Title: Minimally Interesting

Abstract: The vagueness of the phrase "simplest possible" is shown through the sometimes coinciding sometimes wildly diverging notions of *prime model*, a model which can be embedded inside any other model of a given theory, and a *minimal model*, a model which does not contain any submodels of a given theory. Hijinks ensue. The highlight will be the exhibition of a theory with no prime model and $2^{\aleph_0}$ minimal models along with a proof of this fact due to Baldwin, Blass, Glass, and Kueker.

This talk is about simple structures. By simple I mean "least complicated"; nothing in this talk will refer to normal subgroups. There are two notions which one can use to define a simple model. One way says a simple model contains only the bare minimum to satisfy the given theory. The other says a simple model does not contain any proper submodels. Of course, since model theory mainly deals with infinite models, this is a slippery requirement since the very definition of an infinite set is that there can be an injective but not surjective map from that set into itself.

Since this is a logic talk, let me begin with the obligatory run-down of concepts and terminology. Like last time lets begin groups. Everyone knows what a group is: a set G with a binary operation $\times$ and a distinguished element e such that the following rules are satisfied:

1. For all $a, b, c \in G$, $a \times (b \times c) = (a \times b) \times c$.
2. For all $a \in G$, $a \times e = e \times a = a$.
3. For all $a \in G$ there is an element $b \in G$ such that $a \times b = b \times a = e$.

And that is all a group is.

Usually we just write that G is a group, but sometimes we write $(G, \times)$ or $(G, \times, e)$. Notice that there are two parts to defining a group: we first require a set, a binary function and a distinguished element. We then require that these things satisfy certain rules.

Moreover, maps between groups are defined so that they respect the operation. That is if G and H are groups and $f : G \to H$ is a function then we require for all $a, b \in G$ that $f(a \times^G b) = f(a) \times^H f(b)$. One also requires that the identity elements are mapped to each other, $f(e^G) = e^H$. In this case of groups one can prove that from the second condition follows necessarily from the first, but since we are aiming to generalize this idea we keep it in.

In a similar manner we can define ordered groups, rings, fields, posets, and vector spaces and the maps between them, etc.

Model theory was characterized by Chang and Keisler as "Universal algebra + Logic" in 1973. (Nowadays it is more like "algebraic geometry + logic".) A lot of the notions of of models is lifted almost directly from algebra with suitable generalizations.

We begin with a *language*, which is a collection of symbols for constants, relations, and functions. Given an language L we define an L-structure to be a set along with constants, functions and relations on this set to interpret the symbols in the language—much like a group begins with a set and a binary operation.

For a set and a binary operation to be a group it must also satisfy some rules. Instead a a fixed list of rules we will allow any collection of rules, calling a collection *consistent* if there is a model which can satisfy all of them. Such collections are called *theories* and they are simply a set of L-sentences. (An L-sentence is a formula with no free variables.)

For example with groups we have the language $L = \{e, \cdot\}$ with e a constant, $\cdot$ a binary function. We would then define the theory T_{Group} using the axioms listed earlier.

Given a model A and a sentence φ we can ask whether φ is satisfied in A. If so we write $A \models \varphi$.

Notice both $\mathbb{Z}$ and S_3 are models in the theory of groups but they are not both models of the sentence $\sigma \doteq \forall xy\,[x \cdot y = y \cdot x]$ giving the abelian condition. Using our notation $\mathbb{Z} \models \sigma$ and $S_3 \not\models \sigma$. If a theory allows this kind of ambiguity then we say it is *incomplete*. (n.b. there is a result by Gödel saying "the first-order axioms of arithmetic are incomplete"). The converse of an incomplete theory is, naturally, a *complete* theory. This means the truth of every first order sentence is determined by the theory. An easy way to get a complete theory is to construct a model and then put every first order sentence true of the model into the theory. In fact, this is so convenient there is notation for it: given a structure A notate and define the *theory of* A as $Th(A) = \{\sigma : \sigma \text{ is an } L\text{-sentence and } A \models \sigma\}$.

The idea of two structures satisfying the same first order sentences is very nice, and it also gives an equivalence relation called *elementary equivalence*. Write A is elementary equivalent to B by $A \equiv B$. We already have some intuitive idea of this. It can be shown that the theory of Algebraically closed fields is complete, up to the characteristic of the field. Thus, since both $\mathbb{Q}^{\text{alg}}$, the algebraic completion of the rationals, and $\mathbb{C}$ are models of this theory and have characteristic 0 they are elementary equivalent: $\mathbb{Q}^{\text{alg}} \equiv \mathbb{C}$. But they are certainly not isomorphic. For starters $\pi \notin \mathbb{Q}^{\text{alg}}$.

