JOURNAL OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 00, Number 0, Pages 000–000
S 0894-0347(XX)0000-0

ON A LATTICE PROBLEM OF H. STEINHAUS

STEVE JACKSON AND R. DANIEL MAULDIN

1. Introduction

Sometime in the 1950's, Steinhaus posed the following problem. Do there exist two sets A and S in the plane such that every set congruent to A has exactly one point in common with S? The trivial case where one of the sets is the plane and the other consists of a single point is ruled out. The first appearance of this problem in the literature seems to be in a 1958 paper of Sierpiński [14]. In this paper, he showed the answer is yes, a result later rediscovered by Erdős [5]. Of course, there are many variants of this problem. For example, one could specify the set A. In this direction, Komjáth showed that such a set exists if $A = \mathbb{Z}$, the set of all integers [13]. Steinhaus also asked about the specific case where $A = \mathbb{Z}^2$. The first reference to this problem also seems to be Sierpiński's 1958 paper where he mentions that in this case there is no set S which is bounded and open or else bounded and closed. This specific problem has been widely noted, see e.g. [3, 4] but has remained unsolved until now. In this paper we answer this question in the affirmative:

Theorem 1.1. *There is a set $S \subseteq \mathbb{R}^2$ such that for every isometric copy L of the integer lattice $\mathbb{Z}^2$ we have $|S \cap L| = 1$.*

We note that throughout this paper we work in the theory ZFC; the usual axioms of set theory with the axiom of choice (AC). AC is used heavily in the main construction as we require, for example, an enumeration of the equivalence classes of the lattices under a certain equivalence relation. Also throughout this paper by "lattice" we mean a set in the plane which is isometric with the integer lattice $\mathbb{Z}^2$ (a brief exception occurs in lemmas 2.2, 2.3 where we consider scaled versions).

Let us point out that there are several things proven in this paper which are stronger than what is needed to prove theorem 1.1. Stronger forms of our two main technical lemmas, lemma A (lemma 1.3) and lemma B (lemma 1.5), are proven here than is required for the main theorem. In [9] a shorter argument is given for the main theorem. For example, a shorter proof of lemma A of this paper is given there. Here we give a more involved induction argument in §3. This argument, which uses only basic number theory and combinatorics, shows something much stronger and interesting in its own right. We feel that these stronger results may be useful in resolving whether the main theorem holds for other lattices and other dimensions. We note that the geometric lemma B is also stronger than what is

2000 *Mathematics Subject Classification.* Primary 04A20; Secondary 11H31.
Key words and phrases. lattice points, Steinhaus problem, four-bar linkage.
Research supported by NSF Grant DMS-0097181.
Research supported by NSF Grant DMS-9801583.

required for a proof of the main theorem. A weaker alternative is also indicated in §4. It is also quite possible that something like lemma B may be needed to resolve the problem for other lattices.

We note that theorems similar to lemma B may be found in theory of mechanical linkages [10]. Recall a four-bar linkage may be described as two circles C_1, C_2, and a rigid "bar" connecting two points p_1, p_2 constrained to lie on C_1, C_2 respectively. If we consider a third point p_3, and require that the triangle $\triangle p_1 p_2 p_3$ be rigid, then the locus of points traced out by p_3 is called a coupler curve for the linkage. We say the coupler point p_3 is non-trivial if it is not one of the endpoints p_1, p_2. In this terminology lemma B is the statement that the curve traced out by a non-trivial coupler point of a four-bar linkage has, except in the degenerate case noted, a finite intersection with any circle. In particular, lemma B is implicit in the analysis of Gibson and Newstead [8] (we give a brief sketch in §4). Their analysis uses a fair amount of machinery from algebraic geometry. However, since we were not able to find the precise statement of the lemma and as it is crucial to our methods, we give in §4 two very different elementary proofs of it.

