6c Lecture 15: May 22, 2014

12 Tarski-Seidenberg

Despite the key role that algorithms play in math, it wasn't until the early twentieth century that mathematicians began to ask abstract questions about algorithms themselves. Can we give a mathematically precise definition of what an algorithm is? What parts of mathematics can be solved by algorithms? At the time, many people were optimistic about this latter question; they thought eventually algorithms would be found to solve essentially all mathematical problems. Part of this optimism stemmed from their past successes. However, the strongest argument for this view was a program suggested by David Hilbert. Hilbert thought that we could find a complete set of axioms for mathematics; a set of starting assumptions from which we could prove or disprove any mathematical proposition. If such a set of axioms could be found, then we could use the following algorithm for determining the truth of any mathematical statement: look through the proofs from these axioms one by one until we find a proof that the statement is true, or that it is false. At the time, Hilbert's program seemed within reach; work of Frenkel, Russell, Whitehead, Zermelo, and others had essentially isolated all axioms used by mathematicians to date.

In the mid 1930s, a mathematically precise theory of algorithms was finally created. Alan Turing defined a mathematical model of a type of *computer*, a machine for performing algorithms, and gave a convincing (albeit informal) argument that this type of computer could execute any possible algorithm (defined in the informal sense we've given above)[1]. Using this precise definition, Turing was then able to prove that there are mathematical problems which can never be solved by algorithms. A line had forever been drawn through the middle of mathematics, splitting it into those problems which are computable, and those which are not. And this was just the tip of a giant iceberg; the theory of computation provided a new perspective and new tools which were to about to have a revolutionary effect on mathematics.

12.1 The Tarski-Seidenberg theorem

Our goal for the remainder of the class is to discuss computability, undecidability, and its relationship with logic. However, before we start our quest towards incomputability outlined above, and by way of contrast to most of the remaining results we will prove, we will prove the that there is an algorithm for deciding

[1]Earlier models of computation had been suggested by Church, Gödel, Herbrand, and Kleene, (who had given definitions which turned out later to be equivalent to Turing's)

which statements are true in what might be termed "elementary geometry". Precisely:

Theorem 12.1 (Tarski-Seidenberg). *Let $\mathcal{R}$ be the model whose universe is $\mathbb{R}$, and whose language contains a constant for every rational number, the functions $+$ and $\cdot$, and the relation $<$. Then there is an algorithm which decides (in finite time, always outputting the correct answer) what sentences are true in $\mathcal{R}$.*

Note that such sentences include quite of lot of interesting mathematics. For example, Morley's trisector theorem which says that the lines trisecting the angles of any triangle intersect at points forming an equilateral triangle. This was proved by Morley in 1899, and generalized in a pretty way to arbitrary fields by Connes in 2004.

Another example of interesting sentences in this structure is given by the kissing spheres problems. One can arrange 12 unit spheres so that they each touch a central unit sphere without intersecting each other, but one cannot do the same for 13 spheres (see Figure 12.1). This problem was the source of a famous disagreement between Isaac Newton and David Gregory, and remained unsolved for a few hundred years. Several sketched solutions were given in the nineteenth century. However, it wasn't until 1953 that the first detailed correct proof was given by Schütte and van der Waerden[2].

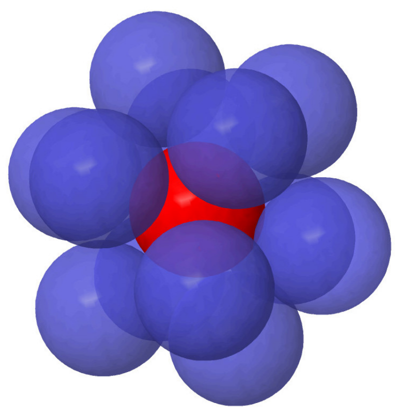

Figure 1: Twelve unit spheres kissing a central (red) one. Based on Sage code of Robert Bradshaw: `http://en.wikipedia.org/wiki/File:Kissing-3d.png`.

From now on, we'll often use abbreviations for obviously definable functions and relations such as x^2 to represent $x \cdot x$, and $x \geq y$ for $x > y \vee x = y$.

