MATH 4820/5820-3: EXAMPLE PROJECT 6
THERE ARE DIOPHANTINE EQUATIONS OVER $\mathbb{Z}$ FOR WHICH HAVING A $\mathbb{Z}$ SOLUTION IS UNDECIDABLE

PROF. MICHAEL D. FRIED, OFFICE MATH. DEPT. #223

This project sets out to discuss a chain of results (corresponding to Stillwell's Chap. 25). These use the results we discussed in class on Pells equation. The conclusion will be to discuss that there are specific equations that – by any ordinary standard – cannot be decided.

As with the negative solution of solving the general degree n polynomial for its roots, to get going required some precise notions of what this problem is about. That is, it is necessary to know what it means to be *decidable*. Giving a procedure for deciding a problem is one thing. Showing it is undecidable is another.

1. Consider the problem Galois raised

For the problem Galois explained, he came up with a precise statement about his Group G_P attached to $P(y)$, an irreducible polynomial of degree n, that said yes or no to the following statement.

> Its roots have an expression in terms of taking successive roots,
> of expressions starting from the coefficients of P.

His statement is that $P(y)$ is *solvable* as in this statement, if and only if G_P is a *solvable* group. He also noted in important new situations where groups turned out not to be solvable. Indeed, they were simple, the subject of Chap. 23 of Stillwell.

We will have one lecture before the semester ends on Chap. 23 which will be more historical, but including the people who Stillwell only knows secondarily through reading expositions about them.

Church and Turing influenced all of computer science by considering the framework for considering problems akin to Hilbert's question, A general notion: You have a language, L, a set of axioms, A, for L, and you look at a conjecture, C, about L. They literally wrote the idea of deciding C as an abstract computer program.

Proposition 1.1. *There were always going to be conjectures C for which no program would come to a conclusion about C. This was their notion of undecidable.*

Suppose, given a polynomial $P(y)$you could not decide if G_P is solvable. Then the problem of finding roots would be undecidable. That isnt, however, the case.

Suppose, however, we asked whether for every group G, there is $(\exists)$ a polynomial $P(y)$ such that G_P is a particular group. Can this be phrased as a kind of problem that Hilbert was discussing?

Answer: It almost can, though you have to consider that it requires an infinite number of variables. In the usual view of Hilbert's problem, you are allowed only a finite number of variables at a time.

2. The notion of a Diophantine set

Such a set is given by a Diophantine equation with two sets of variables $\boldsymbol{a}$ and $\boldsymbol{x}$, and an equation $D(\boldsymbol{a},\boldsymbol{x}) = 0$. The Diophantine set is called

$$M_D : \{\boldsymbol{a} \mid D(\boldsymbol{a},\boldsymbol{x}) = 0 \text{ has a solution in } \boldsymbol{x}\}.$$

We regard D as a diophantine representation of M_D.

An undecidability result for Hilberts problem started with this.

Conjecture 2.1 (Tarski)**.** For the set of powers of 2, $M = (1, 2, 2^2, \dots)$, there is no D so that $M_D = M$.

Curt Gödels incompleteness paper showed that, given any axiomatic system T (containing a typical set of our usual axioms about how integers work), there is a true statement that you cant prove in T. Further, it has a special form:

$$f(\boldsymbol{x}) \text{ is never 0 no matter what the integers } \boldsymbol{x} \text{ are.}$$

Here, though, f is a particular type of function called *primitive recursive*. So it wasn't precisely answering Hilbert's question.

Martin Davis simplified Gödels equation so there was just one variable, u, quantified with $\exists$ and the rest of the expression involves a polynomial P in the variables. That is, he came closer to reducing it to considering what we considered in discussing projective geometry.

Further, Davis showed that if he could eliminate the existential variable u then he would really have a solution of unsolvability as in Hilbert's question for ordinary polynomial equations.

3. The role of Pell's equation

When we discussed Pells equation in class, we found hints that set of solutions had some resemblance to Tarskis problem. That is, if you had one solution, $a+b\sqrt{N}$, b $\not\emptyset$, then its powers defined infinitely many solutions of $x^2 - Ny^2 = 1$.

This led to the notion of *exponentially Diophantine*, and a negative solution of Hilberts problem. The presentation should trace the work on Pell's equation in modern form to the final result of Davis-Matiesevich-Putnam-Robinson.

E-mail address: michael.fried@Colorado.edu
E-mail address: michaeldavidfried@gmail.com