DECISION PROBLEMS IN EUCLIDEAN GEOMETRY

Harvey M. Friedman*
Ohio State University
August 29, 2010
ADVANCED DRAFT

Abstract. We show the algorithmic unsolvability of a number of decision procedures in ordinary two dimensional Euclidean geometry, involving lines and integer points. We also consider formulations involving integral domains of characteristic 0, and ordered rings. The main tool is the solution to Hilbert's Tenth Problem. The limited number of facts used from recursion theory are isolated at the beginning.

0. Preliminaries.

We show the algorithmic unsolvability of a number of decision procedures in ordinary two dimensional Euclidean geometry. The main tool is the solution to Hilbert's Tenth Problem.

More generally, we demonstrate algorithmic reductions between various decision problems in two dimensional Euclidean geometry over integral domains of characteristic zero, and ordered rings, with (variants of) Hilbert's 10th Problem for such rings.

All of our algorithmic reductions are uniform in the rings from the category of rings. Thus we view the reductions as algebraic or geometric, rather than combinatorial.

The basic construction that drives the result is a reduction of ring addition and ring multiplication in any integral domain of characteristic zero, to collinear relations, through Lemmas 1.3 and 1.5. For addition, the realizations of the collinear relations are unique as stated in Lemma 1.3. However, for multiplication, the realizations are not unique (see Lemma 1.5).

We begin with a brief account of the relevant background from recursion theory. It is convenient to work within a fixed "universal" space that is rich enough to naturally support the kind of finitary objects that our algorithms operate on.

Accordingly, we use the least set T that contains the integers and the 52 lower case and upper case alphabetic characters, and where every finite sequence from T (possibly empty) is an element of T.

We use the basic notion of partial recursive $f:T \to T$ from recursion theory. Informally, this is a partial function from T into T such that the following holds. There exists an algorithm such that at each input $x \in T$, if $f(x) = y$ then the algorithm yields the output y; if $f(x)$ is undefined, then the algorithm yields no output.

A recursive $f:T \to T$ is a partial recursive $f:T \to T$ whose domain is T. A recursive subset of T is a subset of T whose characteristic function is recursive. An r.e. (recursively enumerable) subset of T is the domain of a partial recursive $f:T \to T$.

Let $A,B \subseteq T$. We say that A is reducible to B if and only if there is a recursive $f:T \to T$ such that for all $x \in T$, $x \in A \leftrightarrow f(x) \in B$. This is written $A \leq B$. We write $A \geq B$ if and only if $B \leq A$.

It is obvious that $\leq$ is a reflexive and transitive relation.

We say that $A \subseteq T$ is complete r.e. if and only if A is r.e. and for all r.e. $B \subseteq T$, $B \leq A$.

Let $A,B \subseteq T$. We write $A \equiv B$ if and only if there exists a recursive bijection $f:A \to B$ such that for all $x \in T$, $x \in A \leftrightarrow f(x) \in B$. This is the strongest notion of equivalence that is normally studied in recursion theory.

We have the following well known fundamental result.

THEROEM 0.1. There exist complete r.e. sets $A \subseteq T$. If $A,B \subseteq T$ are complete r.e. then A,B are not recursive, and $A \equiv B$. If $A \subseteq T$ is complete r.e., $B \subseteq T$ is r.e., and $A \leq B$, then B is complete r.e.

Proof: See [Roxx] and [Soxx]. QED

In this setup, a problem is merely a subset of T. A problem is solvable if and only if it is a recursive subset of T.

We now state Hilbert's 10th Problem for any ring J. There are many results and open questions regarding H10(J) for various rings J. See [Po03] for a survey.

H10(J). Does a given finite list of polynomials with integer coefficients have a common zero in J?

An ordered ring is a commutative ring J with unit, and a reflexive linear ordering $\leq$, such that for all $a,b,c \in J$,

$$a \leq b \rightarrow a+c \leq b+c, \text{ and}$$
$$0 \leq a,b \rightarrow 0 \leq ab.$$

H10(J) is more commonly stated for a single polynomial. This is "equivalent" to H10(J) for ordered rings in the following strong sense.

THEOREM 0.2. If J is an ordered ring then H10(J) is reducible to H10(J) for single polynomials. The reduction is uniform in ordered rings J.

Proof: Let $P_1,\ldots,P_n$ be polynomials with integer coefficients. We can assume that they are all in variables $v_1,\ldots,v_k$. Let J be an ordered ring. Then

$$(\exists v_1,\ldots,v_k \in J)(P_1(v_1,\ldots,v_k) = 0 \wedge \ldots \wedge P_n(v_1,\ldots,v_k) = 0)$$
$$\leftrightarrow$$
$$(\exists v_1,\ldots,v_k \in J)(P_1(v_1,\ldots,v_k)^2 + \ldots + P_n(v_1,\ldots,v_k)^2 = 0).$$

QED

Theorem 0.2 holds for a wider class of rings. See section 6.

The following modified form of H10 plays an important role.

H10(J\{0}). Does a given finite list of polynomials with integer coefficients have a common zero in J\{0}?

An integral domain is a commutative ring J with unit, where for all $a,b \in J$,

$$ab = 0 \rightarrow a = 0 \vee b = 0.$$

A ring of characteristic zero is a ring where 0 is not the sum of one or more 1's.

Every ordered ring is an integral domain of characteristic zero.

If J is an ordered ring, then we write J^+ for the set of all positive elements of J. Here is another special case of Hilbert's Tenth Problem that plays an important role.

$H10(J^+)$. Does a given finite list of polynomials with integer coefficients have a common zero in J^+?

What can we say about the relationship between $H10(J)$, $H10(J\backslash\{0\})$, $H10(J^+)$?

THEOREM 0.3. For all rings J, $H10(J) \leq H(J\backslash\{0\})$. For all fields J, $H10(J\backslash\{0\}) \leq H10(J)$. For all ordered fields J, where every positive element has a square root, $H10(J) \leq\geq H10(J^+)$. For some subfield J of the reals, $H10(J^+) \leq H10(J)$ fails.

Proof: Let J be a ring. Let P be a polynomial with integer coefficients. P has a zero in J if and only if P has a zero in $J\backslash\{0\} + J\backslash\{0\}$. If J is a field, we can write

$(\exists v_1,\ldots,v_n \neq 0)(P_1(v_1,\ldots,v_k) = 0 \wedge \ldots \wedge P_n(v_1,\ldots,v_k) = 0)$
$\leftrightarrow$
$(\exists v_1,\ldots,v_{2k})(P_1(v_1,\ldots,v_k) = 0 \wedge \ldots \wedge P_n(v_1,\ldots,v_k) = 0 \wedge v_1 \bullet v_{k+1} = 1 \wedge \ldots v_k \bullet v_{2k} = 1)$,

If J is an ordered field where every positive element has a square root, we can write

$(\exists v_1,\ldots,v_k > 0)(P_1(v_1,\ldots,v_k) = 0 \wedge \ldots \wedge P_n(v_1,\ldots,v_k) = 0)$
$\leftrightarrow$
$(\exists v_1,\ldots,v_{2k})(P_1(v_1,\ldots,v_k) = 0 \wedge \ldots \wedge P_n(v_1,\ldots,v_k) = 0 \wedge v_1 \bullet v_{k+1} = 1 \wedge \ldots v_k \bullet v_{2k} = 1 \wedge v_{k+1}^2 = \pm v_1 \wedge \ldots v_{2k}^2 = \pm v_k) \leftrightarrow$
$(\exists v_1,\ldots,v_{2k})$(a conjunction of disjunctions of polynomial equations) $\leftrightarrow$
$(\exists v_1,\ldots,v_{2k})$(a conjunction of polynomial equations)

using products of polynomials.

Let x be any transcendental real number. Consider the subfield Q<x> of $\mathfrak{R}$ generated by Q and x. Clearly Q<x> is, field theoretically, the field Q with a single transcendental element adjoined. Hence H10(Q<x>) is r.e.

However, H10(Q<x>$^+$) will have Turing degree at least that of x (as a left Dedekind cut). So H10(Q<x>$^+$) ≤ H10(Q<x>) fails for x of Turing degree > 0'. QED

In this paper we will only consider integral domains of characteristic zero.

The following is well known.

THEOREM 0.4. H10(Z), H10(Z$^+$) are complete r.e. H10(Q) ≤≥ H10(Q$^+$).

Proof: From the solution to Hilbert's Tenth Problem over Z, H10(Z), H10(Z$^+$) are complete r.e. See ??? By Theorem 0.2, H10(Q) ≤ H10(Q$^+$). Now let P1,...,Pn be a finite list of polynomials with integer coefficients. Then. using Lagrange's four squares theorem,

$(\exists v_1,...,v_k \in Q^+)(P_1(v_1,...,v_k) = 0) \wedge ... \wedge P_n(v_1,...,v_k) = 0) \leftrightarrow$
$(\exists v_1,...,v_k \in Q)(P(v_1,...,v_k) \wedge v_1,...,v_k$ are each sums of four squares $\wedge$ $v_1,...,v_k$ each have multiplicative inverses)

which can be put in the form of an existentialized conjunction of equations, with quantifiers ranging over Q, and then an existentialized equation, with quantifiers ranging over Q. QED

It is not known if H10(Q) is recursive.

