MATH 141A: COMPUTABILITY AND ARITHMETIC

SEBASTIEN VASEY

In these notes, we investigate some consequences of the completeness and compactness theorem to computability and models of arithmetic. We have observed that one advantage of working syntactically rather than semantically is that there are algorithms to check proofs. Let's make this precise:

Definition 1. Fix a countable signature σ. A set A of formulas in the language of σ is *decidable* if there is a computer program that, given as input a formula ϕ will output yes or no depending on whether $\phi \in A$.

Note that we are not making precise here what a computer program is (one possible definition is the notion of a Turing machine, that you may encounter in a class such as CS-121). Also, there are no requirements on how fast the computer program should be. All that is asked is that in a finite time (that may depend on ϕ) it will terminate and output yes or no. Finally, we are assuming that the computer program has some way to read ϕ, i.e. that ϕ is coded in some way as a string of 0 and 1's. For example, one could represent the ith constant symbol by a pair $\langle 0, i \rangle$, the ith function symbol by a pair $\langle 1, i \rangle$, etc. Then further fix a way to code $\langle a, b \rangle$ into a single string of 0 and 1's. All of this can be done. In the rest of these notes, σ denotes a *countable* signature.

For example, any finite set is decidable (one can just hardcode the formulas in the program). Thus the axioms of non-empty dense chains without endpoints are decidable. On the other hand, there are uncountably-many sets of formulas, but only countably-many computer programs (say if we think of them as finite strings of zeroes and ones), so in fact "most" sets will not be decidable. Still, almost all of the sets of axioms that one would write down explicitly in practice are decidable (even if they are infinite): for example the axioms of generic graphs, or of infinite sets are decidable.

We will often be interested in whether the set of *consequences* of the axioms are decidable. This will enable us to figure out, for example, whether a specific sentence ϕ is true of any non-empty dense chain without endpoints. For this, it will be helpful to know that we can check proofs using computers:

Remark 2. Given a decidable set A, there is a computer program that takes as input a sequence $\phi_1, \ldots, \phi_n$ of formulas and outputs yes or no depending on whether $\phi_1, \ldots, \phi_n$ is a formal proof of ϕ_n from A.

Proof. For each $i \leq n$, the program checks whether $\phi_i \in A$ (this can be done because A is assumed to be decidable), whether for some $j, k < i$ ϕ_i the formula ϕ_k is $\phi_j \to \phi_k$ (this is easy to do), or whether ϕ_i is a logical axiom. The latter can also be done, because the set of all logical axioms is decidable: just check whether the formula given as input is of one of the types. For example, to check a formula is a propositional tautology, one just enumerates its basic subformulas (there are only finitely-many) and check for all truth assignment of these basic formulas whether the corresponding assignment evaluates to 1 on the input formula. □

Let us now recall some definitions: a sentence ϕ is a *consequence* of a set of sentences A (written $A \models \phi$) if any model of A is a model of ϕ. We write $\mathrm{Th}(A)$ (the *theory of* A) for the set $\{\phi \mid A \models \phi\}$. For a model M, we write $\mathrm{Th}(M)$ for $\{\phi \mid M \models \phi\}$. A *theory* is a set of sentences A that is consistent and is closed under consequences (i.e. $A \models \phi$ implies $\phi \in A$). A theory T is *complete* if for any sentence ϕ, $\phi \in T$ or $\neg\phi \in T$. A consistent set A of sentences is *complete* if $\mathrm{Th}(A)$ is complete.

In general, for a σ-structure M, $\mathrm{Th}(M)$ is always a complete theory, and if $M \models A$, then $\mathrm{Th}(A) \subseteq \mathrm{Th}(M)$, with equality if and only if A is itself complete. These statements follow quickly from the definitions, you should be able to give the proofs.

The following gives a criteria for when the set of consequences is decidable:

Theorem 3. If A is decidable and complete, then $\mathrm{Th}(A)$ is decidable.

