An introduction to model theory

Byunghan Kim

Yonsei University

Korea Logic Day
January 14, 2021

Outline

An introduction to model theory

Byunghan Kim

Yonsei University

Korea Logic Day
January 14, 2021

Kurt Gödel (1906-1978)

Axioms for PA (Peano Arithmetic):

1. $\forall x \;\; Sx \neq 0.$
2. $\forall x \forall y \;\; (Sx = Sy \to x = y).$
3. $\forall x \;\; x + 0 = x.$
4. $\forall x \forall y \;\; x + Sy = S(x + y).$
5. $\forall x \;\; x \cdot 0 = 0.$
6. $\forall x \forall y \;\; x \cdot Sy = x \cdot y + x.$
7. For any arithmetical property $P(x)$ on a variable x (more precisely any arithmetical formula $P(x)$ with a free variable x),

$$(P(0) \wedge \forall x(P(x) \to P(Sx)) \to \forall x P(x).$$

Gödel's 1st Incompleteness Theorem

PA (ZFC, resp.) is incomplete, i.e. there is an arithmetical (mathematical, resp.) sentence σ such that neither σ nor its negation $\neg\sigma$ is provable from PA (ZFC resp.).

Gödel's 1st Incompleteness Theorem

PA (ZFC, resp.) is incomplete, i.e. there is an arithmetical (mathematical, resp.) sentence σ *such that neither* σ *nor its negation* $\neg\sigma$ *is provable from PA (ZFC resp.).*

Gödel's 2nd Incompleteness Theorem

Con(PA) (Con(ZFC), resp.) is not provable from PA (ZFC resp.).

More generally

Gödel's 1st Incompleteness Theorem

Assume that a logical system

1. *is consistent;*
2. *has a recursive(=computable) set of axioms;*
3. *and it can express PA.*

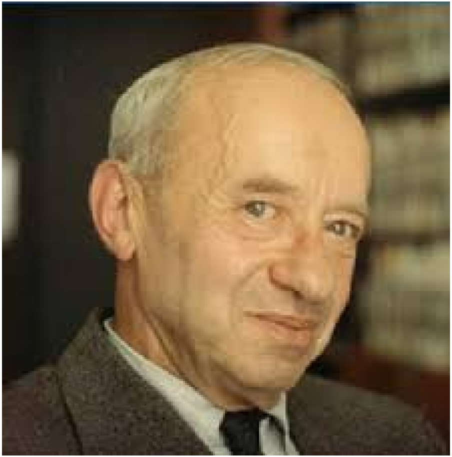
Then the system is incomplete.

Gödel's 2nd Incompleteness Theorem

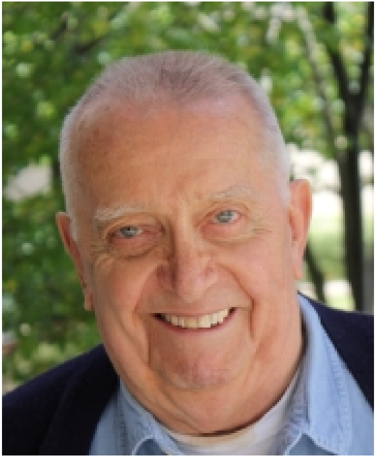
Under the same 3 assumptions above, the system can not prove its own consistency.

Gödel's Completeness Theorem

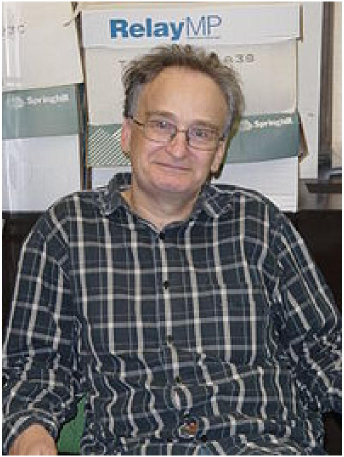
In a fixed logical system; a sentence σ is provable from some set Σ of sentences iff the sentence σ is true in every model of Σ.