We establish reductions between H10(J), H10(J\{0}), H10(J$^+$), and various decision problems of a geometric nature in J^2, where J is an integral domain of characteristic zero, and in some contexts, where J is an ordered ring.

Fix an integral domain J of characteristic zero. The lines in J^2 are the subsets of J^2 of the form

$$\{(x,y) \in J^2: ax + by = c\},$$
$$a,b,c \in J,\ a \neq 0 \vee b \neq 0$$

which have at least one element.

Integral domains of characteristic zero are adequate for treating lines in two dimensional space, as indicated by Theorem 0.5.

THEOREM 0.5. Every line in J^2 has infinitely many elements. Let $(d,e),(f,g) \in J^2$ be distinct. There is a unique line containing $(d,e),(f,g)$. If $d = f$, it is defined by the equation $x = d$. If $e = g$, it is defined by the equation $y - e$. Otherwise, it is defined by the equation $(g-e)(x-d) = (f-d)(y-e)$. The intersection of any two distinct lines has cardinality at most 1.

Proof: Let $ax + by = c$ be given, $a \neq 0 \vee b \neq 0$. If $a = 0$ then $ax + by = c$ has the solutions (n,y), where (x,y) is a solution.

Now suppose $a \neq 0$ and $ax + by = c$. Then $a(x+nb) + b(y-na) = c$, where $n \in Z$. This provides infinitely many solutions.

Let $d,e,f,g \in J$, $(d,e) \neq (f,g)$. Set $a = e-g$, $b = f-d$, $c = d(e-g) + e(f-d) = f(e-g) + g(f-d)$. Then $ax + by = c$ defines a line containing $(d,e),(f,g)$.

Now let $(d,e) \neq (f,g) \in J2$. Suppose $d = f$. Then $e \neq g$. The line defined by $x = d$ contains $(d,e),(f,g)$. Suppose $ax + by = c$ defines a line L containing $(d,e),(f,g)$. Then $ad + be = ad + bg$, and so $be = bg$, $b(e-g) = 0$, and hence $b = 0$, $a \neq 0$. Hence L is defined by $ax = c$. Hence $c = ad$, and L is defined by $ax = ad$. This is the same as the line defined by $x = d$.

The same argument shows that if $e = g$ then the line containing $(d,e),(f,g)$ must be defined by $y = e$.

Now we assume $d \neq f \wedge e \neq g$. Let $ax + by = c$, $a'x + b'y = c'$ define lines that both contain $(d,e),(f,g)$. Clearly $a,b,a',b' \neq 0$. We have

$$
\begin{aligned}
&ad + be = af + bg = c\\
&a'd + b'e = a'f + b'g = c'\\
&a(d-f) = b(g-e)\\
&a'(d-f) = b'(g-e)\\
&ab'(d-f)(g-e) = a'b(d-f)(g-e)\\
&ab' = a'b\\
&a'ad + a'be = a'c\\
&aa'd + ab'e = ac'\\
&a'c = ac'
\end{aligned}
$$

We are ready to show that the lines are equal. Let $ax + by = c$. Then $a'c = aa'x + ba'y = aa'x + ab'y = ac'$. Hence $a'x + b'y = c'$. Let $a'x + b'y = c'$. Then $ac' = aa'x + ab'y = aa'x + a'by = a'c$. Hence $ax + by = c$.

Obviously, $(g-e)(x-d) = (f-d)(y-e)$ defines a line - and hence the line - containing $(d,e),(f,g)$.

Suppose L_1,L_2 are two distinct lines each containing $x \neq y$ from J^2. This violates the uniqueness of the line containing any two distinct points. QED

In the definitions below, we use x_i, $i \geq 1$, for variables representing unknown elements of J^2.

In the case of line, parallel, and equidistance, the definitions below make clear sense for integral domains of characteristic zero. For betweenness, we assume J is an ordered ring. We use the canonical embedding of Z into any ring of characteristic zero.

A line condition is an assertion

α,β,γ lie on a common line in J^2
written $[\alpha,\beta,\gamma]$

where each of α,β,γ is a variable x_i, $i \geq 1$, or a specific element of Z^2. E,g,$[[x_5,(0,-5),x_4]$. Note that $[y,y,z]$ holds for all $y \in J^2$ by Theorem 0.4.

A parallel condition is an assertion

the line $\alpha\beta$ is parallel to the line $\gamma\delta$
written $\alpha\beta||\gamma\delta$

where each of $\alpha,\beta,\gamma,\delta$ is a variable x_i, $i \geq 1$, or a specific element of Z^2. E.g., $x_5,(0,-5)||(3,4)(3,4)$. In order for this to hold, we require $\alpha \neq \beta$, $\gamma \neq \delta$, and the line containing α,β is disjoint from the line containing γ,δ.

Equidistance is defined in an ordered ring as follows. Let $(a,b),(c,d),(e,f),(g,h) \in J^2$. We say that $(a,b)(c,d)$ and $(e,f)(g,h)$ are equidistant if and only if

$$(a-c)^2 + (b-d)^2 = (e-g)^2 + (f-h)^2.$$

An equidistance condition is an assertion

α,β and γ,δ are equidistant, and $\alpha \neq \beta$, $\gamma \neq \delta$
written $\alpha\beta$ E $\gamma\delta$

where each of $\alpha,\beta,\gamma,\delta$ is a variable x_i, $i \geq 1$, or a specific element of Z^2. E.g., $x_5(0,-5)$ E $(3,4)(3,4)$.

Betweenness is defined in an ordered ring as follows. Let $(d,e),(f,g),(h,i) \in J^2$. We say that (f,g) is between (d,e) and (b,i) if and only if

$$\begin{gathered} (d,e),(f,g),(h,i) \text{ are distinct} \\ (d,e),(f,g),(h,i) \text{ lie on a common line} \\ d < f < h \vee h < f < d \vee \\ e < g < i \vee i < g < e. \end{gathered}$$

A betweenness condition, or b-condition, is an assertion

$$\begin{gathered} \beta \text{ lies strictly between } \alpha \text{ and } \gamma \\ \text{written } <\alpha,\beta,\gamma> \end{gathered}$$

where each of α,β,γ is a variable xi, $i \geq 1$, or a specific element of Z^2. E.g., $<x_5,(0,-5),x_4>$.

Note that we have presented four kinds of conditions. A condition over $V \subseteq Z^2$ is a condition whose constants pairs all lie in V.

We consider finite sets of conditions, W. A realization of W in J is a sequence $x_1,\ldots,x_n \in J^2$ such that all conditions in W hold. This requires that all variables used in W be among $x_1,\ldots,x_n$.

Below, LDP, PDP, EDP, BDP are read "line decision problem", "parallel decision problem, "equidistance decision problem", "betweenness decision problem", respectively.

For LDP, PDP, EDP we assume that J is an integral domain of characteristic zero. For BDP, we assume that J is an ordered ring.

LDP(J,V), PDP(J,V), EDP(J,V), BDP(J,V),. Does a given finite set of line, betweenness, parallel, equidistance conditions, respectively, over V, have a realization in J?

LDP(J;n), PDP(J;n), EDP(J;n), BDP(J;n). Does a given list of at most n line, betweenness, parallel, equidistance conditions, respectively, have a realization in J?

It is clear that each of these problems can be naturally viewed as single subsets of our "universal" space T.

In connection with our results on LDP(J;n), BDP(J;n), PDP(J;n), EDP(J;n), we use J (and $J\backslash\{0\}$, J^+) Diophantine sets. These can have any dimension and take the respective form

$$\{x \in Z^k\text{: } (\exists y \in J^r)(P_1(x,y) = 0 \wedge \ldots \wedge P_n(x,y) = 0)\}$$
$$\{x \in Z^k\text{: } (\exists y \in (J\backslash\{0\})^r)(P_1(x,y) = 0 \wedge \ldots \wedge P_n(x,y) = 0)$$
$$\{x \in Z^k\text{: } (\exists y \in J^{+r})(P_1(x,y) = 0 \wedge \ldots \wedge P_n(x,y) = 0)\}.$$

In the crucial case where J is the ring of integers, Z, we prove the unsolvability of LDP(Z,Z^2), PDP(Z,Z^2), EDP(Z,Z^2), BDP(Z,Z^2), as well as LDP(Z;n), PDP(Z;n), EDP(Z;n), BDP(Z;n) for sufficiently large n. In fact, we show that these problems are complete r.e.

1. Realizing Colinearity.

LDP TABLE

Unsolvability for LDP with Z

LDP(Z,Z^2), LDP(Z,{0,1,2} × {0,1}) are complete r.e. For sufficiently large n, LDP(Z;n) is complete r.e.

Reductions for LDP with Integral Domain J
of Characteristic Zero

LDP(J,Z) $\leq\geq$ LDP(J,{0,1,2} × {0,1}) $\leq\geq$ H10(J).
Every J Diophantine set is $\leq$ some LDP(J;n).
Every LDP(J;n) is $\leq\geq$ some J Diophantine set.
Reductions and n are constructed uniformly in J.

In this section, we will establish all claims in the LDP Table.

We will use C (or Ci) for finite sets of line conditions. Here "C" indicates "collinearity".

We say that C uses $x_1,\ldots,x_n$ if and only if all variables present in C are among $x_1,\ldots,x_n$.

Throughout this section, fix J to be an integral domain of characteristic zero.