Proof. We use that (by the completeness theorem), ϕ is a consequence of A if and only if $A \vdash \phi$. So given a sentence ϕ as input, the program enumerates all the possible sequences $\bar{\psi}^0 = (\psi_i^0)_{i \le n^0}, \bar{\psi}^1 = (\psi_i^1)_{i \le n^1}$, ... of sentences (there are only countably many). For each j, the program checks whether $\bar{\psi}^j$ is a formal proof of ϕ from A (this is possible by Remark 2, we are using that A is decidable). If it is, then output "yes". If it is not, check whether $\bar{\psi}^j$ is a formal proof of $\neg\phi$ from A. If it is, output "no". The program will terminate: since A is complete, we know that either $\phi \in \mathrm{Th}(A)$ or $\neg\phi \in \mathrm{Th}(A)$. By the completeness theorem, this means that either $A \vdash \phi$ or $A \vdash \neg\phi$. Since we are going through *all* possible sequences of sentences, we must eventually hit on one witnessing that $A \vdash \phi$ or $A \vdash \neg\phi$. □

This simple proof has several interesting consequences:

- We have shown (using the back and forth method) that the set A of axioms of non-empty dense chains without endpoints is complete. Since A is finite, it is also decidable. Therefore by the theorem, $\mathrm{Th}(A)$ is decidable. In words, the theory of non-empty dense chains without endpoints is decidable. In particular, there is an algorithm that takes as input a sentence ϕ and outputs yes or no depending on whether $(\mathbb{Q}, <) \models \phi$. In the assignments, you saw another (more constructive) algorithm that proceeded by removing the quantifiers from ϕ.
- The theory of non-empty discrete chains without endpoints is decidable (it is complete by 1.8 in Poizat). Thus there is for example an algorithm to decide whether a formula holds of $(\mathbb{Z}, <)$.
- The theory of generic graphs is also decidable (you proved in assignment 4 that it was complete).
- We will see later in the class that $T = \mathrm{Th}((\mathbb{C}, +, \cdot, 0, 1))$ can be axiomatized by a complete and decidable set, and hence is decidable by the theorem. The theory T is called the *theory of algebraically closed fields of characteristic zero.*

- We may also see later in the class that $T = \mathrm{Th}((\mathbb{R}, +, \cdot, 0, 1))$ is axiomatized by a complete and decidable set. The theory T is called the *theory of real closed fields.*

Of course, the fact that there is an algorithm may not necessarily mean that there is a *fast* algorithm. Even for the simple case of non-empty dense chains without endpoints, the best algorithm has (in the worst case) double exponential complexity (if the input formula has n symbols, the program will take approximately 2^{2^n} steps before returning an answer). Figuring out algorithms that will run fast in "practice" (while maybe still being inefficient in the worst case) is an active research area in computer science.

We have looked at $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ and $\mathbb{Z}$ (with varying operations). What about $\mathbb{N}$? Specifically, what about $(\mathbb{N}, +, \cdot, 0, 1)$? Here is one attempt to axiomatize it:

Definition 4. *Peano's arithmetic* (PA) is the following set of axioms, in the signature $\{+, \cdot, 0, 1\}$ (where $+$ and $\cdot$ are binary function symbols and 0, 1 are constant symbols):

- $(\forall x \forall y)(x + y = y + x \wedge x \cdot y = y \cdot x)$ [Addition and multiplication are commutative]
- $(\forall x)(x + 1 \neq 0)$ [Zero is not the sucessor of any natural number]
- $(\forall x \forall y)(x + 1 = y + 1 \rightarrow x = y)$ [The successor function is injective]
- $(\forall x)(x + 0 = x)$ [Zero is the additive identity]
- $(\forall x)(x \cdot 0 = 0)$ [Zero times anything is zero]
- $(\forall x \forall y)(x + y) + 1 = x + (y + 1)$ [Relationship between addition and the successor operation]
- $(\forall x \forall y)(x \cdot (y + 1)) = (x \cdot y) + x$ [Relationship between multiplication and the successor operation]
- For any formula $\phi(x)$,
$$(\phi(0) \wedge (\forall x)(\phi(x) \rightarrow \phi(x + 1))) \rightarrow (\forall x)\phi(x)$$
This is the induction axiom schema (it really is a set of axioms, one for each formula ϕ).