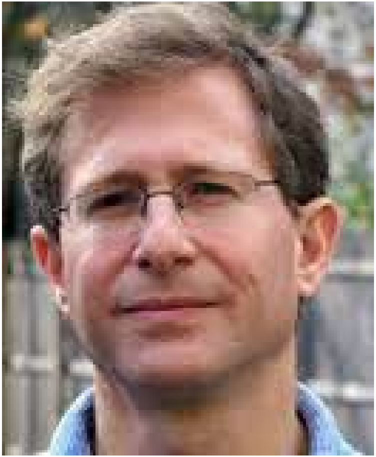
Alfred Tarski (1901-1983)



Michael D. Morley (1930-)



Saharon Shelah (1945-)



Ehud Hrushovski (1959-)

By a *model* (or a *structure*)

$$\mathcal{M} = (|\mathcal{M}|, (P_i)_{i\in I}, (f_j)_{j\in J}, (c_k)_{k\in K}),$$

we mean a non-empty set $|\mathcal{M}|$, called the *universe* of the model, equipped with

$$\begin{aligned} \text{predicates } & P_i \subseteq |\mathcal{M}|^{n_i}, \\ \text{operations } & f_j : |\mathcal{M}|^{n_j} \to |\mathcal{M}|, \text{and} \\ \text{constants } & c_k \in |\mathcal{M}|. \end{aligned}$$

In this talk, for simplicity, we assume $I \cup J \cup K$ is *countable* (can be empty).

Example

$\mathbb{N} = (\mathbb{N}, +, \times, S, 0)$: The structure of natural numbers
$\mathbb{Z} = (\mathbb{Z}, +, -, \times, 0)$: The structure of integers
$\mathbb{Q} = (\mathbb{Q}, +, -, \times, 0, 1)$: The field of rational numbers
$\mathbb{C} = (\mathbb{C}, +, -, \times, 0, 1)$: The field of complex numbers
$\mathbb{R}_{\text{ord}} = (\mathbb{R}, +, -, \times, <, 0, 1)$: The ordered field of real numbers
$G = (G, \cdot, e)$: a group
$G = (V, E)$: a graph

Fix a model $\mathcal{M} = (\mathcal{M}, (P_i)_{i \in I}, (f_j)_{j \in J}, (c_k)_{k \in K})$.
By a *formula* (of $\mathcal{M}$), we mean a finite sequence of symbols from

$$\{P_i, f_j, c_k\} \cup \{=, \forall, \exists, \neg, \to, \leftrightarrow, \wedge, \vee\} \cup \{x, y, z, ...\}$$

which can be interpreted as a mathematical proposition.

Example

- $P \to \forall xy \vee f$ is not a formula.
- $\sigma_k := \forall a_0 a_1 \cdots a_k (a_k \neq 0 \to \exists x (a_0 + a_1 x + \cdots + a_k x^k = 0))$ is a formula (of a field) saying that every polynomial equation of degree k has a root.

Example

- $\varphi_1(x, y) := \exists z(x - y = z^2)$ is a formula (of a field).
- $\varphi_2 := \forall xy \exists z(x - y = z^2)$ is a formula.

In φ_1, x, y are called *free* variables. We write a formula

$$\varphi = \varphi(x_1, ...x_n)$$

when free variables of φ are in $\{x_1, ..., x_n\}$, i.e. φ can be understood as a **proposition of the variables** $x_1, \ldots, x_n$.

Hence the truth or falsity of a formula $\varphi(x_1, ..., x_n)$ in $\mathcal{M}$ depends on the realization $(a_1, ..., a_n) \in \mathcal{M}$. For example,

$$\mathbb{R} \models \varphi_1(x, y)[3, 1], \text{ but } \mathbb{R} \not\models \varphi_1(1, 3) \text{ or } \mathbb{R} \models \neg\varphi_1(1, 3).$$

On the other hand,

$$\mathbb{Q} \not\models \varphi_1(x, y)[3, 1], \text{ but } \mathbb{Q} \models \varphi_1(x, y)[5, 1].$$

A *sentence* is a formula having no free variable. For example φ_2 and σ_k. Hence the truth or falsity of a *sentence* only depends on the model.
For example, for any $k \geq 1$.

$$\mathbb{R} \not\models \varphi_2, \sigma_{2k}, \quad \mathbb{R} \models \sigma_{2k-1}, \quad \mathbb{C} \models \varphi_2, \sigma_k$$

Note that in $\mathbb{R}_{\text{ord}}$, the formula $\varphi_1(x, y)$ is equivalent to another formula $y \leq x$. Similarly, a formula $\exists z(z^2 + xz + y = 0)$ saying the quadratic polynomial with coefficients x, y has a root is equivalent to another formula $4y \leq x^2$.

