Proof Theory.

 **Theorem** (Gentzen).
Let $T \supseteq \mathbf{PA}$ such that T proves the existence and wellfoundedness of (a code for) all ordinals $\alpha < \varepsilon_0$. Then $T \vdash \mathrm{Cons}(\mathbf{PA})$.

Questions:

- What is ε_0?
- How can a theory in the language of arithmetic prove anything about ordinals?

Operations on ordinals (1).

If $\mathbf{L} = \langle L, \leq \rangle$ and $\mathbf{M} = \langle M, \sqsubseteq \rangle$ are linear orders, we can define their sum and product:

$\mathbf{L} \oplus \mathbf{M} := \langle L \dot{\cup} M, \preceq \rangle$ where $x \preceq y$ if

- $x \in L$ and $y \in M$, or
- $x, y \in L$ and $x \leq y$, or
- $x, y \in M$ and $x \sqsubseteq y$.

$\mathbf{L} \otimes \mathbf{M} := \langle L \times M, \preceq \rangle$ where $\langle x, y \rangle \preceq \langle x^*, y^* \rangle$ if

- $y \sqsubset y^*$, or
- $y = y^*$ and $x \leq x^*$.

Operations on ordinals (2).

Fact. $\mathbb{N} \oplus \mathbb{N}$ is isomorphic to $\mathbb{N} \otimes \mathbf{2}$.

Exercise. These operations are not commutative: there are linear orders such that $\mathbf{L} \oplus \mathbf{M}$ is not isomorphic to $\mathbf{M} \oplus \mathbf{L}$ and similarly for $\otimes$. (Exercise 37.)

Observation. If $\mathbf{L}$ and $\mathbf{M}$ are wellorders, then so are $\mathbf{L} \oplus \mathbf{M}$ and $\mathbf{L} \otimes \mathbf{M}$.

Based on $\otimes$, we can define exponentiation by transfinite recursion for ordinals α and β:

$$\begin{aligned} \alpha^0 &:= \mathbf{1} \\ \alpha^{\beta+1} &:= \alpha^\beta \otimes \alpha \\ \alpha^\lambda &:= \bigcup\{\alpha^\beta\,;\,\beta < \lambda\} \end{aligned}$$

Hauptzahlen

An ordinal ξ is called γ-number ("Hauptzahl der Addition") if for all $\alpha, \beta < \xi$, we have $\alpha \oplus \beta < \xi$.

Example. $\omega \otimes \omega$ is a γ-number.

An ordinal ξ is called δ-number ("Hauptzahl der Multiplikation") if for all $\alpha, \beta < \xi$, we have $\alpha \otimes \beta < \xi$.

Example. ω^ω is a δ-number.

An ordinal ξ is called ε-number ("Hauptzahl der Exponentiation") if for all $\alpha, \beta < \xi$, we have $\alpha^\beta < \xi$.

ε_0 is the least ε-number.

Arithmetic and orderings (1).

Ordinals are not objects of arithmetic (neither first-order not second-order). So what should it mean that an arithmetical theory proves that "ε_0 is well-ordered"?

Let α be a countable ordinal. By definition, there is some bijection $f : \mathbb{N} \to \alpha$. Define

$$n <_f m :\leftrightarrow f(n) < f(m).$$

Clearly, f is an isomorphism between $\langle \mathbb{N}, <_f \rangle$ and α.

If $g : \mathbb{N} \times \mathbb{N} \to \{0, 1\}$ is an arbitrary function, we can interpret it as a binary relation on $\mathbb{N}$:

$$n <_g m :\leftrightarrow g(n, m) = 1.$$

Arithmetic and orderings (2).

Let us work in second-order arithmetic

$$\langle \mathbb{N}, \mathbb{N}^{\mathbb{N}}, 2^{\mathbb{N}\times\mathbb{N}}, +, \times, 0, 1, \mathrm{app} \rangle$$

$g : \mathbb{N} \times \mathbb{N} \to \{0,1\}$ codes a wellfounded relation if and only if

$$\neg \exists F \in \mathbb{N}^{\mathbb{N}} \forall n \in \mathbb{N} (g(F(n+1), F(n)) = 1).$$

"Being a code for an ordinal $< \varepsilon_0$" is definable in the language of second-order arithmetic (ordinal notation systems).
$\mathrm{TI}(\varepsilon_0)$ is defined to be the formalization of "every code g for an ordinal $< \varepsilon_0$ codes a wellfounded relation".

More proof theory (1).

