcal{L}$-structure has a countable elementary substructure.

2 Quantifier elimination

2.1 Skolem functions

Definition. Let $\mathcal{T}$ be an $\mathcal{L}$-theory, and let $\varphi(\mathbf{x}, y)$ be an $\mathcal{L}$-formula where $\mathbf{x}$ is nonempty. A *Skolem function* for φ is an $\mathcal{L}$-term t such that

$$\mathcal{T} \vdash \forall \mathbf{x}.\, (\exists y.\, \varphi(\mathbf{x}, y) \to \varphi(\mathbf{x}, t(\mathbf{x})))$$

A *skolemisation* of an $\mathcal{L}$-theory $\mathcal{T}$ is a language $\mathcal{L}^+ \supseteq \mathcal{L}$ and an $\mathcal{L}^+$-theory $\mathcal{T}^+ \supseteq \mathcal{T}$ such that
(i) every $\mathcal{L}$-structure that models $\mathcal{T}$ can be expanded to an $\mathcal{L}^+$-structure that models $\mathcal{T}^+$;
(ii) $\mathcal{T}^+$ has Skolem functions for any $\mathcal{L}^+$-formula $\varphi(\mathbf{x}, y)$ where $\mathbf{x}$ is nonempty.
A theory is called a *Skolem theory* if it is a skolemisation of itself.

By 'expanded', we mean that $\mathcal{T}$ is given interpretations to the elements of $\mathcal{L}^+ \setminus \mathcal{L}$, but no new objects are added.

Proposition. Let $\mathcal{T}$ be an $\mathcal{L}$-theory, and let $\mathcal{F}$ be a collection of $\mathcal{L}$-formulae including all atomic formulae and closed under Boolean operations. Suppose that for every formula $\psi(\mathbf{x}, y) \in \mathcal{F}$, there exists $\varphi(\mathbf{x}) \in \mathcal{F}$ with

$$\mathcal{T} \vdash \forall \mathbf{x}.\, (\exists y.\, \psi(\mathbf{x}, y) \leftrightarrow \varphi(\mathbf{x}))$$

Then, every $\mathcal{L}$-formula is equivalent to one in $\mathcal{F}$ with the same free variables modulo $\mathcal{T}$ (that is, $\mathcal{T}$ proves they are equivalent).

Proof. We proceed by induction on the length of formulae. The case of existential formulae is the only nontrivial inductive step. Consider the formula $\exists y,\ \psi(\mathbf{x}, y)$. By the inductive hypothesis, $\psi(\mathbf{x}, y)$ is $\mathcal{T}$-equivalent to $\psi'(\mathbf{x}, y) \in \mathcal{F}$. Then, there is some $\varphi(\mathbf{x}) \in \mathcal{F}$ such that

$$\mathcal{T} \vdash \forall \mathbf{x}.\, (\exists y.\, \psi'(\mathbf{x}, y) \leftrightarrow \varphi(\mathbf{x}))$$

Thus the formula $\exists y,\ \psi(\mathbf{x}, y)$ in question is $\mathcal{T}$-equivalent to $\varphi(\mathbf{x}) \in \mathcal{F}$. □

Proposition. Let $\mathcal{T}$ be a Skolem theory. Then,
(i) every $\mathcal{L}$-formula $\varphi(\mathbf{x})$ where $\mathbf{x}$ is nonempty is equivalent modulo $\mathcal{T}$ to some quantifier-free $\varphi^\star(\mathbf{x})$;
(ii) if $\mathcal{N} \vDash \mathcal{T}$ and $X \subseteq \mathcal{N}$, then either $\langle X \rangle_{\mathcal{N}} = \varnothing$ or $\langle X \rangle_{\mathcal{N}} \preceq \mathcal{N}$.

Remark. When $\mathcal{N}$ is a model of a Skolem theory, $\langle X \rangle_{\mathcal{N}}$ is sometimes called the *Skolem hull* of X.

Proof. Part (i). Clearly, $\varphi(\mathbf{x}, t(\mathbf{x})) \to \exists y.\, \varphi(\mathbf{x}, y)$ in any model. So having Skolem functions means that

$$\mathcal{T} \vdash \forall \mathbf{x}.\, (\exists y.\, \varphi(\mathbf{x}, y) \leftrightarrow \varphi(\mathbf{x}, t(\mathbf{x})))$$

completing the proof by the previous proposition.

Part (ii). We proceed by the Tarski–Vaught test. Let $\mathcal{M} = \langle X \rangle_{\mathcal{N}}$, $\mathbf{m} \in \mathcal{M}$, and let $\varphi(\mathbf{x}, y)$ be such that

$$\mathcal{N} \vDash \exists y.\, \varphi(\mathbf{m}, y)$$

Then as $\mathcal{N}$ has Skolem functions, there exists an $\mathcal{L}$-term t such that

$$\mathcal{N} \vDash \varphi(\mathbf{m}, t(\mathbf{m}))$$

But $\mathcal{M}$ is closed under the interpretation of function symbols as it is a substructure, so $t(\mathbf{m}) \in \mathcal{M}$. Thus

$$\mathcal{M} \vDash \exists y.\, \varphi(\mathbf{m}, y)$$

as required. $\square$

2.2 Skolemisation theorem

Theorem. Every first-order language $\mathcal{L}$ can be expanded to some $\mathcal{L}^+ \supseteq \mathcal{L}$ that admits an $\mathcal{L}^+$-theory Σ such that

(i) Σ is a Skolem $\mathcal{L}^+$-theory;
(ii) any $\mathcal{L}$-structure can be expanded to an $\mathcal{L}^+$-structure that models Σ; and
(iii) $|\mathcal{L}^+| = |\mathcal{L}|$.

Proof. We will design $\mathcal{L}^+$ to include Skolem functions for each suitable formula. If $\chi(\mathbf{x}, y)$ is an $\mathcal{L}$-formula with $\mathbf{x}$ nonempty, we add a function symbol F_χ of arity $|\mathbf{x}|$. Performing this for all $\mathcal{L}$-formulae of this form, we obtain a language $\mathcal{L}' \supseteq \mathcal{L}$. Next, define $\Sigma(\mathcal{L})$ to be the set of $\mathcal{L}$-sentences that enforce the correct behaviour of the F_χ:

$$\forall \mathbf{x}.\, (\exists y.\, \chi(\mathbf{x}, y) \to \chi(\mathbf{x}, F_\chi(\mathbf{x})))$$

Note that $\Sigma(\mathcal{L})$ is an $\mathcal{L}'$-theory, not an $\mathcal{L}$-theory; there may be existentials in $\mathcal{L}'$ without explicit witnesses. We can overcome this issue by iterating this construction ω times and taking the union. Formally, we recursively define

$$\mathcal{L}_0 = \mathcal{L}; \quad \mathcal{L}_{n+1} = \mathcal{L}_n'; \quad \Sigma_0 = \varnothing; \quad \Sigma_{n+1} = \Sigma_n \cup \Sigma(\mathcal{L}_n)$$

Then we can set

$$\mathcal{L}^+ = \bigcup_{n<\omega} \mathcal{L}_n; \quad \Sigma = \bigcup_{n<\omega} \Sigma_n$$

First, note that Σ is a Skolem theory. This is because each $\mathcal{L}^+$-formula is in $\mathcal{L}_n$ for some $n < \omega$, so $\Sigma_{n+1} \subseteq \Sigma$ asserts that it has a Skolem function. It is also clear to see that $|\mathcal{L}^+| = |\mathcal{L}|$ using basic cardinal arithmetic.

To prove property (ii), it suffices to show that each $\mathcal{L}$-theory can be expanded into an $\mathcal{L}'$-theory that models $\Sigma(\mathcal{L})$; we can then proceed by induction. Note that this argument will use the axiom of choice. Let $\mathcal{M}$ be an $\mathcal{L}$-structure. We can assume $\mathcal{M} \neq \varnothing$; if $\mathcal{M} = \varnothing$ then all sentences in Σ would be vacuously true and there would be nothing to prove. We now expand $\mathcal{M}$ into an $\mathcal{L}'$-structure $\mathcal{M}$ in the following way. Consider $\chi(\mathbf{x}, y)$ where $\mathbf{x}$ is nonempty and $\mathbf{m} \in \mathcal{M}$. If

$$\mathcal{M} \vDash \exists b.\, \chi(\mathbf{m}, b)$$

then we can choose such a b and interpret $F_\chi(\mathbf{m})$ as this value. If

$$\mathcal{M} \nvDash \exists b.\, \chi(\mathbf{m}, b)$$

then we interpret $F_\chi(\mathbf{m})$ as an arbitrary model element, say, $\mathbf{m}_0$. By construction, $\mathcal{M}'$ models $\Sigma(\mathcal{L})$. $\square$

Corollary. Any $\mathcal{L}$-theory $\mathcal{T}$ admits a skolemisation $\mathcal{T}^+$ in a language $\mathcal{L}^+$ of the same size as $\mathcal{L}$.

Proof. Take $\mathcal{T}^+ = \mathcal{T} \cup \Sigma$. Any model of $\mathcal{T}^+$ models Σ, so $\mathcal{T}^+$ has Skolem functions. Moreover, any $\mathcal{L}$-structure that models $\mathcal{T}$ can be extended to one that models Σ, which will therefore model $\mathcal{T}^+$. □

Corollary (downward Löwenheim–Skolem theorem)**.** Let $\mathcal{M}$ be an $\mathcal{L}$-structure, and let $X \subseteq \mathcal{M}$. Let κ be a cardinal such that

$$|\mathcal{L}| + |X| \leq \kappa \leq |\mathcal{M}|$$

Then $\mathcal{M}$ has an elementary substructure of size κ that contains X.

Proof. Let $X \subseteq Y \subseteq \mathcal{M}$ and $|Y| = \kappa$. Let $\mathcal{M}'$ be an expansion of $\mathcal{M}$ to a Skolem theory, and consider the Skolem hull $\langle Y \rangle_{\mathcal{M}'}$. $\langle Y \rangle_{\mathcal{M}'}$ must be an elementary substructure of $\mathcal{M}'$ as $Y \neq \varnothing$. Let $\mathcal{N}$ be the $\mathcal{L}$-reduct of $\langle Y \rangle_{\mathcal{M}'}$. Then $\mathcal{N}$ is an elementary substructure of $\mathcal{N}$, and $X \subseteq \mathcal{N}$. It remains to check $|\mathcal{N}| = \kappa$.

$$|\mathcal{N}| \leq |Y| + |\mathcal{L}^+| = \kappa + |\mathcal{L}| = \kappa = |Y| \leq |\mathcal{N}|$$

So $|\mathcal{N}| = \kappa$. □

2.3 Elimination sets

Definition. Let $\mathcal{T}$ be an $\mathcal{L}$-theory. A set F of $\mathcal{L}$-formulae is an *elimination set* for $\mathcal{T}$ if, for every $\mathcal{L}$-formula φ, there is a Boolean combination $\varphi^\star$ of formulae in F such that

$$\mathcal{T} \vdash \varphi \leftrightarrow \varphi^\star$$

A theory $\mathcal{T}$ has *quantifier elimination* if the family of quantifier-free formulae forms an elimination set for $\mathcal{T}$.

Note that a theory having quantifier elimination depends on its underlying language. Every Skolem theory has quantifier elimination.

Example. (i) Let $p \in \mathbb{C}[x]$ be the polynomial $x^3 - 31x^2 + 6$ over $\mathbb{C}$. The sentence $\exists x.\ p(x) = 0$ contains a quantifier. But as $\mathbb{C}$ is algebraically closed, it is equivalent to the quantifier-free sentence $1 \neq 0 \vee (-31) \neq 0$.

(ii) A real-valued matrix is invertible if there exists a two-sided inverse. This has a quantifier, but there is a quantifier-free sentence equivalent to it, namely, 'its determinant is nonzero'.

Remark. (i) We can check if two models of $\mathcal{T}$ are elementarily equivalent by considering just those formulae in an elimination set. In particular, to check if a theory is complete, it suffices to check that all sentences in an elimination set are either deducible from the theory or inconsistent with it.

(ii) Suppose $\mathcal{L}$ is a recursive language, and the map $\varphi \mapsto \varphi^\star$ is computable. Then an algorithm to decide whether $\mathcal{T}$ proves any sentence can be produced from one that operates only on the elimination set.

(iii) The elementary embeddings $\mathcal{M} \rightarrowtail \mathcal{N}$ are precisely those embeddings that preserve φ and $\neg\varphi$ for all φ in F. So a theory with quantifier elimination is model-complete.

(iv) The definable sets of a model are precisely the Boolean combinations of sets definable with only formulae in an elimination set.

In the next result, we use the notation $\neg F$ for the set of negations of formulae in F.

Proposition (syntactic quantifier elimination)**.** Let $\mathcal{T}$ be an $\mathcal{L}$-theory, and let F be a family of $\mathcal{L}$-formulae including all atomic formulae. Suppose that, for every $\mathcal{L}$-formula of the form

$$\theta(\mathbf{x}) = \exists y.\ \bigwedge_{i<n} \varphi_i(\mathbf{x}, y); \quad \varphi_i \in F \cup \neg F$$

there exists a Boolean combination $\theta^\star(\mathbf{x})$ of formulae in F such that

$$\mathcal{T} \vdash \forall \mathbf{x}.\, (\theta(\mathbf{x}) \leftrightarrow \theta^\star(\mathbf{x}))$$

Then F is an elimination set for $\mathcal{T}$.

The proof is similar to a previous proposition.

Example. Consider the theory $\mathcal{T}_\infty$ of infinite sets in the language with empty signature. The only atomic formulae are equalities, and the only terms in the language are variables. Using the above proposition, it suffices to eliminate the existential quantifier in formulae $\varphi(x_0, \dots, x_{n-1})$ of the form

$$\exists y. \left(\bigwedge_{i \in I} y = x_i \right) \wedge \left(\bigwedge_{i \in J} y \neq x_i \right) \wedge \left(\bigwedge_{i,j \in K} x_i = x_j \right) \wedge \left(\bigwedge_{i,j \in L} x_i \neq x_j \right)$$

where $I, J, K, L \subseteq \{0, \dots, n-1\}$. Without loss of generality we can assume I is empty, as we can easily remove the quantifier in this situation. We may also push the quantifier inside the first conjunct.

$$\left(\exists y. \bigwedge_{i \in J} y \neq x_i \right) \wedge \psi(x_0, \dots, x_{n-1}); \quad \psi(x_0, \dots, x_{n-1}) = \left(\bigwedge_{i,j \in K} x_i = x_j \right) \wedge \left(\bigwedge_{i,j \in L} x_i \neq x_j \right)$$

But the theory of infinite sets proves $\exists y.\ \bigwedge_{i \in J} y \neq x_i$, so we can conclude that φ and ψ are equivalent modulo $\mathcal{T}$.

2.4 Amalgamation

Definition. Let $\mathcal{M}$ and $\mathcal{N}$ be $\mathcal{L}$-structures. We write $\mathcal{M} \to_1 \mathcal{N}$ if every existential sentence modelled by $\mathcal{M}$ is also modelled by $\mathcal{N}$.

Theorem (existential amalgamation)**.** Let $\mathcal{M}$ and $\mathcal{N}$ be $\mathcal{L}$-structures, with $S \subseteq \mathcal{M}$. Suppose there is a homomorphism $f : \langle S \rangle_{\mathcal{M}} \to \mathcal{N}$ such that $(\mathcal{N}, f(S)) \to_1 (\mathcal{M}, S)$. Then there is an elementary extension $\mathcal{K}$ of $\mathcal{N}$ and an embedding $g : \mathcal{M} \rightarrowtail \mathcal{K}$ making the following diagram commute.

$$\begin{tikzcd} & \mathcal{K} & \\ \mathcal{M} \arrow[ur, tail, "\preceq"] & & \mathcal{N} \arrow[ul, tail, "g"'] \\ & \langle S \rangle_{\mathcal{M}} \arrow[ul, tail] \arrow[ur, "f"'] & \end{tikzcd}$$

Proof. Let $\mathcal{M}, \mathcal{N}$ be disjoint without loss of generality. Consider the $\mathcal{L}_{\mathcal{M} \sqcup \mathcal{N}}$-theory

$$\mathcal{T} = \mathrm{Diag}_{\mathrm{el}} \mathcal{M} \cup \mathrm{Diag} \mathcal{N} \cup \bigcup_{s \in S} \{s = f(s)\}$$

We show this is consistent by compactness; then, a model $\mathcal{K}$ will be an elementary extension of $\mathcal{M}$, and $\mathcal{N}$ embeds into it in such a way that makes the above diagram commute due to the sentences $s = f(s)$. If $\mathcal{T}$ is inconsistent, there is a finite set of formulae in $\mathrm{Diag}\,\mathcal{N}$ that are inconsistent with

$$\mathcal{T}' = \mathrm{Diag}_{\mathrm{el}} \mathcal{M} \cup \bigcup_{s \in S} \{s = f(s)\}$$

Taking the conjunction, we can suppose it is a single formula $\varphi(\mathbf{n})$, where $\mathbf{n} \in \mathcal{N}$ is a tuple of pairwise distinct elements.

$$\mathcal{T}' \vdash \neg\varphi(\mathbf{n})$$

Then, using the sentences $s = f(s)$ and the fact that $\langle S \rangle_{\mathcal{M}}$ is generated by S, the formula $\varphi(\mathbf{n})$ is equivalent modulo $\mathcal{T}'$ to some quantifier-free formula $\psi(\mathbf{s}, \mathbf{n}')$ where $\mathbf{s} \in S$ and $\mathbf{n}' \in \mathcal{N} \setminus \operatorname{im} f$.

$$\mathcal{T}' \vdash \neg\psi(\mathbf{s}, \mathbf{n}')$$

Now, note that $\mathcal{T}'$ has nothing to say about $\mathbf{n}'$, so in fact

$$\mathcal{T}' \vdash \forall \mathbf{x}.\, \neg\psi(\mathbf{s}, \mathbf{x})$$

As $(\mathcal{N}, f(S)) \rightarrow_1 (\mathcal{M}, S)$, we can convert the universal quantifier above into the negation of an existential quantifier to conclude

$$\mathcal{N} \vdash \neg\exists \mathbf{x}.\, \psi(\mathbf{s}, \mathbf{x})$$

so

$$\mathcal{N} \vdash \neg\exists \mathbf{x}.\, \psi(\mathbf{s}, \mathbf{x})$$

But $\varphi(\mathbf{n})$ is in the diagram of $\mathcal{N}$, so $\mathcal{N} \vdash \exists \mathbf{x}.\, \psi(\mathbf{s}, \mathbf{x})$, giving a contradiction. $\square$

We can make the following more general definition.