LEMMA 1.1. There exists C over {0,1,2} × {0,1} using $x_1,\ldots,x_{19}$ whose unique realization $x_1,\ldots,x_{19}$ is an enumeration of $\{0,\ldots,4\}^2\backslash(\{0,1,2\} \times \{0,1))$.

Proof: Consider the diagram

x_{15}	x_{16}	x_{17}	x_{18}	x_{19}
x_{10}	x_{11}	x_{12}	x_{13}	x_{14}
x_5	x_6	x_7	x_8	x_9
(1,0)	(1,1)	(1,2)	x_3	x_4
(0,0)	(1,0)	(2,0)	x_1	x_2

Take C to consist of all line conditions satisfied by this diagram if this diagram is interpreted as a layout of $\{0,...,4\}^2$ in the obvious way. Obviously, we have a realization $x_1,...,x_{19}$ of C where $x_1,...,x_{19}$ is the enumeration of $\{0,...,4\}^2\backslash(\{0,1,2\} \times \{0,1))$ given by the diagram.

Now suppose that we have a realization $x_1,...,x_{19}$ of C.

Note that x_5,x_7 each lie on two determined lines, and so must have their correct values.

Then x_6 is on two determined lines, and so must have its correct value. Hence x_8,x_1 are each on two determined lines, and so they have their correct values. Hence x_3 is on two determined lines, and so it is also has its correct value.

Hence x_9,x_2 are on two determined lines, and so they have their correct values. Hence x_4 is on two determined lines, and so it has its correct value.

Thus we have taken care of the bottom three rows. Now note that each entry in the next higher row is on two determined lines, and so they have their correct values. Then the entries in the top row are also each on two determined lines, and so they must have their correct values. QED

LEMMA 1.2. $LDP(J,\{0,...,4\}^2) \leq LDP(J,\{0,1,2\} \times \{0,1\})$.

Proof: Immediate from Lemma 1.1. The reduction is uniform in J. QED

In light of Lemma 1.2, we will focus on finite sets of line conditions over $\{0,...,4\}^2$.

LEMMA 1.3. There exists C_1 over $\{0,...,4\}^2$ using $x_1,...,x_7$, whose realizations $x_1,...,x_7$ are exactly the $x_1,...,x_7$ such that for some $z,w \in J$,
$x_1 = (z,1)$.
$x_2 = (w,1)$.

$x_3 = (2z,0)$.
$x_4 = (2z,2)$.
$x_5 = (2w,0)$.
$x_6 = (2w,2)$.
$x_7 = (z+w,1)$.

Proof: Let C_1 consist of the line conditions

1. $[(0,1),(1,1),x_1]$
$[(0,1),(1,1),x_2]$

2. $[(0,2),x_1,x_3]$
$[(0,0),(1,0),x_3]$

3. $[(0,0),x_1,x_4]$
$[(0,2),(1,2),x_4]$

4. $[(0,2),x_2,x_5]$
$[(0,0),(1,0),x_5]$

5. $[(0,0),x_2,x_6]$
$[(0,2],(1,2),x_6]$

6. $[x_3,x_6,x_7]$
$[x_5,x_4,x_7]$
$[(0,1),(1,1),x_7]$

Suppose $x_1,\ldots,x_7$ obey the equations for some $z,w \in J$. Then $x_1,\ldots,x_7$ is a realization of C_1 by inspection.

Conversely, Let $x_1,\ldots,x_7$ be a realization of C_1.

Group 1 guarantees that x_1,x_2 lie on the line $y = 1$. So write $x_1 = (z,1)$, $x_2 = (w,1)$.

Group 2 guarantees that x_3 lies on the x axis and the line containing (0,2) and (z,1). Hence $x_3 = (2z,0)$.

Group 3 guarantees that x_4 lies on the line $y = 2$, and the line containing (0,0) and (z,1). Hence $x_4 = (2z,2)$.

Group 4 guarantees that x_5 lies on the x axis and the line containing (0,2) and (w,1). Hence $x_5 = (2w,0)$.

Group 5 guarantees that x_6 lies on the line $y = 2$ and the line containing (0,0) and (w,1). Hence $x_6 = (2w,2)$.

Group 6 guarantees that x_7 lies on the line containing (2z,0),(2w,2), the line containing (2w,0),(2z,2), and the line y = 1. If z ≠ w then x_7 = (z+w,1). If z = w then x_7 lies on the line x = 2z and the line y = 1. Hence x_7 = (2z,1) = (z+w,1). QED

LEMMA 1.4. There exists C_2 over $\{0,...,4\}^2$ using $x_1,...,x_{22}$, such that
i. If $x_1,...,x_{22}$ is a realization of C_2, then the second coordinates of x_1,x_2,x_{22} are 1.
ii. The realizations $x_1,...,x_{22}$ where the first coordinate of x_2 is nonzero are exactly the $x_1,...,x_{22}$ such that for some z,w ∈ J with w ≠ 0,
x_1 = (z,1).
x_2 = (w,1).
x_3 = (2z,0).
x_4 = (2z,2).
x_5 = (2w,0).
x_6 = (2w,2).
x7 = (2w,4).
x8 = (w,2).
x9 = (w,w).
x10 = (2w,w)
x11 = (2w,2w).
x12 = (zw,w).
x13 = (4w,4).
x14 = (2,8).
x15 = (4,8).
x16 = (4w,8).
x17 = (4w,2w).
x18 = (2z,1).
x19 = (2zw,w).
x20 = (2zw,2w).
x21 = (2zw,2).
x22 = (zw,1).

Proof: Let C_2 consist of the 21 pairs of line conditions

1. [(0,1),(1,1),x_1]
[(0,1),(1,1),x_2]

2. [(0,2),x_1,x_3]
[(0,0),(1,0),x_4]

3. [(0,0),x_1,x_4]
[(0,2),(1,2),x_4]

4. [(0,2),x_2,x_5]

$[(0,0),(1,0),x_5]$

5. $[(0,0),x_2,x_6]$
$[(0,2),(1,2),x_6]$

6. $[x_5,x_6,x_7]$
$[(0,4),(1,4),x_7]$

7. $[(0,0),x_7,x_8]$
$[(0,2),(1,2),x_8]$

8. $[(0,0),(1,1),x_9]$
$[x_2,x_8,x_9]$

9. $[x_5,x_6,x_{10}]$
$[(0,0),(2,1),x_{10}]$

10. $[(0,0),(1,1),x_{11}]$
$[x_5,x_6,x_{11}]$

11. $[x_9,x_{10},x_{12}]$
$[(0,0),x_1,x_{12}]$

12. $[(0,0),x_2,x_{13}]$
$[(0,4),(1,4),x_{13}]$

13. $[(0,0),(1,4),x_{14}]$
$[(2,0),(2,1),x_{14}]$

14. $[(0,0),(2,4),x_{15}]$
$[(4,0),(4,1),x_{15}]$

15. $[(0,0),x_8,x_{16}]$
$[x_{14},x_{15},x_{16}]$

16. $[(0,0),(2,1),x_{17}]$
$[x_{13},x_{16},x_{17}]$

17. $[x_3,x_4,x_{18}]$
$[(0,1),(1,1),x_{18}]$

18. $[(0,0),x_{18},x_{19}]$
$[x_9,x_{10},x_{19}]$

19. $[(0,0),x_1,x_{20}]$
$[x_{11},x_{17},x_{20}]$

20. $[x_{19},x_{20},x_{21}]$

$[(0,2),(1,2),x_{21}]$

21. $[(0,0),x_{21},x_{22})]$
$[(0,1),(1,1),x_{22}]$

Note that i) is immediate by groups 1, 21 of the line conditions above.

Let $x_1,...,x_{22}$ and $z,w \in J$, $w \neq 0$, where the 22 equations hold. Then by inspection, $x_1,...,x_{22}$ is a realization of C_2.

Now let $x_1,...,x_{22}$ be a realization of C_2, where the first coordinate of x_2 is nonzero. Set z to be the first coordinate of x_1 and w the first coordinate of x_2. Then $w \neq 0$.

Group 1 of the line conditions guarantee that x_1 and x_2 lie on the line $y = 1$. Hence $x_1 = (z,1)$, $x_2 = (w,1)$.

Group 2 guarantees that x_3 lies on the line containing $(0,2)$ and $(z,1)$, and on the x axis. Hence $x_3 = (2z,0)$.

Group 3 guarantees that x_4 lies on the line containing $(0,0)$ and $(z,1)$, and the line $y = 2$. Hence $x_4 = (2z,2)$.

Group 4 guarantees that x_5 lies on the line containing $(0,2)$ and $(w,1)$, and the x axis. Hence $x_5 = (2w,0)$.

Group 5 guarantees that x_6 lies on the line containing $(0,0)$ and $(w,1)$, and the line $y = 2$. Hence $x_6 = (2w,2)$.

Group 6 guarantees that x_7 lies on the line $x = 2w$ and the line $y = 4$. Hence $x_7 = (2w,4)$.

Group 7 pair guarantees that x_8 lies on the line containing $(0,0)$ and $(2w,4)$, and the line $y = 2$. Hence $x_8 = (w,2)$.

Group 8 guarantees that x_9 lies on the line containing $(0,0)$ and $(1,1)$, and the line $x = w$. Hence $x_9 = (w,w)$.