We call a set S as in theorem 1.1 a Steinhaus set and note that whether there can be a Lebesgue measurable Steinhaus set remains unsolved. (We also do not know whether a Steinhaus set can be connected although one can prove that if it is measurable then it is totally disconnected.) Concerning measurable Steinhaus sets, T. H. Croft [2] and independently, J. Beck showed that there is no bounded measurable Steinhaus set [1] and Koulountzakis obtained some further refinements [11]. Also, Kolountzakis and Wolff showed that there is no measurable Steinhaus set for the higher dimensional version of Steinhaus' problem [12]. It is relatively easy to see that no Steinhaus set can be a Borel set or even have the Baire property if one follows the agruments given by Croft. We briefly sketch this argument. Suppose S has the Baire property. Since $\mathbb{R}^2 = \bigcup_{z \in \mathbb{Z}^2}(S + z)$, S cannot be meager. Fixing a ball with respect to which S is comeager and noting the the gaps between successive lattice distances converges to 0, we see that there is some some ball M such that the part of S outside this ball is meager. Let E be the set of points where neither S nor $\mathbb{R}^2 \setminus S$ is meager in any neighborhood. Then E is a nonempty closed nowhere dense set and following the proof of Lemma 3 of Croft's paper, we see that there is an isometric copy L of $\mathbb{Z}^2$ which meets E in exactly one point, p. Thus, there is a ball $B(p, d)$ such that neither S nor $\mathbb{R}^2 \setminus S$ is meager in that ball but $\mathbb{R}^2 \setminus S$ is comeager in $B(x, d)$ for every $x \in L$ with $x \neq p$. But, this would mean there is a small translation of L which would entirely miss S. We also note that the question of whether there is a bounded Steinhaus set remains unsolved. Steinhaus' problem and variants were discussed in some detail by Croft [2] and have been updated in sections E10 and G9 of [3]. In particular, Steinhaus also asked about sets meeting each copy of the lattice points in exactly n points. The fact that the answer to this question is yes follows directly from our main theorem and is discussed in our concluding remarks.

The authors thank C. Freiling, D. Goldstein, J. Rosenberg, and R. Solovay for helpful conversations. We also thank the referees for several valuable suggestions and corrections.

Let us say a lattice distance is a real number of the form $\sqrt{n^2 + m^2}$ where $n, m \in \mathbb{Z}$. Theorem 1.1 is clearly equivalent to the existence of a set $S \subseteq \mathbb{R}^2$ satisfying the following two properties:

(1) For every isometric copy L of $\mathbb{Z}^2$, $S \cap L \neq \emptyset$.

(2) For all distinct $z_1, z_2 \in S$, $\rho(z_1, z_2)$ is not a lattice distance, where ρ denotes the usual Euclidean distance.

In fact, we prove in this paper a slight strengthening of theorem 1.1:

Theorem 1.2. *There is a set $S \subseteq \mathbb{R}^2$ satisfying:*

(1) *For every isometric copy L of $\mathbb{Z}^2$ we have $S \cap L \neq \emptyset$.*
(2) *For all distinct $z_1, z_2 \in S$, $\rho(z_1, z_2)^2 \notin \mathbb{Z}$.*

We call a set $S \subseteq \mathbb{R}^2$ satisfying (2) of theorem 1.2 a *partial Steinhaus set*.

Note that viewed this way, the Steinhaus problem has a natural interpretation for smaller sets of lattices. Namely, given an arbitrary set $\mathcal{L}$ of lattices (each of which is an isometric copy of $\mathbb{Z}^2$), we may ask whether there is a partial Steinhaus set S such that $S \cap L \neq \emptyset$ for all $L \in \mathcal{L}$. Indeed, establishing this restricted version of the problem for the case where $\mathcal{L}$ is the (countable) family of rational translations of $\mathbb{Z}^2$ is a central step toward proving theorem 1.2. Actually, we need a slight technical strengthening of this "rational translation" case, which we state below.