Definition. A class $\mathbb{K}$ of $\mathcal{L}$-structures has the *amalgamation property* if, given a diagram of elements of $\mathbb{K}$

$$\begin{tikzcd} \mathcal{B} & & \mathcal{A} \\ & \mathcal{C} \arrow[ul, tail] \arrow[ur, tail] & \end{tikzcd}$$

there is a structure $\mathcal{D}$ in $\mathbb{K}$ and embeddings making the following diagram commute.

$$\begin{tikzcd} & \mathcal{D} & \\ \mathcal{B} \arrow[ur, tail] & & \mathcal{A} \arrow[ul, tail] \\ & \mathcal{C} \arrow[ul, tail] \arrow[ur, tail] & \end{tikzcd}$$

Definition. Let $\mathbb{K}$ be a class of $\mathcal{L}$-structures and $\mathcal{M} \in \mathbb{K}$. We say that $\mathcal{M}$ is *existentially closed in* $\mathbb{K}$ if, for every existential formula $\psi(\mathbf{x})$ and tuple $\mathbf{m} \in \mathcal{M}$, the existence of an extension $\mathcal{M} \subseteq \mathcal{N} \in \mathbb{K}$ with $\mathcal{N} \vDash \psi(\mathbf{m})$ forces $\mathcal{M} \vDash \psi(\mathbf{m})$.

Note that being existentially closed in $\mathbb{K}$ depends on the choice of $\mathbb{K}$. For example, an existentially closed ordered field need not be an existentially closed field.

Example. (i) Every field that is existentially closed in the class of fields is algebraically closed. Let A be an existentially closed field, and view a nontrivial polynomial $f(\mathbf{y})$ over A as a statement $p(\mathbf{a}, y)$ where $p(\mathbf{x}, y)$ is a term in the language of rings, and $\mathbf{a}$ is a tuple. For instance, y^2+2y-3 can be seen as $p(1,2,3,y)$, where $p(x_0, x_1, x_2, y) = x_0y^2 + x_1y + (-x_2)$. We can replace f with an irreducible factor and consider the quotient ring ${}^{A[y]}\!/_{(f)}$, which is an extension of A over which f has a root.

$$^{A[y]}\!/_{(f)} \vDash \exists y.\ p(\mathbf{a}, y) = 0$$

Since f is irreducible, this is an extension of fields. Thus, as A is existentially closed,

$$A \vDash \exists y.\ p(\mathbf{a}, y) = 0$$

so f has a root in A. The converse is true, and is one way that Hilbert's Nullstellensatz can be stated.

(ii) The existentially closed linear orders are precisely the dense linear orders without endpoints.

(iii) The existentially closed ordered fields are precisely the *real closed fields*, which are the ordered fields elementarily equivalent to the real numbers. Equivalently, all nonnegative elements are squares, and all odd-degree elements have a root.

Theorem. Let $\mathbb{K}$ be a class of $\mathcal{L}$-structures that is closed under isomorphism. Suppose that the class of all of the substructures of the structures in $\mathbb{K}$ has the amalgamation property. Then, every existential $\mathcal{L}$-formula $\varphi(\mathbf{x})$ is equivalent to a quantifier-free $\mathcal{L}$-formula in all existentially closed structures in $\mathbb{K}$. In particular, if $\mathcal{T}$ is a theory axiomatising existentially closed structures in $\mathbb{K}$, then $\mathcal{T}$ has quantifier elimination.

Proof. Let $\varphi(\mathbf{x})$ be an existential formula. We will call a pair $(\mathcal{M}, \mathbf{m})$ a *witnessing pair* if $\mathcal{M}$ is existentially closed in $\mathbb{K}$ and $\mathcal{M} \vDash \varphi(\mathbf{m})$. For each such pair, let

$$\theta_{(\mathcal{M},\mathbf{m})}(\mathbf{x}) = \bigwedge \{\psi(\mathbf{x}) \text{ a literal} \mid \mathcal{M} \vDash \psi(\mathbf{m})\}$$

where the *literals* are the atomic formulae and their negations. Let

$$\chi(\mathbf{x}) = \bigvee_{(\mathcal{M},\mathbf{m})} \theta_{(\mathcal{M},\mathbf{m})}(\mathbf{x})$$

It suffices to show that if $\mathcal{N}$ is existentially closed in $\mathbb{K}$ then

$$(\mathcal{N} \vDash \varphi(\mathbf{n})) \iff (\mathcal{N} \vDash \chi(\mathbf{n}))$$

Then we can use the compactness theorem twice to reduce χ to a first-order finitary formula as required. If $\mathbf{n} \in \mathcal{N}$ is such that $\mathcal{N} \vDash \varphi(\mathbf{n})$, then $(\mathcal{N}, \mathbf{n})$ is a witnessing pair, and thus $\mathcal{N} \vDash \chi(\mathbf{n})$ by construction. For the converse, if $\mathcal{N} \vDash \chi(\mathbf{n})$, there is a witnessing pair $(\mathcal{M}, \mathbf{m})$ such that $\mathcal{N} \vDash \theta_{(\mathcal{M},\mathbf{m})}(\mathbf{n})$. Hence, for each literal $\psi(\mathbf{x})$,

$$(\mathcal{M} \vDash \psi(\mathbf{m})) \implies (\mathcal{N} \vDash \psi(\mathbf{n}))$$

There is thus an embedding $e : \langle \mathbf{m} \rangle_{\mathcal{M}} \rightarrowtail \mathcal{N}$ mapping $\mathbf{m}$ to $\mathbf{n}$. Applying the amalgamation property, we obtain

$$\begin{tikzcd}
& \mathcal{D} & \\
& \mathcal{C} \arrow[u, tail] & \\
\mathcal{M} \arrow[ur, tail] \arrow[uur, dashed, tail, bend left, "g"] & & \mathcal{N} \arrow[ul, tail] \arrow[uul, dashed, tail, bend right, "h"'] \\
& \langle \mathbf{m} \rangle_{\mathcal{M}} \arrow[ul, tail] \arrow[ur, tail, "e"'] &
\end{tikzcd}$$

where $\mathcal{D} \in \mathbb{K}$, and both $\mathcal{M}, \mathcal{N}$ embed into $\mathcal{C}$ and therefore into $\mathcal{D}$. Note that $g(\mathbf{m}) = h(\mathbf{n})$. Replacing $\mathcal{D}$ with an isomorphic copy if required, we may assume that h is an inclusion, so $g(\mathbf{m}) = \mathbf{n}$. We know that $(\mathcal{M}, \mathbf{m})$ is a witnessing pair, so $\mathcal{M} \vDash \varphi(\mathbf{m})$. Then $\mathcal{D} \vDash \varphi(g(\mathbf{m}))$ as existential formulae are preserved under taking extensions. Since $\mathcal{N}$ is existentially closed in $\mathbb{K}$, $\mathcal{D} \in \mathbb{K}$, and $\mathcal{N} \subseteq \mathcal{D}$, we conclude that $\mathcal{N} \vDash \varphi(g(\mathbf{m}))$ so $\mathcal{N} \vDash \varphi(\mathbf{n})$ as required.

In particular, if $\mathcal{T}$ is a theory axiomatising existentially closed structures in $\mathbb{K}$, then $\mathcal{T}$ has quantifier elimination by applying the completeness theorem and then using the syntactic criterion for quantifier elimination proven previously. □

Example. We show that the theory ACF of algebraically closed fields has quantifier elimination. First, recall that ACF axiomatises the existentially closed fields, so it suffices to check that the class of substructures of fields has the amalgamation property. Note that a substructure of a field must satisfy all universal sentences in the theory of fields, so the substructures of fields are precisely the integral domains. General field theory shows that the class of fields has the amalgamation property; we can then prove that the class of integral domains has the amalgamation property by passing to fraction fields.

Example. The theory DLO of dense linear orders without endpoints has quantifier elimination. The class of substructures of dense linear orders has the amalgamation property: indeed, any two linear orders embed into a poset, which can be extended into a linear order by Zorn's lemma, and is thus a substructure of some dense linear order.

2.5 Inductive classes

Definition. A class $\mathbb{K}$ of $\mathcal{L}$-structures is *inductive* if it is closed under isomorphisms and under unions of chains of embeddings.

Theorem. Let $\mathcal{M}$ be a structure in an inductive class $\mathbb{K}$. Then $\mathcal{M} \subseteq \mathcal{N}$ for some $\mathcal{N}$ existentially closed in $\mathbb{K}$.

This is analogous to the theorem that every field has an algebraic closure, and is proven in a similar way.

Proof. We show that $\mathcal{M}$ can be extended to some structure $\mathcal{M}^\star \in \mathbb{K}$ with the property that for all $\mathbf{m} \in \mathcal{M}$ and $\varphi(\mathbf{x})$ an existential $\mathcal{L}$-formula, if $\varphi(\mathbf{m})$ holds in some extension of $\mathcal{M}^\star$ in $\mathbb{K}$, then $\varphi(\mathbf{m})$ holds in $\mathcal{M}^\star$.

We now show that this suffices to complete the proof. Indeed, we then recursively define a chain of $\mathbb{K}$-structures by setting $\mathcal{M}^{(0)} = \mathcal{M}$ and $\mathcal{M}^{(i+1)} = (\mathcal{M}^{(i)})^\star$, then taking their union to form $\mathcal{N}$. Then $\mathcal{N}$ lies in $\mathbb{K}$ as $\mathbb{K}$ is inductive, and moreover it extends $\mathcal{M}$.

This $\mathcal{N}$ is existentially closed in $\mathbb{K}$. Suppose $\varphi(\mathbf{x})$ is an existential formula, $\mathbf{n} \in \mathcal{N}$, and $\mathcal{D}$ is a structure in $\mathbb{K}$ such that $\mathcal{D} \vDash \varphi(\mathbf{n})$. As $\mathbf{n} \in \bigcup_{i<\omega} \mathcal{M}^{(i)}$ and the $\mathcal{M}^{(i)}$ form a chain, there must be $k < \omega$ such that $\mathbf{n} \in \mathcal{M}^{(k)}$. Then $(\mathcal{M}^{(k)})^\star = \mathcal{M}^{(k+1)} \vDash \varphi(\mathbf{n})$, so in particular, $\mathcal{N} \vDash \varphi(\mathbf{n})$.

We now construct $\mathcal{M}^\star$. Using the axiom of choice, create an ordinal-indexed list of pairs $(\varphi_\beta, \mathbf{m}_\beta)_\beta$ where φ is an existential formula and $\mathbf{m} \in \mathcal{M}$, and β ranges over all ordinals less than some ordinal δ. We then construct a chain of $\mathbb{K}$-structures by transfinite induction. Let $\mathcal{M}_0 = \mathcal{M}$. At each successor stage, let $\mathcal{M}_{\beta+1}$ be a $\mathbb{K}$-structure $\mathcal{D}$ that extends $\mathcal{M}_\beta$ and models $\varphi_\beta(\mathbf{m}_\beta)$, if this exists. If such a model does not exist, define $\mathcal{M}_{\beta+1} = \mathcal{M}_\beta$. At each limit stage, let $\mathcal{M}_\lambda = \bigcup_{\beta<\lambda} \mathcal{M}_\beta$. Finally, set $\mathcal{M}^\star = \mathcal{M}_\delta$.

If $\varphi(\mathbf{x})$ is existential, $\mathbf{m} \in \mathcal{M}$, and $\mathcal{D}$ is some $\mathbb{K}$-structure that extends $\mathcal{M}^\star$ and models $\varphi(\mathbf{m})$, then $(\varphi, \mathbf{m}) = (\varphi_\beta, \mathbf{m}_\beta)$ for some $\beta < \delta$. Then $\mathcal{M}_\beta \subseteq \mathcal{M}^\star \subseteq \mathcal{D}$, so $\mathcal{M}_{\beta+1}$ models $\varphi_\beta(\mathbf{m}_\beta) = \varphi(\mathbf{m})$ by definition. But as φ is existential and $\mathcal{M}^\star$ extends $\mathcal{M}_\beta$, we must also have that $\mathcal{M}^\star$ models $\varphi(\mathbf{m})$, as required. $\square$

2.6 Characterisations of quantifier elimination

Theorem. Let $\mathcal{T}$ be an $\mathcal{L}$-theory. Then the following are equivalent.

(i) The theory $\mathcal{T}$ is model-complete.

(ii) Every model of $\mathcal{T}$ is an existentially closed model of $\mathcal{T}$.

(iii) Given an embedding $e : \mathcal{A} \rightarrowtail \mathcal{B}$ between models of $\mathcal{T}$, there is an elementary extension $\mathcal{D}$ of $\mathcal{A}$ and an embedding $g : \mathcal{B} \rightarrowtail D$ such that $g \circ e = \mathrm{id}_{\mathcal{A}}$.

(iv) For any quantifier-free $\mathcal{L}$-formula $\varphi(\mathbf{x}, \mathbf{y})$, the formula $\exists \mathbf{y}.\, \varphi(\mathbf{x}, \mathbf{y})$ is equivalent to some universal $\mathcal{L}$-formula $\psi(\mathbf{x})$ modulo $\mathcal{T}$.

(v) Every $\mathcal{L}$-formula is equivalent to some universal $\mathcal{L}$-formula modulo $\mathcal{T}$.

Proof. (i) implies (ii). As all embeddings between models are elementary, if a superstructure has a witness to an existential, so does the substructure.

(ii) implies (iii). We use the existential amalgamation theorem. Take S to be the set of all elements of $\mathcal{A}$, then by (ii), $(\mathcal{B}, e(S)) \to_1 (\mathcal{A}, S)$. We obtain

$$\begin{tikzcd}
 & \mathcal{D} & \\
\mathcal{A} \arrow[ur, "\preceq"] & & \mathcal{B} \arrow[ul, tail, "g"'] \\
 & \mathcal{A} \arrow[ul, "1_A"] \arrow[ur, tail, "e"'] &
\end{tikzcd}$$

as required.

(iii) implies (iv). It suffices to show that any universal formula $\varphi(\mathbf{x})$ is preserved under embeddings. If so, then $\varphi(\mathbf{x})$ is equivalent to an existential $\mathcal{L}$-formula, so in particular, any existential formula is equivalent to a universal formula. Let $e : \mathcal{A} \rightarrowtail \mathcal{B}$ be an embedding. Then by (iii) we have an elementary extension $\mathcal{A} \preceq \mathcal{D}$, so if $\mathcal{A} \vDash \varphi(\mathbf{a})$, then $\mathcal{D} \vDash \varphi(\mathbf{a})$, and as $\mathcal{B}$ is a substructure of $\mathcal{D}$, we have $\mathcal{B} \vDash \varphi(e(\mathbf{a}))$. The reverse implication follows from the fact that φ is universal.

(iv) implies (v). We proceed by induction on the structure of $\mathcal{L}$-formulae. We can iteratively convert existential quantifiers to universal quantifiers, noting that (iv) allows us to convert a sequence of existentials to a sequence of universals simultaneously.

(v) implies (i). Note that universal formulae are preserved under extensions, and every formula and its negation can be represented as a universal formula. This directly gives the result. □

Let $\mathcal{M}, \mathcal{N}$ be $\mathcal{L}$-structures. If $\mathcal{M}, \mathcal{N}$ satisfy the same quantifier-free sentences, we write $\mathcal{M} \equiv_0 \mathcal{N}$.

Theorem. Let $\mathcal{T}$ be an $\mathcal{L}$-theory. Then the following are equivalent.

(i) $\mathcal{T}$ has quantifier elimination.
(ii) If $\mathcal{A}, \mathcal{B} \vDash \mathcal{T}$ and $\mathbf{a} \in \mathcal{A}, \mathbf{b} \in \mathcal{B}$ are tuples of the same length, then $(\mathcal{A}, \mathbf{a}) \equiv_0 (\mathcal{B}, \mathbf{b})$ implies $(\mathcal{A}, \mathbf{a}) \to_1 (\mathcal{B}, \mathbf{b})$.
(iii) Whenever $\mathcal{A}, \mathcal{B} \vDash \mathcal{T}$, $S \subseteq \mathcal{A}$ and $e : \langle S \rangle_{\mathcal{A}} \rightarrowtail \mathcal{B}$, then there is an elementary extension $\mathcal{D}$ of $\mathcal{B}$ and an embedding $f : \mathcal{A} \rightarrowtail \mathcal{D}$ extending e.
(iv) $\mathcal{T}$ is model-complete and $\mathcal{T}_\forall$ has the amalgamation property.
(v) For every quantifier-free $\mathcal{L}$-formula $\varphi(\mathbf{x}, y)$, the formula $\exists y.\, \varphi(\mathbf{x}, y)$ is $\mathcal{T}$-equivalent to a quantifier-free formula $\psi(\mathbf{x})$.

Proof. (i) implies (ii) is clear.

(ii) implies (iii). It suffices to show that $(\mathcal{A}, S) \to_1 (\mathcal{B}, e(S))$ by the existential amalgamation theorem. Since a sentence in $\mathcal{L}_S$ is finite, it can only mention finitely many of the new constants in S, so it is enough to check that $(\mathcal{A}, \mathbf{a}) \to_1 (\mathcal{B}, e(\mathbf{a}))$ for all tuples $\mathbf{a}$ obtainable from S. Now, if $\mathbf{a}$ is such a tuple and $e : \langle S \rangle_{\mathcal{A}} \rightarrowtail \mathcal{B}$ is an embedding, then $(\mathcal{A}, \mathbf{a}) \equiv_0 (\mathcal{B}, e(\mathbf{a}))$, giving the required result by (ii).