Group 9 guarantees that x_{10} lies on the line $x = 2w$ and the line containing $(0,0)$ and $(2,1)$. Hence $x_{10} = (2w,w)$.

Group 10 guarantees that x_{11} lies on the line containing $(0,0)$ and $(1,1)$, and the line $x = 2w$. Hence $x_{11} = (2w,2w)$.

Group 11 guarantees that x_{12} lies on a line containing (w,w) and (2w,w). and the line containing (0,0) and (z,1). Since $w \neq 0$, x_{12} lies on the line y = w. Hence x_{12} = (zw,w).

Group 12 guarantees that x_{13} lies on the line containing (0,0) and (w,1), and the line y = 4. Hence x_{13} = (4w,4).

Group 13 guarantees that x_{14} lies on the line containing (0,0) and (1,4), and the line x = 2. Hence x_{14} = (2,8).

Group 14 guarantees that x_{15} lies on the line containing (0,0) and (2,4), and the line x = 4. Hence x_{15} = (4,8).

Group 15 guarantees that x_{16} lies on the line containing (0,0) and (w,2), and the line x = 4w. Hence x_{16} = (4w,8).

Group 16 guarantees that x_{17} lies on the line containing (0,0) and (2,1), and the line x = 4w. Hence x_{17} = (4w,2w).

Group 17 guarantees that x_{18} lies on the line x = 2z and the line y = 1. Hence x_{18} = (2z,1).

Group 18 guarantees that x_{19} lies on the line containing (0,0) and (2z,1), and a line containing (w,w) and (2w,w). Since $w \neq 0$, x_{19} lies on the line y = w. Hence x_{19} = (2zw,w).

Group 19 guarantees that x_{20} lies on the line containing (0,0) and (z,1), and a line containing (2w,2w) and (4w,2w). Since $w \neq 0$, x_{20} lies on the line y = 2w. Hence x_{20} = (2zw,2w).

Group 20 guarantees that x_{21} lies on a line containing (2zw,w) and (2zw,2w), and the line y = 2. Since $w \neq 0$, x_{20} lies on the line x = 2zw. Hence x_{21} = (2zw,2).

Group 21 guarantees that x22 lies on the line containing (0,0) and (2zw,2), and the line y = 1. Hence x_{22} = (zw,1).

QED

LEMMA 1.5. There exists C_3 over $\{0,\ldots,4\}^2$ using $x_1,\ldots,x_{22}$, such that
i. For all $z,w \in J$, the $x_1,\ldots,x_{46}$ given by the equations below is a realization of C_3.
ii. If $x_1,\ldots,x_{46}$ is a realization of B_3, then there exists $z,w \in J$ such that x_1 = (z,1), x_2 = (w,1), and x_{22} = (zw,1).
x_1 = (z,1).
x_2 = (w,1).

x23 = (z,1)
x24 = (w+1,1)

x_3 = (2z,0).
x_4 = (2z,2).
x_5 = (2w,0).
x_6 = (2w,2).
x7 = (2w,4).
x8 = (w,2).
x9 = (w,w).
x10 = (2w,w)
x11 = (2w,2w).
x12 = (zw,w).
x13 = (4w,4).
x14 = (2,8).
x15 = (4,8).
x16 = (4w,8).
x17 = (4w,2w).
x18 = (2z,1).
x19 = (2zw,w).
x20 = (2zw,2w).
x21 = (2zw,2).
x22 = (zw,1).
x45 = (2zw,0).
x46 = (2zw,2).

x25 = (2z,0).
x26 = (2z,2)
x27 = (2(w+1)),0)
x28 = (2(w+1),2)
x29 = (2(w+1),4)
x30 = (w+1,2)
x31 = (w+1,w+1)
x32 = (2(w+1),w+1)
x33 = (2(w+1),2(w+1))
x34 = (z(w+1),w+1)
x35 = (4(w+1),4)
x36 = (2,8)
x37 = (4,8)
x38 = (4(w+1),8)
x39 = (4(w+1),2(w+1))
x40 = (2z,1)
x41 = (2z(w+1),w+1)
x42 = (2z(w+1),2(w+1))
x43 = (2z(w+1),2)
x44 = (z(w+1),1)

Proof: Note that $x_1,\ldots,x_{22}$ is the same as in Lemma 1.4, and $x_{23},\ldots,x_{44}$ is the same as $x_1,\ldots,x_{22}$, except w is replaced by w+1. Let C_3 consist of the line conditions in C_2, the line conditions in C_2 with all subscripts incremented by 22, and the following additional line conditions.

1. $[x_1,x_{23},(0,0)]$
$[x_1,x_{23},(1,0)]$
$[x_1,x_{23},(0,1)]$

2. $[(2,0),x_6,x_{24}]$
$[(2,2),x_5,x_{24}]$

3. $[(0,2),x_{22},x_{45}]$
$\{(0,0),(1,0),x_{45}]$

4. $[(0,0),x_{22},x_{46}]$
$[(0,2),(1,2),x_{46}]$

5. $[x_{25},x_{46},x_{44}]$
$[x_{26},x_{45},x_{44}]$

Suppose that $x_1,\ldots,x_{46}$ obeys the above equations for some $z,w \in J$. Then $x_1,\ldots,x_{46}$ is a realization of C_3 by inspection.

Now let $x_1,...,x_{46}$ be a realization of C3. By Lemma 1.4, $x_1,x_2,x_{23},x_{24},x_{44}$ lie on the line $y = 1$. Write $x_1 = (z,1)$, $x_2 = (w,1)$. Write $x_{22} = (\alpha,1)$. We will show that $\alpha = zw$.

Group 1 guarantees that (0,0),(1,0),(0,1) each lie on some line containing x_1,x_{23}. If $x_1 \neq x_{23}$ then (0,0),(1,0),(0,1) each lie on the line containing x_1,x_{23}, which is impossible. Hence $x_1 = x_{23} = (z,1)$.

Group 2 guarantees that x_{24} lies on the line containing (2,0) and (2w,2), the line containing (2,2) and (2w,0). Furthermore, x_{24} lies on the line $y = 1$. If $2 \neq 2w$ then $x_{24} = (w+1,1)$. If $2 = 2w$ then x_{24} lies on the line $x = 2$. Hence $x_{24} = (2,1)$, and so $x_{24} = (w+1,1)$.

Group 3 guarantees that x_{45} lies on the line containing (0,2) and $(\alpha,1)$, and the x axis. Hence $x_{45} = (2\alpha,0)$.

Group 4 guarantees that x_{46} lies on the line containing (0,0) and $(\alpha,1)$, and the line $y = 2$. Hence $x_{46} = (2\alpha,2)$.

Group 5 guarantees that x_{44} lies on the line containing (2z,0) and $(2\alpha,2)$, and the line containing (2z,2) and $(2\alpha,0)$. Furthermore, x_{44} lies on the line $y = 1$. If $2z \neq 2\alpha$ then $x_{44} = (z+\alpha,1)$. If $2z = 2\alpha$ then x_{44} lies on the line $x = 2z$, and $x_{44} = (2z,1) = (z+\alpha,1)$.

case 1. $w \neq 0$. By Lemma 1.4, $x_{22} = (zw,1)$.

case 2. $w = 0$. Since $x_{23} = (z,1)$, $x_{24} = (w+1,1)$, we see that by Lemma 1.4, $x_{44} = (zw+z,1) = (z+\alpha,1)$. Hence $\alpha = zw$, and so $x_{22} = (zw,1)$.

QED

Note that Lemma 1.3 provides an interpretation of addition for $z,w \in J$, using x_1,x_2,x_7, and Lemma 1.5 gives us an interpretation of multiplication for $z,w \in J$, using x_1,x_2,x_{22}, all in terms of realizations.

Specifically, in all realizations of C_1, $x_7 = x_1 + x_2$ in first coordinates. In all realizations of C_3, $x_{22} = x_1 \bullet x_2$ in first coordinates. Also, in all realizations of C1, x_1,x_2,x_7 lie on the line $y = 1$, and in all realizations of C_3, x_1,x_2,x_{22} lie on the line $y = 1$.

Fix a polynomial $P(v_1,...,v_k)$ with integer coefficients. We are going to construct a set P# of equations associated with the equation $P(v_1,...,v_k) = 0$.

First write P in the form

$$Q_1 + ... + Q_m - (R_1 + ... + R_t)$$

where the Q's and R's are monomials with coefficient 1.

Use the variables $v_{k+1},...,v_{k+m+t}$ for $Q_1,...,Q_m,R_1,...,R_t$, respectively. We want to use the equations

$$\begin{gathered} v_{k+1} = Q_1 \\ ... \\ v_{k+m} = Q_m \\ v_{k+m+1} = R_1 \\ ... \\ v_{k+m+t} = R_t \end{gathered}$$

which need to be broken down in the obvious way by introducing yet more variables, with multiplicative equations of the form $a = b \bullet c$, for variables a,b,c.

Finally, we want to use the equation

$$v_{k+1} + ... + v_{k+m} = v_{k+m+1} + ... + v_{k+m+t}$$

which also needs to be broken down in the obvious way by introducing even more variables, with additive equations of the form $a = b + c$, for variables a,b,c.