$\mathrm{TI}(\varepsilon_0)$: “every code g for an ordinal $< \varepsilon_0$ codes a wellfounded relation”

Generalization: If “being a code for an ordinal $< \alpha$” can be defined in second-order arithmetic, then let $\mathrm{TI}(\alpha)$ mean “every code g for an ordinal $< \alpha$ codes a wellfounded relation”.

The proof-theoretic ordinal of a theory T.

$$|T| := \sup\{\alpha\,;\, T \vdash \mathrm{TI}(\alpha)\}$$

Rephrasing Gentzen. $|\mathrm{PA}| = \varepsilon_0$.

More proof theory (2).

Results from Proof Theory.

- The proof-theoretic ordinal of primitive recursive arithmetic is ω^ω.
- (Jäger-Simpson) The proof-theoretic ordinal of arithmetic with arithmetical transfinite recursion is Γ_0 (the limit of the Veblen functions).

These ordinals are all smaller than ω_1^{CK}, the least noncomputable ordinal, *i.e.*, the first ordinal α such that there is no computable function $g : \mathbb{N} \times \mathbb{N} \to \{0, 1\}$ such that $\langle \mathbb{N}, <_g \rangle$ is isomorphic to α.

Our open question in set theory...

- inaccessible cardinal – a regular, strong limit cardinal.
- measurable cardinal – a cardinal κ such that there is a nonprincipal κ-complete ultrafilter on κ ("κ is a generalized solution to the measure problem").

Theorem (Tarski-Ulam, 1930). Every measurable cardinal is inaccessible.

Question. Is every inaccessible cardinal measurable?

Łoś

Jerzy Łoś
1920-1998

- Invented ultraproducts.
- Introduced the notion of categoricity.
- Conjectured Morley's theorem: If a theory is κ-categorical for an uncountable κ, then it is κ-categorical for all uncountable κ.
- **1955.** *Quelques remarques, théorèmes et problèmes sur les classes définissable d'algèbres*.

Products (1).

Let $\mathcal{L} = \{\dot{\mathrm{f}}_n, \dot{\mathrm{R}}_m \,;\, n, m\}$ be a first-order language and S be a set.

Suppose that for every $i \in S$, we have an $\mathcal{L}$-structure

$$\mathbf{M}_i = \langle M_i, f_n^i, R_m^i \,;\, n, m \rangle.$$

Let $M_S := \prod_{i \in S} M_i$. For $X_0, ..., X_k \in M$, we let

$$f_n^S(X_0, ..., X_k)(i) := f_n^i(X_0(i), ..., X_k(i)) \text{ and}$$

$$R_m^S(X_0, ..., X_k) :\leftrightarrow \forall i \in S(R_m^i(X_0(i), ..., X_k(i))).$$

Products (2).

In general, classes of structures are not closed under products:

Let $\mathcal{L}_{\mathrm{F}} := \{+, \times, 0, 1\}$ be the language of fields and Φ_{F} be the field axioms. Let $S = \{0, 1\}$ and $\mathbf{M}_0 = \mathbf{M}_1 = \mathbb{Q}$. Then $\mathbf{M}_S = \mathbb{Q} \times \mathbb{Q}$ is not a field: $\langle 1, 0 \rangle \in \mathbb{Q} \times \mathbb{Q}$ doesn't have an inverse.

Theorem (Birkhoff, 1935). If a class of algebras is equationally definable, then it is closed under products.

Garrett Birkhoff
(1884-1944)

Garrett **Birkhoff**, On the structure of abstract algebras, **Proceedings of the Cambridge Philosophical Society** 31 (1935), p. 433-454

Ultraproducts (1).

Suppose S is a set, $\mathbf{M}_i$ is an $\mathcal{L}$-structure and U is an ultrafilter on S.

Define $\equiv_U$ on M_S by

$$X \equiv_U Y :\leftrightarrow \{i\,;\, X(i) = Y(i)\} \in U,$$

and let $M_U := M_S/{\equiv_U}$.
The functions f_n^S and the relations R_m^S are welldefined on M_U (*i.e.*, if $X \equiv_U Y$, then $f_n^S(X) \equiv_U f_n^S(Y)$), and so they induce functions and relations f_n^U and R_m^U on M_U.
We call

$$\mathbf{M}_U := \mathrm{Ult}(\langle \mathbf{M}_i\,;\, i \in S\rangle, U) := \langle M_U, f_n^U, R_m^U\,;\, n, m\rangle$$

the ultraproduct of the sequence $\langle \mathbf{M}_i\,;\, i \in S\rangle$ with U.