(iii) implies (iv). By the previous theorem, to check model-completeness it suffices to check that for each embedding $h : \mathcal{M} \rightarrowtail \mathcal{N}$ between models of $\mathcal{T}$, there is an elementary extension $\mathcal{D}$ of $\mathcal{M}$ and an embedding $g : \mathcal{N} \to \mathcal{D}$ such that $g \circ h = \mathrm{id}_{\mathcal{M}}$. Consider the instance of (iii) where $S = h(\mathcal{M})$ and $e = h^{-1}$ as a map $h(\mathcal{M}) \xrightarrow{\sim} \mathcal{M}$. Then there is an elementary extension $\mathcal{D}$ of $\mathcal{M}$ and an embedding

$g : \mathcal{M} \rightarrowtail \mathcal{D}$ extending e.

$$\begin{tikzcd}
 & \mathcal{D} & \\
\mathcal{N} \arrow[ur, tail, "g"] & & \mathcal{M} \arrow[ul, tail, "\preceq"'] \\
 & \langle S \rangle_{\mathcal{N}} = h(\mathcal{M}) \arrow[ul, tail] \arrow[ur, "e"'] &
\end{tikzcd}$$

This means that for all $m \in \mathcal{M}$, we have $g(h(m)) = e(h(m)) = m$. To see that $\mathcal{T}_\forall$ has the amalgamation property, consider models $\mathcal{A}', \mathcal{B}', \mathcal{C}$ of $\mathcal{T}_\forall$ where $\mathcal{C}$ embeds into both $\mathcal{A}'$ and $\mathcal{B}'$. Models of $\mathcal{T}_\forall$ are precisely the substructures of models of $\mathcal{T}$, so $\mathcal{A}'$ and $\mathcal{B}'$ are substructures of models $\mathcal{A}$ and $\mathcal{B}$ of $\mathcal{T}$ respectively. Consider the instance of (iii) where $S = \mathcal{C} = \langle \mathcal{C} \rangle_{\mathcal{A}}$ and e is the embedding of $\mathcal{C}$ into $\mathcal{B}$. Then we have an elementary extension $\mathcal{D}$ of $\mathcal{B}$ and an embedding $f : A \rightarrowtail \mathcal{D}$ that extends e.

$$\begin{tikzcd}
 & \mathcal{D} & \\
\mathcal{A} \arrow[ur, tail, "f"] & & \mathcal{B} \arrow[ul, "\preceq"'] \\
\mathcal{A}' \arrow[u, tail] & & \mathcal{B}' \arrow[u, tail] \\
 & \mathcal{C} \arrow[ul, tail] \arrow[ur, tail] &
\end{tikzcd}$$

Now, $\mathcal{D} \equiv \mathcal{B} \vDash \mathcal{T} \vdash \mathcal{T}_\forall$, we must have that $\mathcal{D}$ is a model of $\mathcal{T}_\forall$ giving the amalgamation property as desired.

(iv) implies (v). Model-completeness implies that every model of $\mathcal{T}$ is an existentially closed model of $\mathcal{T}$. Then, by the theorem characterising theories axiomatising existentially closed structures, this proof is complete, as the models of $\mathcal{T}_\forall$ are precisely the substructures of models of $\mathcal{T}$.

(v) implies (i). Immediate from the syntactic criterion for quantifier elimination. □

Corollary. Let $\mathcal{A}$ be a finite $\mathcal{L}$-structure. The theory $\mathrm{Th}(\mathcal{A})$ of $\mathcal{A}$ has quantifier elimination if and only if every isomorphism between finitely generated substructures of $\mathcal{A}$ can be extended to an automorphism of $\mathcal{A}$.

Proof. For the forward direction, consider case (iii) of the previous theorem applied to $\mathcal{A} = \mathcal{B}$ where e is the composite $\langle \mathbf{a} \rangle_{\mathcal{A}} \xrightarrow{\sim} \langle \mathbf{b} \rangle_{\mathcal{A}} \rightarrowtail \mathcal{A}$. We obtain an elementary extension $\mathcal{D}$ of $\mathcal{A}$. If $|\mathcal{A}| = n < \aleph_0$, then the theory of $\mathcal{A}$ must include a sentence that states this fact. Thus $\mathcal{D}$ models the same sentence, so $|\mathcal{D}| = n = |\mathcal{A}|$. Thus $\mathcal{A}$ and $\mathcal{D}$ are elementarily equivalent finite structures, so the elementary embedding $h : \mathcal{A} \rightarrowtail \mathcal{D}$ is an isomorphism.

$$\begin{tikzcd}
\mathcal{A} \arrow[r, tail, "f"] & \mathcal{D} \arrow[r, "h^{-1}"] & \mathcal{A} \\
\langle \mathbf{a} \rangle_{\mathcal{A}} \arrow[u, tail] \arrow[rr, "\sim"] & & \langle \mathbf{b} \rangle_{\mathcal{A}} \arrow[u, tail]
\end{tikzcd}$$

Now, as $|\mathcal{A}| = |\mathcal{D}| = n < \aleph_0$ and f is an embedding, it must also be surjective by the pigeonhole principle, and thus an isomorphism. Hence $h^{-1} \circ f$ is an automorphism of $\mathcal{A}$ extending our isomorphism $\langle \mathbf{a} \rangle_{\mathcal{A}} \xrightarrow{\sim} \langle \mathbf{b} \rangle_{\mathcal{A}}$, as required.

For the converse, we prove case (ii) in the previous theorem. Let $\mathbf{b} \in \mathcal{B} \vDash \mathrm{Th}(\mathcal{A})$ and $\mathbf{c} \in \mathcal{C} \vDash \mathrm{Th}(\mathcal{A})$ be tuples of the same length. As $\mathrm{Th}(\mathcal{A})$ is a complete theory, the models $\mathcal{B}$ and $\mathcal{C}$ are elementarily equivalent to $\mathcal{A}$, and thus by finiteness they are isomorphic. Thus, without loss of generality, we can set $\mathcal{A} = \mathcal{B} = \mathcal{C}$. By hypothesis, $(\mathcal{A}, \mathbf{b}) \equiv_0 (\mathcal{A}, \mathbf{c})$. Thus we obtain an isomorphism $\langle \mathbf{b} \rangle_{\mathcal{A}} \xrightarrow{\sim} \langle \mathbf{c} \rangle_{\mathcal{A}}$ mapping $\mathbf{b}$ to $\mathbf{c}$, which can be extended to an automorphism of $\mathcal{A}$ by assumption. If $\mathbf{m}$ is a witness to

$$(\mathcal{A}, \mathbf{b}) \vDash \exists \mathbf{y}.\, \varphi(\mathbf{b}, \mathbf{y})$$

then $f(\mathbf{m})$ must witness the truth of

$$(\mathcal{A}, \mathbf{c}) \vDash \exists \mathbf{y}.\, \varphi(\mathbf{c}, \mathbf{y})$$

Thus, $(\mathcal{A}, \mathbf{b}) \to_1 (\mathcal{A}, \mathbf{c})$ as required. □

Example. Let V be a finite vector space. Any isomorphism between subspaces can be extended to an automorphism using the Steinitz exchange lemma, so $\mathrm{Th}(V)$ has quantifier elimination.

Corollary. Let $\mathcal{T}$ be an $\mathcal{L}$-theory such that

(i) If $\mathcal{A}, \mathcal{B} \vDash \mathcal{T}$ with $\mathcal{A} \subseteq \mathcal{B}$, and $\varphi(\mathbf{x}, y)$ is a quantifier-free formula, then for all $\mathbf{a} \in \mathcal{A}$,

$$(\mathcal{B} \vDash \exists y.\, \varphi(\mathbf{a}, y)) \implies (\mathcal{A} \vDash \exists y.\, \varphi(\mathbf{a}, y))$$

(ii) For any $\mathcal{C} \subseteq \mathcal{A} \vDash \mathcal{T}$, there is an *initial intermediate model* $\mathcal{A}' \vDash \mathcal{T}$: that is, $\mathcal{C} \subseteq \mathcal{A}' \subseteq \mathcal{A}$, and for any other model $\mathcal{C} \subseteq \mathcal{B} \subseteq \mathcal{A}$, there is an embedding $\mathcal{A}' \rightarrowtail \mathcal{B}$ that fixes $\mathcal{C}$.

Then $\mathcal{T}$ has quantifier elimination.

Proof. We show that condition (ii) of the theorem above holds. Let $\mathcal{A}, \mathcal{B}$ be models of $\mathcal{T}$, and $\mathbf{a} \in \mathcal{A}, \mathbf{b} \in \mathcal{B}$ be such that $(\mathcal{A}, \mathbf{a}) \equiv_0 (\mathcal{B}, \mathbf{b})$. It suffices to show that $(\mathcal{A}, \mathbf{a}) \to_1 (\mathcal{B}, \mathbf{b})$. Let $\varphi(\mathbf{x}, y)$ be quantifier-free, and such that $\mathcal{A} \vDash \exists \mathbf{y}.\, \varphi(\mathbf{a}, \mathbf{y})$. Let $\mathbf{c} = (c_0, \dots, c_{k-1}) \in \mathcal{A}$ be such a witness, so $\mathcal{A} \vDash \varphi(\mathbf{a}, \mathbf{c})$.

We claim that there is an elementary extension $\mathcal{B}_0$ of $\mathcal{B}$ and an element $d_0 \in \mathcal{B}_0$ such that $(\mathcal{A}, \mathbf{a}, c_0) \equiv_0 (\mathcal{B}_0, \mathbf{b}, d_0)$. If we can do this, we can iterate the process to obtain a chain of elementary extensions

$$\mathcal{B} \preceq \mathcal{B}_0 \preceq \mathcal{B}_1 \preceq \cdots \preceq \mathcal{B}_{k-1}$$

and elements $d_i \in \mathcal{B}_i$ such that $(\mathcal{A}, \mathbf{a}, \mathbf{c}) \equiv_0 (\mathcal{B}, \mathbf{b}, \mathbf{d})$. Then $\mathcal{B}_{k-1} \vDash \varphi(\mathbf{b}, \mathbf{d})$ as φ is quantifier-free, so $\mathcal{B}_{k-1} \vDash \exists y.\, \varphi(\mathbf{b}, \mathbf{y})$, giving $\mathcal{B} \vDash \exists y.\, \varphi(\mathbf{b}, \mathbf{y})$ as $\mathcal{B}_{k-1} \equiv \mathcal{B}$ as required.

To find $\mathcal{B}_0$ and d_0, we use the hypotheses and the compactness theorem. As $(\mathcal{A}, \mathbf{a}) \equiv_0 (\mathcal{B}, \mathbf{b})$, there is an isomorphism $\langle \mathbf{a} \rangle_{\mathcal{A}} \to \langle \mathbf{b} \rangle_{\mathcal{B}}$. Take $\mathcal{C} = \langle \mathbf{a} \rangle_{\mathcal{A}} \subseteq \mathcal{A}$. By hypothesis (ii), there is an initial intermediate model $\mathcal{C} \subseteq \mathcal{A}' \subseteq \mathcal{A}$ with $\mathcal{A}' \vDash \mathcal{T}$, and there is an embedding $\mathcal{A}' \rightarrowtail \mathcal{B}$ fixing $\mathcal{C}$. Without loss of generality, let us assume that this embedding is an inclusion. Write

$$\Psi = \{\psi(\mathbf{x}, y) \mid \mathcal{A} \vDash \psi(\mathbf{a}, c_0),\ \psi \text{ quantifier-free}\}$$

As $\mathbf{a} \in \mathcal{A}'$, we have that $\mathcal{A}' \vDash \exists y.\, \psi(\mathbf{a}, y)$ for all $\psi \in \Psi$ by hypothesis (a). Now, $\mathcal{A}' \subseteq \mathcal{B}$, and existential formulae are preserved under extension, so $\mathcal{B} \vDash \exists y.\, \psi(\mathbf{b}, y)$ for all $\psi \in \Psi$. We conclude that every finite subset of Ψ is satisfied by some element of $\mathcal{B}$, as finite conjunctions of quantifier-free formulae are also quantifier-free. Thus, by compactness, there is an elementary extension $\mathcal{B} \preceq \mathcal{B}_0$ and $d_0 \in \mathcal{B}_0$ satisfying the formulae in Ψ. In particular, $(\mathcal{A}, \mathbf{a}, c_0) \equiv_0 (\mathcal{B}_0, \mathbf{b}, d_0)$. □

2.7 Applications

Example. The theory RCF of *real closed fields* is the theory of ordered fields for which every nonnegative element is a square, and that all odd polynomials have a root. Equivalently, it is the theory of ordered fields elementarily equivalent to $\mathbb{R}$. We show that this theory, with signature $(+, \times, 0, 1, <)$, has quantifier elimination. We will assume that every ordered field has a *real closure*, and that a real closed field satisfies the intermediate value theorem for polynomials.

We show that hypothesis (i) of the corollary above holds. Suppose we have an embedding $\mathcal{A} \subseteq \mathcal{B}$ of real closed fields, $\mathbf{a} \in A$, and a quantifier-free formula $\varphi(\mathbf{x}, y)$ such that $\mathcal{B} \vDash \exists y.\, \varphi(\mathbf{a}, y)$. By considering the disjunctive normal form, we may assume that φ is a disjunction of a conjunction of literals. Moreover, the formulae $y \neq z$ and $y \not< z$ can be written in terms of $=$ and $<$. Thus, we may assume that $\varphi(\mathbf{a}, y)$ is of the form

$$\left(\bigwedge_{i<r} p_i(y) = 0\right) \vee \left(\bigwedge_{j<s} 0 < q_j(y)\right)$$

where p_i, q_j are polynomials with coefficients in $\mathcal{A}$. If φ contains a nontrivial equation $p_i(y) = 0$, then if a witness exists in $\mathcal{B}$, it must be algebraic over $\mathcal{A}$. One can show algebraically that this witness must lie in $\mathcal{A}$. Therefore, let us suppose $r = 0$.

There are only finitely many points $c_0, \dots, c_{n-1} \in \mathcal{A}$ that are roots for the $q_j(y)$. Since the real closed fields satisfy the intermediate value theorem for polynomials, the $q_j(y)$ can only change sign at the c_i. Note that

$$\mathcal{A} \vDash \forall xy.\, x < y \to \exists z.\, (x < z \wedge z < y)$$

Since the c_i lie in $\mathcal{A}$, there is an element of $\mathcal{A}$ between any pair of distinct c_i. Suppose b witnesses $\exists y.\, \varphi(\mathbf{a}, y)$ in $\mathcal{B}$. If there is a smallest interval (c_i, c_j) containing $\mathcal{B}$, we can pick $a \in \mathcal{A}$ also inside this interval, giving $\mathcal{A} \vDash \varphi(\mathbf{a}, a)$ as required. The other cases are similar.

We now show hypothesis (ii). Suppose $\mathcal{C} \subseteq \mathcal{A}$ where $\mathcal{A}$ is a real closed field. Then $\mathcal{C}$ is an ordered integral domain. The field of fractions of $\mathcal{C}$ can be made an ordered field in a canonical way, by saying $\frac{a}{b} > 0$ if $ab > 0$. The embedding $\mathcal{C}$ into $\mathcal{A}$ is an injective homomorphism of ordered rings, into an ordered field. By the universal property of the fraction field, there is a unique homomorphism of ordered fields from $FF(\mathcal{C})$ to $\mathcal{A}$ that extends the inclusion of $\mathcal{C}$ into $\mathcal{A}$. Let $\mathcal{A}'$ be the real closure of $FF(\mathcal{C})$, so that $\mathcal{C} \subseteq FF(\mathcal{C}) \subseteq \mathcal{A}' \subseteq \mathcal{A}$. If $\mathcal{B} \vDash \mathsf{RCF}$ and $\mathcal{C} \subseteq B$, then by the same argument we have a unique ordered ring homomorphism $FF(\mathcal{C}) \to \mathcal{B}$ extending the embedding $\mathcal{C} \subseteq \mathcal{B}$. Thus $\mathcal{A}' \subseteq \mathcal{B}$ as well, and this embedding fixes $\mathcal{C}$.

Corollary (Hilbert's Nullstellensatz)**.** Let k be an algebraically closed field, and I be a proper ideal of $k[x_1, \dots, x_n]$. Then there exists $\mathbf{a} \in k^n$ such that $f(\mathbf{a}) = 0$ for all $I \in f$.

Proof. By Zorn's lemma, every proper ideal can be extended to a maximal ideal, so without loss of generality we may assume that I is a maximal ideal. Let L be the residue field ${k[x_1, \dots, x_n]}/{I}$, and let $\overline{L}$ be its algebraic closure. By Hilbert's basis theorem, there exists a finite set of generators $f_1, \dots, f_r$ for I. Note that $\mathbf{0}$ is a witness to

$$\overline{L} \vDash \exists \mathbf{x}.\, (f_1(\mathbf{x}) = 0 \wedge \dots \wedge f_r(\mathbf{x}) = 0)$$

We have embeddings $k \subseteq L \subseteq \overline{L}$, where both k and $\overline{L}$ are algebraically closed fields. The theory of algebraically closed fields has quantifier elimination, so is model-complete. Thus the embedding

$k \subseteq \overline{L}$ is elementary, so

$$k \vDash \exists \mathbf{x}.\, (f_1(\mathbf{x}) = 0 \wedge \cdots \wedge f_r(\mathbf{x}) = 0)$$

We can then take $\mathbf{a}$ to be a witness to this existential. □

Corollary (Chevalley's theorem)**.** Let k be an algebraically closed field. Then the image of a constructible set in k^n under a polynomial map is constructible.

Proof. The quantifier-free-definable subsets of k^n are precisely the finite Boolean combinations of the Zariski closed subsets of k^n, which are by definition the constructible sets. As ACF has quantifier elimination, these are exactly the definable subsets using arbitrary formulae. Now, if $X \subseteq k^n$ is constructible and $p : k^n \to k^m$ is a polynomial map, then

$$p(X) = \{y \in k^m \mid \exists x.\, p(x) = y\}$$

This is definable in the same language, so is a constructible set. □

3 Ultraproducts

3.1 Products

We will use the symbol λ to define functions without giving them explicit names. The syntax $\lambda x.\, y$ represents the function f such that $f(x) = y$.

Let $\{\mathcal{M}_i\}_{i \in I}$ be a set of $\mathcal{L}$-structures. The *product* $\prod_{i \in I} \mathcal{M}_i$ of this family is the $\mathcal{L}$-structure with carrier set

$$\prod_{i \in I} \mathcal{M}_i = \left\{\alpha : I \to \bigcup M_i \,\middle|\, \alpha(i) \in \mathcal{M}_i\right\}$$

such that

- an n-ary function symbol f is interpreted as

  $$f^{\prod_I \mathcal{M}_i} : \left(\prod_I \mathcal{M}_i\right)^n \to \prod_I \mathcal{M}_i$$

  given by

  $$(\alpha_1, \dots, \alpha_n) \mapsto \lambda i.\, f^{\mathcal{M}_i}(\alpha_1(i), \dots, \alpha_n(i))$$

- an n-ary relation symbol R is interpreted as the subset

  $$R^{\prod_I \mathcal{M}_i} \subseteq \left(\prod_I \mathcal{M}_i\right)^n$$

  given by

  $$R^{\prod_I \mathcal{M}_i} = \left\{(\alpha_1, \dots, \alpha_n) \in \left(\prod_I \mathcal{M}_i\right)^n \,\middle|\, \forall i \in I.\, (\alpha_1(i), \dots, \alpha_n(i)) \in R^{\mathcal{M}_i}\right\}$$

The relation symbols in this kind of product are not particularly useful. We want to construct a different kind of product in such a way that φ holds in the product if the set of $\mathcal{M}_i$ that model φ is 'large'.

