Julia Robinson: The art of definition

February 19, 2021

Model theory is a branch of logic that typically studies mathematical structures from the perspective of first-order logic. Communicating the what and why is often challenging, but today we will stick to familiar structures, namely the integers $\mathbb{Z}$, the rationals $\mathbb{Q}$, and the reals $\mathbb{R}$, with $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$. We will talk about these structures, these models, using the language of rings: three binary functions plus $+$, times $\cdot$ and subtraction $-$. For good measure we will use names for 0 and 1. It is irresistible to use shortcuts such as 2 for $1 + 1$ and x^2 for x times x and it makes things readable.

The game for us today, and for Julia Robinson in her marvelous research, is to see what is expressible, what notions we can define, for our three rings using the language of rings to create formulae using variables, quantifiers "for all" $\forall$ and "there exist" $\exists$, together with finite conjunctions $\wedge$, negations, and implications $\Rightarrow$.

Actually we won't fuss over formalities: definability has a specific meaning in our setting and examples will guide our understanding better than technicalities.

For example, each ring in our trio has a natural ordering, but $<$ is not in the language of rings. No worry, we can define $<$ in each case, by showing that we can pick out the nonnegative elements in our given structures.

For $\mathbb{R}$ this is easy: a real number r is non-negative just in case it has a square root, so we can say:
r is non-negative if and only if $\exists s(s^2 = r)$.
The rules of definability here require that such an s be found in the ambient structure $\mathbb{R}$. And it can be.
What about the same question for $\mathbb{Z}$: can we find a condition that holds exactly when an integer is non-negative? Well, squares are non-negative but unlike in the real numbers, not every non-negative integer is a square in $\mathbb{Z}$, e.g., 2.

Here comes our first call to number theory: Lagrange's Theorem states that every non-negative integer is a sum of four squares (again, squares of integers). So for an integer n, we have n is nonnegative if and only if $\exists x_1 \exists x_2 \exists x_3 \exists x_4 (n = x_1^2 + x_2^2 + x_3^2 + x_4^2)$. Again the x_i's must be integers since our definition is meant to work inside $\mathbb{Z}$,. Thus Lagrange gives a definition of the natural numbers $\mathbb{N}$ inside $\mathbb{Z}$. (It turns out the same approach works to define the non-negative rationals inside $\mathbb{Q}$.)

Something to think about: how to define " p is prime, or" n is composite," or "x is (or is not) a power of 2" in $\mathbb{Z}$.

Quantifier complexity. In the examples above, the defining formulae only required the use of $\exists$, but as we will soon see, things are not always so easy. We could say a specific polynomial has a root, say $\exists x(x^3 + x^2 - 3x + 1 = 0)$ but suppose now we want to say every monic polynomial of degree 3 has a root. One way is to say $\forall a \forall b \forall c \exists x(x^3 + ax^2 + bx + c = 0)$, which is "universal-existential" or "$\forall\exists$". There are three $\forall$'s here but what matters more is the number of alternations. Thus this statement is more complicated than the formula which picked out non-negative elements. And things can get worse, in general much worse, and formulas can have many (finite) alternations of quantifiers, truly a nightmare. But not here, not today.

Already three alternations can be mystifying, either $\forall\exists\forall$ or $\exists\forall\exists$. One reason the $\epsilon - \delta$ definition of limit in calculus is hard to fathom, it seems to me, is the alternation of quantifiers: to say that the limit of $f(x)$ equals L as x approaches a is an $\forall\exists\forall$: $\forall\epsilon\exists\delta\forall x(\epsilon > 0 \Rightarrow (\delta > 0 \wedge (|x - a| < \delta \Rightarrow |f(a) - L| < \epsilon)$

David Kazhdan: Often the experience of learning model theory is similar to the one of learning physics: for a while everything is so simple and so easily reformulated in familiar terms that "there is nothing to learn" but suddenly one find himself in a place when Model theoreticians "jump from a tussock to a hummock" while we mathematicians don't see where to put a foot and are at a complete loss.

Given an element of $\mathbb{Q}$, how can one recognize whether it is an integer? Hmmm. Write it in lowest terms and check to see if the denominator is 1 (or -1). But how to find a single formula in our language which is true of any rational number x just in case x is an integer? MUCH harder.

Theorem (Julia Robinson 1949) $\mathbb{Z}$ is definable in $\mathbb{Q}$.

t is an integer in $\mathbb{Q}$ if and only if

$\forall a \forall b(\{\exists X \exists Y \exists Z(2+bZ^2 = X^2+aY^2)) \wedge \forall M[(\exists X \exists Y \exists Z(2+abM^2+bZ^2 = X^2+aY^2) \Rightarrow (\exists X \exists Y \exists Z(2+ab(M+1)^2+bZ^2 = X^2+aY^2)]\} \Rightarrow (\exists X \exists Y \exists Z(2+abt^2+bZ^2 = X^2+aY^2)))$

With some effort this can be unpacked and shown to be equivalent to an $\forall\exists\forall$ formula. One example (thanks to Koenigsmann) :

t is an integer in $\mathbb{Q}$ if and only if

$\forall a \forall b \exists a_1 \exists a_2 \exists a_3 \exists a_4 \exists a_5 \exists a_6 \exists a_7 \forall b_1 \forall b_2 \forall b_3 \forall b_4 \forall b_5 \forall b_6$
$(f(t, a, b, a_1, a_2, a_3, a_4, a_5, a_6, a_7, b_1, b_2, b_3, b_4, b_5, b_6) = 0)$, where the f here is a polynomial with integer coefficients in 16 variables.