Exercise 5. Using the induction axiom schema, show that PA $\models (\forall x)\,(x = 0 \vee (\exists y)(x = y + 1))$.

It is easily seen that $(\mathbb{N}, +, \cdot, 0, 1) \models$ PA. What do the other models of PA look like? Let $M \models$ PA. Then $(\mathbb{N}, +, \cdot, 0, 1)$ is isomorphic to a substructure of M (the one induced by sums of 1's). So by some renaming we can assume without loss of generality that $\mathbb{N}$ is already a substructure of M. If $M \neq \mathbb{N}$, M has other numbers than sums of ones (called "nonstandard numbers") that sit above all the regular natural numbers. More precisely, we can define an ordering $<$ on M by $a < b$ if and only if there exists $x \in M$ such that $b = a + x$ (note that this is a definable subset of M^2). This coincides with the usual orderings on the natural numbers. Also, it follows from the axioms of PA that 0 is minimal in that ordering (exercise!). In fact it can be shown (see the extra credit problem of assignment 7) that $(\mathrm{univ}(M), <)$ is isomorphic to $(\mathbb{N}, <) + \mathbb{Z} \times D$, where D is a dense chain without endpoints! The structure of nonstandard models of PA is very mysterious, yet they satisfy all the consequences of PA (for example, $M \models (\forall x \exists y) x = (1 + 1) \cdot y \vee x = (1 + 1) \cdot y + 1$: every nonstandard number is either even or odd).

While the orderings of each countable nonstandard models of PA are all isomorphic (why?), once we add the extra structure we get a lot of different models. Note first that a nonstandard model is not isomorphic to $(\mathbb{N}, +, \cdot, 0, 1)$, so PA has at least two non-isomorphic countable models. In fact:

Theorem 6. PA has $2^{\aleph_0}$ non-isomorphic countable models.

Proof. First, PA (or really any set of axiom in a countable signature) has at most $2^{\aleph_0}$ non-isomorphic countable models (exercise!). We show that PA has at least $2^{\aleph_0}$-many. First, add a constant symbol c to the signature of PA. Call the resulting signature σ'. For each set of (standard!) primes P, build (as in assignment 6) a countable model M_P of PA such that (M_P, a_P) satisfies the sentence saying that c is divisible by a prime p if and only if $p \in P$. Clearly, for $P_1 \neq P_2$, the expanded σ'-structure (M_{P_1}, a_{P_1}) is not isomorphic to (M_{P_2}, a_{P_2}): in fact they do not even satisfy the same sentences. Since there are $2^{\aleph_0}$-many sets of primes, that tells us that there are $2^{\aleph_0}$ countable σ'-structures that are models of PA. Still, that may not tell us that M_{P_1} (without the interpretation of the constant symbol) is not isomorphic to M_{P_2} (because an isomorphism may send a^{M_1} elsewhere than to a^{M_2}). Instead, we will do a little bit of (infinite) counting.

For each set P of primes, let $\mathcal{F}_P$ denote the collection of all sets of primes Q such that M_P has an element divisible exactly by the primes in Q. For example, $P \in \mathcal{F}_P$, but $\mathcal{F}_P$ will contain more elements (for example it will contain all finite sets of primes). Still, $\mathcal{F}_P$ is a countable set, because M_P has only countably-many elements, and two elements with a distinct set of prime divisors must be different. We now build sets of primes $(P_\alpha)_{\alpha < 2^{\aleph_0}}$ by transfinite induction on α as follows:

- For $\alpha = 0$, take any set of primes. For example $P_0 = \emptyset$.
- Given any other $\beta > 0$ and $(P_\alpha)_{\alpha < \beta}$, we know that $\mathcal{F}_{P_\alpha}$ is countable for all $\alpha < \beta$, and $\beta < 2^{\aleph_0}$. Therefore $\mathcal{F} = \bigcup_{\alpha < \beta} \mathcal{F}_{P_\alpha}$ has cardinality at most $\aleph_0 \cdot |\beta| < 2^{\aleph_0}$. Thus by cardinality considerations, there must exist a set of prime not in $\mathcal{F}$. Let that set be P_β.