3.2 Lattices

Definition. A *lattice* is a set L equipped with binary operations $\wedge$ and $\vee$ that are associative and commutative, and satisfy the *absorption laws*

$$a \vee (a \wedge b) = a; \quad a \wedge (a \vee b) = a$$

A lattice is called

- *distributive*, if $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$;
- *bounded*, if there are elements $\perp$ and $\top$ such that $a \vee \perp = a$ and $a \wedge \top = a$;
- *complemented*, if it is bounded and for each $a \in L$ there exists $a^\star \in L$ called its *complement* such that $a \wedge a^\star = \perp$ and $a \vee a^\star = \top$;
- a *Boolean algebra*, if it is distributive, bounded, and complemented.

Remark. (i) Distributive lattices model the fragment of a deduction system with only the conjunction and disjunction operators. Boolean algebras model classical propositional logic.

(ii) Every lattice has an ordering, defined by $a \leq b$ when $a \wedge b = a$. This ordering models the provability relation between propositions.

Example. (i) Let I be a set. The power set $\mathcal{P}(I)$ can be made into a Boolean algebra by taking $\wedge = \cap$ and $\vee = \cup$.

(ii) More generally, let X be a topological space. The set of closed and open sets of X form a Boolean algebra; they can also be thought of as the propositions in classical logic. In fact, all Boolean algebras are of this form. This result is known as Stone's representation theorem.

(iii) For any $\mathcal{L}$-structure $\mathcal{M}$ and subset $B \subseteq \mathcal{M}$, the set $\{\varphi(\mathcal{M}) \mid \varphi(\mathbf{x}) \in \mathcal{L}_B\}$ of definable subsets with parameters in B is a Boolean algebra.

3.3 Filters

Definition. Let X be a lattice. A *filter* $\mathcal{F}$ on X is a subset of X such that

(i) $\mathcal{F} \neq \varnothing$;
(ii) $\mathcal{F}$ is *upward closed*: if $f \leq x$ and $f \in \mathcal{F}$ then $x \in \mathcal{F}$;
(iii) $\mathcal{F}$ is *downward directed*: if $x, y \in \mathcal{F}$, then $x \wedge y \in \mathcal{F}$.

A filter on X may be thought of as a collection of 'large' subsets of X: subsets that are so large that the intersection of any two large subsets is also large. For property (ii), we might also say that $\mathcal{F}$ is a *terminal segment* of X.

Example. (i) Given an element $j \in I$, the family $\mathcal{F}_j$ of all subsets of I containing j is a filter on $\mathcal{P}(I)$. A filter of this form is called *principal*. A filter that is not principal is called *free*.

(ii) The family of all cofinite subsets of I forms a filter on $\mathcal{P}(I)$, called the *Fréchet filter*. One can show that any free maximal filter on an infinite set must contain the Fréchet filter.

(iii) The family of measurable subsets of $[0, 1]$ with Lebesgue measure 1 is a filter.

Definition. A filter $\mathcal{F}$ on a lattice L is *proper* if it is not equal to L. A maximal proper filter is called an *ultrafilter*.

The ultrafilters on $\mathcal{P}(I)$ are precisely those filters $\mathcal{F}$ where for each $U \subseteq I$, either $U \in \mathcal{F}$ or $I \setminus U \in \mathcal{F}$.

Proposition (the ultrafilter principle)**.** Given a set I, every proper filter on $\mathcal{P}(I)$ can be extended to an ultrafilter.

The ultrafilter principle is a choice principle that is strictly weaker than the axiom of choice.

Proof. Apply Zorn's lemma. □

3.4 Łoś' theorem

For $\boldsymbol{\alpha} \in \prod_{i \in I} \mathcal{M}_i$ and $\varphi(\mathbf{x})$ an $\mathcal{L}$-formula, we write

$$[\varphi(\boldsymbol{\alpha})] = \{i \in I \mid \mathcal{M}_i \vDash \varphi(\boldsymbol{\alpha}(i))\}$$

Let I be a set and $\mathcal{F}$ be a filter on $\mathcal{P}(I)$. Let $\{\mathcal{M}_i\}_{i \in I}$ be a family of $\mathcal{L}$-structures. The carrier set for the reduced product $\prod \mathcal{M}_i/_{\mathcal{F}}$ is the quotient of the cartesian product $\prod_{i \in I} \mathcal{M}_i$ by the equivalence relation defined by $\alpha \sim \beta$ if and only if $[\alpha = \beta] \in \mathcal{F}$. We write $\langle \alpha \rangle$ for the equivalence class of α in the reduced product. If $\mathcal{F}$ is an ultrafilter, we call the reduced product an *ultraproduct*. If all of the factors $\mathcal{M}_i$ are equal, the ultraproduct is called an *ultrapower*.

We turn the reduced product into an $\mathcal{L}$-structure as follows.

$$f^{\prod \mathcal{M}_i/_{\mathcal{F}}}(\langle \alpha_1 \rangle, \dots, \langle \alpha_n \rangle) = \langle \lambda i.\, f^{\mathcal{M}_i}(\alpha_1(i), \dots, \alpha_n(i)) \rangle$$

$$(\langle \alpha_1 \rangle, \dots, \langle \alpha_n \rangle) \in R^{\prod \mathcal{M}_i/_{\mathcal{F}}} \iff [R(\alpha_1, \dots, \alpha_n)] \in \mathcal{F}$$

Note that if $\mathcal{F} = \mathcal{F}_j$ is a principal filter, then $\prod \mathcal{M}_i/_{\mathcal{F}} \cong \mathcal{M}_j$.

Theorem. Let $\{\mathcal{M}_i\}_{i \in I}$ be a set of $\mathcal{L}$-structures, and $\mathcal{U}$ be an ultrafilter on $\mathcal{P}(I)$. Then for all $(\langle \alpha_1 \rangle, \dots, \langle \alpha_n \rangle) \in \left(\prod \mathcal{M}_i/_{\mathcal{U}}\right)^n$ and $\mathcal{L}$-formulae $\varphi(x_1, \dots, x_n)$,

$$\prod \mathcal{M}_i/_{\mathcal{U}} \vDash \varphi(\langle \alpha_1 \rangle, \dots, \langle \alpha_n \rangle) \iff [\varphi(\alpha_1, \dots, \alpha_n)] \in \mathcal{U}$$

In particular, if each $\mathcal{M}_i$ is a model for some theory $\mathcal{T}$, then so is the ultraproduct.

Proof. We prove the result by induction on the length of φ. The result holds for atomic formulae by the definition of the interpretations of function and relation symbols. Since all first-order formulae are equivalent to one composed of atomic formulae under negations, conjunctions, and existential quantification, it suffices to check these cases.

If the theorem holds for ψ, and $\varphi = \neg\psi$, we can negate both sides of the induction hypothesis to show that

$$\prod \mathcal{M}_i/_{\mathcal{U}} \vDash \neg\psi \iff [\psi] \notin \mathcal{U}$$

As $\mathcal{U}$ is an ultrafilter, the right hand side holds if and only if the complement of $[\psi]$ lies in $\mathcal{U}$. But this complement is precisely $[\neg\psi]$, as required.

If the theorem holds for ψ_1, ψ_2, then

$$\prod \mathcal{M}_i/_{\mathcal{U}} \vDash \psi_i \iff [\psi_i] \in \mathcal{U}$$

$$\begin{aligned}\prod \mathcal{M}_i/_{\mathcal{U}} \vDash \psi_1 \wedge \psi_2 &\iff [\psi_1] \in \mathcal{U} \text{ and } [\psi_2] \in \mathcal{U} \\ &\iff [\psi_1 \wedge \psi_2] \in \mathcal{U}\end{aligned}$$

Indeed, if $[\psi_1 \wedge \psi_2] \in \mathcal{U}$, then both $[\psi_1]$ and $[\psi_2]$ are in $\mathcal{U}$, since $[\psi_1 \wedge \psi_2] \subseteq [\psi_1], [\psi_2]$. Conversely, if $[\psi_1], [\psi_2] \in \mathcal{U}$, then $[\psi_1] \cap [\psi_2] \subseteq [\psi_1 \wedge \psi_2]$ as they are equal, but $[\psi_1] \cap [\psi_2] \in \mathcal{U}$, so $[\psi_1 \wedge \psi_2] \in \mathcal{U}$.

For the case of existential quantification, we will use the axiom of choice. Let x be free in ψ. We have

$$\prod \mathcal{M}_i/_{\mathcal{U}} \vDash \exists x.\, \psi(x) \iff \exists \langle \alpha \rangle.\, \prod \mathcal{M}_i/_{\mathcal{U}} \vDash \psi(\langle \alpha \rangle)$$

By the inductive hypothesis, the right hand side holds if and only if $[\psi(\alpha)] \in \mathcal{U}$. Suppose that

$$\prod \mathcal{M}_i/_{\mathcal{U}} \vDash \psi(\langle \alpha \rangle)$$

Then $[\psi(\alpha)] \subseteq [\exists x.\, \psi(x)] \in \mathcal{U}$, as $\mathcal{U}$ is a filter.

Conversely, suppose $[\exists x.\, \psi(x)] \in \mathcal{U}$. Using the axiom of choice, we can choose a witness $\alpha(i)$ to $\mathcal{M}_i \vDash \exists x.\, \psi(x)$ for each $i \in [\exists x.\, \psi(x)]$. For each $i \notin [\exists x.\, \psi(x)]$, we choose an arbitrary element of $\mathcal{M}_i$. Hence,

$$\prod \mathcal{M}_i/_{\mathcal{U}} \vDash \psi(\langle \alpha \rangle)$$

□

Remark. (i) Since $\mathcal{U}$ is an ultrafilter, the complement of $[\exists x.\, \psi(x)]$ is not in $\mathcal{U}$. Thus, the set of indices I for which $\alpha(i)$ was chosen arbitrarily does not lie in the ultrafilter, so this choice does not change the equivalence class of α.

(ii) The use of the axiom of choice in the above theorem is essential.

Example. We will show that the class of torsion groups is not first-order axiomatisable in the usual language of abelian groups with signature $(+, 0)$. Let $\mathcal{U}$ be a free ultrafilter on ω, and consider the ultraproduct

$$G = \prod_{i<\omega} C_{i+1}/_{\mathcal{U}}$$

where C_i is the cyclic group of order i, generated by g_i. Consider the element

$$g = \langle \lambda i.\, g_i \rangle \in G$$

This has finite order if and only if $[ng = 0] \in \mathcal{U}$ for some $n > 0$. However, for each such n, the set $[ng = 0]$ is finite, so $[ng \neq 0] \in \mathcal{U}$ as $\mathcal{U}$ contains the Fréchet filter, thus $[ng = 0] \notin \mathcal{U}$. But if the class of torsion groups were axiomatisable, this ultraproduct would also model that theory, and thus would be torsion.

Example. Let $\mathcal{U}$ be a free ultrafilter on ω, and consider the ultrapower

$$\mathbb{N}^{\mathcal{U}} = \prod_{i<\omega} \mathbb{N} \big/ \mathcal{U}$$

Its elements are equivalence classes of sequences of natural numbers, where $\langle(a_n)\rangle = \langle(b_n)\rangle$ if and only if $\{n \mid a_n = b_n\} \in \mathcal{U}$. It has elements such as $\langle(n)_{n<\omega}\rangle$, which represent infinitely large numbers. If $\mathbb{N}$ has its usual structure for the language of arithmetic $\mathcal{L}_{\mathrm{arith}}$, then the ultrapower $\mathbb{N}^{\mathcal{U}}$ is a *nonstandard model* of Peano arithmetic by Łoś' theorem, and is an elementary extension of $\mathbb{N}$.

Example. Let $\mathcal{U}$ be a free ultrafilter on ω, and consider the ultrapower $\mathbb{R}^{\mathcal{U}}$, which is an elementary extension of $\mathbb{R}$. This includes 'large numbers' bigger than any standard real number, such as $\omega = \langle(n)_{n<\omega}\rangle$, and also includes 'infinitesimal numbers' such as $\frac{1}{\omega}$. This is not zero, but is smaller than any positive standard real.

We can give a semantic proof of the compactness theorem without using completeness, by using Łoś' theorem.

Corollary. Let $\mathcal{T}$ be a first-order theory such that every finite subset of $\mathcal{T}$ has a model. Then $\mathcal{T}$ has a model.

Proof. If $\mathcal{T}$ is finite, the result is trivial, so we may suppose it is infinite. Let I be the set of all finite subtheories of $\mathcal{T}$, and let

$$D = \{Y \subseteq I \mid \exists \Delta \in I.\, \forall X \in Y.\, \Delta \subseteq X\}$$

Then D is a proper filter on I, so by the ultrafilter principle, it can be extended to an ultrafilter $\mathcal{U}$. Using the axiom of choice, let $\mathcal{M}_\Delta$ be a model of Δ for each finite subtheory $\Delta \in I$. Then, for any $\varphi \in \mathcal{T}$, we have

$$\{Y \subseteq I \mid \forall X \in Y.\, \varphi \in X\} \in D \subseteq \mathcal{U}$$

Then by Łoś' theorem, the ultraproduct $\prod_{\Delta\in I} \mathcal{M}_\Delta \big/ \mathcal{U}$ models φ. In particular, the ultraproduct models $\mathcal{T}$. □

4 Types

4.1 Definitions

Definition. Let $X \subseteq \mathcal{M}^n$ be a subset of an $\mathcal{L}$-structure $\mathcal{M}$, and let $P \subseteq \mathcal{M}$. We say that X is *definable* in $\mathcal{L}$ with *parameters* in P if there is a tuple $\mathbf{p} \in P$ and an $\mathcal{L}_P$-formula $\varphi(\mathbf{x}, \mathbf{y})$ such that

$$X = \varphi(\mathbf{x}, \mathbf{p}) = \{\mathbf{m} \in \mathcal{M}^n \mid \mathcal{M} \vDash \varphi(\mathbf{m}, \mathbf{p})\}$$

If $P = \mathcal{M}$, we say that X is *definable*.

Example. Consider the usual natural numbers as a structure for the language generated by the signature $(+, \cdot, 0, 1)$. Then there is an $\mathcal{L}$-formula $T(e, x, s)$ such that $\mathbb{N} \vDash T(e, x, s)$ if and only if the Turing machine encoded by the number e halts on input x in at most s steps. Thus, the set of halting computations is definable in this language. In particular, this implies that the theory of $\mathbb{N}$ is not decidable.

Definition. Let $\mathcal{T}$ be a theory and $n \in \mathbb{N}$. We obtain an equivalence relation $\sim$ on the set $\mathcal{L}(\mathbf{x})$ of $\mathcal{L}$-formulae with free variables $\mathbf{x}$, where $\mathbf{x}$ is a tuple of length n, by setting

$$\varphi(\mathbf{x}) \sim \psi(\mathbf{x}) \iff \mathcal{T} \vdash \forall \mathbf{x}.\, (\varphi(\mathbf{x}) \leftrightarrow \psi(\mathbf{x}))$$

The quotient $\mathcal{B}_n(\mathcal{T}) = {}^{\mathcal{L}(\mathbf{x})}\!/\!_{\sim}$ becomes a Boolean algebra by setting $[\varphi] \bowtie [\psi] = [\varphi \bowtie \psi]$ for any logical connective $\bowtie$, called the *Lindenbaum–Tarski algebra* of $\mathcal{T}$ on variables $\mathbf{x}$.

Definition. Let $\mathcal{M}$ be an $\mathcal{L}$-structure and $A \subseteq \mathcal{M}$. Let $\mathcal{T}$ be the $\mathcal{L}_A$-theory of sentences with parameters in A that hold in $\mathcal{M}$, denoted $\mathrm{Th}_A(\mathcal{M})$. The proper filters on the Boolean algebra $\mathcal{B}_n(\mathcal{T})$ are called the *n-types* of $\mathcal{M}$ over A.

Remark. If $\mathcal{F}$ is a proper filter on $\mathcal{B}_n(\mathcal{T})$, it cannot include the bottom element $[\bot]$. This motivates the following more convenient definition of an n-type.

Definition. Let $\mathcal{M}$ be an $\mathcal{L}$-structure and $A \subseteq \mathcal{M}$. A set p of $\mathcal{L}_A$-formulae with n free variables $\mathbf{x}$ is an *n-type* of $\mathcal{M}$ over A if $p \cup \mathrm{Th}_A(\mathcal{M})$ is satisfiable. More generally, if $\mathcal{T}$ is a theory, we say that a set p of $\mathcal{L}$-formulae with n free variables $\mathbf{x}$ is an *n-type* of $\mathcal{T}$ if

$$\mathcal{T} \cup \left\{\exists \mathbf{x}.\, \bigwedge \Psi\right\}$$

is consistent for all finite subsets Ψ of p. An n-type p is called *complete* if it is maximal among the collection of n-types, in the sense that for any $\mathcal{L}$-formula $\varphi(\mathbf{x})$, either $\varphi \in p$ or $\varphi \notin p$. We denote the set of complete n-types by $S_n(\mathcal{T})$, or $S_n^{\mathcal{M}}(A)$ if $\mathcal{T} = \mathrm{Th}_A(\mathcal{M})$. An element $\mathbf{m} \in \mathcal{M}^n$ *realises* an n-type p in $\mathcal{M}$ if $\mathcal{M} \vDash \varphi(\mathbf{m})$ holds for all φ in p. If no element realises a type, we say that the type is *omitted* in $\mathcal{M}$.

Example. (i) Let $\mathcal{M} = (\mathbb{Q}, <)$, and consider the formulae $n < x$ for each natural number n. This collection of formulae is a 1-type, as any finite subset is consistent with $\mathrm{Th}_{\mathbb{N}}(\mathbb{Q})$. This type is omitted in $\mathbb{Q}$ as no rational number x satisfies all of the formulae $n < x$ for $n \in \mathbb{N}$. However, this type is realised in an elementary extension of $\mathbb{Q}$. The realisers can be thought of as imaginary, infinitely large rationals.

(ii) Consider $\mathbb{R}$ as a structure for the theory of ordered fields. The set of formulae

$$\left\{0 < x < \frac{1}{n} \,\middle|\, 0 < n \in \mathbb{N}\right\}$$

form a 1-type of infinitesimal real numbers. This type is omitted in $\mathbb{R}$, but there is an elementary extension realising this type, such as the ultrapower with respect to a free ultrafilter.

