$x = \pm yz \pm 1$ AND ALGORITHMIC UNSOLVABILITY

by
Harvey M. Friedman
Distinguished University Professor of Mathematics, Philosophy, and Computer Science Emeritus
Ohio State University
Columbus, Ohio
October 15, 2017

Abstract. Does a given finite system of equations x = yz+1 have a solution in integers? We show that this problem is algorithmically unsolvable. We also show unsolvability using x = -yz-1, and solvability using x = yz-1, and using x = -yz+1.

1. INTRODUCTION

This paper is a contribution to the search for yet more elementary examples of algorithmic unsolvability. We have previously developed quite a number of fundamental examples in elementary Euclidean geometry [Fr10], and also more recently involving inner products [Fr17]. Also see [Ma93], [Poxx], [Po14].

Many examples of (algorithmic) unsolvability are proved by reduction from the known unsolvable Hilbert's 10th Problem, [Da73]. We proceed in this way here as well as in [Fr10]. A considerable portion of [Poxx], [Po14] also proceeds in this way. Also see [Ma93], sections 9,10.

One problem is reducible to another if and only if there is an algorithm that converts any instance of the first problem to an equivalent instance of the second problem. So if the second problem is solvable then the first problem is solvable. If the first problem is unsolvable then the second problem is unsolvable.

The original unsolvable problem is the Halting Problem. Given a Turing Machine initialized with a blank tape, does it eventually halt?

HILBERT'S TENTH PROBLEM/Z. H10(Z). Does a given polynomial with integer coefficients vanish over Z?

H10(Z) is unsolvable, and in fact mutually reducible with the halting problem. See [Da73], [Ma93].

DEFINITION 1.1. An algebra, in the present sense, is a system (D,...) where the finitely many components are functions of several arguments from D into D (no constants and no relations). Let M be an algebra. $\Theta(M)$ is the following decision problem. Let V be a finite set of equations of the form $F(x_1,...,x_k) = y$, where F is a component of M. Is V solvable over D?

Note that we put no restrictions on the variables $x_1,...,x_k,y$, and the variables used in the different equations may share variables in unrestricted intricate ways.

The four problems stated in the Abstract are just $\Theta(M)$ for the following four algebras M: (Z,x=yz+1), (Z,x=-yz-1), (Z,x=yz-1), (Z,x=-yz+1).

For our unsolvability results of section 2 it is convenient, but by no means necessary, to bring in the notion of "very definable relation".

DEFINITION 1.2. A relation $R \subseteq Z^k$ is very definable over the algebra M if and only if we can define $(\forall x_1,...,x_k)(R(x_1,...,x_k) \leftrightarrow (\exists y_1,...,y_n)(\varphi))$, where φ is a conjunction of equations $F(x_1,...,x_k) = y$, where $x_1,...,x_k,y$ are variables among the distinct variables $x_1,...,x_k,y_1,...,y_n$. We will often view a function as a relation (the graph).

THEOREM 1.1. Let M = (Z,...) be an algebra. The nonemptiness problem for very definable relations over M is reducible to $\Theta(M)$. So if the nonemptinss problem for very definable relations over M is unsolvable, then $\Theta(M)$ is unsolvable.

Proof: Nonemptiness of the k-ary relation R defined by $(\forall x_1,\ldots,x_k)(R(x_1,\ldots,x_k) \leftrightarrow (\exists y_1,\ldots,y_n)(\varphi))$ is equivalent to the existence of a solution to φ. QED

In applying Theorem 1.1 to obtain unsolvability, it is convenient to know that the very definable relations over M have good closure properties.

THEOREM 1.2. Let K be the least class of formulas in the language of the algebra M such that
i. All atomic formulas of M are in K, equality allowed.
ii. Conjunctions of formulas in K are formulas in K.
iii. If φ is a formula in K then any $(\exists y_1,\ldots,y_n)(\varphi)$ is a formula in K.
Every formula in K defines a relation over M that is very definable over M.
Let M,M',M'' be algebras with the same domain. Suppose the components of M are very definable over M', and the components of M' are very definable over M''. Then every relation very definable over M is very definable over M''.

Proof: By standard quantifier manipulations. We use additional quantifiers to break down compound equations s = t into the form $F(x_1,\ldots,x_k) = y$. QED

THEOREM 1.3. H10(Z) reduces to Θ(x=yz,x=y+z,≡1). Here ≡1 is the unary constantly 1 function.

Proof: This is well known. The standard argument is sketched, e.g., in [Fr17], Lemma 2.7. θ(x=yz,x=y+z,≡1) is r.e. by search. QED

THEOREM 1.4. The relations x = yz, x = y+z, ≡1, used in Theorem 1.3, are very definable over (Z,x=yz,x=y+1).

Proof: See [Fr17], Lemma 3.4. QED

THEOREM 1.5. If the relations x = yz and x = y+1 are very definable over an algebra M with domain Z, then the Halting Problem is reducible to Θ(M).

Proof: By chaining together Theorem 1.1 - 1.4, and reducing the Halting Problem to H10(Z) by the MRDP theorem ([Da73], [Ma93]). QED

Of the four problems, Θ(x=yz+1), Θ(x=-yz-1), Θ(x=yz-1), Θ(x=-yz+1), we show that the first two are unsolvable in section 2, and the latter two are solvable in section 3.