More digestible are the ingredients of her proof. As we used Lagrange's Theorem earlier, Robinson drew on number theory, in particular Hasse's work on representing integers via quadratic forms. For a given prime p, this allowed her to produce a criterion for when a denominator of a fraction is not divisible by p. But there are infinitely many primes and our language doesn't allow infinite conjunctions. Roughly speaking she was able to deal with the prime 2 and to group the criteria for odd primes according to congruence class mod 4, in combination with some use of the Legendre symbol. This brought the matter of checking infinitely many primes down to looking at finitely many classes of primes, hence making the result definable. Her proof is readable, requiring nothing more sophisticated than the definition of the Legendre symbol. Also quite accessible is the account by Flath and Wagon in the Math Monthly.

Undecidability phenomenon

Why should we care about defining $\mathbb{Z}$ in $\mathbb{Q}$? In 1931 Godel proved a profound result about $\mathbb{Z}$, called undecidability, showing it is provably impossible to list all the true facts about $\mathbb{Z}$ in the language of rings. (Motto: "number theory is hard!") JR's result transfers this fact to all true facts about $\mathbb{Q}$. This is typical of many undecidability results: link the question to $\mathbb{Z}$.

In contrast, Tarski (JR's advisor) showed that $\mathbb{R}$ is decidable. As a corollary, neither $\mathbb{Z}$ nor $\mathbb{Q}$ is definable in $\mathbb{R}$. Much more has been shown about what is definable in $\mathbb{R}$.

A related question, and a central source of JR's fame, is Hilbert's 10th problem. Can one decide whether a polynomial over the integers in several variables has a solution? If it has a solution, then a search will find it. If it doesn't have a solution, how will we ever know? JR worked on this for decades, as did others (notably Martin Davis and Hilary Putnam) . They obtained useful criteria. JR showed that if they could find a single such equation whose solution set grew exponentially then undecidability was proved. In 1970 Yuri Matiasevich provided the final, crucial piece, thus showing that this problem is undecidable. Indeed, any listable set of integers is the set of solutions of some such equation.

However, this leaves open whether Hilbert's 10th problem is true or false if we replace integers by rationals, since the definition JR gave of the integers in the rationals is complicated. If it were existential, then the result would transfer from integers to rationals.

Progress?

Definability and decidability questions have been asked, and some answered, in the intervening years. There have been many players, including Leonard Lipshitz, Jan Denef, Lou van den Dries, Kirsten Eisentraeger, Jennifer Park, Alexandra Schlapentokh, Barry Mazur, J.-L. Colliot-Thelene, Hector Pasten, Carlos Videla....

In 2009 (60 years after JR's work) Bjorn Poonen improved the definition down to $\forall\exists$, two alternations of quantifiers!

t is an integer in $\mathbb{Q}$ if and only if

$$(\forall a \forall b)(\exists a_1 \exists a_2 \exists a_3 \exists a_4 \exists b_1 \exists b_2 \exists b_3 \exists b_4 \exists x_1 \exists x_2 \exists x_3 \exists x_4 \exists y_1 \exists y_2 \exists y_3, \exists y_4 \exists n)((a+ a_1^2 + a_2^2 + a_3^2 + a_4^2)(b + b_1^2 + b_2^2 + b_3^2 + b_4^2)((x_1^2 - ax_2^2 - bt_3^2 + abx_4^2 - 1)^2 + (y_1^2 - ay_2^2 - by_3^2 + aby_4^2 - 1)^2 + n^2(n-1)^2(n-2309)^2 + (2x_1 + 2y_1 + n - t)^2)) = 0.$$

Poonen's result involved number theory yet again, including Hasse-Minkowski local-global results and quaternion algebras.

And in 2016 Jochen Koenigsmann brought it down to universal quantifiers only!

There is an integer n and a polynomial $g(t, x_1, ..., x_n)$ such that t is an integer in $\mathbb{Q}$ if and only if $\forall x_1, ..., \forall x_n (g(t, x_1, ..., x_n) \neq 0)$.

Koenigsmann's proof involves the earlier ingredients, together with existential definitions of certain Jacobson radicals and some quantifier manipulations.

Still open: Hilbert's 10th problem for $\mathbb{Q}$.

A few references:

M. Davis, H. Putnam, and J. Robinson, The decision problem for exponential diophantine equations, Ann. of Math. (2) 74 (1961), 425436.

Dan Flath and Stan Wagon, How to pick out the integers in the rationals: an application of number theory to logic. Amer. Math. Monthly 98 (1991), no. 9, 812823.

Jochen Koenigsmann, Defining Z in Q. Ann. of Math. (2) 183 (2016), no. 1, 7393.

Yuri Matiyasevich, The Diophantineness of enumerable sets, Dokl. Akad. Nauk SSSR 191 (1970), 279282 (Russian)

Jennifer Park, A universal first order formula for defining the ring of integers in a number field, Math. Res. Lett. 20 (2013), 961-980.

Bjorn Poonen, Characterizing integers among rational numbers with a universal-existential formula, American Journal of Mathematics, Volume 131, Number 3, June 2009, pp. 675-682.

Constance Reid, Julia, A Life in Mathematics, The Mathematical Association of America, 1996.
(This is out of print but should not be. I will pester someone about this next week!)

Julia Robinson, Definability and decision problems in arithmetic, J. Symbolic Logic 14 (1949), 98-114.

also, see the video of Lenore Blum's public lecture at the MSRI celebration in December 2019 of Julia Robinson's 100th birthday: https://www.msri.org/workshops/955/schedules/27749#5-Blum