The key to the Tarski-Seidenberg theorem is the following lemma:

[2]The four dimensional generalization of the kissing spheres problem was settled by Musin in 2003: it turns out there can be 24 kissing spheres. The five dimensional version remains open, though the answer is known to be between 40 and 44.

Lemma 12.2. *Suppose ϕ is a quantifier-free formula having x as a free variable. Then there is an algorithm which given ϕ finds a quantifier-free formula ϕ' such that $\exists x \phi$ is equivalent to ϕ' in the model $\mathcal{R}$.*

Note that this means we can also do the same thing for universal quantifiers.

Corollary 12.3. *Suppose ϕ is a quantifier-free formula in the language L having x as a free variable. Then there is an algorithm which given ϕ finds a quantifier-free formula ϕ' such that $\forall x \phi$ is equivalent to ϕ' in the model $\mathcal{R}$.*

Proof. Since $\forall x \phi$ is equivalent to $\neg \exists x \neg \phi$, we can use the above lemma to find θ equivalent to $\exists x \neg \phi$, and then $\forall x \phi$ is equivalent to $\phi' = \neg \theta$. $\square$

We say this lemma allows us to *eliminate quantifiers*. You already know several instances of this idea. For example, you probably learned in a high school algebra class that when ϕ is $a^2x+bx+c = 0$, then the formula $\exists x(a^2x+bx+c = 0)$ is equivalent to the quantifier-free formula $a \neq 0 \wedge b^2 - 4ac \geq 0 \vee (a = 0 \wedge b \neq 0) \vee (a = 0 \wedge b = 0 \wedge c = 0)$.

Assuming this lemma, the Tarski-Seidenberg theorem is easy.

Proof of Theorem 12.1. Given a sentence ψ, we can find an equivalent sentence in prenex normal form:

$$Qx_1 \dots Qx_{n-1} Qx_n \phi$$

But now we can eliminate all the quantifiers. Starting from the inside, we can find a quantifier-free ϕ' equivalent $Qx_n\phi$. Then we find a quantifier-free formula ϕ'' equivalent to $Qx_{n-1}\phi'$, and so on until we are left with a quantifier-free formula with no free variables which is equivalent to our original sentence. (Formulas like $2+2 = 4$ and $3 > 5 \vee 7 < 10$.) However, for such formulas (which are essentially basic arithmetic problems) there is obviously an algorithm for evaluating their truth. $\square$

For example, suppose we are given the statement $\forall a \forall b \forall c \exists x(ax^2+bx+c = 0)$. Then an equivalent sequence of statements where we remove the quantifiers one by one is the following:

$$\begin{aligned}
&\forall a \forall b \forall c \exists x(ax^2 + bx + c = 0) \\
\leftrightarrow &\forall a \forall b \forall c((b^2 - 4ac \geq 0 \wedge a \neq 0) \vee (a = 0 \wedge b \neq 0) \vee (a = 0 \wedge b = 0 \wedge c = 0)) \\
\leftrightarrow &\forall a \forall b(a = 0 \wedge b \neq 0) \\
\leftrightarrow &\forall a(\bot) \\
\leftrightarrow &\bot
\end{aligned}$$

The Tarski-Seidenberg algorithm builds on an earlier algorithm due to Sturm, which can be used to decide whether a polynomial with rational coefficients has a root. One of the main tools used in Strum's algorithm is polynomial division, and we use the notation remainder$(p_1(x), p_0(x))$ to indicate the remainder when $p_1(x)$ is divided into $p_0(x)$, so that $p_0(x) = p_1(x)q(x) + \text{remainder}(p_1(x), p_0(x))$, for some $q(x)$.