This results in the list P# of equations of the forms

$$\begin{gathered} v_i = v_j + v_k \\ v_i = v_j \bullet v_k \\ v_i = v_j \\ v_i = 1 \end{gathered}$$

The use of $v_i = v_j$ and $v_i = 1$ will safely take care of various degenerate cases. We arrange for the variables in P# to be exactly $v_1,...,v_{k'}$, $1 \leq k < k'$.

We generalize this construction as follows. Let $P_1(v_1,...,v_k),...,P_n(v_1,...,v_k)$ be polynomials with integer coefficients. For each $P_i(v_1,...,v_k)$, we create P_i#. We make sure that the variables introduced for the various P_i# have no overlap. We take $(P_1,...,P_n)$# to be the concatenated list

(P_1#,...,P_n#). We arrange for the variables used in (P_1,...,P_n)# to be exactly $v_1,...,v_{k'}$, $1 \leq k < k'$. Of course, k' depends on $n,k,P_1,...,P_n$.

LEMMA 1.6. Let $P_1(v_1,...,v_k),...,P_n(v_1,...,v_k)$ be polynomials with integer coefficients.
i. If $P_1(v_1,...,v_k) = 0 \wedge ... \wedge Pn(v_1,...,v_n) = 0$, then there is a unique solution of (P_1,...,P_n)# extending $v_1,...,v_k$.
ii. In any solution of (P_1,...,P_k)#, we have $P_1(v_1,...,v_k) = 0 \wedge ... \wedge P_n(v_1,...,v_k) = 0$.

Proof: Standard. QED

LEMMA 1.7. Let $P_1(v_1,...,v_k),...,P_n(v_1,...,v_k)$ be polynomials with integer coefficients. There exists a finite set C of line conditions over $\{0,...,4\}^2$ using some $x_1,...,x_m$, $m \geq k$, such that the following holds.
i. If $P_1(v_1,...,v_k) = 0 \wedge ... \wedge P_n(v_1,...,v_k) = 0$, then there is a realization $x_1,...,x_m$ of C such that the first coordinates of $x_1,...,x_k$ are $v_1,...,v_k$.
ii. In every realization $x_1,...,x_m$ of C, the first coordinates of $x_1,...,x_k$ are a common zero of $P_1,...,P_n$, and the second coordinates are 1.
Furthermore, there is an algorithm for constructing C from $P_1,...,P_n$ which does not depend on J.

Proof: Let $P_1(v_1,...,v_k),...,P_n(v_1,...,v_k)$ be as given. We now work with (P_1,...,P_n)#, which uses $x_1,...,x_{k'}$.

For each $1 \leq i \leq k'$, we use $[(0,1),(1,1),x_i]$, to guarantee that each x_i, $1 \leq i \leq k'$, has second coordinate 1 in all realizations.

For each equation $v_i = v_j$ in (P_1,...,P_n)#, add $[(0,1),(1,1),x_i]$, $[(0,1),(1,1),x_j]$, $[(0,0),x_i,x_j]$. In any realization, the second coordinates of x_i,x_j are 1, and hence also $x_i = x_j$.

For each equation $v_i = 1$ in (P_1,...,P_n)#, add $[(1,0),(1,1),x_i]$. In any realization, the first coordinate of x_i is 1.

Process the equations $v_i = v_j + v_k$, in (P_1,...,P_n)#, one by one, as follows. Construct an associated copy of C_1, obtained by changing x_1 to x_j, x_2 to x_k, and x_7 to x_i. Change the remaining variables in C_1 to distinct x's which have not been used thus far. By Lemma 1.3, this will guarantee that in all realizations, $x_i = x_j + x_k$ in first coordinates.

Now process the equations $v_i = v_j \bullet v_k$, in $(P_1,...,P_n)\#$, one by one, as follows. Construct an associated copy of C_3, obtained by changing x_1 to x_j and x_2 to x_k, and x_{22} to v_i. Change the remaining variables in C_3 to distinct x's which have not been used thus far. By Lemma 1.5, this will guarantee that in all realizations, $x_i = x_j \bullet x_k$ in first coordinates.

Let $P_1(v_1,...,v_k) = 0 \wedge ... \wedge P_n(v_1,...,v_k) = 0$. Let $v_1,...,v_{k'}$ be the unique solution to $(P_1,...,P_n)\#$. The construction of C involves the constructions in Lemmas 1.3, 1.5, and by looking at the equations in Lemmas 1.3, 1.5, we obtain a realization $x_1,..,x_m$ of C for i) of Lemma 1.7.

In any realization $x_1,...,x_m$ of C, the first coordinates of $x_1,...,x_{n'}$ are a solution to $(P_1,...,P_n)\#$, and hence the first coordinates of $x_1,...,x_k$ are a common zero of $P_1,...,P_n$. QED

LEMMA 1.8. $H10(J) \leq LDP(J,\{0,...,4\}^2)$. Every J Diophantine set is ≤ some LDP(J;n).

Proof: Let $P_1(v_1,...,v_k),...,P_n(v_1,...,v_k)$ be polynomials with integer coefficients. Let B be algorithmically given by Lemma 1.7, using $x_1,...,x_m$.

Let $P_1(v_1,...,v_k) = 0 \wedge ... \wedge P_n(v_1,...,v_k) = 0$, $v_1,...,v_k \in J$. By Lemma 1.7 i), there is a realization $x_1,...,x_m$ of C in J.

Let $x_1,...,x_m$ be a realization of C in J. By Lemma 1.7 ii), the first coordinates of $x_1,...,x_k \in J$ are a common zero of $P_1,...,P_n$. This establishes the first claim.

Now let S be the J Diophantine set

$$\{y \in Z^k: (\exists z \in J^r)(P_1(y,z) = 0 \wedge ... \wedge P_n(y,z) = 0)\}$$

Let C be the finite set of line conditions over $\{0,...,4\}^2$ using $x_1,...,x_m$, $m \geq k+r$, given by Lemma 1.7 from $P_1(v_1,...,v_{k+r}),...,P_n(v_1,...,v_{k+r})$. Let t be the number of line conditions in C. We claim S ≤ LDP(J;t). To see this, let $x \in Z^k$ be given.

We claim $y \in S$ if and only if C<y> has a realization $x_{k+1},...,x_m$ in J, where C<y> is the result of replacing the variables $x_1,\dots,x_k$ in C by $(y_1,1),\dots,(y_k,1)$, where $y = (y_1,\dots,y_k)$.

To see this, suppose $y \in S$. Let $P_1(y,z) = 0 \wedge \dots \wedge P_n(y,z) = 0$. By Lemma 1.7 i), there is a realization $x_1,\dots,x_m$ of C in J such that the first coordinates of $x_1,\dots,x_{k+r}$ are $y_1,\dots,y_k,z_1,\dots,z_r$. By Lemma 1.7 ii), the second coordinates of $x_1,\dots,x_{k+r}$ are 1. Clearly $x_{k+1},\dots,x_m$ is a realization of C<y>.

Now suppose $x_{k+1},\dots,x_m$ is a realization of C<y>, $y \in Z^k$. Then $x_1,\dots,x_m$ is a realization of C, where $x_1,\dots,x_k = (y_1,1),\dots,(y_k,1)$. Hence by Lemma 1.7 ii), y is a common zero of $P_1,\dots,P_n$. Hence $y \in S$. QED

LEMMA 1.9. For all $x,y,z,u,v,w \in J$, $(x,y),(z,w),(u,v)$ lie on a common line if and only if

$$(w-y)(u-x)-(v-y)(z-x) = 0 \wedge (w-y)(u-z)-(v-w)(z-x) = 0$$
$$\wedge (v-y)(u-z)-(v-w)(u-x) = 0.$$

Proof: We first prove the equivalence under the assumption that $(x,y) = (z,w)$. In this case, $(x,y),(z,w),(u,v)$ lie on a line, and the three equations obviously hold. By symmetry, we can use $(x,y) = (u,v)$, or we can use $(z,w) = (u,v)$.

We now assume that $(x,y),(z,w),(u,v)$ are distinct pairs. Let us prove the equivalence under the assumption $x = z$. Then $y = \neq w$. Suppose $(x,y),(x,w),(u,v)$ lie on a common line. The common line must be the vertical through (x,y). Hence $u = x$, and the three equations hold. Conversely, suppose the three equations hold. We have

$$(w-y)(u-x) = 0 \wedge (w-y)(u-z) = 0.$$
$$u = x \wedge u = z.$$

Hence $(x,y)(z,w),(u,v)$ lie on a common line.

By symmetry, we obtain the equivalence under any of the assumptions

$$x = z,\ x = u,\ z = u,\ y = w,\ y = v,\ w = v.$$

So now we assume that none of the above six equations hold. Suppose $(x,y),(z,w),(u,v)$ lie on a common line. We can apply Theorem 0.4 to $(x,y),(z,w)$. We have $(w-y)(u-x) = (z-x)(v-y)$. We can also apply Theorem 0.4 to $(x,y),(u,v)$, and also to (z,w),(u,v). These yield the three equations in the statement of the Lemma.

Now suppose the three equations hold. By Theorem 0.4, the first equation tells us that (u,v) lies on the unique line containing (x,y),(z,w). Hence (x,y),(z,w),(u,v) lie on a common line. QED

LEMMA 1.10. LDP(J,Z^2) ≤ H10(J).