(iii) For any $\mathcal{L}$-structure $\mathcal{M}$, subset $A \subseteq \mathcal{M}$, and tuple $\mathbf{m} \in \mathcal{M}$, we can form the n-type of all of the $\mathcal{L}_A$-formulae that hold in $\mathcal{M}$ of $\mathbf{m}$.

$$\mathrm{tp}^{\mathcal{M}}(\mathbf{m}/A) = \{\varphi(\mathbf{x}) \in \mathcal{L}_A \mid \mathcal{M} \vDash \varphi(\mathbf{m})\}$$

This is a complete n-type, called *the type of* $\mathbf{m}$ over A. This is a type corresponding to the principal filter on an equivalence class corresponding to an equality formula.

Proposition. Let $\mathcal{M}$ be an $\mathcal{L}$-structure with $A \subseteq \mathcal{M}$ and let p be an n-type of $\mathcal{M}$ over A. Then there is an elementary extension $\mathcal{N}$ of $\mathcal{M}$ that realises p.

Proof. We use the method of diagrams, and show that

$$\Gamma = p \cup \mathrm{Diag}_{\mathrm{el}}(\mathcal{M})$$

is satisfiable by compactness. Let Δ be a finite subset of Γ, and let

$$\varphi = \bigwedge_{\varphi' \in \Delta \cap p} \varphi'; \quad \psi = \bigwedge_{\psi' \in \Delta \cap \mathrm{Diag}_{\mathrm{el}}(\mathcal{M})} \psi'$$

Note that Δ is satisfiable if and only if

$$\varphi(\mathbf{x}, \mathbf{a}) \wedge \psi(\mathbf{a}', \mathbf{b})$$

is satisfiable, where $\mathbf{a}, \mathbf{a}' \in A$ and $\mathbf{b} \in \mathcal{M} \setminus \mathcal{A}$, and

$$\varphi \in p; \quad \mathcal{M} \vDash \psi(\mathbf{a}', \mathbf{b})$$

As p is an n-type, there is an $\mathcal{L}_A$-structure $\mathcal{N}_0$ that satisfies $p \cup \mathrm{Th}_A(\mathcal{M})$. As $\mathcal{M} \vDash \psi(\mathbf{a}', \mathbf{b})$, we have $\mathcal{M} \vDash \exists \mathbf{y}.\, \psi(\mathbf{a}', \mathbf{y})$. Note that this is an $\mathcal{L}_A$-formula, so

$$(\exists \mathbf{y}.\, \psi(\mathbf{a}', \mathbf{y})) \in \mathrm{Th}_A(\mathcal{M})$$

Hence,

$$\mathcal{N}_0 \vDash \varphi(\mathbf{c}, \mathbf{a}) \exists y.\, \psi(\mathbf{a}', \mathbf{y})$$

for some $\mathbf{c} \in \mathcal{N}_0$. Note that $\mathcal{N}_0$ is an $\mathcal{L}_A$-structure, not an $\mathcal{L}_{\mathcal{M}}$-structure. However, by interpreting $\mathbf{b}$ in $\mathcal{N}_0$ as the witness $\mathbf{y}$ to $\exists \mathbf{y}.\, \psi(\mathbf{a}', \mathbf{y})$, we make $\mathcal{N}_0$ into an $\mathcal{L}_{\mathcal{M}}$-structure; elements of $\mathcal{M}$ not in A or $\mathbf{b}$ are interpreted arbitrarily. In this $\mathcal{L}_{\mathcal{M}}$-structure, Δ is satisfiable. Thus Γ is satisfiable by compactness.

Now, let $\mathcal{N}$ be an $\mathcal{L}_{\mathcal{M}}$-structure satisfying Γ, so $\mathcal{N}$ is an elementary extension of $\mathcal{M}$. As $\mathcal{N}$ satisfies p, there must be a tuple $\mathbf{n} \in \mathcal{N}$ with $\mathcal{N} \vDash \varphi(\mathbf{n})$ for each $\varphi \in p$. In other words, $\mathbf{n}$ realises p in $\mathcal{N}$. $\square$

Corollary. An n-type p of $\mathcal{M}$ over $A \subseteq \mathcal{M}$ is complete if and only if there is an elementary extension $\mathcal{N}$ of $\mathcal{M}$ and some $\mathbf{a} \in \mathcal{N}$ such that $p = \mathrm{tp}^{\mathcal{N}}(\mathbf{a}/A)$.

Proof. If $\mathcal{N}$ is an elementary extension of $\mathcal{M}$ and $\mathbf{a} \in \mathcal{N}$, then

$$\mathrm{tp}^{\mathcal{N}}(\mathbf{a}/A) \in S_n^{\mathcal{N}}(A) = S_n^{\mathcal{M}}(A)$$

as the extension is elementary.

Conversely, if p is a complete n-type, then by the previous result, there is an elementary extension $\mathcal{N}$ of $\mathcal{M}$ with a tuple $\mathbf{a}$ realising the type. As p is complete, every $\mathcal{L}_A$-formula φ, either $\varphi \in p$ or $\varphi \notin p$, but not both. If $\varphi \in \mathrm{tp}^{\mathcal{N}}(\mathbf{a}/A)$, then $\mathcal{N} \vDash \varphi(\mathbf{a})$, so we cannot have $\varphi \notin p$, thus $\varphi \in p$. Conversely, if $\varphi \in p$, then $\mathcal{N} \vDash \varphi(\mathbf{a})$ as $\mathbf{a}$ realises p, so $\varphi \in \mathrm{tp}^{\mathcal{N}}(\mathbf{a}/A)$. Thus $p = \mathrm{tp}^{\mathcal{N}}(\mathbf{a}/A)$ as required. $\square$

4.2 Stone spaces

Let $\mathcal{M}$ be an $\mathcal{L}$-structure and let $A \subseteq \mathcal{M}$. For each formula φ on n variables, we consider the set of all complete types that include this formula, denoted

$$[\![\varphi]\!] = \{p \in S_n^{\mathcal{M}}(A) \mid \varphi \in p\}$$

Note that

$$[\![\varphi \vee \psi]\!] = [\![\varphi]\!] \cup [\![\psi]\!]; \quad [\![\varphi \wedge \psi]\!] = [\![\varphi]\!] \cap [\![\psi]\!]$$

These serve as the basic open sets for a topology on $S_n^{\mathcal{M}}(A)$, so an open set is an arbitrary union of open sets of this form. Moreover, each of these basic open sets $[\![\varphi]\!]$ is the complement of another basic open set $[\![\neg\varphi]\!]$, so these open sets are also closed. The $S_n^{\mathcal{M}}(A)$ are called *Stone spaces*, which are compact and totally disconnected topological spaces.

Example. Let F be an algebraically closed field, and let k be a subfield of F. The complete n-types $p \in S_n^F(k)$ are determined by the prime ideals of $k[x_1, \dots, x_n]$. For such a type p, we can define a prime ideal by

$$I_p = \{f \in k[x_1, \dots, x_n] \mid (f(x_1, \dots, x_n) = 0) \in p\}$$

These ideals are prime, and all prime ideals arise in this way. The map $p \mapsto I_p$ is a continuous bijection from the type space $S_n^F(k)$ to the prime spectrum $\operatorname{Spec} k[x_1, \dots, x_n]$ with the Zariski topology. Also, note that $|S_n^F(k)| \leq |k| + \aleph_0$ by Hilbert's basis theorem.

4.3 Isolated points

Recall that a point p in a topological space is *isolated* if $\{p\}$ is an open set. If p is isolated in $S_n^{\mathcal{M}}(A)$, then

$$\{p\} = \bigcup_I [\![\varphi_i]\!]$$

so as $\{p\}$ is a singleton, there must be a single formula $\varphi = \varphi_i$ such that $\{p\} = [\![\varphi]\!]$; we say that φ *isolates* the type.

Definition. Let $\mathcal{T}$ be an $\mathcal{L}$-theory. We say that a formula $\varphi(x_1, \dots, x_n)$ *isolates* the n-type p of $\mathcal{T}$ if $\mathcal{T} \cup \{\varphi\}$ is satisfiable, and

$$\mathcal{T} \vDash \forall \mathbf{x}.\, (\varphi(\mathbf{x}) \to \psi(\mathbf{x}))$$

for all $\psi \in p$.

Proposition. If φ isolates p, then p is realised in any model of $\mathcal{T} \cup \{\exists \mathbf{x}.\, \varphi(\mathbf{x})\}$. In particular, if $\mathcal{T}$ is a complete theory, then all isolated types are realised.

Proof. If $\mathcal{M}$ is a model of $\mathcal{T}$ and there exists $\mathbf{a}$ such that $\mathcal{M} \vDash \varphi(\mathbf{a})$, then clearly $\mathbf{a}$ realises p in $\mathcal{M}$. If $\mathcal{T}$ is complete, then either

$$\mathcal{T} \vDash \exists \mathbf{x}.\, \varphi(\mathbf{x})$$

or

$$\mathcal{T} \vDash \forall \mathbf{x}.\, \neg\varphi(\mathbf{x})$$

If φ isolates $\mathcal{T}$, then $\mathcal{T} \cup \{\varphi\}$ is satisfiable by definition, so the latter case is impossible. $\square$

4.4 Omitting types

Theorem (omitting types theorem). Let $\mathcal{L}$ be a countable language and let $\mathcal{T}$ be an $\mathcal{L}$-theory. Let p be a non-isolated n-type of $\mathcal{T}$. Then there is a countable model $\mathcal{M} \vDash \mathcal{T}$ that omits p.

Proof. Let $C = \{c_0, c_1, \dots\}$ be a countable set of new constants. We expand $\mathcal{T}$ to a consistent $\mathcal{L}_C$-theory $\mathcal{T}^\star$ by adding recursively defined sentences $\theta_0, \theta_1, \dots$. We will do this in such a way that $\theta_t \to \theta_s$ for all $s < t$. To build the θ, we first enumerate the n-tuples $C^n = \{\mathbf{d}_0, \mathbf{d}_1, \dots\}$, and enumerate the $\mathcal{L}_C$-sentences $\varphi_0, \varphi_1, \dots$.

Start with $\theta_0 = \forall x.\, x = x$, which is trivially true. Suppose we have already constructed θ_s in such a way that $\mathcal{T} \cup \{\theta_s\}$ is consistent.

First, suppose $s = 2i$. These sentences will be designed to turn C into the domain of an elementary substructure of some model of $\mathcal{T}^\star$. Suppose that $\varphi_i = \exists x.\, \psi(x)$ is existential, with parameters in C as φ is an $\mathcal{L}_C$-formula. Suppose also that $\mathcal{T} \vDash \theta_s \to \varphi_i$. As only finitely many constants from C have been used so far, we can find some unused $c \in C$. Let

$$\theta_{s+1} = \theta_s \wedge \psi(c)$$

If $\mathcal{N}$ models $\mathcal{T} \cup \{\theta_s\}$, then there is a witness to ψ in $\mathcal{N}$, so we can interpret c as this witness. Thus, $\mathcal{N}$ models $\mathcal{T} \cup \{\theta_{s+1}\}$, so this theory is consistent. If φ_i is not existential, or $\mathcal{T} \nvDash \theta_s \to \varphi_i$, then define $\theta_{s+1} = \theta_s$.

Now, suppose $s = 2i + 1$. These sentences will be designed to ensure that C omits p. Let $\mathbf{d}_i = (e_1, \dots, e_n)$. Remove every occurrence of the e_j from θ_s by replacing it with the variable x_j, and replace every occurrence of other constants in C with a fresh variable x_c, together with a quantifier $\exists x_c$ in front of the formula. This yields an $\mathcal{L}$-formula $\psi(x_1, \dots, x_n)$. For example, if

$$\theta_s = \forall x.\, \exists y.\, (rx + e_1 e_2 = y^2 + te_2); \quad r \neq t \in C$$

then

$$\psi(x_1, x_2) = \exists x_r.\, \exists x_t.\, \forall x.\, \exists y.\, (x_r x + x_1 x_2 = y^2 + x_t x_2)$$

As p is not isolated, there is no $\mathcal{L}$-formula that isolates it, so there must be some $\varphi(\mathbf{x}) \in p$ that is not implied by $\psi(\mathbf{x})$; otherwise ψ would isolate the type p. We define θ_{s+1} in such a way that $\mathbf{d}_i$ cannot realise p.

$$\theta_{s+1} = \theta_s \wedge \neg\varphi(\mathbf{d}_i)$$

This is consistent, because there must be some $\mathbf{n} \in \mathcal{N} \vDash \mathcal{T}$ such that

$$\mathcal{N} \vDash \psi(\mathbf{n}) \wedge \neg\varphi(\mathbf{n})$$

and we can turn $\mathcal{N}$ into an $\mathcal{L}_C$-structure that models θ_{s+1} by interpreting $\mathbf{d}_i$ as $\mathbf{n}$, and interpreting the constants in C but not in $\mathbf{d}$ as the respective witnesses to the existential statements $\exists x_c$ within ψ.

Let $\mathcal{T}^\star$ be $\mathcal{T}$ together with all of the θ_s. Note that each $\mathcal{T} \cup \{\theta_s\}$ is consistent, and each θ_{s+1} implies θ_s, so by compactness, $\mathcal{T}^\star$ must be consistent. Moreover, if $\mathcal{M}$ is a model of $\mathcal{T}^\star$, the construction of θ_{2i+1} ensures that C has a witness to φ_i that holds in $\mathcal{M}$. Thus, by the Tarski–Vaught test, C is the domain of an elementary substructure of $\mathcal{M}$. If $\mathbf{c} \in C \vDash \mathcal{T}^\star$, then $\mathbf{c} = \mathbf{d}_i$ for some i. As $C \vDash \theta_{2i+2}$, we have $\neg\varphi(\mathbf{c})$ for some φ in the type p. Hence $\mathbf{c}$ cannot realise the type p in C. ☐

Remark. The proof can be generalised to omit countably many types at the same time.

5 Indiscernibles

5.1 Introduction

Given a linear order η, we will write $[\eta]^k$ for the set of ordered k-tuples in η:

$$[\eta]^k = \{\mathbf{a} \in \eta^k \mid a_0 <^\eta a_1 <^\eta \cdots <^\eta a_{k-1}\}$$

Definition. Let $\mathcal{M}$ be an $\mathcal{L}$-structure, let Φ be a set of $\mathcal{L}$-formulae, and let η be a strict chain of elements of $\mathcal{M}$. We say that η is Φ-*indiscernible* in $\mathcal{M}$ if

$$\mathcal{M} \vDash \varphi(\mathbf{a}) \leftrightarrow \varphi(\mathbf{b})$$

for all $\mathbf{a}, \mathbf{b} \in [\eta]^k$ of the correct length and $\varphi \in \Phi$. We simply say that η is a sequence of indiscernibles if the above holds where Φ is the set of every $\mathcal{L}$-formula.

Example. (i) Any linearly ordered basis $\mathcal{B}$ for a vector space provides a sequence of indiscernibles. Indeed, given $\mathbf{a}, \mathbf{b} \in [\mathcal{B}]^k$, there is an automorphism of the vector space that maps $\mathbf{a}$ to $\mathbf{b}$.

(ii) Any chain of algebraically independent elements in a field $k \vDash \mathsf{ACF}_0$ is a sequence of indiscernibles.

(iii) If R is a ring, then the variables $X_1, \dots, X_n$ form a set of indiscernibles of $R[X_1, \dots, X_n]$.

Definition. An *Ehrenfeucht–Mostowski functor* is a mapping F that takes each linear order η to an $\mathcal{L}$-structure $F(\eta)$, and each order embedding $g : \eta \rightarrowtail \varepsilon$ to an embedding of $\mathcal{L}$-structures $F(g) : F(\eta) \rightarrowtail F(\varepsilon)$, in such a way that

(i) each η generates $F(\eta)$, that is, $\eta \subseteq F(\eta)$ as sets, and every element of $F(\eta)$ is of the form $t^{F(\eta)}(\mathbf{a})$ where $t(\mathbf{x})$ is an $\mathcal{L}$-term and $\mathbf{a} \in [\eta]^k$;

(ii) for each order embedding $g : \eta \rightarrowtail \varepsilon$, the embedding of $\mathcal{L}$-structures $F(g)$ extends g;

(iii) for every linear order η, we have $F(1_\eta) = 1_{F(\eta)}$;

(iv) for each composable pair of embeddings f, g, we have $F(g \circ f) = F(g)F(f)$.

In particular, every automorphism of a linear order η induces an automorphism of $F(\eta)$.

Proposition (sliding property)**.** Let F be an Ehrenfeucht–Mostowski functor, let η, ε be linear orders, and let $\mathbf{a} \in [\eta]^k, \mathbf{b} \in [\varepsilon]^k$. Then for every quantifier-free formula $\varphi(x_1, \dots, x_k)$, we have

$$F(\eta) \vDash \varphi(\mathbf{a}) \iff F(\varepsilon) \vDash \varphi(\mathbf{b})$$

Proof. Embed η and ε into some linear order ρ in which $\mathbf{a}$ and $\mathbf{b}$ are identified. Let $f : \eta \to \rho$ and $g : \varepsilon \to \rho$ be the embeddings. Suppose that $F(\eta) \vDash \varphi(\mathbf{a})$. As embeddings preserve quantifier-free formulae and the map $F(f) : F(\eta) \rightarrowtail F(\rho)$ extends f, we must have that $F(\rho) \vDash \varphi(f(\mathbf{a}))$. As $f(\mathbf{a}) = g(\mathbf{b})$, we must have $F(\rho) \vDash \varphi(g(\mathbf{b}))$, and so for the same reason, $F(\varepsilon) \vDash \varphi(\mathbf{b})$. □

We see that the chain $\eta \subseteq F(\eta)$ is indiscernible by quantifier-free formulas.

Definition. Let $\mathcal{M}$ be an $\mathcal{L}$-structure containing a linear order $\eta \subseteq \mathcal{M}$ as sets. Then, we define the theory of η in $\mathcal{M}$, denoted $\mathrm{Th}(\mathcal{M}, \eta)$, to be the set of all $\mathcal{L}$-formulae $\varphi(\mathbf{x})$ that are satisfiable in $\mathcal{M}$ by every ordered tuple $\mathbf{a} = a_0 < \cdots < a_{k-1}$ in η. The theory $\mathrm{Th}(F)$ of an Ehrenfeucht–Mostowski functor F is the set of all $\mathcal{L}$-formulae $\varphi(\mathbf{x})$ such that $F(\eta) \vDash \varphi(\mathbf{a})$ for every linear order η and ordered tuple $\mathbf{a}$ in η.