Theorem 12.4 (Sturm)**.** *Given a polynomial $p(x)$ and its derivative $p'(x)$, consider the sequence of polynomials given by repeatedly doing polynomial division, and taking remainders, stopping just before we obtain* 0*.*

$$\begin{aligned}
p_0(x) &= p(x) \\
p_1(x) &= p'(x) \\
p_2(x) &= -\operatorname{remainder}(p_1(x), p_0(x)) \\
p_3(x) &= -\operatorname{remainder}(p_2(x), p_1(x)) \\
&\vdots \\
p_n(x) &= -\operatorname{remainder}(p_{n-1}(x), p_{n-2}(x))
\end{aligned}$$

so $p_n(x)$ is nonzero, but $p_n(x)$ divides into $p_{n-1}(x)$ with a remainder of 0*. Now let $s(-\infty)$ be the sequence giving the sign of each $p_i(x)$ as $x \to -\infty$, and $s(\infty)$ be the sequence giving the sign of each p_i as $x \to \infty$. Then $p(x)$ has a root if and only if there are more sign changes in the sequence $s(-\infty)$ than in the sequence $s(\infty)$.*

Before we prove this theorem, we give an example. If $p(x) = x^3 - 3x^2 + x - 1$, then the sequence of polynomials from Sturm's theorem is[3]:

$$\begin{aligned}
p_0(x) &= x^3 - 3x^2 + x - 1 \\
p_1(x) &= 3x^2 - 6x + 1 \\
p_2(x) &= 4/3x + 2/3 \\
p_3(x) &= -19/4
\end{aligned}$$

Now taking the limit as $x \to -\infty$, we see $p_0(x)$ is negative, $p_1(x)$ is positive, $p_2(x)$ is negative, and $p_3(x)$ is negative. So $s(-\infty) = + - -+$ and the sign changes twice in this sequence. As $x \to \infty$, we see that $p_0(x)$ is positive, $p_1(x)$ is positive, $p_2(x)$ is positive, and $p_3(x)$ is negative, so $s(\infty) = + + +-$ and the sequence changes sign once. Since there are more sign changes in the first sequence, Sturm's theorem says the polynomial has a real root. We're ready now to prove the theorem.

Proof. First, we do the case when $p_n(x)$ is a constant (which is not zero). This implies that $p(x) = p_0(x)$ and $p'(x) = p_1(x)$ do not have any common polynomial factor; a common factor of $p_0(x)$ and $p_1(x)$ must also be a common factor of $p_2(x)$, since $p_0(x) = p_1(x)q(x) - p_2(x)$ for some $q(x)$ and inductively, a common factor of $p(x)$ and $p'(x)$ must be a common factor of $p_i(x)$ for all i between 0 and n.

We will show that as x increases, whenever $p_0(x)$ has a root, the number of sign changes in the sign sequence from the p_i drops, and whenever any other $p_i(x)$ has a root, the number of sign changes in the sequence stays the same. This is enough to prove the theorem.

[3]since for example, $x^3 - 3x^2 + x - 1 = (x/3 - 1/3)(3x^2 - 6x + 1) + (-4/3x - 2/3)$

Note that by the definition of division, for each $i \geq 0$, $p_i = p_{i+1}(x)q(x) - p_{i+2}(x)$, for some quotient polynomial $q(x)$, since $-p_{i+2}$ is the remainder when we do the division. This implies that for each x, if $p_i(x) = 0$, then $p_{i+1}(x) \neq 0$. Otherwise, $p_{i+2}(x) = 0$ would be zero by the formula above, but then the same argument shows $p_j(x) = 0$ for all $j \geq i$ contradicting the fact that $p_n(x)$ is a nonzero constant.

Thus, for all $i \geq 0$, if $p_{i+1}(x) = 0$, then $p_i(x) \neq 0$ and $p_{i+2}(x) \neq 0$, and further, $p_i(x)$ and $p_{i+2}(x)$ have opposite signs. Hence, whenever $p_{i+1}(x)$ changes sign, (so $i+1 \neq n$), then the total number of sign changes in our sequence says the same; these three signs either flip from $++-$ to $+--$ or vice versa, or $-++$ to $--+$ or vice versa.

Finally, if $p_0(x)$ has a root, then then $p'(x)$ must be the opposite sign; if $p_0(x)$, then its derivative must be negative to get a root, and if $p_0(x)$ is negative, then $p'(x)$ must be positive to get a root. Thus, the start of the sign sequence either changes from $+-$ to $--$, decreasing the number of sign changes, or $-+$ to $++$, also decreasing the number of sign changes.