Ultraproducts (2).

Theorem (Łoś.) Let $\langle \mathbf{M}_i \, ; \, i \in S \rangle$ be a family of $\mathcal{L}$-structures and U be an ultrafilter on S. Let φ be an $\mathcal{L}$-formula. Then the following are equivalent:

1. $\mathbf{M}_U \models \varphi([X_0]_{\equiv_U}, ..., [X_k]_{\equiv_U})$, and
2. $\{i \in S \, ; \, \mathbf{M}_i \models \varphi(X_0(i), ..., X_k(i))\} \in U$.

Ultraproducts (2).

Theorem (Łoś.) Let $\langle \mathbf{M}_i\,;\, i \in S\rangle$ be a family of $\mathcal{L}$-structures and U be an ultrafilter on S. Let σ be an $\mathcal{L}$-sentence. Then the following are equivalent:

1. $\mathbf{M}_U \models \sigma$, and
2. $\{i \in S\,;\, \mathbf{M}_i \models \sigma\} \in U$.

Applications.

- If for all $i \in S$, $\mathbf{M}_i$ is a fi eld, then $\mathbf{M}_U$ is a fi eld.
- Let $S = \mathbb{N}$. Sets of the form $\{n\,;\, N \leq n\}$ are called fi nal segments. An ultrafi lter U on $\mathbb{N}$ is called nonprincipal if it contains all fi nal segments. If $\langle \mathbf{M}_n\,;\, n \in \mathbb{N}\rangle$ is a family of $\mathcal{L}$-structures, U a nonprincipal ultrafi lter, and Φ an (infi nite) set of sentences such that each element is "eventually true", then $\mathbf{M}_U \models \Phi$.
- **Nonstandard analysis** (Robinson). Let $\mathcal{L}$ be the language of fi elds with an additional 0-ary function symbol $\dot{c}$. Let $\mathbf{M}_i \models \mathrm{Th}(\mathbb{R}) \cup \{\dot{c} \neq 0 \wedge \dot{c} < \frac{1}{i}\}$. Then $\mathbf{M}_U$ is a model of $\mathrm{Th}(\mathbb{R})$ plus "there is an infi nitesimal".

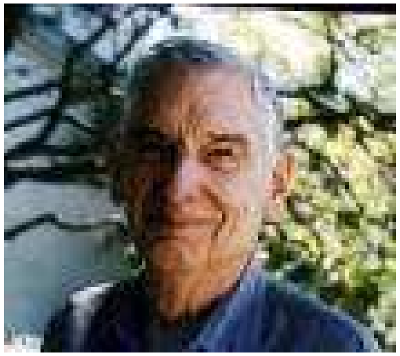
Tarski (1).

Alfred Tarski
1902-1983

- *Teitelbaum* (until c. 1923).
- 1918-1924. Studies in Warsaw. Student of Lesniewski.
- 1924. Banach-Tarski paradox.
- 1924-1939. Work in Poland.
- 1933. *The concept of truth in formalized languages*.
- From 1942 at the University of California at Berkeley.
- **Students. 1946.** Bjarni Jónsson (b. 1920). **1948.** Julia Robinson (1919-1985).

Tarski (1).

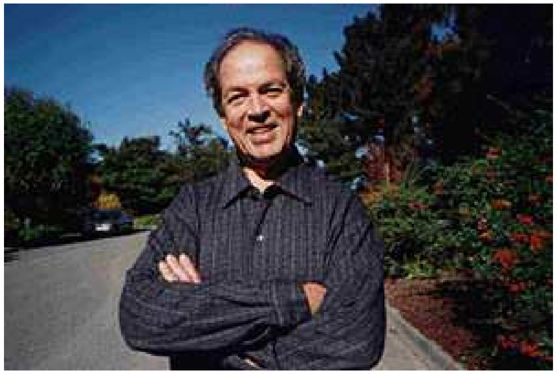
Alfred Tarski
1902-1983



- *Teitelbaum* (until c. 1923).
- 1918-1924. Studies in Warsaw. Student of Lesniewski.
- 1924. Banach-Tarski paradox.
- 1924-1939. Work in Poland.
- 1933. *The concept of truth in formalized languages*.
- From 1942 at the University of California at Berkeley.
- **Students. 1946.** Bjarni Jónsson (b. 1920). **1948.** Julia Robinson (1919-1985). **1954.** Bob Vaught (1926-2002).