Definition

- $\mathrm{Th}(\mathcal{M}) = \{\sigma \mid \sigma \text{ is a sentence true in } \mathcal{M}\}$.
- $\mathcal{M} \equiv \mathcal{N}$ (elementarily equivalent) if $\mathrm{Th}(\mathcal{M}) = \mathrm{Th}(\mathcal{N})$ (a priori $\mathcal{L}(\mathcal{M}) = \mathcal{L}(\mathcal{N})$).
- Let $\Sigma = \{\sigma_i \mid i \in I\}$ be a set of sentences (in $\mathcal{L}$).
    - We say Σ is *satisfiable* if there is some model $\mathcal{M}$ such that all σ_i is true in $\mathcal{M}$.
    - Σ is *finitely satisfiable* if for each finite subset J of I, $\Sigma_J := \{\sigma_i \mid i \in J\}$ is satisfiable.

The most important consequences of Gödel's completeness theorem are:

Gödel's Compactness Theorem

Given a set Σ of sentences, it is finitely satisfiable iff it is satisfiable.

Theorem

(Löwenheim-Skolem) *For any infinite model $\mathcal{M}$, and any infinite cardinal κ, there is $\mathcal{M}_\kappa$ of cardinality κ such that $\mathcal{M}_\kappa \equiv \mathcal{M}$.*

Corollary

For $\mathbb{N}$ (or $\mathbb{Q}$, $\mathbb{R}$..), there is a non-standard one.

Notation

Give an infinite model $\mathcal{M}$ and an infinite cardinal κ, $I(\mathcal{M}, \kappa)$ is the number of non-isomorphic models $\mathcal{M}_\kappa$ of cardinality κ such that $\mathcal{M}_\kappa \equiv \mathcal{M}$.

Theorem

Morley's Categoricity Theorem *If $I(\mathcal{M}, \kappa) = 1$ for some uncountable κ, then for any uncountable cardinal κ', $I(\mathcal{M}, \kappa') = 1$.*

Example) For $\mathbb{C}$, given any uncountable κ, there is a unique field $F_\kappa \equiv \mathbb{C}$, which simply is an algebraically closed field of Char=0 of cardinality κ. (But there are *countably many* countable ones.)

- An **elliptic curve** over a field F is a curve defined by the polynomial equation $y^2 = x^3 + ax + b$ where we assume $a, b \in F$.
- A basic fact on elliptic curves is that one can geometrically associate the canonical abelian group structure E_{ab} on a given elliptic curve $y^2 = x^3 + ax + b$ $(a, b \in F)$. Mordell-Weil theorem says that if $F = \mathbb{Q}$ then every such group E_{ab} is finitely generated so that it is of the form $\mathbb{Z}^r \oplus G$ where r is some finite number (possibly 0) and G is some finite abelian group. r is said to be the **rank** of the elliptic curve.
- A question remains as to whether the ranks of elliptic $y^2 = x^3 + ax + b$ are bounded as a, b range over $\mathbb{Q}$.
- In Seoul ICM2014, Manjul Bhargava received Fields prize due to his work on that an average rank of elliptic curves over $\mathbb{Q}$ is bounded.

Theorem (Junguk Lee)

The following are equivalent.

- *Ranks of elliptic curves over* $\mathbb{Q}$ *are bounded.*
- *Some (any) uncountable model* $\widetilde{\mathbb{Q}}(\equiv \mathbb{Q})$ *satisfies the weak Mordell-Weil condition, that is, for any* E_{ab} $(a, b \in \widetilde{\mathbb{Q}})$ *and every* $m \geq 1$, E_{ab}/mE_{ab} *is finite.*

- Hilbert's 17th problem: If a polynomial $f(x_1, \ldots, x_n) \in \mathbb{R}[x_1, \ldots, x_n]$ is positive definite (i.e. $f(a_1, \ldots, a_n) \geq 0$ for any real a_i) then can f be a sum of squares of rational functions?
- James Ax's solution to Schanuel's conjecture for function fields: Given formal power series $f_1, \ldots, f_n \in t\mathbb{C}[[t]]$, if they are linearly independent over $\mathbb{Q}$, then

$$\text{tr.degree}_{\mathbb{C}(t)}(t, f_1, \ldots, f_n, e^{f_1}, \ldots, e^{f_n}) \geq n.$$

- Hardy's conjecture: the inverse of $(\log x)(\log\log x)$ is not asymptotic to a composition of exp, log and semialgebraic functions.
- A solution to Hilbert's 5th problem for local groups by I. Goldbring: Every locally Euclidean local group is locally isomorphic to a Lie group.