Lets consider the theory $Th(\mathbb{Z}, +)$. It contains the basic abelian group statements. It also says that it is torsion free: for each $n \in \mathbb{N}$ there is a formula $\forall x\,[(x + x = x) \vee (x + x + \cdots + x \neq x)]$. It seems like we can't say much with this limited language, but more can be expressed than one would think at first.

For example, $\mathbb{Q}$ is not a model of this theory. Consider the sentence $\exists x\,[x \neq 0 \wedge \forall y\,[y + y \neq x]]$ which says there is an element that is not divisible by 2. Clearly this sentence is true in $\mathbb{Z}$, but it is not true in $\mathbb{Q}$ since for any element $a \in \mathbb{Q}$ we know $\frac{a}{2} + \frac{a}{2} = a$.

For another example, $\mathbb{Z} \times \mathbb{Z}$ is not a model of this theory by considering the sentence $\exists xy \forall wvz\,[w + w \neq x \wedge v + v \neq y \wedge z + z \neq x + y]$ This is not satisfied in $\mathbb{Z}$ since it says the sum of two odd numbers is odd. But it is satisfied in $\mathbb{Z} \times \mathbb{Z}$ by taking x and y to be the two generating elements $(1, 0)$ and $(0, 1)$.

But this talk is about simple structures. That is, even though two structures may satisfy be elementary equivalent they could still be non-isomorphic. So, given a complete theory, can we find a "simplest" possible structure?

But first, we need to pin down what we mean by "simplest". One idea is that a simple structure should only contain the kinds of elements that absolutely must contain and none of the optional elements. (e.g. $\mathbb{C}$ is not simple since it contains many more transcendental elements than necessary to be an algebraically closed field.) How do we know which elements are necessary? Simple! A model is simple if it can be embedded into any other model of the theory. If this is the case, the structure is called a *prime model* of the theory T.

Even though you understood what I mean by *embedding*, let me quickly define it. The definition is lifted almost exactly from group theory and is exactly what one would expect. Given two L-structures A, B then we define an L-embedding from one to the other as a function $\phi : A \to B$ which preserves the interpretation of the constants, functions and relations. To wit:

1. $\phi(c^A) = c^B$, for each constant $c \in L$
2. $\phi(f^A(a_1, \ldots, a_{n_f})) = f^B(\phi(a_1), \ldots, \phi(a_{n_f}))$ for each function $f \in L$
3. $(a_1, \ldots, a_{m_R}) \in R^A$ if and only if $(\phi(a_1), \ldots, \phi(a_{m_R})) \in R^B$ for each relation symbol $R \in L$

Notice that every L-embedding is injective since for any $a, b \in A$ and L-embedding $\phi : A \to B$ if we have $B \models \phi(a) = \phi(b)$ then $A \models a = b$. (There is a notion of an L-homomorphism which doesn't require this, but we not interested in it since what we are really concerned with is the preservation of formulas.)

And then since we care about the preservation of the truth of formulas we also require a map $\pi : A \to B$ such that for every formula ψ and tuple $a \in A$ we have $A \models \psi(a)$ if and only if $B \models \psi(\pi(a))$ is an elementary embedding. It is called an embedding since the map π must necessarily be injective. If A is a substructure of B and the inclusion map is an elementary embedding then we say A is an elementary-substructure of B and write $A \prec B$

And so what we really meant to say is that a *prime model of a theory T* is a model which elementary embeds into any other model of that theory. (Since it will come up again later define an *algebraically prime model* to be a model which merely embeds into any other model of T).

Another way of defining a "simple" model is as one for which no proper subset is a model of the theory. (A *minimal model* of a theory T is a model $A \models T$ such that for any proper substructure $B \subset A$ is not a model of the theory, i.e. $B \not\models T$.)

What about the relationship between prime models and minimal models? Clearly if a theory has both a prime model and a minimal model then they must coincide. Believe it or not, but this is about the best result we have in general.

An example of a prime model and a minimal model coinciding is with algebraically closed fields.

An example of a theory with a prime model but no minimal models is the theory of "dense linear orders without endpoints", i.e. $Th(\mathbb{Q}, <)$. In this theory the model $\mathbb{Q}$ is prime since it is a countable dense linear order, but it is not minimal since there is a proper subset of it which is also a dense linear order, say $\{\frac{a}{2^b} : b \geq 0\}$.

I will present a proof giving the opposite: a theory with no prime models and $2^{\aleph_0}$ minimal models.

First a lemma. It allows us to deduce elementary equivalence of a given group and $\mathbb{Z}$ from some relatively strong group theoretic conditions.