Proof: By Lemma 1.9, realizability in J is equivalent to the existence of solutions in J of a finite set of polynomial equations with integer coefficients. This reduces to H10(J). QED

LEMMA 1.11. Each LDP(J;n) is ≤≥ some J Diophantine set.

Proof: Below, we will argue a bit informally, using "corresponds to" to indicate ≤≥.

Fix n ≥ 0. LDP(J;n) is the family of lists C of at most n line conditions in variables $x_1,x_2,...$ and constants from Z^2, that have a realization in J. It is clear by changing variables that this is corresponds to the family of lists C of at most n line conditions in variables $x_1,...,x_{3n}$ and constants from Z2, that have a realization in J.

We can view each C as a list C' of at most n line conditions in $x_1,...,x_{3n}$ and some extra variables x3n+p, 0 ≤ p ≤ 3n, with no constants from Z^2, paired with an assignment of elements of Z2 to the extra variables $x_{3n+1},...,x_{3n+p}$.

These C' naturally split into finitely many pieces according to its line conditions, suppressing the assignment. Each piece corresponds to a J Diophantine set whose dimension is twice the number of extra variables.

Thus we arrive at a finite list of J Diophantine sets $S_1,...,S_p$, of various dimensions. We can assume that the dimensions have been raised to a common dimension d, so that $S_1,...,S_p \subseteq Z^d$.

Now let S = {(i,x): 1 ≤ i ≤ p ∧ x ∈ S_i}. Now use the fact that a finite disjunction of finite conjunctions of polynomial equations can be written as a finite conjunction of finite disjunctions of polynomial equations, and therefore as a finite conjunction of polynomial equations, to conclude that S is J Diophantine, and LDP(J;n) ≤≥ S. QED

LEMMA 1.12. LDP(Z,Z^2), LDP($Z,\{0,1,2\} \times \{0,1\}$) are complete r.e. For sufficiently large n, LDP(Z;n) is complete r.e.

Proof: By Lemma 1.10, LDP(Z,Z^2) ≤ H10(Z), and so LDP(Z,Z^2) is r.e. By Lemmas 1.2, 1.8, H10(Z) ≤ LDP($Z,\{0,1,2\} \times \{0,1\}$). Since H10(Z) is complete r.e., this establishes the first claim.

By Lemma 1.11, each LDP(Z;n) ≤≥ some Z Diophantine set. Hence each LDP(Z;n) is r.e. By Lemma 1.8, every Z Diophantine set is ≤ some LDP(Z;n). Since there is a Z Diophantine set that is complete r.e., we see that some LDP(Z;n) is complete r.e. Hence for sufficiently large n, LDP(Z;n) is complete r.e. QED

This establishes the entire LDP Table.

2. Realizing Parallels.

PDP TABLE

Unsolvability for PDP with Z

PDP($Z,\{(0,0),(1,0),(0,1)\}$), PDP(Z,Z^2) are complete r.e. For sufficiently large n, PDP(Z;n) is complete r.e.

Reductions for PDP with Ordered Ring J

PDP(J,Z^2) ≤ PDP($J,\{0,1,2\} \times \{0,1\}$) ≤≥ H10($J\backslash\{0\}$).
Every $J\backslash\{0\}$ Diophantine set is ≤ some PDP(J;n).
Every PDP(J;n) is ≤≥ some $J\backslash\{0\}$ Diophantine set.
Reductions and n are constructed uniformly in J.

In this section, we will establish all claims in the PDP Table.

We will use P (or P_i) for finite sets of parallel conditions.

Throughout this section, fix J to be an integral domain of characteristic zero.

LEMMA 2.1. Let $x,y,z \in J^2$. The following are equivalent.
i. [x,y,z].
ii. $(\exists u,v,w \in J)(xu||vw \wedge yu||vw \wedge zu||vw)$.

Proof: Suppose $[x,y,z]$. By Theorem 0.5, lines are infinite. Hence let $u,u' \in J^2$ be distinct points on a line containing x,y,z, where $x,y,z \notin \{u,u'\} + \{(0,0),(1,0),(0,1)\}$. If u,u' have the same first coordinate, set $v = u + (1,0)$, $w = u' + (1,0)$. Otherwise, set $v = u + (0,1)$, $w = u' + (0,1)$. QED

Now let u,v,w witness ii). We use Theorem 0.5. Then $x,y,z \neq u$, $v \neq w$. The line containing v,w is disjoint from the lines containing x,u, containing y,u, containing z,u. Hence these latter three lines must be the same line. Therefore x,y,z all lie on a common line. QED

LEMMA 2.2. $H10(J\backslash\{0\}) \leq PDP(J,\{0,1,2\} \times \{0,1\})$. Every $J\backslash\{0\}$ Diophantine set is $\leq$ some $PDP(J;n)$.

Proof: Let α be the algorithm given by Lemma 1.7, with constants converted to lie in $\{0,1,2\} \times \{0,1\}$, by Lemma 1.1. Let $P_1(v_1,...,v_k),...,P_n(v_1,...,v_k)$ be polynomials with integer coefficients. Then $\alpha(P_1,...,P_n)$ is a finite set of line conditions over $\{0,1,2\} \times \{0,1\}$ using some $x_1,...,x_m$, $m \geq k$, such that the following holds.

i. In every realization $x_1,...,x_m$ of $\alpha(P_1,...,P_n)$, the second coordinates of $x_1,...,x_n$ are 1.
ii. If $P_1(v_1,...,v_k) = 0 \wedge ... \wedge P_n(v_1,...,v_k) = 0$, then there is a realization $x_1,...,x_m$ of $\alpha(P_1,...,P_n)$ such that the first coordinates of $x_1,...,x_k$ are $v_1,...,v_k$.
iii. In every realization $x_1,...,x_k$ of $\alpha(P_1,...,P_n)$, the first coordinates of $x_1,...,x_k$ are a common zero of $P_1,...,P_n$.

Let $\beta(P)$ consist of $\alpha(P)$ and the parallel conditions

$(0,1)x_i||z_iz_i'$, $1 \leq i \leq n$
$ux||vw$, $uy||vw$, $uz||vw$

where $[x,y,z]$ is a line condition in $\alpha(P_1,...,P_n)$, u,v,w are new distinct variables associated with the line condition $[x,y,z]$, and $z_1,...,z_k,z_1',...,z_k'$ are new distinct variables. Thus we have introduced $k+2m$ new variables, where there are m line conditions in $\alpha(P_1,...,P_n)$. Clearly the following holds.

iii. Every realization of $\beta(P_1,...,P_n)$ is a realization of $\alpha(P_1,...,P_n)$.
iv. For every $P_1(v_1,...,v_k) = 0 \wedge ... \wedge P_n(v_1,...,v_k) = 0$, $v_1,...,v_k \in J\backslash\{0\}$, there exists a realization of $\beta(P_1,...,P_n)$

where $x_1 = (v_1,1),\ldots,x_k = (v_k,1)$, whose coordinates lie in $J\backslash\{0\}$.

It is now clear that $P_1,\ldots,P_n$ has a common zero in $J\backslash\{0\}$ if and only if $\beta(P_1,\ldots,P_n)$ has a realization in J.

Now let S be a $J\backslash\{0\}$ Diophantine set, and write

$S = \{y \in Z^n: (\exists z \in (J\backslash\{0\})^m)(P(y,z) = 0)\}$.

Now argue as in the proof of Lemma 1.8. QED

LEMMA 2.3. For all $x,y,z,u,v,w,a,b \in J$, $(x,y)(z,u)||(v,w)(a,b)$ if and only if $(y-u)(v-a) = (w-b)(x-z) \wedge x \neq y \wedge z \neq u \wedge v \neq w \wedge a \neq b \wedge (x = z \leftrightarrow v = a)$.

Proof: Suppose $(x,y)(z,u)||(v,w)(a,b)$. Then $x \neq y \wedge z \neq u \wedge v \neq w \wedge a = b$. If $x = z$ then $v = a$. If $v = a$ then $x = z$. Conversely, suppose $(y-u)(v-a) = (w-b)(x-z) \wedge x \neq y \wedge z \neq u \wedge v \neq w \wedge a \neq b \wedge (x = z \leftrightarrow v = a)$. First suppose $x-z$ and $v-a$ are nonzero. Then the slopes are defined and equal, and so $(x,y)(z,u)||(v,w)(a,b)$. Now suppose $x = z$. Then $v = a$, and so $(x,y)(z,u)||(v,w)(a,b)$. Finally, suppose $v = a$. Then $x = z$, and hence $(x,y)(z,u)||(v,w)(a,b)$. REWORK TO REPLACE SLOPES BY CROSS PRODUCTS, MAKING SURE WE STAY IN INTEGRAL DOMAINS OF CHARACTERISTIC ZERO. QED

LEMMA 2.4. $PDP(J,Z^2) \leq H10(J\backslash\{0\})$.

Proof: It suffices to write the existentialization of a conjunction of formulas

$(y-u)(v-a) = (w-b)(x-z) \wedge x \neq y \wedge z \neq u \wedge v \neq w \wedge a \neq b \wedge (x = z \leftrightarrow v = a)$

as an existentialized equation, where the quantifiers range over $J\backslash\{0\}$. First rewrite this conjunction as a disjunction of formulas of the form

$P_1(v_1,\ldots,v_k) = 0 \wedge \ldots \wedge P_r(v_1,\ldots,v_k) = 0 \wedge y_1 \neq z_1 \wedge \ldots \wedge y_p \neq z_p$

where the P's are polynomials with integer coefficients, and the y's,z's are variables among $v_1,\ldots,v_k$.