- Mordell-Lang conjecture by E. Hrushovski.
- Due to T. Scanlon using Hrushovki-Zilber dichotomy: abc conjecture for a certain case; Voloch's conjecture in number theory; and more.
- André-Oort conjecture by J. Pila using A. Wilkie's work on o-minimality.
- Hrushovski's work on approximate groups and its evolvement toward combinatorial regularity theory for groups and graphs.
- O-minimal GAGA and a conjecture of Griffiths.
- And many more .....

S. Shelah singled out (in 60-70s) a larger class of structures, called *stable*, properly containing that of uncountable categorical structures, which commonly shares the dimension property crucial in the proof of Morley's Theorem.

Definition

- $\mathcal{M}$ is *unstable* if there is $\varphi(x, y)$ and $a_i \in \mathcal{M}$ $(i = 1, 2, 3..)$ such that $\mathcal{M} \models \varphi(a_i, a_j)$ iff $i < j$.
- $\mathcal{M}$ is *stable* if it is not unstable.

uncountable categorical (ACF) $\subseteq$ superstable (DCF) $\subseteq$ stable (SCF). Ordered fields are unstable.

Definition

For $A, B, C \subseteq \mathcal{M}$, write $A \mathop{\smile\!\!\!\!\!\!|}_B C$ if $\mathrm{tp}(A/B \cup C)$ *does not fork* over A. (Never mind ! In ACF, algebraic independence; in VS, linear independence.)

Theorem

(Shelah, late 60s) *$\mathcal{M}$ stable. Then for $A, B, C, D \subseteq \mathcal{M}$,*

- (Symmetry) *$A \mathop{\smile\!\!\!\!\!\!|}_B C$ iff $C \mathop{\smile\!\!\!\!\!\!|}_B A$,*
- (Transitivity) *when $B \subseteq C \subseteq D$, we have $A \mathop{\smile\!\!\!\!\!\!|}_B C$ and $A \mathop{\smile\!\!\!\!\!\!|}_C D$ iff $A \mathop{\smile\!\!\!\!\!\!|}_B D$.*
- (Local Character) *if A is finite, then there is countable $B' \subseteq B$ such that $A \mathop{\smile\!\!\!\!\!\!|}_{B'} B$.*

Theorem

(B. Kim, late 90s): (Symmetry), (Transitivity) *and* (Local Character) *are equivalent, for* any $\mathcal{M}$.

Definition

- $\mathcal{M}$ *simple* if $\mathcal{M}$ has one of the equivalent conditions.
- $\mathcal{M}$ *supersimple* if for B, finite $A \subseteq \mathcal{M}$, there is *finite* $B' \subseteq B$ such that $A \mathop{\smile\!\!\!\!\!\!|}_{B'} B$.

$$\text{superstable} \quad \begin{array}{l} \subseteq \text{supersimple (PsF)} \\ \\ \subseteq \text{stable} \end{array} \quad \subseteq \text{simple (PAC)}$$

Theorem (K., Pillay)

- *If $\mathcal{M}$ is simple then it has 3-amalgamation.*
- *Moreover in any $\mathcal{M}$, suppose that there is a ternary relation among subsets of $\mathcal{M}$ satisfying basic independence properties, i.e., (Symmtery), (Transitivity), (Local Character), (Extension), (Finite character), (3-amalgamation). Then $\mathcal{M}$ is simple and the ternary relation is $\smile\!\!\!\!\!\!|\;\;$.*

Definition

For $A, B, C \subseteq \mathcal{M}$ write $A \mathop{\smile\!\!\!\!\!\!\mid}\nolimits_B^K C$ if $\mathrm{tp}(A/B \cup C)$ *does not Kim-fork over* A.

Fact

$A \mathop{\smile\!\!\!\!\!\!\mid}\nolimits_B C$ implies $A \mathop{\smile\!\!\!\!\!\!\mid}\nolimits_B^K C$.