To do the general case now, if $p(x)$ and $p'(x)$ have a common factor $f(x)$, then the theorem follows by dividing the sequence $p_0(x), p_1(x), \ldots, p_n(x)$ by $f(x)$, and then applying the above argument; if a root of $p(x)$ has multiplicity greater than 1, its multiplicity in $p'(x)$ is one less. $\square$

The proof of the Tarski-Seidenberg finishes by then generalizing Sturm's algorithm so that it can determine whether some finite collection of polynomials satisfies some combination of inequalities. Lets first reduce the types of formulas we need to consider.

Suppose ϕ is quantifier free. We may as well assume that ϕ is in conjunctive normal form:

$$\phi = \psi_1 \vee \theta_2 \vee \ldots \vee \theta_n$$

Then since $\exists x \phi$ is equivalent to

$$\exists x \psi_1 \vee \exists x \theta_2 \vee \ldots \vee \exists x \theta_n$$

Now since each $\phi_i = \theta_1 \wedge \ldots \wedge \theta_{n_i}$ is a conjunction of atomic formulas or their negations, it is enough to eliminate quantifiers from formulas of the form $\exists x(\theta_1 \wedge \ldots \wedge \theta_{n_i})$ where each θ_i is of the form $p(x) = 0$ or $\neg(p(x) = 0)$ or $p(x) > 0$ or $\neg(p(x) > 0)$.

Now,

- $\neg(p(x) = 0)$ is equivalent to $(p(x))^2 > 0$
- $\neg(p(x) > 0)$ is equivalent to $p(x) \leq 0$ which is equivalent to $-p(x) > 0 \vee p(x) = 0$.
- $p_1(x) = 0 \wedge p_2(x) = 0 \wedge \ldots \wedge p_n(x) = 0$ is equivalent to $(p_1(x))^2 + (p_2(x))^2 + \ldots + (p_n(x))^2 = 0$.

Thus, it is enough to eliminate quantifiers for a formula of the form:

$$\exists x(p(x) = 0 \wedge q_1(x) > 0 \wedge \ldots \wedge q_n(x) > 0$$

Now it will be a homework problem for you to adapt Strum's algorithm to eliminate quantifiers for formulas when there is a single q.

Exercise 12.5. Suppose $p(x)$ and $q(x)$ are polynomials in x of degree $\leq n$. Then for each $k \leq n$ there is a quantifier free formula ϕ_k which is true iff there are k different values of x for which $p(x) = 0$ and $q(x) > 0$.

Given this homework problem, we can do the general case as follows. Suppose first that we want to find the number of roots of $p(x) = 0$ where $q_1(x) > 0$ and $q_2(x) > 0$. Then

- Let A be the number of roots of $p(x) = 0$ where $q_1(x) > 0$ and $q_2(x) \neq 0$.
- Let B be the number of roots of $p(x) = 0$ where $q_1(x) \neq 0$ and $q_2(x) > 0$.
- Let C be the number of roots of $p(x) = 0$ where $q_1(x) \neq 0$ and $q_2(x) \neq 0$.
- Let D be the number of roots of $p(x) = 0$ where $q_1(x) > 0$ and $q_2(x) > 0$ or $q_1(x) < 0$ and $q_2(x) < 0$.

Then the number of roots of $p(x) = 0$ where $q_1(x) > 0$ and $q_2(x) > 0$ is equal to $(A + B - (C - D))/2$.

But

- A is the number of roots of $p(x) = 0$ where $q_1(x)q_2^2(x) > 0$.
- B is the number of roots of $p(x) = 0$ where $q_1(x)^2q_2(x) > 0$. and $q_2(x) > 0$.
- C is the number of roots of $p(x) = 0$ where $q_1(x)^2q_2^2(x) > 0$.
- D is the number of roots of $p(x) = 0$ where $q_1(x)q_2(x) > 0$.

So by the homework problem, and an inductive argument if $p(x)$ and $q_1(x), \ldots, q_n(x)$ are polynomials in x all of degree $\leq n$, then for each $k \leq n$ there is a quantifier free formula ϕ_k which is true iff there are k different values of x for which $p(x) = 0$ and $q_1(x) > 0 \wedge \ldots \wedge q_n(x) > 0$.