This is equivalent to a disjunction of formulas of the form

$(\exists b_1,\ldots,b_p \in J\backslash\{0\})(P_1(v_1,\ldots,v_k) = 0 \wedge \ldots \wedge P_r(v_1,\ldots,v_k) = 0 \wedge z_1-y_1-b_1 = 0 \wedge \ldots \wedge z_p-y_p-b_p = 0)$

which can be rewritten as a single formula of the above form.

There are still some outermost existential quantifiers ranging over J. Thus we have a sentence of the form

$(\exists v_1,\ldots,v_n \in J)(\exists b_1,\ldots,b_p \in J^+)(Q_1(v_1,\ldots,v_k,w_1,\ldots,w_m) = 0 \wedge \ldots \wedge Q_s(v_1,\ldots,v_k,w_1,\ldots,v_m) = 0)$

which can be put into the form

$(\exists v_1,\ldots,v_{2n},b_1,\ldots,b_p \in J\backslash\{0\})(Q_1(v_1+v_2,\ldots,v_{2k-1}+v_{2k},b_1,\ldots,b_p) = 0 \wedge \ldots \wedge Q_n(v_1+v_2,\ldots,v_{2k-1}+v_{2k},b_1,\ldots,b_p) = 0)$. QED

LEMMA 2.5. Every PDP(J;n) is ≤≥ some J\{0} Diophantine set.

Proof: See the proof of Lemma 1.11. QED

LEMMA 2.6. There is a finite set of parallel conditions over {(0,0),(1.0),(0,1)} using $x_1,\ldots,x_6$, whose unique realization x1,...,x6 in Z is an enumeration of $\{0,1,2\}^2\backslash\{(0,0),(1,0),(0,1)\}$.

Proof: We use the diagram

x_2	x_5	x_6
(0,1)	x_1	x_4
(0,0)	(1,0)	x_3

Let P be the set of parallel conditions that hold in the obvious interpretation of this diagram.

Suppose we have a realization of P in Z. Since $(0,0)(0,1)||(1,0)x_1$, $(0,1)x_1||(0,0)(1,0)$, we see that $x_1 = (1,1)$. Now $(0,1)x_1||(1,0)x_3$, $(0,1)x_1||(0,0)x_3$. Hence x_3 lies on the x axis. Similarly, x_2 lies on the y axis.

Now $x_2x_1||x_5x_6$, $x_2x_3||x_5x_6$, $x_1x_3||x_5x_6$. Hence x_2,x_1,x_3 are collinear. Hence $x_2 = (0,2)$, $x_3 = (2,0)$. Since $x_1x_4||(1,0)x_3$, $(1,0)x_1||x_3x_4$, we have $x_4 = (2,0)$. Similarly, $x_5 = (1,2)$, $x_6 = (2,2)$. QED

LEMMA 2.7. PDP(Z,Z^2), PDP(Z,{(0,0),(1,0),(0,1)) are complete r.e. For sufficiently large n, PDP(Z;n) is complete r.e.

Proof: See the proof of Lemma 1.12. Use Lemma 2.6 to reduce the constants. QED

This establishes the entire PDP Table.

3. Realizing Equidistance.

EDP TABLE

Unsolvability for EDP with Z

EDP(Z,Z^2), EDP(Z,{(0,0),(1,0)}) are complete r.e. For sufficiently large n, EDP(Z;n) is complete r.e.

Reductions for EDP with Ordered Ring J

EDP(J,Z^2) ≤ EDP(J,{(0,0),(1,0)}) ≤≥ H10(J\{0}).
Every J\{0} Diophantine set is ≤ some EDP(J;n).
Every EDP(J;n) is ≤≥ some J\{0} Diophantine set.
Reductions and n are constructed uniformly in J.

In this section, we will establish all claims in the EDP Table.

We will use E (or E_i) for finite sets of equidistance conditions.

Throughout this section, fix J to be an ordered ring.

LEMMA 3.1. There exists a set E_0 of equidistance conditions over {(0,0),(1,0)} using $x_1,...,x_8$ with exactly two realizations $x_1,...,x_8$. One is x_1 = (0,1), x_2 = (1,1), x_3 = (2,1), x_4 = (2,0). The other is x_1 = (0,-1), x_2 = (1,-1), x_3 = (2,-1), x_4 = (2,0).

Proof: We first use

(0,0)x_1 E x_1x_2 E x_2,(1,0) E (1,0)(0,0).

This establishes the two possibilities for x_1,x_2. Next we use

(1,0)x_2 E x_2x_3 E x_3x_4 E x_4(1,0).

This establishes the two possibilities for x_1,x_2,x_3,x_4. QED

LEMMA 3.2. EDP(J,{0,1,2} × {0,1}) ≤ EDP(J,{(0,0),(1,0)}).

Proof: Let E be a set of equidistance conditions over $\{0,1,2\} \times \{0,1\}$ using $x_1,\ldots,x_n$. Let E' be the result of adding 4 to all subscripts of variables in E, and replacing constants $(0,1),(1,1),(2,1),(2,0)$ by x_1,x_2,x_3,x_4, respectively. We claim that E has a realization $x_1,\ldots,x_n$ in J if and only if $E' \cup D_E$ has a realization $x_1,\ldots,x_{n+4}$ in J.

Let $x_1,\ldots,x_n$ be a realization of E in J. Then $(0,1),(1,1),(2,1),(2,0),x_5,\ldots,x_{n+4}$ is a realization of $E' \cup E_0$ in J.

Let $x_1,\ldots,x_{n+4}$ be a realization of $E' \cup E_0$ in J. If $x_1,\ldots,x_4$ are $(0,1),(1,1),(2,1),(2,0)$, respectively, then $x_5,\ldots,x_{n+4}$ is a realization of E in J. If $x_1,\ldots,x_4$ are $(0,-1),(1,-1),(2,-1),(2,0)$, respectively, then $x_5,\ldots,x_{n+4}$ becomes a realization of E in J after minus signs are put in front of the second coordinates. QED

LEMMA 3.3. Let $x,y,z \in J^2$. The following are equivalent.
i. $[x,y,z]$.
ii. $(\exists u,v \in J)(xu\ E\ xv \wedge yu\ E\ yv \wedge zu\ E\ zv \wedge uv\ E\ uv)$.

Proof: Suppose $[x,y,z]$.

case 1. $x = y = z$. Set $u = x+(1,0)$, $v = x+(-1,0)$.

case 2. Otherwise. By symmetry, we can assume $x \neq y$. If x,y have the same first coordinate, then set $u = x+(1,0)$, $v = x+(-1,0)$. If x,y have the same second coordinate, then set $u = x+(0,1)$, $v = x+(0,-1)$. Now assume otherwise. Let $x = (a,b)$, $y = (c,d)$. The line L perpendicular to the line containing x,y, and passing through x takes the form $(b-d)(y^*-b) = (a-c)(x^*-a)$, $x^*,y^* \in \mathfrak{R}$. $x^* = b-d+a$, $y^* = a+b-c$, and $x^* = d-b+a$, $y^* = b+c-a$. Set $u = (b-d+a,a+b-c)$, $v = (d-b+a,b+c-a)$.

Now let u,v witness ii). Then $u \neq v$. The locus of points equidistant to u and v is a line. REWORK TO CONFORM TO ORDERED RINGS. QED

LEMMA 3.4. $H10(J\backslash\{0\}) \leq EDP(J,\{(0,0),(1,0)\})$. Every $J\backslash\{0\}$ Diophantine set is $\leq$ some $EDP(J;n)$.

Proof: See the proof of Lemma 3.2. QED

LEMMA 3.5. $EDP(J,Z2) \leq H10(J\backslash\{0\})$. Every $EDP(J;n)$ is $\leq\geq$ some $J\backslash\{0\}$ Diophantine set.

Proof: See the proof of Lemma 3.4. QED

ADD SOME ELABORATION OF PROOFS FOR LEMMAS 3.4, 3.5.

This establishes the entire EDP Table.

4. Realizing Betweenness.

BDP TABLE

Unsolvability for BDP with Z

BDP(Z,Z2), BDP(Z,{(0,0),(1,0),(0,1)}) are complete r.e. For sufficiently large n, BDP(Z;n) is complete r.e.

Reductions for BDP with Ordered Ring J

BDP(J,Z^2) ≤≥ BDP(J,{0,1,2} × {0,1}) ≤≥ H10(J^+).

Every J^+ Diophantine set is ≤ some BDP(J;n).

Every BDP(J;n) is ≤≥ some J^+ Diophantine set.

Reductions and n are constructed uniformly in J.

In this section, we will establish all claims in the BDP Table.

We will use B (or Bi) for finite sets of b-conditions.

Throughout this section, fix J to be an ordered ring.

LEMMA 4.1. Let x,y,z ∈ J^2. The following are equivalent.

i. [x,y,z].

ii. (∃u,v ∈ J)(<x,u,v> ∧ <y,u,v> ∧ <z,u,v> ∧ the coordinates of u,v lie in the ring generated by the coordinates of x,y,z).

