# INTEGRAL PIECEWISE $F:Z^5 \to Z$ AND ALGORITHMIC UNSOLVABILITY

by
Harvey M. Friedman
Distinguished University Professor of Mathematics, Philosophy, and Computer Science Emeritus
The Ohio State University
October 26, 2017

Abstract. Is a given integral piecewise quadratic $F:Z^5 \to Z$ surjective? We show that this is algorithmically unsolvable.

Most negative results arising from the MRDP solution to Hilbert's Tenth Problem (Lemma 3 below) involve polynomials of a large number of variables or polynomials of high degree or both. See, e.g., [Ma93], p. 163, [Jo82]. Here we prove a negative result related to Hilbert's Tenth Problem - involving surjectivity - for degree 2 and 5 variables. Note that the original Hilbert's Tenth Problem - the existence of a zero - has been solved positively for degree 2 integral polynomials over Z with any number of variables; see [GS81], [GS04], [Si71]. It seems unlikely that our result is close to any border between solvability and unsolvability.

DEFINITION 1. We use Z for the set of all integers and N for the set of all nonnegative integers. An integral piecewise quadratic $F:Z^k \to Z$ is a function $F:Z^k \to Z$ defined in the following way. $F(x) = P_1(x)$ if $R_1(x)$; $P_2(x)$ if $\neg R_1(x) \wedge R_2(x)$; ...; $P_k(x)$ if $\neg R_1(x) \wedge ... \wedge \neg R_{k-1}(x) \wedge R_k(x)$; $P_{k+1}(x)$ if $\neg R_1(x) \wedge ... \wedge \neg R_k(x)$, where $k \geq 1$, each $P_i$ is an integral quadratic function, and each $R_i$ is a finite conjunction of one or more integral quadratic inequalities. This corresponds to integral piecewise linear except it is at degree $\leq 2$.

LEMMA 1. If in Definition 1, each $R_i$ is a propositional combination of integral quadratic inequalities, then $F:Z^k \to Z$ is piecewise quadratic.

Proof: Put each $R_i$ in disjunctive normal form, and use the conjuncts of the $R_i$'s. QED

LEMMA 2. The rational quadratic function $\delta:N^2 \to N$ given by $\delta(x,y) = P(x,y) = (x+y)(x+y+1)/2 + y$ is one-one onto.

Proof: This is the well known Cantor pairing function. QED

LEMMA 3. The problem of determining whether a given polynomial $P:Z^2 \to Z$ with integer coefficients has a zero over N is algorithmically unsolvable.

Proof: This is part of the MRDP theorem, which solves Hilbert's Tenth Problem over Z. See [Da73], [Ma93]. QED

LEMMA 4. There is an algorithm that converts any polynomial P with integer coefficients and variables $x_1,...,x_k$ to a finite list P* of equations of the form $x_i+x_j = x_p$, $x_ix_j = x_p$, $x_i = 1$, such that the following holds. P has a zero over N if and only if P* has a solution over N.

Proof: This well known construction proceeds as follows. Let P be as given, and write P = Q-R, where Q,R have only positive coefficients. P = 0 is therefore equivalent to Q = R. For each monomial $cy_1...y_n$, $c > 0$, $n \geq 0$, in Q,R, we first associate the set of equations $z_1 = c$, $z_2 = z_1y_1$, ..., $z_{n+1} = z_ny_n$. Now replace $z_1 = c$ by breaking into $w_1 = 1,...,w_c = w_{c-1}+w_1, z_1 = w_c$. Make sure that the new variables introduced are distinct across monomials.

We now write Q = R in the form $u_1+...+u_n = v_1+...+v_m$, since Q,R are each sums of these monomials. Here the u's and v's are among the variables introduced above. Then we introduce more new variables to break up both sums, with a final equation of the form $\alpha = \beta$, where $\alpha,\beta$ are variables. Finally, we replace $\alpha = \beta$ by the two equations $\alpha = \gamma\beta$, $\gamma = 1$. QED

LEMMA 5. There is an algorithm that converts any finite list S of equations of the form $x_i+x_j = x_p$, $x_ix_j = x_p$, $x_i = 1$, to a finite list S' of equations of the form $x_j+x_j = x_p$, $x_i^2 = x_j$, $x_i = 1$, such that the following holds. S has a solution over N if and only if S' has a solution over N.