Tarski (1).

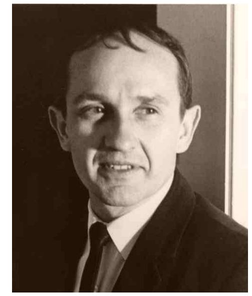
Alfred Tarski
1902-1983



- *Teitelbaum* (until c. 1923).
- 1918-1924. Studies in Warsaw. Student of Lesniewski.
- 1924. Banach-Tarski paradox.
- 1924-1939. Work in Poland.
- 1933. *The concept of truth in formalized languages*.
- From 1942 at the University of California at Berkeley.
- **Students. 1946.** Bjarni Jónsson (b. 1920). **1948.** Julia Robinson (1919-1985). **1954.** Bob Vaught (1926-2002). **1957.** Solomon Feferman (b. 1928).

Tarski (1).

Alfred Tarski
1902-1983



- *Teitelbaum* (until c. 1923).
- 1918-1924. Studies in Warsaw. Student of Lesniewski.
- 1924. Banach-Tarski paradox.
- 1924-1939. Work in Poland.
- 1933. *The concept of truth in formalized languages*.
- From 1942 at the University of California at Berkeley.
- **Students. 1946.** Bjarni Jónsson (b. 1920). **1948.** Julia Robinson (1919-1985). **1954.** Bob Vaught (1926-2002). **1957.** Solomon Feferman (b. 1928). **1957.** Richard Montague (1930-1971).

Tarski (1).

Alfred Tarski
1902-1983

- *Teitelbaum* (until c. 1923).
- 1918-1924. Studies in Warsaw. Student of Lesniewski.
- 1924. Banach-Tarski paradox.
- 1924-1939. Work in Poland.
- 1933. *The concept of truth in formalized languages*.
- From 1942 at the University of California at Berkeley.
- **Students. 1946.** Bjarni Jónsson (b. 1920). **1948.** Julia Robinson (1919-1985). **1954.** Bob Vaught (1926-2002). **1957.** Solomon Feferman (b. 1928). **1957.** Richard Montague (1930-1971). **1961.** Jerry Keisler.

Tarski (1).

Alfred Tarski
1902-1983

- *Teitelbaum* (until c. 1923).
- 1918-1924. Studies in Warsaw. Student of Lesniewski.
- 1924. Banach-Tarski paradox.
- 1924-1939. Work in Poland.
- 1933. *The concept of truth in formalized languages*.
- From 1942 at the University of California at Berkeley.
- **Students. 1946.** Bjarni Jónsson (b. 1920). **1948.** Julia Robinson (1919-1985). **1954.** Bob Vaught (1926-2002). **1957.** Solomon Feferman (b. 1928). **1957.** Richard Montague (1930-1971). **1961.** Jerry Keisler. **1961.** Donald Monk (b. 1930). **1962.** Haim Gaifman. **1963.** William Hanf.

Tarski (2).

- **Undefinability of Truth.**
  If a language can correctly refer to its own sentences, then the truth predicate is not definable.

  Limitative Theorems.

Provability	*Truth*	*Computability*
1931	1933	1935
Gödel	Tarski	Turing

  More in the last lecture (Dec 15th).

Tarski (2).

- **Undefinability of Truth.**
- **Algebraic Logic.**
  - Leibniz called for an analysis of relations (“Plato is taller than Socrates” $\rightsquigarrow$ “Plato is tall in as much as Socrates is short”).
  - **Relation Algebras:** Steve Givant, István Németi, Hajnal Andréka, Ian Hodkinson, Robin Hirsch, Maarten Marx.
  - **Cylindric Algebras:** Don Monk, Leon Henkin, Ian Hodkinson, Yde Venema, Nick Bezhanishvili.

Tarski (2).

- **Undefinability of Truth.**
- **Algebraic Logic.**
- **Logic and Geometry.**
  - A theory T admits elimination of quantifiers if every first-order formula is T-equivalent to a quantifier-free formula (Skolem, 1919).
  - **1955.** Quantifier elimination for the theory of real numbers (“real-closed fields”).
  - Basic ideas of modern algebraic model theory.
  - Connections to theoretical computer science: running time of the quantifier elimination algorithms.

Ultraproducts in Set Theory.

Recall: A cardinal κ is called measurable if there is a κ-complete nonprincipal ultrafi lter on κ.