Lemma. Let η be an infinite linear order, let F be an Ehrenfeucht–Mostowski functor, and let φ be a universal sentence that is true in $F(\eta)$. Then $\varphi \in \mathrm{Th}(F)$.

Proof. Let $\varphi = \forall \mathbf{x}.\, \psi(\mathbf{x})$ where ψ is quantifier-free. Let ε be a linear order, and let $\mathbf{a} \in F(\varepsilon)$; we need to show $F(\varepsilon) \vDash \psi(\mathbf{a})$. As ε generates $F(\varepsilon)$, there is a finite suborder ε_0 such that $\mathbf{a} \in F(\varepsilon_0)$. But η is infinite, so there is an embedding $f : \varepsilon_0 \rightarrowtail \eta$. By assumption, $F(f)(\mathbf{a})$ satisfies ψ in $F(\eta)$, so $F(\varepsilon_0) \vDash \psi(\mathbf{a})$, as ψ is quantifier-free so is preserved under substructures. Similarly, $F(\varepsilon) \vDash \psi(\mathbf{a})$, as required. □

5.2 Existence of Ehrenfeucht–Mostowski functors

Lemma (stretching property)**.** Let $\mathcal{M}$ be an $\mathcal{L}$-structure that contains the linear order ω as a generating set. Suppose that ω is indiscernible by quantifier-free formulae. Then there is an Ehrenfeucht–Mostowski functor F such that $\mathcal{M} = F(\omega)$. Moreover, if G is another such functor, then there is an isomorphism $\alpha : F(\eta) \to G(\eta)$ for each linear order η, and $\alpha|_\eta = 1_\eta$.

F is unique up to natural isomorphism.

Definition. Let F be an Ehrenfeucht–Mostowski functor, and let $\mathcal{T}$ be a theory. The models of $\mathcal{T}$ that are of the form $F(\eta)$ are called *Ehrenfeucht–Mostowski models* of $\mathcal{T}$.

Theorem (Ramsey)**.** Let X be a countable linear order, and let k, n be positive integers. Then for every function $f : [X]^k \to n$, there is an infinite subset $Y \subseteq X$ such that f is constant on $[Y]^k$.

We will use Ramsey's theorem to show that Ehrenfeucht–Mostowski models for Skolem theories with infinite models always exist.

Lemma. Let F be an Ehrenfeucht–Mostowski functor such that $\mathrm{Th}(F(\omega))$ is Skolem. Then $\mathrm{Th}(F)$ includes either $\varphi(\mathbf{x})$ or $\neg\varphi(\mathbf{x})$ for every $\mathcal{L}$-formula $\varphi(\mathbf{x})$. In particular, all of the $F(\eta)$ are elementarily equivalent, and each linear order η is indiscernible in $F(\eta)$.

Proof. Since $\mathrm{Th}(F(\omega))$ is Skolem, it admits a universal axiomatisation. Moreover, every formula is equivalent to a quantifier-free formula modulo $\mathrm{Th}(F(\omega))$. The result then follows from the sliding property and the lemma on universal sentences. □

Theorem (Ehrenfeucht–Mostowski theorem). Let $\mathcal{M}$ be an $\mathcal{L}$-structure, and suppose that $\mathrm{Th}(\mathcal{M})$ is Skolem. If η is infinite linear order that is contained as a set in $\mathcal{M}$, then there is an Ehrenfeucht–Mostowski functor F in $\mathcal{L}$ whose theory expands $\mathrm{Th}(\mathcal{M}, \eta)$.

Proof. We want to build a theory expanding $\mathrm{Th}(\mathcal{M}, \eta)$, whose models include an indiscernible copy of ω. First, expand $\mathcal{L}$ to add ω-many constants $C = \{c_i \mid i \in \omega\}$, and we build an $\mathcal{L}_C$-theory $\mathcal{T}$ with the following axioms:

(i) $\varphi(\mathbf{a}) \leftrightarrow \varphi(\mathbf{b})$, for each $\mathcal{L}$-formula $\varphi(\mathbf{x})$ and ordered tuples $\mathbf{a}, \mathbf{b} \in [C]^{|\mathbf{x}|}$;

(ii) $\varphi(c_0, \dots, c_{k-1})$, for each formula $\varphi(x_0, \dots, x_{k-1})$ in $\mathrm{Th}(\mathcal{M}, \eta)$.

We will show that this theory has a model by compactness. Let $\mathcal{U}$ be a finite subset of $\mathcal{T}$, and list the formulae in $\mathcal{U}$ as $\varphi_0, \dots, \varphi_{m-1}$. Note that there is some finite k such that the new constants that show up in the formulae in $\mathcal{U}$ are among $c_0, \dots, c_{k-1}$. By adding redundant variables, we may assume that each of these formulae all have free variables $c_0, \dots, c_{k-1}$ for simplicity.

Define an equivalence relation $\sim$ on $[\eta]^k$ by declaring that $\mathbf{a} \sim \mathbf{b}$ if $\mathcal{M} \vDash \varphi_j(\mathbf{a})$ if and only if $\mathcal{M} \vDash \varphi_j(\mathbf{b})$ for each $j < m$. This equivalence relation partitions $[\eta]^k$ into finitely many equivalence classes. Hence, by Ramsey's theorem, there is an infinite sequence $\mathbf{e} = e_0 < e_1 < \dots < e_{2k-1}$ in η such that any two ordered k-tuples extracted from $\mathbf{e}$ are in the same equivalence class. We can interpret each c_j in $\mathcal{M}$ as e_j for each $j < k$, making $\mathcal{M}$ into an $\mathcal{L}_{\mathbf{c}}$-structure that models $\mathcal{U}$.

Let $\mathcal{N}$ be a model of $\mathcal{T}$. The new constants c_i must be interpreted as different elements of $\mathcal{N}$, as $\mathrm{Th}(\mathcal{M}, \eta)$ includes the sentence $x_0 \neq x_1$. Hence $\mathcal{N}$ contains a copy of ω, by seeing c_i in $\mathcal{N}$ as i. Consider $\mathcal{N}^\star$, which is the $\mathcal{L}$-reduct of $\mathcal{N}$, and let $\mathcal{S} = \langle \omega \rangle_{\mathcal{N}^\star}$. Note that $\mathrm{Th}(\mathcal{M}, \eta)$ is contained in $\mathrm{Th}(\mathcal{N}^\star, \omega)$. This in particular implies that $\mathrm{Th}_{\mathcal{L}}(\mathcal{N}^\star)$ is Skolem, as $\mathrm{Th}(\mathcal{M})$ is Skolem and $\mathrm{Th}(\mathcal{M}) \subseteq \mathrm{Th}(\mathcal{M}, \eta)$. It then follows that $\mathcal{S}$ is an elementary substructure of $\mathcal{N}^\star$, and is generated by ω. Then, $\mathrm{Th}(\mathcal{M}, \eta) \subseteq \mathrm{Th}(\mathcal{S}, \omega)$. Finally, sentences in $\mathcal{T}$ ensure that ω is indiscernible in $\mathcal{S}$ by construction, so the stretching lemma gives an Ehrenfeucht–Mostowski functor F with $\mathcal{S} = F(\omega)$, which completes the proof by the previous lemma. □

6 Intuitionistic logic and lambda calculi

6.1 The Brouwer–Heyting–Kolmogorov interpretation

We will construct a system of logic in which every proof contains evidence of its truth. Our system will have the following properties, known as the Brouwer–Heyting–Kolmogorov interpretation.

(i) $\bot$ has no proof.

(ii) To prove $\varphi \wedge \psi$, one must provide a proof of φ together with a proof of ψ.

(iii) To prove $\varphi \to \psi$, one must provide a mechanism for translating a proof of φ into a proof of ψ. In particular, to prove $\neg\varphi$, we must provide a way to turn a proof of φ into a contradiction.

(iv) To prove $\varphi \vee \psi$, we must specify either φ or ψ, and then provide a proof for it. Note that in a classical setting, a proof of $\varphi \vee \psi$ need not specify which of the two disjuncts is true.

(v) The law of the excluded middle LEM, which states $\varphi \vee \neg\varphi$, is not valid. If this held for some proposition, we could decide whether the proposition was true or its negation is true, because any proof of $\varphi \vee \neg\varphi$ contains this information.

(vi) To prove $\exists x.\, \varphi(x)$, one must provide a term t together with a proof of $\varphi(t)$.

(vii) To prove $\forall x.\, \varphi(x)$, one must provide a mechanism that converts any term t into a proof of $\varphi(t)$.

This will be called *intuitionistic (propositional) logic* IPC.

Theorem (Diaconescu)**.** In intuitionistic ZF set theory, the law of the excluded middle LEM can be deduced from the axiom of choice AC.

Proof. Let φ be a proposition; we want a proof of $\varphi \vee \neg\varphi$. Using the axiom of separation, we have proofs that the following sets exist.

$$A = \{x \in \{0,1\} \mid \varphi \vee (x = 0)\}; \quad B = \{x \in \{0,1\} \mid \varphi \vee (x = 1)\}$$

These sets are *inhabited*: there exists an element in each of them; in particular, $0 \in A$ and $1 \in A$ are intuitionistically valid. Note that being inhabited is strictly stronger than being nonempty in intuitionistic logic. This is because any proof that a set is inhabited contains information about an element in the set. The set $\{A, B\}$ is a family of inhabited sets, so by the axiom of choice, we have a choice function $f : \{A, B\} \to A \cup B$, and we have a proof that $f(A) \in A$ and $f(B) \in B$. Thus, we have a proof of

$$(\varphi \vee (f(A) = 0)) \wedge (\varphi \vee (f(B) = 1))$$

We also have a proof that $f(A), f(B) \in \{0,1\}$. In particular, we either have a proof that $f(A) = 0$ or we have a proof that $f(A) = 1$, and the same holds for B. We have the following cases.

(i) Suppose we have a proof that $f(A) = 1$. Then we have a proof of $\varphi \vee (1 = 0)$, so we must have a proof of φ.

(ii) Suppose we have a proof that $f(B) = 0$. Then similarly we have a proof of $\varphi \vee (0 = 1)$, so we must have a proof of φ.

(iii) Suppose we have proofs that $f(A) = 0$ and $f(B) = 1$. We will prove $\neg\varphi$. Suppose that we have a proof of φ. Then from a proof of $\varphi \vee (x = 0)$ or $\varphi \vee (x = 1)$ we can derive a proof of the other, so by the axiom of extensionality, $A = B$. Then $0 = f(A) = f(B) = 1$ as f is a function, giving a contradiction. Thus, we have constructed a proof of $\neg\varphi$.

We can always specify a proof of φ or a proof of $\neg\varphi$, so we have $\varphi \vee \neg\varphi$. □

Remark. (i) Intuitionistic mathematics is more general than classical mathematics, because it operates on fewer assumptions.

(ii) Notions that are classically conflated may be different in intuitionistic logic. For example, there is no classical distinction between inhabited and nonempty sets, but they are not the same in intuitionistic logic. Other examples include finiteness, or disequality and apartness.

(iii) Intuitionistic proofs have computational content attached to them, but classical proofs may not.

(iv) Intuitionistic logic is the internal logic of an arbitrary topos.

6.2 Natural deduction

We will use the notation $\Gamma \vdash \varphi$, or $\Gamma \vdash_{\mathsf{IPC}} \varphi$, to denote that the set of *open assumptions* Γ let us conclude φ. Γ is also called the *context*. We will inductively define this provability relation. Some rules, called *introduction rules*, let us construct proofs.

$$\frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}\ {\wedge\text{-I}} \qquad \frac{\Gamma \vdash A}{\Gamma \vdash A \vee B}\ {\vee\text{-I}} \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}\ {\vee\text{-I}}$$

Dually, some rules, called *elimination rules*, let us extract information from proofs.

$$\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}\ {\wedge\text{-E}} \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}\ {\wedge\text{-E}} \qquad \frac{\Gamma, A \vdash C \qquad \Gamma, B \vdash C \qquad \Gamma \vdash A \vee B}{\Gamma \vdash C}\ {\vee\text{-E}}$$

We now define the principle of explosion, which is an elimination rule for $\bot$. We do not construct an introduction rule for $\bot$.

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash A}\ {\bot\text{-E}}$$

We now define the introduction and elimination rules for implication. The elimination rule is known as *modus ponens*.

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \to B}\ {\to\text{-I}} \qquad \frac{\Gamma \vdash A \to B \qquad \Gamma \vdash A}{\Gamma \vdash B}\ {\to\text{-E}}$$

We finally define a rule called the *axiom schema*, that allows us to prove our assumptions.

$$\frac{}{\Gamma, A \vdash A}\ \mathsf{Ax}$$

If an inference rule moves an assumption out of the context, we say that the assumption is *discharged* or *closed*. We are allowed to drop assumptions that we do not use; this is called the *weakening* rule. We obtain classical propositional logic CPC by additionally adding one of the following two rules.

$$\frac{}{\Gamma \vdash A \vee \neg A}\ \mathsf{LEM} \qquad \frac{\Gamma, \neg A \vdash \bot}{\Gamma \vdash A}\ {\neg\neg\text{-E}}$$

We will additionally use the informal notation

$$\frac{\begin{matrix}[A] \\ \vdots \\ X\end{matrix} \qquad \begin{matrix}[B] \\ \vdots \\ Y\end{matrix}}{C}\ (A, B)$$

to mean that if we can prove X assuming A and we can prove Y assuming B, then we can infer C by discharging the open assumptions A and B. For example, we can write an instance of $\to$-I as

$$\frac{\begin{matrix}\Gamma, [A] \\ \vdots \\ B\end{matrix}}{\Gamma \vdash A \to B}\ (A)$$

To extend this to intuitionistic predicate logic IQC, we need to add rules for quantifiers.

$$\exists\text{-I}\ \frac{\Gamma \vdash \varphi[x := t]}{\Gamma \vdash \exists x.\, \varphi(x)} \qquad \forall\text{-I}\ \frac{\Gamma \vdash \varphi \qquad x \text{ not free in } \Gamma}{\Gamma \vdash \forall x.\, \varphi}$$

$$\exists\text{-E}\ \frac{\Gamma \vdash \exists x.\, \varphi \qquad \Gamma, \varphi \vdash \psi \qquad x \text{ not free in } \Gamma}{\Gamma \vdash \psi} \qquad \forall\text{-E}\ \frac{\Gamma \vdash \forall x.\, \varphi}{\Gamma \vdash \varphi[x := t]}$$

Example. We will show that $\vdash_{\mathsf{IPC}} A \wedge B \to B \wedge A$.

$$\cfrac{\cfrac{\cfrac{[A \wedge B]}{B}\ \wedge\text{-E} \qquad \cfrac{[A \wedge B]}{A}\ \wedge\text{-E}}{B \wedge A}\ \wedge\text{-I}}{A \wedge B \to B \wedge A}\ \to\text{-I}$$

Example. We will show that the logical axioms

$$\varphi \to (\psi \to \varphi); \quad (\varphi \to (\psi \to \chi)) \to ((\varphi \to \psi) \to (\varphi \to \chi))$$

are intuitionistically valid.

$$\cfrac{\cfrac{\cfrac{[\varphi]}{\varphi}\ \text{Ax} \qquad [\psi]}{\psi \to \varphi}\ (\to\text{-I}, \psi)}{\varphi \to (\psi \to \varphi)}\ (\to\text{-I}, \varphi)$$

For the second axiom,

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{[\varphi \to (\psi \to \chi)] \qquad [\varphi]}{\psi \to \chi}\ \to\text{-E} \qquad \cfrac{[\varphi \to \psi] \qquad [\varphi]}{\psi}\ \to\text{-E}}{\chi}\ \to\text{-E}}{\varphi \to \chi}\ (\varphi)}{(\varphi \to \psi) \to (\varphi \to \chi)}\ (\varphi \to \psi)}{(\varphi \to (\psi \to \chi)) \to ((\varphi \to \psi) \to (\varphi \to \chi))}\ (\varphi \to (\psi \to \chi))$$

Lemma. If $\Gamma \vdash_{\mathsf{IPC}} \varphi$, then $\Gamma, \psi \vdash_{\mathsf{IPC}} \varphi$. Moreover, if p is a primitive proposition and ψ is any proposition, then

$$\Gamma[p := \psi] \vdash_{\mathsf{IPC}} \varphi[p := \psi]$$

Proof. This follows easily by induction over the length of the proof. □

6.3 The simply typed lambda calculus

For now, we will assume we are given a set Π of *simple types*, generated by the grammar

$$\Pi ::= \mathcal{U} \mid \Pi \to \Pi$$

where $\mathcal{U}$ is a countable set of *primitive types* or *type variables*.

Let V be an infinite set of variables. The set Λ_Π of *simply typed λ-terms* is defined by the grammar

$$\Lambda_\Pi ::= V \mid \underbrace{\lambda V : \Pi.\, \Lambda_\Pi}_{\lambda\text{-abstraction}} \mid \underbrace{\Lambda_\Pi\, \Lambda_\Pi}_{\lambda\text{-application}}$$

A *context* Γ is a set of pairs $\{x_1 : \tau_1, \dots, x_n : \tau_n\}$, where the x_i are distinct variables, and the τ_n are types. We write $\mathcal{C}$ for the set of all contexts. Given a context $\Gamma \in \mathcal{C}$, we also write $\Gamma, x : \tau$ for the context $\Gamma \cup \{x : \tau\}$. The *domain* of Γ is the set $\operatorname{dom}\Gamma$ of variables that appear in Γ; similarly, the *range* of Γ is the set $|\Gamma|$ of types that appear in Γ.

The *typability relation* $(-) \Vdash (-) : (-)$ is a relation on $\mathcal{C} \times \Lambda_\Pi \times \Pi$, defined recursively using the following rules.

(i) For every context Γ, variable $x \notin \operatorname{dom}\Gamma$, and type τ, we have $\Gamma, x : \tau \Vdash x : \tau$.

(ii) Let Γ be a context, $x \notin \operatorname{dom}\Gamma$, let σ, τ be types, and let M be a λ-term. If $\Gamma, x : \sigma \Vdash M : \tau$, then $\Gamma \Vdash (\lambda x : \sigma. M) : \sigma \to \tau$.

(iii) Let Γ be a context, σ, τ be types, and let M and N be λ-terms. If $\Gamma \Vdash M : (\sigma \to \tau)$ and $\Gamma \Vdash N : \sigma$, then $\Gamma \Vdash (M\,N) : \tau$.