Proof: In the context of N, we replace all $x = yz$ in favor of equations of the first two forms using the new variables a,b,c,d,e,f,g,h as follows. First replace any $x = yz$ by $2x = (y+z)^2-y^2-z^2$, and then by $a = y+z$, $b = a^2$, $c = y^2$, $d = z^2$,

$x+x = b-c-d$. Replace $x+x = b-c-d$ by $x+x+c+d = b$, and then by $e = x+x$, $f = e+c$, $g = f+d$, $g = b$. Replace $g = b$ by $g^2 = i^2$. Replace $g^2 = i^2$ by $h = i^2$, $g^2 = h$. Thus we replace $x = yz$ by

$y+z = a$
$a^2 = b$
$y^2 = c$
$z^2 = d$
$x+x = e$
$e+c = f$
$f+d = g$
$i^2 = h$
$g^2 = h$

Note that for $x,y,z \in N$, $x = yz$ if and only if there is a solution from N of these 9 equations, where $a,b,c,d,e,f,g,h$ uniquely depend on $x,y,z$, assuming $x = yz \wedge x,y,z \in N$. QED

LEMMA 6. Let $k \geq 1$. For all finite sets S of equations of the form $x_i+x_j = x_p$, $x_i^2 = x_j$, $x_i = 1$, using variables among $x_1,...,x_k$, we can effectively construct a sentence $S^* = (\forall s,t \in N)(\exists q_1,q_2,q_3 \in N)(\varphi)$ such that
i. $\varphi$ is a propositional combination of integral quadratic inequalities in $s,t,q_1,q_2,q_3$.
ii. $S^*$ if and only if S has no solution in N.

Proof: Let $S_1 = \{(i,j,p): x_i+x_j = x_p \in S\}$, $S_2 = \{(i,j): x_i^2 = x_j \in S\}$, $S_3 = \{i: x_i = 1 \in S\}$. Let W be the set of all positive integers appearing in $S_1 \cup S_2 \cup S_3$. We first claim that S has no solution $x_1,...,x_k \in N$ if and only if the following sentence A holds:

$(\forall s,t \in N)(\exists i,j,p \in W)(((i,j,p) \in S_1 \wedge$
$RES(t,is+1)+RES(t,js+1) \neq RES(t,ps+1)) \vee ((i,j) \in S_2 \wedge$
$RES(t,is+1)^2 \neq RES(t,js+1)) \vee (i \in S_3 \wedge RES(t,is+1) \neq 1))$.

Here W is finite, we treat $(\forall i,j,p \in W)$ as a disjunction, and we use we can use $i,j,p$ as positive integer scalar coefficients.

To verify the claim, suppose $x_1,...,x_k \in N$ is a solution to S. We show that A is false. By the usual Gödel construction using the Chinese remainder theorem, let $s,t \in N$ be such that for all $1 \leq i \leq k$, $x_i = RES(t,is+1)$. Then none of the

three disjuncts can hold no matter what choice of $i,j,p \in W$ is used because we have equality and not inequality. On the other hand, suppose there is no solution to S over N. We show that A holds. Let $s,t \in N$. Let $x1,...,xk$ be $RES(t,s+1),...,RES(t,kt+1)$. Since $x1,...,xk$ is not a solution to S, we can find $i,j,p \in W$ such that one of the three disjunctions holds, since some equation in S fails for $x1,...,xk$.

The part of A after $(\forall s,t \in N)$ is equivalent to a disjunction of sentences of the following forms.

$(\exists i,j,p \in S_1)(\exists q_1,q_2,q_3 \in N)(0 \leq t-q_1(is+1) < is+1 \wedge 0 \leq t-q_2(js+1) < js+1 \wedge 0 \leq t-q_3(ps+1) < ps+1 \wedge t-q_1(is+1)+t-q_2(js+1) \neq t-q_3(ps+1))$.
$(\exists i,j \in S_2)(\exists q_1,q_2 \in N)(0 \leq t-q_1(is+1) < is+1 \wedge 0 \leq t-q_2(js+1) < js+1 \wedge (t-q_1(is+1))^2 \neq t-q_2(js+1))$.
$(\exists i \in S_3)(\exists q_1 \in N)(t-q1(is+1) \neq 1)$.