Idea: Apply the theory of ultraproducts to the ultrafilter witnessing measurability.
Let $\mathbf{V}$ be a model of set theory and $\mathbf{V} \models$"κ is measurable".
Let U be the ultrafilter witnessing this. Define $\mathrm{M}_\alpha := \mathbf{V}$ for all $\alpha \in \kappa$ and $\mathrm{M}_U := \mathrm{Ult}(\mathbf{V}, U)$.

By Łoś, M_U is again a model of set theory with a measurable cardinal.

Theorem (Scott / Tarski-Keisler, 1961). If κ is measurable, then there is some $\alpha < \kappa$ such that α is inaccessible.

Corollary. The least measurable is not the least inaccessible.

More on large cardinals.

Reflection. Some properties of a large cardinal κ reflect down to some (many, almost all) cardinals $\alpha < \kappa$.

- **Lévy** (1960); **Montague** (1961). Reflection Principle.
- **Hanf** (1964). Connecting large cardinal analysis to infi nitary logic.
- **Gaifman** (1964); **Silver** (1966). Connecting large cardinals and inner models of constructibility ("iterated ultrapowers").
- **Gödel's Programme.**
  1947. "What is Cantor's Continuum Problem?"

  Use new axioms (in particular large cardinal axioms) in order to resolve questions undecidable in ZF.
- **Lévy-Solovay** (1967). Large Cardinals don't solve the continuum problem.

Modal logic (1).

Modalities.

- *"the standard modalities"*. "necessarily", "possibly".
- *temporal*. "henceforth", "eventually", "hitherto".
- *deontic*. "it is obligatory", "it is allowed".
- *epistemic*. "p knows that".
- *doxastic*. "p believes that".

Modal logic (2).

Modalities as operators.

McColl (late XIXth century); Lewis-Langford (1932). $\Diamond$ as an operator on propositional expressions:

$$\Diamond\varphi \rightsquigarrow \text{“Possibly } \varphi\text{”.}$$

$\Box$ for the dual operator:

$$\Box\varphi \rightsquigarrow \text{“Necessarily } \varphi\text{”.}$$

Iterated modalities:

$$\Box\Diamond\varphi \rightsquigarrow \text{“It is necessary that } \varphi \text{ is possible”.}$$

Modal logic (3).

What modal formulas should be axioms? This depends on the interpretation of $\Diamond$ and $\Box$.

Example. $\Box\varphi \to \varphi$ ("axiom $\mathbf{T}$").

- *Necessity interpretation.* "If φ is necessarily true, then it is true."
- *Epistemic interpretation.* "If p knows that φ, then φ is true."
- *Doxastic interpretation.* "If p believes that φ, then φ is true."

Early modal semantics.

Topological Semantics (McKinsey / Tarski).
Let $\langle X, \tau \rangle$ be a topological space and $V : \mathbb{N} \to \wp(X)$ a valuation for the propositional variables.

$\langle X, \tau, x, V \rangle \models \Diamond\varphi$ if and only if x is in the closure of $\{z\,;\,\langle X, \tau, z, V \rangle \models \varphi\}$.

$\langle X, \tau \rangle \models \varphi$ if for all $x \in X$ and all valuations V, $\langle X, \tau, x, V \rangle \models \varphi$.

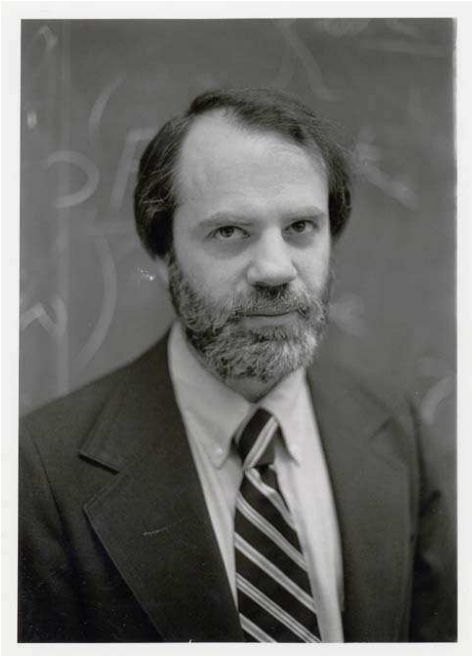
Theorem (McKinsey-Tarski; 1944). $\langle X, \tau \rangle \models \varphi$ if and only if $\mathbf{S4} \vdash \varphi$.