Proof: Suppose [x,y,z].

case 1. x = y = z. Write x = (a,b). Set u = (a,b+1), v = (a,b+2).

case 2. Otherwise. By symmetry, we can assume x ≠ y. Write x = (a,b), y = (c,d). If a = c then set u = (a,max(b,d)+1), v = (a,max(b,d)+2). If b = d then set u = (max(a,c)+1,b), v = (max(a,c)+2,d). Suppose otherwise. The line containing x,y takes the form

$$(y^*-b)(a-c) = (x^*-a)(b-d)$$

where $x^*,y^* \in \Re$. Let $n < m$ be sufficiently large integers. Then set $u = (a+n(a-c),b+n(b-d))$, $v = (a+m(a-c),b+m(b-d))$.

Now let u,v witness ii). Then $u \neq v$ and x,y,z all lie on the line containing u,v. Hence [x,y,z]. QED

LEMMA 4.2. $H10(J^+) \leq BDP(J,\{0,1,2\} \times \{0,1\})$. Every J^+ Diophantine set is $\leq$ some BDP(J;n).

Proof: Let α be the algorithm given by Lemma 1.7, with constants converted to lie in $\{0,1,2\} \times \{0,1\}$. Let $P(v_1,\ldots,v_n)$ be a polynomial with integer coefficients. Then $\alpha(P)$ is a finite set of line conditions over $\{0,1,2\} \times \{1,1\}$ using some $x_1,\ldots,x_m$, $m \geq n$, such that the following holds.

i. If $P(v_1,\ldots,v_n) = 0$, then there is a realization $x_1,\ldots,x_m$ of $\alpha(P)$ such that the first coordinates of $x_1,\ldots,x_n$ are $v_1,\ldots,v_n$, and all coordinates of the $x_1,\ldots,x_m$ lie in the ring generated by $v_1,\ldots,v_n$.
ii. In every realization $x_1,\ldots,x_m$ of $\alpha(P)$, the first coordinates of $x_1,\ldots,x_n$ are a zero of P, and the second coordinates are 1.

Let $\beta(P)$ be the set of all b-conditions

$<(-1,1),(0,1),x_i>$, $1 \leq i \leq n$
$<x,u,v>$, $<y,u,v>$, $<z,u,v>$

where [x,y,z] is a line condition in $\alpha(P)$, and u,v are new distinct variables associated with the line condition [x,y,z].

Unfortunately, we cannot use (-1,1) here since $(-1,1) \notin \{0,1,2\} \times \{0,1\}$. Consider the diagram

$$\begin{array}{llll} w_4 & (0,1) & (1,1) & (2,1) \\ & (0,0) & (1,0) & (2,0) \\ & w_1 & w_3 & w_2 \end{array}$$

and use all b-conditions true in the diagram. Then in all realizations, $w_1 = (0,-1)$, $w_2 = (2,-1)$, $w_3 = (1,-1)$, $w_4 = (-1,0)$. This means that we have access to (-1,1) by introducing the new variables w_1,w_2,w_3,w_4. Clearly the following holds.

iii. Every realization of $\beta(P)$ is a realization of $\alpha(P)$, where the first coordinates of $x_1,\ldots,x_n$ are positive.

iv. For every $P(v_1,...,v_n) = 0$, $v_1,...,v_n \in J^+$, there exists a realization of $\beta(P)$ where $x_1 = (v_1,1),...,x_n = (v_n,1)$, whose coordinates lie in J^+.

It is now clear that P has a zero in J^+ if and only if $\beta(P)$ has a realization in J.

Now let S be a J^+ Diophantine set, and write

$S = \{y \in Z^n: (\exists z \in J^{+m})(P(y,z) = 0)\}$.

TO BE COMPLETED. QED

LEMMA 4.3. For all $x,y,z,u,v,w \in J$, $<(x,y),(z,w),(u,v)>$ if and only if $P(x,y,z,u,v,w) = 0 \wedge (x < z < u \vee z > z > u \vee y < w < v \vee y > w > v)$, where P is from Lemma 1.9.

Proof: Immediate. QED

LEMMA 4.4. $BDP(J,Z^2) \leq H10(J^+)$. Every $BDP(J;n)$ is $\leq\geq$ some J^+ Diophantine set.

Proof: It suffices to write the existentialization of a conjunction of formulas

$P(x,y,z,u,v,w) = 0 \wedge (x < z < u \vee x > z > u \vee y < w < v \vee y > w > v)$

as an existentialized equation, where the quantifiers range over J+. First rewrite this conjunction as a disjunction of formulas of the form

$P_1(v_1,...,v_n) = 0 \wedge ... \wedge P_r(v_1,...,v_n) = 0 \wedge y_1 < z_1 \wedge ... \wedge y_p < z_p)$

where the P's are polynomials with integer coefficients, and the y's,z's are variables among $v_1,...,v_n$.

This is equivalent to a disjunction of formulas of the form

$(\exists b_1,...,b_p \in J^+)(P_1(v_1,...,v_n) = 0 \wedge ... \wedge P_r(v_1,...,v_n) = 0 \wedge z_1-y_1-b_1 = 0 \wedge ... \wedge z_p-y_p-b_p = 0)$

which can be rewritten as

$(\exists b_1,...,b_p \in J^+)(Q(v_1,...,v_n,b_1,...,b_p) = 0)$.

There are still some outermost existential quantifiers ranging over J. Thus we have a sentence of the form

$(\exists v_1,\ldots,v_n \in J)(\exists b_1,\ldots,b_p \in J^+)(Q(v_1,\ldots,v_n,w_1,\ldots,w_m) = 0)$

which can be put into the form

$(\exists v_1,\ldots,v_{2n},b_1,\ldots,b_p \in J^+)(Q(v_1+v_2,\ldots,v_{2n-1}+v_{2n},b_1,\ldots,b_s) = 0)$.

For the second claim, use the above construction, and argue as in the proof of Lemma 1.12. QED

We will use the notation (+,+),(+,-),(-,+),(-,-) for the four open quadrants in J^2. We will use obvious variants of this notation for other convenient subsets of J^2. E.g., (-,0) = $\{x \in J^2\text{: } x < 0 \wedge y = 0\}$.

LEMMA 4.5. There exists a set C_0 of b-conditions over {(0,0),(1,0),(0,1)} using $x_1,\ldots,x_8$ with a realization in Z, where every realization in Z has $x_1 = (1,1)$, $x_6 = (2,0)$, $x_8 = (2,1)$.

Proof: Consider the diagram

1)

		x_2	
	(0,1)	x_1	x_8
x_3	(0,0)	(1,0)	x_6
	x_4	x_5	
	x_7		

where adjacent entries are adjacent in Z^2. E.g., $x_2 = (1,2)$, $x_7 = (0,-2)$. The order of the variables $x_2,\ldots,x_7$ is of no importance.

Let C_0 be the set of all b-conditions satisfied by diagram 1).

It is obvious by the definition of C_0 that C_0 has a realization in Z^2. Now let a realization of C_0 in Z^2 be given. We use diagram 1), without prejudging $x_1,\ldots,x_8$, except for the b-conditions in C_0.

It is clear that we have

$x_4 \in$ (0,-), by $<(0,1),(0,0),x_4>$
$x_7 \in$ (0,-) by $<(0,0),x_4,x_7>$
$x_3 \in$ (-,0) by $<x_3,(0,0),(1,0)>$

$x_6 \in (+,0)$ by $<(0,0),(1,0),x_6>$
$x_2 \in (+,+)$ by $<x_3,(0,1),x_2>$
$x_1 \in (+,+)$ by $<(1,0),x_1,x_2>$
$x_5 \in (+,-)$ by $<x_5,(1,0),x_1>$ and $<x_7,x_5,x_6>$

We now use that the realization is in Z several times. We have $x_5 \in (\geq 1,-)$. By $<x_5,(1,0),x_1>$, $x_1 \in (+,+)$, the first coordinate of x_1 must lie in (0,1]. Hence the first coordinates of x_1,x_5 are 1 (using Z^2). Hence the first coordinate of x_2 is also 1. I.e., x_1,x_2,x_5 lie on the line x = 1.

From the fact that x_3 lies on the negative x axis, $<x_3,(0,1),x_2>$, and x_2 lies on the line x = 1, we see that $x_3 = (-1,0)$ and $x_2 = (2,0)$, using Z^2. By $<(1,0),x_1,x_2>$, we have $x_1 = (1,1)$, again using Z^2.

Since x_6 is on the axis and the line through (2,0),(1,1), clearly $x_6 = (2,0)$. Since x_8 lies on the line y = 1 to the right of (1,1), its first coordinate is ≥ 2. If the first coordinate of x_8 is greater than 2 then this is incompatible with $<x_4,(1,0),x_8>$. Hence $x_8 = (2,1)$. QED

LEMMA 4.6. $BDP(Z,Z^2) \leq BDP(Z,\{(0,0),(1,0),(0,1)\})$.

Proof: From Lemma 4.4. QED

This establishes the entire BDP Table.

5. Further Results.

TO BE COMPLETED.

REFERENCES

[Po03] B. Poonen, http://math.mit.edu/~poonen/papers/aws2003.pdf 2003.

Rogers, Soare, and H10 references.

*This research was partially supported by John Templeton Foundation Grant ID#15557.