Theorem

(K.) *If $\mathcal{M}$ is simple then $A \mathop{\smile\!\!\!\!\!\!\mid}\nolimits_B C$ iff $A \mathop{\smile\!\!\!\!\!\!\mid}\nolimits_B^K C$ for any $A, B, C \subseteq \mathcal{M}$.*

Fix stable or simple $\mathcal{M}$. Wlog assume $\mathcal{M}$ is saturated, has QE, EI, and $\mathrm{acl}(\emptyset) = \emptyset$. Fix a strong type p (i.e. an $\mathrm{Aut}(\mathcal{M})$-orbit) of $\mathcal{M}$. We let $\mathcal{C}$ denote the category of all small subsets of $\mathcal{M}$, where morphisms are embeddings.

If X is a family of sets, ordered by inclusion then we consider it to be a category with a single inclusion map $\iota_{u,v} : u \to v$ between any sets $u, v \in X$ with $u \subseteq v$. The set X is called *downward-closed* if whenever $u \subseteq v \in X$, then $u \in X$. For a downward closed X and a functor $f : X \to \mathcal{C}_B$ and $u \subseteq v \in X$, we write $f^u_v := f(\iota_{u,v})$ and $f^u_v(u) := f^u_v(f(u)) \subseteq f(v)$.

Definition

A *(closed independent) p-functor* is a functor $f : X \to \mathcal{C}_B$ such that:

1. For some finite $s \subseteq \omega$, X is a downward-closed subset of $\mathcal{P}(s)$;
2. $f(\emptyset) = \emptyset$; and for $i \in s$, $f(\{i\})$ (if it is defined) is of the form $\mathrm{acl}(b)$ where $b \in p$.
3. For all non-empty $u \in X$, we have that $f(u) = \mathrm{acl}(\bigcup_{i \in u} f_u^{\{i\}}(\{i\}))$ and the set $\{f_u^{\{i\}}(\{i\}) : i \in u\}$ is independent over $\emptyset$.

Definition

Let $n \geq 0$ be a natural number. An *n-simplex in p* is a p-functor $f : \mathcal{P}(s) \to \mathcal{C}$ for some set $s \subseteq \omega$ with $|s| = n + 1$. The set s is called the *support of f*, or $\text{supp}(f)$.

Let $\mathcal{S}_n(p)$ denote the collection of all n-simplices in p; and let $\mathcal{C}_n(p)$ denote the free abelian group generated by $\mathcal{S}_n(p)$; its elements are called *n-chains in p*. The *support of a chain c* is the union of the supports of all the simplices that appear in c with a nonzero coefficient.

Definition

Let $n \geq 1$ and $0 \leq i \leq n$. The *ith boundary operator* $\partial_n^i : \mathcal{C}_n(p) \to \mathcal{C}_{n-1}(p)$ is defined as follows: If $f \in \mathcal{S}_n(p)$ is an n-simplex with domain $\mathcal{P}(s)$, where $s = \{s_0 < \ldots < s_n\}$, then we define

$$\partial_n^i(f) := f \upharpoonright \mathcal{P}(s \setminus \{s_i\}).$$

The definition is extended linearly to all chains in $\mathcal{C}_n(p)$.
If $n \geq 1$ and $0 \leq i \leq n$, then the *boundary map* $\partial_n : \mathcal{C}_n(p) \to \mathcal{C}_{n-1}(p)$ is defined as

$$\partial_n(c) := \sum_{0 \leq i \leq n} (-1)^i \partial_n^i(c).$$

We write ∂^i and ∂ for ∂_n^i and ∂_n, respectively, if the n is clear from context.

Definition

The kernel of ∂_n is denoted by $\mathcal{Z}_n(p)$, and its elements are called *(n-)cycles*. The image of ∂_{n+1} in $\mathcal{C}_n(p)$ is denoted by $\mathcal{B}_n(p)$, and its elements are called *(n-)boundaries*.

It can be shown (by the usual combinatorial argument) that $\mathcal{B}_n(p) \subseteq \mathcal{Z}_n(p)$, or more briefly, "$\partial_n \circ \partial_{n+1} = 0$." Therefore we can define simplicial homology groups relative to p:

Definition

The *nth (simplicial) homology group of the type* $p \in S(B)$ is

$$H_n(p) = \mathcal{Z}_n(p)/\mathcal{B}_n(p).$$

Definition

Let $n \geq 1$.
We say p has *n-amalgamation* (or *n-existence*) if for any p-functor $f : \mathcal{P}^{-}(n)(:= \mathcal{P}(n) \setminus \{n\}) \to \mathcal{C}$, there is an $(n-1)$-simplex g in p such that $g \supseteq f$.