We will refer to the λ-calculus of Λ_Π with this typability relation as $\lambda(\to)$.

An occurrence of a variable x in a λ-abstraction is called *bound*, otherwise it is called *free*. A term with no free variables is called *closed*. λ-terms that differ only in the names of bound variables are called *α-equivalent*, so for example, $(\lambda x : \sigma. x)$ and $(\lambda y : \sigma. y)$ are α-equivalent. Whenever it is convenient, we will replace terms with α-equivalent terms to avoid reusing variable names.

If M and N are λ-terms and x is a variable, we can define the *substitution* of N for x in M recursively:

(i) $x[x \coloneqq N] = N$;

(ii) $y[x \coloneqq N] = y$ if $x \neq y$;

(iii) $(\lambda y : \sigma. M)[x \coloneqq N] = (\lambda y : \sigma. M[x \coloneqq N])$ if $x \neq y$ (which can be done without loss of generality by α-equivalence);

(iv) $(P\,Q)[x \coloneqq N] = (P[x \coloneqq N])\,(Q[x \coloneqq N])$.

We define the *β-reduction* relation $\to_\beta$ on Λ_Π to be the smallest relation that is closed under the following rules:

(i) $(\lambda x : \sigma. P)\,Q \to_\beta P[x \coloneqq Q]$;

(ii) if $P \to_\beta P'$, then for any $x \in V$ and $\sigma \in \Pi$, we have $(\lambda x : \sigma. P) \to_\beta (\lambda x : \sigma. P')$;

(iii) if $P \to_\beta P'$ and Z is a λ-term, then $P\,Z \to_\beta P'\,Z$ and $Z\,P \to_\beta Z\,P'$.

We define the β-*equivalence* relation $\equiv_\beta$ to be the smallest equivalence relation containing $\to_\beta$. For example, we have

$$(\lambda x : \mathbb{Z}.\,(\lambda y : \tau.\,x))\,2 \equiv_\beta (\lambda y : \tau.\,2)$$

An expression $(\lambda x : \sigma.\,P)\,Q$ to be β-reduced is called a β-*redex*; the resulting term $P[x \coloneqq Q]$ is called its β-*reduct* or β-*contractum*. If no β-reductions can be carried out on a λ-term, we say that the term is in β-*normal form*. We write $M \twoheadrightarrow_\beta N$ if M reduces to N after potentially multiple applications of β-reduction.

If x is not free in P, the term $(\lambda x : \sigma.\,(P\,x))$ is said to η-*reduce* to P, written $(\lambda x : \sigma.\,(P\,x)) \to_\eta P$, and we say that $(\lambda x : \sigma.\,(P\,x))$ and P are η-*equivalent*.

By convention, we will write

(i) KLM for $(KL)M$;

(ii) $\lambda x : \sigma.\,\lambda y : \tau.\,M$ for $\lambda x : \sigma.\,(\lambda y : \tau.\,M)$;

(iii) $\lambda x : \sigma.\,M\,N$ for $\lambda x : \sigma.\,(M\,N)$;

(iv) $M\,\lambda x : \sigma.\,N$ for $M\,(\lambda x : \sigma.\,N)$.

6.4 Basic properties

The following technical lemmas can be proven by induction.

Lemma (generation lemma). (i) For every variable x, context Γ, and type σ, if $\Gamma \Vdash x : \sigma$, then $x : \sigma \in \Gamma$.
(ii) If $\Gamma \Vdash (\lambda x : \tau.\,N) : \sigma$, then there is a type ρ such that $\Gamma, x : \tau \Vdash N : \rho$, and $\sigma = (\tau \to \rho)$.
(iii) If $\Gamma \Vdash (M\,N) : \sigma$, then there is a type τ such that $\Gamma \Vdash M : \tau \to \sigma$ and $\Gamma \Vdash N : \tau$.

Lemma (free variables lemma). Suppose that $\Gamma \Vdash M : \sigma$. Then
(i) if $\Gamma \subseteq \Delta$, then $\Delta \Vdash M : \sigma$;
(ii) the free variables of M occur in Γ;
(iii) $\Delta \Vdash M : \sigma$ for some $\Delta \subseteq \Gamma$ containing only the free variables of M in its domain.

Lemma (substitution lemma). The typability relation respects substitution.

Lemma (subject reduction). If $\Gamma \Vdash M : \sigma$ and $M \to_\beta N$, then $\Gamma \Vdash N : \sigma$.

The following theorem establishes the *confluence* property of λ-terms.

Theorem (Church–Rosser theorem for $\lambda(\to)$). Suppose that $\Gamma \Vdash M : \sigma$. If $M \twoheadrightarrow_\beta N_1$ and

$M \twoheadrightarrow_\beta N_2$, then there exists P such that $N_1 \twoheadrightarrow_\beta L$ and $N_2 \twoheadrightarrow_\beta L$, and $\Gamma \Vdash L : \sigma$.

$$\begin{tikzcd}
& M \arrow[dl, two heads] \arrow[dr, two heads] & \\
N_1 \arrow[dr, two heads] & & N_2 \arrow[dl, two heads] \\
& L &
\end{tikzcd}$$

Corollary. If a simply typed λ-term admits a β-normal form, then this β-normal form is unique.

Proposition (uniqueness of types). (i) Suppose $\Gamma \Vdash M : \sigma$ and $\Gamma \Vdash M : \tau$. Then $\sigma = \tau$.
(ii) Suppose $\Gamma \Vdash M : \sigma$ and $\Gamma \Vdash N : \tau$, and that $M \equiv_\beta N$. Then $\sigma = \tau$.

Proof. The first part is by induction on M. For the second part, by the Church–Rosser theorem there is a term L to which M and N both eventually reduce, so the result holds by subject reduction. □

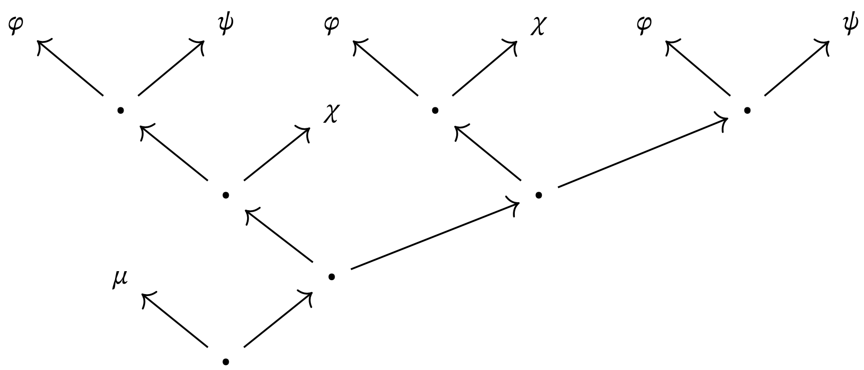
Example. There is no way to assign a type to the expression $\lambda x.\, x\, x$. Indeed, if x has type τ, then it must also have type $\tau \to \sigma$ for some σ, but this contradicts uniqueness of types.

6.5 The normalisation theorems

We will measure the complexity of a type by looking at it as a binary tree. For example, for

$$\rho = \mu \to [((\varphi \to \psi) \to \chi) \to ((\varphi \to \chi) \to (\varphi \to \psi))]$$

the corresponding binary tree is



The height of this tree is the complexity of the type, which in this case is 4. For convenience, we will annotate types of terms with superscripts.

Definition. The *height* function is the map $h : \Pi \to \mathbb{N}$ that maps a type variable to 0, and maps a function type $\sigma \to \tau$ to $1+\max(h(\sigma), h(\tau))$. We extend the height function to β-redexes: if $(\lambda x : \sigma.\, P^\tau)^{\sigma\to\tau} R^\sigma$ is a redex, its height is $h(\sigma \to \tau)$.

Theorem (weak normalisation theorem)**.** Suppose $\Gamma \Vdash M : \sigma$. Then there is a finite reduction path

$$M = M_0 \to_\beta M_1 \to_\beta \dots \to_\beta M_n$$

where M_n is in β-normal form.

Proof (taming the hydra). First, we define the function $m : \Lambda_\Pi \to \mathbb{N} \times \mathbb{N}$ by $m(M) = (0,0)$ if M is in β-normal form, and otherwise, $m(M)$ is the pair $(h(M), \mathrm{redex}(M))$ where $h(M)$ is the maximal height of redexes in M and $\mathrm{redex}(M)$ is the number of redexes in M. We will use induction on the well-founded relation given by the lexicographic order on $\mathbb{N} \times \mathbb{N}$ to show that if M is typeable, it can be reduced to β-normal form.

If $\Gamma \Vdash M : \sigma$ and M is in β-normal form, then the claim is trivial. Otherwise, let Δ be the rightmost redex of maximal height $h = h(M)$. By reducing Δ, we may introduce copies of existing redexes, or create new redexes. Creation of new redexes can occur in one of the following ways.

(i) Suppose Δ is of the form

$$(\lambda x : (\rho \to \mu).\, \dots x P^\rho \dots)(\lambda y : \rho.\, Q^\mu)^{\rho\to\mu}$$

Then it reduces to

$$\dots (\lambda y : \rho.\, Q^\mu)^{\rho\to\mu} P^\rho \dots$$

which is a new redex of height $h(\rho \to \mu) < h$.

(ii) Suppose Δ is of the form

$$(\lambda x : \tau.\, \lambda y : \rho.\, R^\mu) P^\tau$$

occurring in the position $\Delta^{\rho\to\tau} Q^\rho$. Suppose that Δ reduces to $\lambda y : \rho.\, R_1^\mu$. Then we have created a new redex $(\lambda y : \rho.\, R_1^\mu) Q^\rho$ of height $h(\rho \to \mu) < h(\tau \to \rho \to \mu) = h$.

(iii) Suppose Δ is of the form

$$(\lambda x : (\rho \to \mu).\, x)(\lambda y : \rho.\, P^\mu)$$

occurring in the position $\Delta^{\rho\to\mu} Q^\rho$. Then this reduces to $(\lambda y : \rho.\, P^\mu) Q^\rho$ of height $h(\rho \to \mu) < h$.

There is still the possibility that reduction of Δ introduces copies of existing redexes. Suppose Δ is of the form

$$(\lambda x : \rho.\, P^\rho) Q^\tau$$

and P has more than one free occurrence of x. Then the reduction of Δ will copy all redexes in Q. But as Δ was chosen to be rightmost with maximal height, the height of all redexes in Q have height less than h.

So if $M \to_\beta M'$ by reducing Δ, it is always the case that $m(M') < m(M)$ in the lexicographic order. By the inductive hypothesis, M' can be reduced to β-normal form, so the result also holds for M. $\square$

Theorem (strong normalisation theorem)**.** Let $\Gamma \Vdash M : \sigma$. Then there is no infinite sequence

$$M \to_\beta M_1 \to_\beta M_2 \to_\beta \cdots$$

The proof is omitted.

7 Intuitionistic semantics

7.1 Propositions as types

We will work with the fragment of IPC, denoted IPC($\to$), where the only connective is $\to$, and the deduction rules are $\to$-I, $\to$-E, Ax.

If $\mathcal{L}$ is a propositional language for IPC($\to$) and P is its set of primitive propositions, we can generate a simply typed λ-calculus $\lambda(\to)$ by taking the set of primitive types $\mathcal{U}$ to be P. Then the types Π and the propositions $\mathcal{L}$ are generated by the same grammar

$$\mathcal{U} \mid \Pi \to \Pi$$

A proposition is thus the type of its proofs, and a context is a set of hypotheses.

Proposition (Curry–Howard correspondence for IPC($\to$))**.** Let Γ be a context for $\lambda(\to)$, and let φ be a proposition. Then

(i) If $\Gamma \Vdash M : \varphi$, then

$$|\Gamma| = \{\tau \in \Pi \mid \exists x.\, (x : \tau) \in \Gamma\} \vdash_{\mathsf{IPC}(\to)} \varphi$$

(ii) If $\Gamma \vdash_{\mathsf{IPC}(\to)} \varphi$, then there is a simply typed λ-term M such that

$$\{(x_\tau : \tau) \mid \tau \in \Gamma\} \Vdash M : \varphi$$

Proof. Part (i). We use induction over the derivation of $\Gamma \Vdash M : \varphi$. If x is a variable not occurring in Γ', and the derivation is of the form $\Gamma', x : \varphi \Vdash x : \varphi$, then we must prove that $|\Gamma', x : \varphi| \vdash \varphi$, and this holds as $\varphi \vdash \varphi$.

If the derivation has M of the form $\lambda x : \sigma. N$ and $\varphi = \sigma \to \tau$, then we must have that $\Gamma, x : \sigma \Vdash N : \tau$. By the inductive hypothesis, we have $|\Gamma, x : \sigma| \vdash \tau$, so $|\Gamma|, \sigma \vdash \tau$. Thus we obtain a proof of $\sigma \to \tau$ from $|\Gamma|$ by $\to$-I.

If the derivation is of the form $\Gamma \Vdash (P\,Q) : \varphi$, then we must have $\Gamma \Vdash P : \sigma \to \varphi$ and $\Gamma \Vdash Q : \sigma$ for some σ. By the inductive hypothesis, $|\Gamma| \vdash \sigma \to \varphi$ and $|\Gamma| \vdash \sigma$. Then the result holds by $\to$-E.

Part (ii). We use induction over the proof tree of $\Gamma \vdash_{\mathsf{IPC}(\to)} \varphi$. We write

$$\Delta = \{(x_\tau : \tau) \mid \tau \in \Gamma\}$$

Suppose that we are at a stage of the proof that uses Ax, so $\Gamma, \varphi \vdash \varphi$. If $\varphi \in \Gamma$, then clearly $\Delta \Vdash x_\varphi : \varphi$. Otherwise, $\Delta, x_\varphi : \varphi \Vdash x_\varphi : \varphi$ as required.

Suppose that we are at a stage of the proof that uses $\to$-E, so

$$\frac{\Gamma \vdash \varphi \to \psi \qquad \Gamma \vdash \varphi}{\Gamma \vdash \psi}$$

By the inductive hypothesis, there are λ-terms M, N such that $\Delta \Vdash M : \varphi \to \psi$ and $\Delta \Vdash N : \varphi$. Then $\Delta \Vdash (M\,N) : \psi$ as required.

Finally, suppose we are at a stage of the proof that uses $\to$-I, so

$$\frac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \to \psi}$$

If $\varphi \in \Gamma$, then by the inductive hypothesis, there is a λ-term M such that $\Delta \Vdash M : \psi$. By the weakening rule, $\Delta, x : \varphi \Vdash M : \psi$ where x is a variable that does not occur in Δ. Then $\Delta \Vdash (\lambda x : \varphi. M) : \varphi \to \psi$ as required. Now suppose $\varphi \notin \Gamma$. By the inductive hypothesis we obtain a λ-term M such that $\Delta, x_\varphi : \varphi \Vdash M : \psi$. Then similarly $\Delta \Vdash (\lambda x_\varphi : \varphi. M) : \varphi \to \psi$. $\square$

This justifies the Brouwer–Heyting–Kolmogorov interpretation of intuitionistic logic.

Example. Let φ, ψ be primitive propositions, and consider the λ-term

$$\lambda f : (\varphi \to \psi) \to \varphi. \lambda g : \varphi \to \psi. g(fg)$$

This term has type

$$((\varphi \to \psi) \to \varphi) \to ((\varphi \to \psi) \to \psi)$$

The term encodes a proof of this proposition in $\vdash_{\mathsf{IPC}(\to)}$. The corresponding proof tree is

$$\cfrac{\cfrac{\cfrac{\cfrac{g : [\varphi \to \psi] \qquad f : [(\varphi \to \psi) \to \varphi]}{fg : \varphi}\ \to\text{-E} \qquad g : [\varphi \to \psi]}{g(fg) : \psi}\ \to\text{-E}}{\lambda g : \varphi \to \psi. g(fg) : (\varphi \to \psi) \to \psi}\ \to\text{-I}}{\lambda f : (\varphi \to \psi) \to \varphi. \lambda g : \varphi \to \psi. g(fg) : ((\varphi \to \psi) \to \varphi) \to ((\varphi \to \psi) \to \psi)}\ \to\text{-I}$$

7.2 Full simply typed lambda calculus

The types of the full simply typed λ-calculus $\mathsf{ST}\lambda\mathsf{C}$ are generated by the following grammar.

$$\Pi ::= \mathcal{U} \mid \Pi \to \Pi \mid \Pi \times \Pi \mid \Pi + \Pi \mid 1 \mid 0$$

where $\mathcal{U}$ is a set of primitive types or type variables. The terms are of the form

$$\begin{aligned} \Lambda_\Pi ::= {} & V \mid (\lambda x : \Pi. \Lambda_\Pi) \mid \Lambda_\Pi\, \Lambda_\Pi \mid \\ & \langle \Lambda_\Pi, \Lambda_\Pi \rangle \mid \pi_1(\Lambda_\Pi) \mid \pi_2(\Lambda_\Pi) \mid \\ & \iota_1(\Lambda_\Pi) \mid \iota_2(\Lambda_\Pi) \mid \mathsf{case}(\Lambda_\Pi; V.\Lambda_\Pi; V.\Lambda_\Pi) \mid \\ & \star \mid !_\Pi\, \Lambda_\Pi \end{aligned}$$

where V is an infinite set of variables, and $\star$ is a constant. This expanded syntax comes with new typing rules.

$$\frac{\Gamma \Vdash M : \psi \times \varphi}{\Gamma \Vdash \pi_1(M) : \psi} \qquad \frac{\Gamma \Vdash M : \psi \times \varphi}{\Gamma \Vdash \pi_2(M) : \varphi} \qquad \frac{\Gamma \Vdash M : \psi \qquad \Gamma \Vdash N : \varphi}{\Gamma \Vdash \langle M, N \rangle : \psi \times \varphi} \qquad \frac{\Gamma \Vdash M : \psi}{\Gamma \Vdash \iota_1(M) : \psi + \varphi}$$

$$\frac{\Gamma \Vdash M : \varphi}{\Gamma \Vdash \iota_2(M) : \psi + \varphi} \qquad \frac{\Gamma \Vdash L : \psi + \varphi \qquad \Gamma, x : \psi \Vdash M : \rho \qquad \Gamma, y : \varphi \Vdash N : \rho}{\Gamma \Vdash \mathsf{case}(L; x^\psi.M; y^\varphi.N) : \rho} \qquad \frac{}{\Gamma \Vdash \star : 1}$$

$$\frac{\Gamma \Vdash M : 0}{\Gamma \Vdash !_\varphi M : \varphi}$$

This typing relation captures the Brouwer–Heyting–Kolmogorov interpretation when paired with new reduction rules.

$$\pi_1(\langle M, N \rangle) \to_\beta M \qquad \pi_2(\langle M, N \rangle) \to_\beta N \qquad \langle \pi_1(M), \pi_2(M) \rangle \to_\eta M$$

$$\mathsf{case}(\iota_1(M); x^\psi.K; y^\varphi.L) \to_\beta K[x \coloneqq M] \qquad \mathsf{case}(\iota_2(M); x^\psi.K; y^\varphi.L) \to_\beta L[y \coloneqq M]$$

$$\text{if } \Gamma \Vdash M : 1 \text{ then } M \to_\eta \star$$

We can expand propositions-as-types to our new types:

(i) 0 corresponds to $\bot$;

(ii) 1 corresponds to $\top$;

(iii) product types correspond to conjunctions;

(iv) coproduct types correspond to disjunctions.