Lemma. *If A is a torsion-free abelian group and $A/pA \cong \mathbb{Z}/p\mathbb{Z}$ for each prime p then $A \equiv \mathbb{Z}$.*

Proof. ...I don't have a proof of this. □

We need one other lemma for us to tell when a subgroup of an abelian group is also an elementary sub-model. The following definition gives a closure condition on subgroups saying the divisibility of elements does not change between the larger group and the subgroup.

Definition. *A is a* pure subgroup *of B if for each $a \in A$ and integer n the formula $nx = a$ has a solution in B if and only if it has a solution in A.*

Lemma. *If A and B are abelian groups and A is a pure subgroup of B then $A \equiv B$ implies $A \prec B$*

Proof. ...once again, no proof. □

Our main results concern the following cleverly constructed structure.

Define $Z_{(p)} = \{\frac{a}{b} \in \mathbb{Q} : p \nmid b\}$. The commutative algebraists may recognize this as a kind of localization of $\mathbb{Z}$ at (p), only we are still thinking of it as a group, not a ring. Also, for each prime p we have $p\mathbb{Z}_{(p)} \cong \mathbb{Z}/p\mathbb{Z}$ and $p\mathbb{Z}_{(q)} = \mathbb{Z}_{(q)}$ if q is a prime different from p. Now let $W = \bigoplus_p Z_{(p)}$. Observe that W is abelian and torsion-free. By these observations $W/pW \cong \mathbb{Z}/p\mathbb{Z}$ for each prime p, and so $W \equiv \mathbb{Z}$.

Lets see if those formulas from earlier are satisfied in W. We had $\exists x\, [x \neq 0 \wedge \forall y\, [y + y \neq x]]$ saying there is an element which is not divisible by 2. This is satisfied in W by the element $(1, 0, 0, \ldots)$. This element being divisible by 2 would require the existence of the element $(\frac{1}{2}, 0, 0, 0, \ldots)$, an element which doesn't exist since $\frac{1}{2} \notin Z_{(2)}$.

The other sentence from before is $\not\exists xy \forall wvz\, [w + w \neq x \wedge v + v \neq y \wedge z + z \neq x + y]$ saying there are not two "odd" elements whose sum is also "odd". It is always harder to show certain elements don't exist. Suppose $x = (x_2, x_3, x_5, \ldots)$ and $y = (y_2, y_3, y_5, \ldots)$. Then $x + y = (x_2 + y_2, x_3 + y_3, \ldots)$. Each component except the first can be divided by 2. The first component is then the sum of two odd numbers, meaning it can also be divided by 2. So this formula does not hold in W.

The theorem I want to present is due to Baldwin, Blass, Glass, and Kueker (1972).

Theorem. *Let T be the additive theory of the integers.*

1. *T has a minimal and algebraically prime model (namely $\mathbb{Z}$) which is not a prime model. Hence T has no prime model.*

2. *T has a model (namely $\bigoplus_p \mathbb{Z}_p$) with no minimal elementary submodels.*

3. *T has $2^{\aleph_0}$ minimal models.*

Proof. 1. $\mathbb{Z}$ has no proper elementary submodels so it is a minimal model of T. In particular, $n\mathbb{Z}$ is not a submodel since the inclusion is map is not elementary: $\mathbb{Z} \models \exists x[x + x + \cdots + x = n]$ and $n\mathbb{Z} \not\models \exists x[x + \cdots + x = n]$.

   By previous theorem $\bigoplus_p Z_{(p)} \models T$. However $\mathbb{Z}$ cannot be embedded as an elementary submodel of $\bigoplus_p Z_{(p)}$ since in $\mathbb{Z}$ 1 is not divisible by any prime but each non-zeno member of $\bigoplus_p Z_{(p)}$ is divisible by infinitely many primes.

2. Not shown.

3. To construct $2^{\aleph_0}$ minimal models begin with a function σ from the primes into the positive integers. Define

$$\mathbb{Q}_\sigma = \left\{ \frac{m}{n} : m, n \in \mathbb{Z}, \quad n \neq 0, \quad \text{and for all primes } p, \quad p^{\sigma(p)} \nmid n \right\}$$