12.2 Beyond Tarski-Seidenberg

How good is the Tarski-Seidenberg algorithm from a practical perspective? When we have a computer execute it, can it quickly solve interesting problems, such as the kissing spheres problem? The answer is that the algorithm is almost completely useless. Each time a quantifier is eliminated we add exponentially many new equations and so the formulas involved become massive.

Fortunately, significant progress has been made on finding faster algorithms, using techniques such as cylindrical algebraic decomposition. There is an algorithm which decides sentences with n symbols in $O(2^{2^n})$ time, and an algorithm for deciding existential formulas (ones beginning with a single block of existential quantifiers, and containing no other quantifiers) in $O(2^n)$ time. This first result is known essentially be optimal.

Alas, even these improved algorithms are still rather slow when run on practical problems. For example, modern implementations of quantifier elimination are able to solve the kissing spheres in 2 dimensions (with a little ingenuity to make the problem slightly easier, such as fixing the position of the first sphere). However, the kissing spheres problem in higher dimensions is completely out of reach for now (the four dimensional version requires a hundred quantifiers). Still, these algorithms are an important part of almost all computer algebra systems and receive a great deal of use for people working on practical mathematics; there are lots of interesting formulas which are rather short.

Another interesting avenue of investigation is how much the Tarski-Seidenberg theorem can be generalized. Does the theorem remain true when we add more functions to our language so that we can discuss more complicated phenomena? For example, Tarski asked in 1940 whether one can prove the same theorem when exponentiation is added to our language:

Open Problem 12.6. *Is there an algorithm for deciding what sentences are true of the reals, in the first order language built from* $\{+, \times, \exp, =, 0, 1\}$.

Not only is the question an open problem, but we don't even know if there is an algorithm for deciding the truth of sentences such as $e^{-e^2} - 60e^{-15} = e^{-3e^1+2e^{-1}}$ involving no variables or quantifiers! Are there any surprising identities involving exponentiation and the integers beyond obvious ones that follow from the fact that $e^x e^y = e^{x+y}$? This is a difficult problem in transcendental number theory. However, there is a widely believed conjecture due to Schanuel which implies that indeed, the only such true identities are the obvious ones, and that there is an algorithm for deciding quantifier-free sentences. In fact, if Schanuel's conjecture is true, then Macintyre and Wilkie have shown that there is an algorithm for deciding all sentences in the language with exponentiation, settling the entire problem.

What about if we change what number system we use to something other than the real numbers? For example, if we work over the complex numbers instead, then Tarski showed in 1948 that the analogous theorem is true: there is algorithm to decide the truth of sentences in the first order language built from $\{+, \times, =, <, 0, 1\}$ about the complex numbers[4]. How about the natural numbers? In this setting, we can state many difficult open problems like Goldbach's conjecture:

$$\begin{aligned}&\forall n((n \geq 2 \land \exists k(n = 2k)) \to \exists p \exists q(n = p + q \land \\ &\qquad \forall r \forall s((p = rs \to (r = 1 \lor s = 1)) \land (q = rs \to (r = 1 \lor s = 1)))))\end{aligned}$$

Is there a similar algorithm to decide which of these statements are true or false? In his famous speech outlining 23 important problems for twentieth century

[4]A year later, Abraham Robinson gave a very pretty model-theoretic proof of this fact

mathematics, Hilbert made it a goal to find a process to solve a simple class of such problems: find an algorithm for determining whether a a multivariable polynomial has any integer roots, (perhaps similar to the one we have given above to determine whether there are any *real* roots to such a polynomial). This is known as Hilbert's 10th problem, and it turns out that it is incomputable. While we won't show this in these lecture notes, we will prove a slightly weaker theorem that the theory of the natural numbers under $+$ and $\times$ is undecidable.

We finish this section by stating one more famously open problem:

Open Problem 12.7 (Hilbert's tenth problem over $\mathbb{Q}$)**.** *Is there an algorithm for deciding whether a multivariable polynomial with integer coefficients has any rational roots?*