In this way, propositions correspond to types. Redexes are now those expressions consisting of a constructor (pair formation, λ-abstraction, and injections) followed by the corresponding destructor (projections, applications, and case expressions).

Example. Consider the following proof of $(\varphi \wedge \chi) \to (\psi \to \varphi)$.

$$\cfrac{\cfrac{\cfrac{[\varphi \wedge \chi]}{\varphi} \qquad [\psi]}{\psi \to \varphi}}{(\varphi \wedge \chi) \to (\psi \to \varphi)}$$

Annotating the corresponding λ-terms, we obtain

$$\cfrac{\cfrac{\cfrac{p : [\varphi \wedge \chi]}{\pi_1(p) : \varphi} \qquad b : [\psi]}{\lambda b^\psi.\, \pi_1(p) : \psi \to \varphi}}{\lambda p^{\varphi \times \chi}.\, \lambda b^\psi.\, \pi_1(p) : (\varphi \wedge \chi) \to (\psi \to \varphi)}$$

Hence this proof tree corresponds to the λ-term

$$\lambda p^{\varphi \times \chi}.\, \lambda b^\psi.\, \pi_1(p) : (\varphi \times \chi) \to (\psi \to \varphi)$$

In summary, the Curry–Howard correspondence for the whole of IPC and STλC states that

(i) (primitive) types correspond to (primitive) propositions;

(ii) variables correspond to hypotheses;

(iii) λ-terms correspond to proofs;

(iv) inhabitation of a type corresponds to provability of a proposition;

(v) term reduction corresponds to proof normalisation.

7.3 Heyting semantics

Boolean algebras represent truth-values of classical propositions. We can generalise this notion to intuitionistic logic.

Definition. A *Heyting algebra* H is a bounded lattice equipped with a binary operation $\Rightarrow : H \times H \to H$ such that

$$a \wedge b \leq c \iff a \leq b \Rightarrow c$$

A *morphism* of Heyting algebras is a function that preserves all finite meets and joins (including true and false) and $\Rightarrow$.

In particular, if f is a morphism of Heyting algebras and $a \leq b$, then $f(a) \leq f(b)$.

Example. (i) Every Boolean algebra is a Heyting algebra by defining $a \Rightarrow b$ to be $\neg a \vee b$. Note that $\neg a = a \Rightarrow \bot$.

(ii) Every topology is a Heyting algebra, where $U \Rightarrow V = ((X \setminus U) \cup V)^\circ$.

(iii) Every finite distributive lattice is a Heyting algebra.

(iv) The Lindenbaum–Tarski algebra of a propositional theory $\mathcal{T}$ with respect to IPC is a Heyting algebra.

Definition. Let H be a Heyting algebra and let $\mathcal{L}$ be a propositional language with a set P of primitive propositions. An *H-valuation* is a function $v : P \to H$, recursively expanded to $\mathcal{L}$ by the rules

(i) $v(\bot) = \bot$;

(ii) $v(A \wedge B) = v(A) \wedge v(B)$;

(iii) $v(A \vee B) = v(A) \vee v(B)$;

(iv) $v(A \to B) = v(A) \Rightarrow v(B)$.

We say that a proposition A is *H-valid* if $v(A) = \top$ for all valuations v. A is an *H-consequence* of a finite set of propositions Γ if $v\left(\bigwedge \Gamma\right) \leq v(A)$, and write $\Gamma \vDash_H A$.

Lemma (soundness)**.** Let H be a Heyting algebra and let $v : \mathcal{L} \to H$ be an H-valuation. If $\Gamma \vdash_{\mathsf{IPC}} A$, then $\Gamma \vDash_H A$.

Proof. We proceed by induction over the derivation of $\Gamma \vdash_{\mathsf{IPC}} A$.

(i) (AX) $v\left(\left(\bigwedge \Gamma\right) \wedge A\right) = v\left(\bigwedge \Gamma\right) \wedge v(A) \leq v(A)$.

(ii) ($\wedge$-I) In this case, $A = B \wedge C$ and we have derivations $\Gamma_1 \vdash B, \Gamma_2 \vdash C$ with $\Gamma_1, \Gamma_2 \subseteq \Gamma$. By the inductive hypothesis, $v(\Gamma_1) \leq v(B)$ and $v(\Gamma_2) \leq v(C)$, hence

$$v\big(\bigwedge \Gamma\big) \leq v(\Gamma_1) \wedge v(\Gamma_2) \leq v(B) \wedge v(C) = v(B \wedge C) = v(A)$$

(iii) ($\rightarrow$-I) In this case, $A = B \rightarrow C$ and we have $\Gamma \cup \{B\} \vdash C$. By the inductive hypothesis, $v\big(\bigwedge \Gamma\big) \wedge v(B) \leq v(C)$. But then $v\big(\bigwedge \Gamma\big) \leq v(B) \Rightarrow v(C)$ by definition, so $v\big(\bigwedge \Gamma\big) \leq v(B \rightarrow C)$ as required.

(iv) ($\vee$-I) In this case, $A = B \vee C$, and without loss of generality, we have $\Gamma \vdash B$. By the inductive hypothesis, $v\big(\bigwedge \Gamma\big) \leq v(B)$, but $v(B) \leq v(B) \vee v(C) = v(B \vee C)$ as required.

(v) ($\wedge$-E) By the inductive hypothesis, we have $v\big(\bigwedge \Gamma\big) \leq v(A \wedge B) = v(A) \wedge v(B) \leq v(A), v(B)$ as required.

(vi) ($\rightarrow$-E) We know that $v(A \rightarrow B) = (v(A) \Rightarrow v(B))$. From the inequality $v(A \rightarrow B) \leq (v(A) \Rightarrow v(B))$, we deduce $v(A \rightarrow B) \wedge v(A) \leq v(B)$. Thus, if $v\big(\bigwedge \Gamma\big) \leq v(A \rightarrow B)$ and $v\big(\bigwedge \Gamma\big) \leq v(A)$, we have $v\big(\bigwedge \Gamma\big) \leq v(B)$ as required.

(vii) ($\vee$-E) By the inductive hypothesis,

$$v\Big(A \wedge \bigwedge \Gamma\Big) \leq v(C); \quad v\Big(B \wedge \bigwedge \Gamma\Big) \leq v(C); \quad v\Big(\bigwedge \Gamma\Big) \leq v(A \vee B) = v(A) \vee v(B)$$

Hence,

$$v\Big(\bigwedge \Gamma\Big) = v\Big(\bigwedge \Gamma\Big) \wedge (v(A) \vee v(B)) = \Big(v\Big(\bigwedge \Gamma\Big) \wedge v(A)\Big) \vee \Big(v\Big(\bigwedge \Gamma\Big) \wedge v(B)\Big) \leq v(C) \vee v(C) = v(C)$$

as every Heyting algebra is a distributive lattice.

(viii) ($\perp$-E) If $v\big(\bigwedge \Gamma\big) \leq v(\perp) = \perp$, then $v\big(\bigwedge \Gamma\big) = \perp$. Hence, $v\big(\bigwedge \Gamma\big) \leq v(A)$ for any A.

$\square$

Example. The law of the excluded middle LEM is not provable in IPC. Let p be a primitive proposition, and consider the Heyting algebra given by the Sierpiński topology $\{\varnothing, \{1\}, \{1,2\}\}$ on $X = \{1,2\}$. We define the valuation given by $v(p) = \{1\}$. Then

$$v(\neg p) = \{1\} \Rightarrow \varnothing = (\{1,2\} \setminus \{1\})^\circ = \{2\}^\circ = \varnothing$$

Hence,

$$v(p \vee \neg p) = \{1\} \cup \varnothing = \{1\} \neq \{1,2\} = \top$$

Thus, by soundness, $p \vee \neg p$ is not provable (from the empty context, which has valuation $\top = \{1,2\}$) in IPC.

Example. Peirce's law $((p \rightarrow q) \rightarrow p) \rightarrow p$ is not intuitionistically valid. Let H be the Heyting algebra given by the usual topology on the plane $\mathbb{R}^2$, and let

$$v(p) = \mathbb{R}^2 \setminus \{(0,0)\}; \quad v(q) = \varnothing$$

Classical completeness can be phrased as

$$\Gamma \vdash_{\mathsf{CPC}} A \iff \Gamma \vDash_2 A$$

where 2 is the Boolean algebra $\{0,1\}$. For intuitionistic logic, we cannot replace 2 with a single finite Heyting algebra, so we will instead quantify over all Heyting algebras.

Theorem (completeness)**.** A proposition is provable in IPC if and only if it is H-valid for every Heyting algebra H.

Proof. For the forward direction, if $\vdash_{\mathsf{IPC}} A$, then $\top \leq v(A)$ for every Heyting algebra H and valuation v, by soundness. Then $\top = v(A)$, so A is H-valid.

For the backward direction, suppose A is H-valid for every Heyting algebra H. Note that the Lindenbaum–Tarski algebra $\mathcal{L}/\sim$ for the empty theory, with respect to IPC, is a Heyting algebra. Consider the valuation given by mapping each primitive proposition to its equivalence class in $\mathcal{L}/\sim$. Then, one can easily show by induction that $v : \mathcal{L} \to \mathcal{L}/\sim$ is the quotient map by considering the construction of the Lindenbaum–Tarski algebra. Now, A is valid in every Heyting algebra and with respect to every valuation, so in particular, $v(A) = \top$ in $\mathcal{L}/\sim$. But then $v(A) \in [\top]$, so $\vdash_{\mathsf{IPC}} A \leftrightarrow \top$, so $\vdash_{\mathsf{IPC}} A$ as required. □

7.4 Kripke semantics

Definition. Let S be a poset. For each $a \in S$, we define its *principal up-set* to be

$$a\uparrow = \{s \in S \mid a \leq s\}$$

Note that $U \subseteq S$ is a terminal segment if and only if it contains $a\uparrow$ for each $a \in U$.

Proposition. Let S be a poset. Then the set $T(S)$ of terminal segments of S has the structure of a Heyting algebra.

Proof. The order is given by inclusion: $U \leq V$ if and only if $U \subseteq V$. We define

$$U \wedge V = U \cap V$$
$$U \vee V = U \cup V$$
$$U \Rightarrow V = \{s \mid s\uparrow \cap U \subseteq V\}$$

One can check that this forms a Heyting algebra as required. □

Definition. Let P be a set of primitive propositions. A *Kripke model* is a triple $(S, \leq, \Vdash)$ where S is a poset and $(\Vdash) \subseteq S \times P$ is a relation satisfying the *persistence property*: if $p \in P$ is such that $s \Vdash p$ and $s \leq s'$, then $s' \Vdash p$.

S is a set of possible *worlds*, or states of knowledge, ordered by how knowledgeable they are. The relation $\Vdash$ is called the *forcing* relation; we say that a world *forces* a proposition to be true.

Every valuation v on $T(S)$ induces a Kripke model by setting $s \Vdash p \iff s \in v(p)$. The persistence property corresponds to the fact that $T(S)$ contains only terminal segments.

Definition. Let $(S, \leq, \Vdash)$ be a Kripke model. We can extend the forcing relation to a relation $(\Vdash) \subseteq S \times \mathcal{L}$ recursively as follows.

(i) $s \nVdash \bot$;
(ii) $s \Vdash \varphi \wedge \psi$ if and only if $s \Vdash \varphi$ and $s \Vdash \psi$;
(iii) $s \Vdash \varphi \vee \psi$ if and only if $s \Vdash \varphi$ or $s \Vdash \psi$;
(iv) $s \Vdash \varphi \to \psi$ if and only if for all $s' \geq s$, $s' \Vdash \varphi$ implies $s' \Vdash \psi$.

One can check by induction that persistence holds for arbitrary propositions.

Remark. $s \Vdash \neg\varphi$ if and only if no more knowledgeable world than s forces φ. $s \Vdash \neg\neg\varphi$ is the statement that φ is consistent with every extension of s but need not hold in s itself; that is, for each $s' \geq s$, there exists $s'' \geq s'$ with $s \Vdash \varphi$.

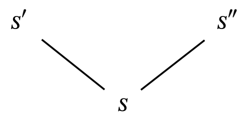
We say that $S \Vdash \varphi$ if every world s forces φ. If S has a bottom element s, then $S \Vdash \varphi$ if and only if $s \Vdash \varphi$ by persistence.

Example. Consider the Kripke models

(i)

where $s' \Vdash p$;

(ii)



where $s'' \Vdash p$;

(iii)

where $s' \Vdash p$ and $s' \Vdash q$.

Note that in (i), we have $s \nVdash \neg p$, since $s' \geq s$ and $s' \Vdash p$. But also $s \nVdash p$ by assumption, thus $s \nVdash p \vee \neg p$. Note that $s \Vdash \neg\neg p$, but $s \nVdash p$, so we also have $s \nVdash \neg\neg p \to p$.

In (ii), $s \nVdash \neg\neg p$, since $s' \geq s$ cannot access a world that forces p. We also have $s \nVdash \neg p$, since $s'' \geq s'$ and $s'' \vDash p$. Thus $s \nVdash \neg\neg p \vee \neg p$.

In (iii), $s \nVdash (p \to q) \to (\neg p \vee q)$. Indeed, all worlds force $p \to q$, and we have $s \nVdash q$, so it suffices to check that $s \nVdash \neg p$, but this holds as $s' \geq s$ and $s' \vDash p$.

A filter $\mathcal{F}$ is called *prime* if whenever $x \vee y \in \mathcal{F}$, either $x \in \mathcal{F}$ or $y \in \mathcal{F}$.

Lemma. Let H be a Heyting algebra and let v be an H-valuation. Then there is a Kripke model $(S, \leq, \Vdash)$ such that for each proposition φ, we have $v \vDash_H \varphi$ if and only if $S \Vdash \varphi$.

Thus we can convert between Kripke models and valuations on Heyting algebras. This will allow us to prove the completeness theorem for Kripke semantics.

Proof. Let S be the set of prime filters on H ordered by inclusion. We say that $\mathcal{F} \Vdash p$ if and only if $v(p) \in \mathcal{F}$, and prove by induction that this extends to arbitrary propositions. Here, we will prove the case of implications; the other connectives are easy, and primality of the filter is required for the case of disjunction. Let $\mathcal{F} \Vdash (\psi \to \psi')$ and suppose $v(\psi \to \psi') = v(\psi) \Rightarrow v(\psi') \notin \mathcal{F}$. Let $\mathcal{G}'$ be the smallest filter containing $\mathcal{F}$ and $v(\psi)$. Then

$$\mathcal{G}' = \{b \mid \exists f \in \mathcal{F}.\, f \wedge v(\psi) \leq b\}$$

Note that $v(\psi') \notin \mathcal{G}'$, otherwise $f \wedge v(\psi) \leq v(\psi')$ for some $f \in \mathcal{F}$, and then $f \leq v(\psi) \Rightarrow v(\psi') \in \mathcal{F}$, giving a contradiction. In particular, $\mathcal{G}'$ is a proper filter, so by Zorn's lemma there is a prime filter $\mathcal{G}$ containing $\mathcal{G}'$ that does not contain $v(\psi')$.

By the inductive hypothesis, $\mathcal{G} \Vdash \psi$, and since $\mathcal{F} \Vdash (\psi \to \psi')$ and $\mathcal{G}'$ contains $\mathcal{G}$ which contains $\mathcal{F}$, we must have $\mathcal{G} \Vdash \psi'$. Then $v(\psi') \in \mathcal{G}$, which is a contradiction. Thus $\mathcal{F} \Vdash \psi \to \psi'$ implies that $v(\psi \to \psi') \in \mathcal{F}$.

Conversely, suppose

$$v(\psi \to \psi') \in \mathcal{F} \subseteq \mathcal{G} \Vdash \psi$$

By the inductive hypothesis, $v(\psi) \in \mathcal{G}$, and so $v(\psi) \Rightarrow v(\psi') \in \mathcal{G}$ as $\mathcal{F} \subseteq \mathcal{G}$. Then $v(\psi') \geq v(\psi) \wedge (v(\psi) \Rightarrow v(\psi')) \in \mathcal{G}$, so again by the inductive hypothesis, $G \Vdash \psi'$ as required.

It thus suffices to show that $v \vDash_H \varphi$ if and only if $S \Vdash \varphi$. If $v \vDash_H \varphi$, then $v(\varphi) = \top$, so $v(\varphi)$ is contained in every filter of H. So $\mathcal{F} \Vdash \varphi$ for every prime filter $\mathcal{F}$. Conversely, suppose $S \Vdash \varphi$ but $v \nvDash_H \varphi$. Then since $v(\varphi) \neq \top$, there must be a proper filter $\mathcal{F}$ that does not contain $v(\varphi)$. We extend this as above to a prime filter $\mathcal{G}$ that does not contain $v(\varphi)$. Then $\mathcal{G} \nVdash \varphi$, contradicting the assumption that $S \Vdash \varphi$. □

Theorem (completeness). For every proposition φ, we have $\Gamma \vdash_{\mathsf{IPC}} \varphi$ if and only if for all Kripke models $(S, \leq, \Vdash)$, if $S \Vdash \Gamma$ then $S \Vdash \varphi$.

Proof. Soundness holds by induction. For adequacy, suppose $\Gamma \nvdash_{\mathsf{IPC}} \varphi$. Then by completeness of Heyting semantics, there is a Heyting algebra H and H-valuation v such that $v \vDash_H \Gamma$ but $v \nvDash_H \varphi$. By the previous lemma, there is a Kripke model $(S, \leq, \Vdash)$ such that $S \Vdash \Gamma$ but $S \nVdash \varphi$, contradicting the hypothesis. □