Now note that for $\alpha < \beta < 2^{\aleph_0}$, M_{P_α} is not isomorphic to M_{P_β}. Indeed, M_{P_β} contains an element a_{P_β} divisible exactly by the primes in P_β. By construction, $P_\beta \notin \mathcal{F}_{P_\alpha}$, but for each element x of M_{P_α}, the set of prime divisors of x must be a member of $\mathcal{F}_{P_\alpha}$. Since any isomorphism of M_{P_β} onto M_{P_α} would send a a_{P_β} to something still divisible exactly by the primes in P_β, we conclude that M_{P_α} and M_{P_β} are not isomorphic. □

It is easily seen that PA itself is decidable: by inspecting it, it is easy to check whether a sentence is an axiom of PA or not. However PA is *not* complete. More generally, Gödel's incompleteness theorem (to be discussed in 141b) says that *any* decidable extension of PA is incomplete. Contrapositively, a complete extension of PA cannot be decidable. For example, the theory TA = $\mathrm{Th}(\mathbb{N}, +, \cdot, 0, 1)$ (TA stands for "true arithmetic") is of course complete, hence cannot be decidable. Thus there is no algorithm that would take as input a sentence and output whether it is true of the natural numbers.

To see what this means, consider for example Goldbach's conjecture, one of the oldest unsolved problems in number theory: any even natural number greater than or equal to 4 is the sum of two primes. There is a sentence ϕ in the signature of Peano's arithmetic that describes it (exercise). Still it seems hard to check using a computer: you can keep checking examples and not know whether your computer fails to find a counterexample because there are no counterexample, or because the counterexample is too big. Is Goldbach's conjecture true or false? What do we even mean? There are *three* possibilities:

(1) PA $\models \phi$: somehow we have managed to figure out that Goldbach's conjecture is true in any model of PA (maybe using lots of fancy proof techniques like transfinite induction, the axiom of choice, etc). In this case, the completeness theorem tells us that PA $\vdash \phi$. Thus there is a proof of ϕ from the axioms of PA in the very simple style we have seen in class (that proof may be *much* longer but nevertheless will exist). In particular, TA $\models \phi$, so Goldbach's conjecture is true of $(\mathbb{N}, +, \cdot, 0, 1)$.

(2) PA $\models \neg\phi$: then similarly we will have a proof from the axioms of PA that Goldbach's conjecture fails. In fact, we will in particular have that $(\mathbb{N}, +, \cdot, 0, 1) \models \neg\phi$, so we will have an explicit (standard) natural number n that is a counterexample (it is even, greater than 4, and cannot be written as a sum of two primes). The proof could for example simply write this number as a sum of ones and check all the lower numbers by hand (there are only finitely many).

(3) PA $\not\models \phi$ and PA $\not\models \neg\phi$: this means that Goldbach's conjecture is independent of the axioms of Peano's arithmetic: some models of PA satisfy it, others don't. But what about the "true" natural numbers? A-priori, there are *two* possibilities here:
   - $\phi \in$ TA. Then Goldbach's conjecture is true of $(\mathbb{N}, +, \cdot, 0, 1)$. Nevertheless, it is *false* in some nonstandard model M of PA. Still, all sums of ones in M satisfy Goldbach's conjecture (since it is true in $\mathbb{N}$). Thus the counterexample will have to be a nonstandard number!
   - $\phi \notin$ TA. Then since TA is complete $\neg\phi \in$ TA. Thus $(\mathbb{N}, +, \cdot, 0, 1) \models \neg\phi$, so as before there must be a counterexample in $\mathbb{N}$. This example can be written as a sum of ones, so since the statement of Goldbach's conjecture is very simple, you should convince yourself that any other model of PA will have to satisfy $\neg\phi$ as well, just because there is a very long finite sentence saying that that finite sum of one is not a sum of two other smaller prime finite sum of ones. Thus in this case we should have that PA $\models \neg\phi$, and so that case does not happen.

Thus in case Goldbach's conjecture is independent of PA, we would still have that it is true for the standard natural numbers! (but we would not have an actual proof for it in PA – though there could be natural extensions of PA that prove it). To get a feeling for what this could mean you will in your assignment construct a model of a weak subset of PA that fails Goldbach's conjecture.