   This is a subgroup of the rationals. Show $\mathbb{Q}_\sigma \equiv \mathbb{Z}$ using our test. To this end let $x = \frac{m}{np^k} \in \mathbb{Q}_\sigma$ be an arbitrary element represented with $\gcd(n, p) = 1$ and $0 \leq k < \sigma(p)$. Since n and p are relatively prime n has a multiplicative inverse modulo p. Let n' be this inverse and let $m' = n'm$. Then $x - \frac{m'}{p^k} = \frac{m - m'n}{np^k} = \frac{p\alpha}{np^k} \in p\mathbb{Q}_\sigma$. Thus $x \equiv \frac{m'}{p^k} \pmod{p\mathbb{Q}_\sigma}$. If $k \neq \sigma(p) - 1$ then $\frac{m}{p^k} \in p\mathbb{Q}_\sigma$ since $\frac{m}{p^k} = p\frac{m}{p^{k+1}}$. This means the map $\mathbb{Z} \to \mathbb{Q}_\sigma/p\mathbb{Q}_\sigma$ given by $m \mapsto \frac{m}{p^{\sigma(p)-1}}$ is surjective and since it has kernel $p\mathbb{Z}$ the first isomorphism theorem tells us $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Q}_\sigma/\mathbb{Q}_\sigma$. Therefore $\mathbb{Q}_\sigma/p\mathbb{Q}_\sigma \cong \mathbb{Z}/p\mathbb{Z}$ and the lemma concludes $\mathbb{Q}_\sigma \equiv \mathbb{Z}$.

   $\mathbb{Q}_\sigma$ is minimal since it has no pure subgroup A If $\frac{m}{n} \in A$ is a non-zero element and $\gcd(m, n) = 1$ then $\frac{1}{n} \in \mathbb{Q}_\sigma$ and since A is pure $\frac{1}{n} \in A$. If $1 \in A$ then so is everything dividing 1 thus $A = \mathbb{Q}_\sigma$.

   Therefore $\mathbb{Q}_\sigma$ is a minimal model.

   Suppose τ is another map from the primes into the positive integers and $f : \mathbb{Q}_\sigma \cong \mathbb{Q}_\tau$. For each prime p the value $\sigma(p) - 1$ is the largest power of p which divides 1 in $\mathbb{Q}_\sigma$. Thus $\sigma(p) - 1$ is the largest power of p which divides $f(1)$ in $\mathbb{Q}_\tau$. (Keep in mind that by "divides" it is meant $\exists y\, [y + y + \cdots + y = x]$). This means $f(1) = yp^{\sigma(p)-1}$ for some $y \in \mathbb{Q}_\tau$. But y, being in $\mathbb{Q}_\tau$ can be written as $\frac{a}{b}\frac{1}{p^{\tau(p)-1}}$ with $\gcd(b, p) = 1$. If $\gcd(a, p) \neq 1$ then y can be written as $y = py'$ for some y'. Then we have $f(1) = yp^{\sigma(p)-1} = py'p^{\sigma(p)-1} = y'p^{\sigma(p)}$. But the maximum power of p that divides $f(1)$ is $\sigma(p) - 1$. Thus $\gcd(a, p) = 1$ and so we can write $f(1) = \alpha p^{\sigma(p)-\tau(p)}$ with $\gcd(\alpha, p) = 1$. If τ and σ disagree on more than a finite number of primes than $f(1)$ would have an infinite prime factorization. Thus σ and τ only disagree on a finite number of primes. This means only a countable number of maps from the primes to the positive natural numbers can give a structure isomorphic to $\mathbb{Q}_\sigma$. Since there are $\aleph_0^{\aleph_0} = 2^{\aleph_0}$ possible maps there are $2^{\aleph_0}$ non-isomorphic $\mathbb{Q}_\sigma$'s.

□

After seeing this proof and the chaos associated with the theory of $(\mathbb{Z}, +)$ consider the theory of $(\mathbb{Z}, +, 1)$. Observe that while the element 0 was definable in $(\mathbb{Z}, +)$, using the formula $x + x = x$, the element 1 wasn't. In fact, the very property of 1, that no other element divides it, cannot be expressed in a single formula. It requires an infinite number of formulas, and the lack of a first order formula is what causes the large number of minimal models. By adding the constant 1 to the language the non-dividability of 1 can be rolled into the base theory, and so any model of $(\mathbb{Z}, +, 1)$ must contain an element 1^M for which no other element divides. This means any model of $(\mathbb{Z}, +, 1)$ must contain a copy of $\mathbb{Z}$, and moreover it can be shown to be an elementary embedding. Thus $\mathbb{Z}$ is a prime model of $(\mathbb{Z}, +, 1)$. Also, since $\mathbb{Z}$ does not contain any submodels, it is also a minimal model.

Here is another theory which does not have a prime model. Consider the language $L = \{P_i : i < \omega\}$ with each P_i a unary predicate symbol. Consider finite sequences of 0's and 1's. (That is $2^{<\omega}$). If $\sigma \in 2^{<\omega}$ write P_σ as shorthand for $\bigwedge P_i^{\sigma(i)} x$ with $P_i^0 x := \neg P_i x$ and $P_i^1 := P_i x$. Let the theory say that there is an element satisfying P_σ for each $\sigma \in 2^{<\omega}$. Since this is a countable language there are theorems saying there is a model of countable cardinality. But a countable model cannot contain enough elements to realize every possible infinite sequence 2^ω.