($\mathbf{S4} = \{\mathbf{T}, \Box\Box\varphi \to \Box\varphi\}$)

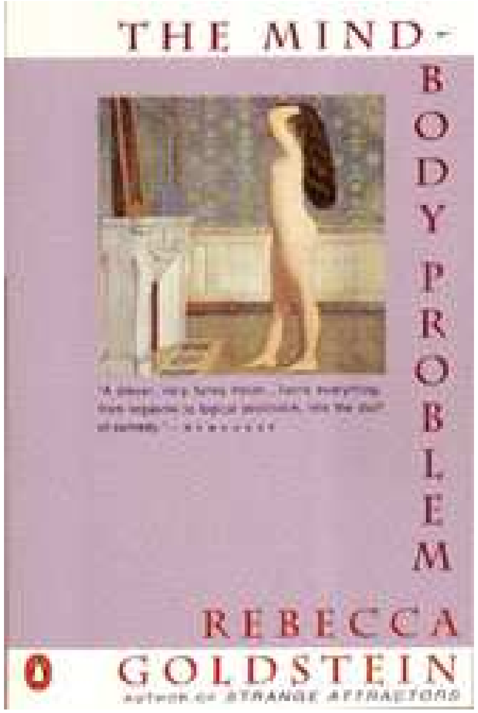
Possible Worlds.

Leibniz: There are as many possible worlds as there are things that can be conceived without contradiction. φ is necessarily true if its negation implies a contradiction.
$\rightsquigarrow$ φ is necessarily true if it is true in all possible worlds.

Kripke.



Saul Kripke
(b. 1940)



- Saul **Kripke**, A completeness theorem in modal logic, **Journal of Symbolic Logic** 24 (1959), p. 1-14.
- "*Naming and Necessity*".

Kripke semantics (1).

Let M be a set and $R \subseteq M \times M$ a binary relation. We call $\mathbf{M} = \langle M, R \rangle$ a Kripke frame. Let $V : \mathbb{N} \to \wp(M)$ be a valuation function. Then we call $\mathbf{M}^V = \langle M, R, V \rangle$ a Kripke model.

$$
\begin{array}{rcl}
\mathbf{M}^V, x \models \mathrm{p}_n & \text{iff} & x \in V(n) \\
\mathbf{M}^V, x \models \Diamond\varphi & \text{iff} & \exists y(xRy \;\&\; \mathbf{M}^V, y \models \varphi) \\
\mathbf{M}^V, x \models \Box\varphi & \text{iff} & \forall y(xRy \to \mathbf{M}^V, y \models \varphi) \\
\mathbf{M}^V \models \varphi & \text{iff} & \forall x(\mathbf{M}^V, x \models \varphi) \\
\mathbf{M} \models \varphi & \text{iff} & \forall V(\mathbf{M}^V \models \varphi)
\end{array}
$$

Kripke semantics (2).

$$\mathbf{M}^V, x \models \Diamond\varphi \quad \text{iff} \quad \exists y(xRy \,\&\, \mathbf{M}^V, y \models \varphi)$$
$$\mathbf{M}^V, x \models \Box\varphi \quad \text{iff} \quad \forall y(xRy \to \mathbf{M}^V, y \models \varphi)$$
$$\mathbf{M}^V \models \varphi \quad \text{iff} \quad \forall x(\mathbf{M}^V, x \models \varphi)$$
$$\mathbf{M} \models \varphi \quad \text{iff} \quad \forall V(\mathbf{M}^V \models \varphi)$$

- Let $\langle M, R\rangle$ be a reflexive frame, *i.e.*, for all $x \in M$, xRx.
  Then $\mathbf{M} \models \mathbf{T}$.
  ($\mathbf{T} = \Box\varphi \to \varphi$)
- Let $\langle M, R\rangle$ be a transitive frame, *i.e.*, for all $x, y, z \in M$, if xRy and yRz, then xRz.
  Then $\mathbf{M} \models \Box\Box\varphi \to \Box\varphi$.

Kripke semantics (3).

Theorem (Kripke).

1. $\mathbf{T} \vdash \varphi$ if and only if for all reflexive frames $\mathbf{M}$, we have $\mathbf{M} \models \varphi$.
2. $\mathbf{S4} \vdash \varphi$ if and only if for all reflexive and transitive frames $\mathbf{M}$, we have $\mathbf{M} \models \varphi$.
3. $\mathbf{S5} \vdash \varphi$ if and only if for all frames $\mathbf{M}$ with an equivalence relation R, we have $\mathbf{M} \models \varphi$.

More about this next week.