By quantifier manipulations, the first and third disjuncts can be written in the form

$(\exists q_1,q_2,q_3 \in Z)(\varphi)$

where $\varphi$ is a propositional combination of integral quadratic inequalities. This is not the case for the second disjunct because of the quartic $(t-q_1(is+1))^2$. However, this can be conveniently fixed by using $q_3$ with a different role:

$(\exists q_1,q_2,q_3 \in N)(0 \leq t-q_1(is+1) < is+1 \wedge 0 \leq t-q_2(js+1) < js+1 \wedge q_3 = t-q_1(is+1) \wedge q_3^2 \neq t-q_2(js+1))$.

So the existential part of A after $(\forall s,t \in N)$ can be equivalently put in the form

$(\exists q_1,q_2,q_3 \in N)(\varphi(s,t,q_1,q_2,q_s)$

where $\varphi$ is a propositional combination of integral quadratic inequalities. QED

LEMMA 7. Let $R \subseteq N^5$ and $F:Z^5 \rightarrow Z$ be defined as follows. $F(s,t,q_1,q_2,q_3) = 2\delta(s,t)$ if $R(s,t,q_1,q_2,q_3)$; $s$ if $s < 0$; $2s+1$ if $s \geq 0 \wedge t < 0$; $-1$ otherwise. The following are equivalent.

i. F is surjective.
ii. $N \subseteq rng(F)$.
iii. $(\forall s,t \in N)(\exists q_1,q_2,q_3 \in N^5)(R(s,t,q_1,q_2,q_3))$.
If R is given by a proposition combination of integral quadratic inequalities then F is integral piecewise quadratic.

Proof: Let R,F be as given. i → ii. Assume ii. Let $s,t \in N$. Let $F(c,d,q_1,q_2,q_3) = 2\delta(s,t)$. Then the first case in the definition of F must apply, and so $F(c,d,q_1,q_2,q_3) = 2\delta(c,d) \wedge R(c,d,q_1,q_2,q_3)$. Hence $\delta(c,d) = \delta(s,t)$ and $c = s \wedge d = t$, and therefore $R(s,t,q_1,q_2,q_3)$. This establishes ii → iii.

Assume iii. Let $b \in Z$. If $b < 0$ then $F(b,...,b) = b$. Suppose $b \in 2N+1$. Then $f((b-1)/2,-1,0,0,0) = b$. Suppose $b \in 2N$. Let $\delta(s,t) = b/2$. Let $q_1,q_2,q_3 \in N$ be such that $R(s,t,q_1,q_2,q_3)$. Then $F(s,t,q_1,q_2,q_3) = 2\delta(s,t) = b$. This establishes i → ii → iii → i.

The second claim is clear from Lemma 1. QED

THEOREM 8. There is no algorithm that determines whether a given integral piecewise quadratic $F:Z^5 \to Z$ is surjective. There is no algorithm that determines whether a given integral piecewise quadratic $F:Z^5 \to Z$ attains all nonnegative values.

Proof: We reduce Hilbert's Tenth Problem over N to these problems, which is algorithmically unsolvable (Lemma 3). Let $P:N^k \to Z$ be an integral polynomial. Then P has a zero over N if and only if the P* of Lemma 4 has a solution over N if and only if the S' of Lemma 5 has a solution over N if and only if the sentence S* of Lemma 6 is true if and only if the corresponding function F of Lemma 7 is surjective if and only if this F has $N \subseteq rng(F)$. QED

# 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

[Fr17] H. Friedman, Integer inner products and algorithmic unsolvability, October 20, 2017, https://u.osu.edu/friedman.8/foundational-adventures/downloadable-manuscripts/, #95.

[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)

[Jo82] J. Jones, Universal Diophantine equation, Journal of Symbolic Logic, 47(3):549-571.

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

[Si72] C.L. Siegel, “Zur Theorie der quadratische Formen”. Nachr. Akad. Wiss. Göttingen MTH.-Phys. Kl. II (1972), 21-46.