2. Θ(x=yz+1),Θ(x=-yz-1)

LEMMA 2.1. The relations x = yz and x = y+1 are very definable over (Z,x=yz+1).

Proof: Consider the following four equations in integer variables x,y,z,w,u,v.

1. x = xy+1.
2. x = yy+1.
3. z = xw+1.
4. z = uv+1.

From 1, we have x(1-y) = 1, and so (x = 1 ∧ y = 0) ∨ (x = -1 ∧ y = 2). From 2, x = 1 ∧ y = 0. From 3, z = w+1. From 4, xw+1 = uv+1, and so w = uv. We claim

z = w+1 ↔ (∃x,y)(1-3 hold). Suppose z = w+1. Set x = 1, y = 0. Conversely, let 1-3 hold for x,y,z,w. By the above, z = w+1.
w = uv ↔ (∃x,y,z)(1-4 hold). Suppose w = uv. Set x = 1, y = 0, z = w+1. Conversely, let 1-4 hold for x,y,z,w,u,v. By the above, w = uv. QED

LEMMA 2.2. A set of equations x=yz+1 has a solution in Z if and only if the corresponding set of equations x =-yz-1 has a solution in Z. In fact, the solutions to any set of equations x=yz+1 and to the corresponding set of equations x=-yz-1 are negatives of each other.

Proof: This follows immediately from the following observation. x = yz+1 if and only if -x = -(-y)(-z)-1. QED

THEOREM 2.3. Θ(x=yz+1), Θ(x=-yz-1) are unsolvable, and in fact complete r.e.

Proof: By Theorem 1.5 and Lemmas 2.1, 2.2. These problems are r.e. by search. QED

3. Θ(x=yz-1),Θ(x=-yz+1)

LEMMA 3.1. Let $\alpha(x) = 0$ if x is even; -1 if x is odd. Suppose $x = yz-1$. Then $\alpha(x) = \alpha(y)\alpha(z)-1$.
Let $\beta(x) = 0$ if x is even; 1 if x is odd. Suppose $x = -yz+1$. Then $\beta(x) = -\beta(y)\beta(z)+1$.

Proof: For the first claim, we argue by cases.

case 1. yz is even. Then (y is even $\vee$ z = even) $\wedge$ x is odd. Hence $\alpha(x) = -1$ and $\alpha(y)\alpha(z)-1 = 0-1 = -1$.

case 2. yz is odd. Then y,z are odd, and x is even. Hence $\alpha(x) = 0$ and $\alpha(y)\alpha(z)-1 = (-1)(-1)-1 = 0$.

For the second claim, we also argue by cases.

case 1. yz is even. Then (y is even $\vee$ z = even) $\wedge$ x is odd. Hence $\alpha(x) = 1$ and $-\alpha(y)\alpha(z)+1 = 1$.

case 2. yz is odd. Then y,z are odd, and x is even. Hence $\alpha(x) = 0$ and $-\alpha(y)\alpha(z)+1 = -(1)(1)+1 = 0$.

QED

THEOREM 3.2. A finite set of equations $x = yz-1$ has a solution in Z if and only if it has a solution in {-1,0}. A finite set of equations $x = -yz+1$ has a solution in Z if and only if has a solution in {0,1}. $\Theta(x=yz-1)$ and $\Theta(x=-yz+1)$ are solvable.

Proof: Immediate from Lemma 3.1. QED

Alternatively, we can use Lemma 2.2 for equations $x=yz-1$, $x=-yz+1$, and just analyze one of the two equations.

REFERENCES

[Da73] M. Davis, Hilbert's Tenth Problem is Unsolvable, The American Mathematical Monthly, Vol. 80, No. 3 (Mar., 1973), pp. 233-269, http://www.math.umd.edu/~laskow/713/Spring17/Diophantine.pdf

[Fr10] H. Friedman, Decision Problems in Euclidean Geometry, https://u.osu.edu/friedman.8/foundational-adventures/downloadable-manuscripts/ #64, August 29, 2010, 33 pages.

[Fr17] H. Friedman, Integer Inner Products and Algorithmic Unsolvability, https://u.osu.edu/friedman.8/foundational-adventures/downloadable-manuscripts/
#95, 23 pages, October 13, 2017.

[GS81] F. Grunewald, D. Segal. How to solve a quadratic equation in integers. Math. Proc. Cambridge Philos. Soc., 89(1):1–5 (1981)

[GS04] F. Grunewald, D. Segal, F., On the integer solutions of quadratic equations. Journal of the Reine Angew. Math., 569:13–45 (2004)

[Ma93] Y. Matiyasevich, Hilbert's Tenth Problem, MIT Press, Cambridge, Massachusetts, 1993.

[Poxx] B. Poonen, Hilbert’s tenth problem over rings of number-theoretic interest, https://math.mit.edu/~poonen/papers/aws2003.pdf.

[Po14] B. Poonen, Undecidable Problems: A Sampler, https://arxiv.org/abs/1204.0299, October 25, 2014.