(Indeed we need to consider p-functor over any set.)

For a tuple c, we write $\overline{c} := \mathrm{acl}(c)$; and for sets A, C, $\mathrm{Aut}(A/C)$ denotes the group of $A \cup C$-permuting embeddings fixing C pointwise.

Fix independent $c_1, \ldots, c_{n+1} \in p$. We let

$$\widetilde{c_1 \ldots c_n} := \overline{c_1 \ldots c_n} \cap \mathrm{dcl}(\bigcup_{i=1}^{n} \overline{c_1 \ldots \hat{c}_i \ldots c_{n+1}});$$

and let

$$\partial(c_1 \ldots c_n) := \mathrm{dcl}(\bigcup_{i=1}^{n} \overline{c_1 \ldots \hat{c}_i \ldots c_n}).$$

We also put

$$\Gamma_n(p) := \mathrm{Aut}(\widetilde{c_1 \ldots c_n} / \partial(c_1 \ldots c_n)).$$

Hurewicz Correspondences

(J. Goodrick, K., A. Kolesnikov) *Assume $\mathcal{M}$ is stable, and p has $(\leq n+1)$-amalgamation. Then*

$$H_n(p) = \Gamma_n(p),$$

which is always a profinite abelian group.

For a proof we need to generalize the notion of groupoids.

Definition

If $n \geq 2$, an *n-ary polygroupoid* is a structure $\mathcal{H} = (I, P_2, \ldots, P_{n-1}, P, Q)$ with n disjoint sorts $I = P_1, P_2, \ldots, P_n = P$ equipped with an $(n+1)$-ary relation $Q \subseteq P^{n+1}$ and a system of maps $\langle \pi^k : 2 \leq k \leq n \rangle$ satisfying the following axioms:

1. For each $k \in \{2, \ldots, n\}$, the function π^k maps an element $u \in P_k$ to a compatible k-tuple $(\pi^k_1(u), \ldots, \pi^k_k(u)) \in (P_{k-1})^k$.
2. If $Q(u_1, \ldots, u_{n+1})$ holds, then $(u_1, \ldots, u_{n+1})$ is a compatible $(n+1)$-tuple of elements of P.
3. Whenever $Q(u_1, \ldots, u_{n+1})$ holds, then for any $i \in \{1, \ldots, n+1\}$, u_i is the unique element x in P such that $Q(u_1, \ldots, u_{i-1}, x, u_{i+1}, \ldots, u_{n+1})$ holds.
4. The Q-relation is associative.

Fact

(Shelah) $\mathcal{M}$ *is simple iff it does not have the* tree property.

Definition

$\mathcal{M}$ is NSOP_1 if it does not have SOP_1 *tree property*.

SOP_1 tree property implies the tree property. Hence if $\mathcal{M}$ is simple then $\mathcal{M}$ is NSOP_1.

Stable	Simple	$NSOP_1$
Infinite set	The random graph	The paramet. equi. rel.s
ACF	Bounded PAC fields	ω-free PAC fields
$V =$ vector sapce	$(V, \langle , \rangle)$ / a finite F	$(V, \langle , \rangle)$ / an ACF

Question

(K., 2009) If $\mathcal{M}$ is $NSOP_1$ then whether $\mathop{\smile\!\!\!\!\!\!|}\,^K$ (with some naivety) supplies a well-behaving independence notion.

The question is corrected and positively answered over submodels by Kaplan and Ramsey ($\mathop{\smile\!\!\!\!\!\!\mid}^K$ is named Kim-independence by them).

- I. Kaplan and N. Ramsey, "On Kim-independence," Journal of European Math. Soc. (2020) 1423–1474.

Later the result is extended to all NSOP_1 $\mathcal{M}$ with existence.

- J. Dobrowolski, B. Kim, and N. Ramsey, "Independence over arbitrary sets in NSOP_1 theories," preprint.

Then recently further studies on NSOP_1 structures are being produced by many other model theory researchers.

Consequently, the maximal solution to Lachlan's problem is obtained.

- B. Kim, "On the number of countable models of a countable NSOP_1 theory without weight ω," J. of Symbolic Logic, 84 (2019) 1168-1175.