In proving theorem 1.2, it is natural to proceed inductively. That is, we build the desired set S in (transfinitely many) stages. At limit stages, we take unions, and at successor stages we enlarge S_α to $S_{\alpha+1}$ so as to meet a new lattice, while at the same time keeping property (2). Note that (2) is then trivially satisfied at limit stages. If we can meet every lattice L along the way, then the final set $S = \bigcup_\alpha S_\alpha$ will be as desired. While this is our general plan, there are several steps that must be taken to ensure its success. For example, we do not simply enumerate the lattices $\mathcal{L}$ in type 2^ω. To appreciate the difference, we note that there does exist a "finite obstruction." That is, there is a finite set of points $F \subseteq \mathbb{R}^2$ (in fact $F \subseteq \mathbb{Q}^2$) which forms a partial Steinhaus set, but which cannot be extended to meet even the integer lattice $\mathbb{Z}^2$ and remain a partial Steinhaus set. For example the following set of 17 points forms such an obstruction (this set was constructed by considering a partial good permutation of 65 of size 17 which cannot be extended to a good permutation of 65; these concepts are explained in §3):

$(216/5, 2/5)$	$(107/5, 4/5)$	$(283/5, 1/5)$	$(174/5, 3/5)$
$(677/13, 5/13)$	$(340/13, 10/13)$	$(744/13, 2/13)$	$(407/13, 7/13)$
$(70/13, 12/13)$	$(474/13, 4/13)$	$(137/13, 9/13)$	$(541/13, 1/13)$
$(204/13, 6/13)$	$(712/13, 11/13)$	$(271/13, 3/13)$	$(779/13, 8/13)$
$(2601/65, 57/65)$			

Rather, it is important that we use the "hull construction" which has played an important role in several other theorems of this general character (see [6, 7]). The idea, described abstractly, is to consider a continuous elementary chain $\{M_\alpha\}_{\alpha<2^\omega}$ of substructures (say of some large V_κ) with each M_α of size $< 2^\omega$, but $\mathbb{R} \subseteq \bigcup_{\alpha<2^\omega} M_\alpha$. Let $\mathcal{L}_\alpha$ denote the isometric copies of $\mathbb{Z}^2$ which are in M_α. At successor steps, we now enlarge S_α to $S_{\alpha+1}$ which meets all lattices $L \in \mathcal{L}_{\alpha+1} - \mathcal{L}_\alpha$, while of course keeping property (2). While this gives us more to do at each successor step, it also provides us with a powerful inductive assumption, namely, the closure of $\mathcal{L}_\alpha$ under various operations. For the reader unfamiliar with the set-theoretic terminology, we may describe the idea as follows. We write the collection of lattices $\mathcal{L}$ as an increasing union of sets $\mathcal{L}_\alpha$ where at limit stages we take unions, and we require each $\mathcal{L}_\alpha$ to be closed under certain finitary functions $F_k\colon (\mathcal{L})^{<\omega} \to \mathcal{L}$. We could specify in advance which functions F_k we need the $\mathcal{L}_\alpha$ to be closed under, but it is more convenient not to. We note that when the continuum is greater than ω_1, the actual construction we will use will be a bit more complicated, essentially an iteration of this hull construction.

We now state precisely two lemmas, which we call lemma A and lemma B, which we will need to carry out the plan sketched above. The first of these is the "rational translation" case mentioned above.

Lemma 1.3 (A). *Let $\mathcal{L}_{\mathbb{Q}}$ denote the set of rational translations of $\mathbb{Z}^2$, that is, lattices of the form $\mathbb{Z}^2+(r,s)$ where $r,s\in\mathbb{Q}$. Then there is a set $S\subseteq\mathbb{R}^2$ satisfying the following.*

(1) *For every lattice $L\in\mathcal{L}_{\mathbb{Q}}$, $S\cap L\neq\emptyset$.*
(2) *For all distinct $z_1,z_2\in S$, $\rho(z_1,z_2)^2\notin\mathbb{Z}$.*

Actually, we require a technical slight strengthening of lemma A, which we call lemma A$'$. In this lemma, and for the rest of this paper, we adopt the following terminology. If $L\subseteq\mathbb{R}^2$ is a lattice, then by a "rational translation" of L we mean a lattice of the form $L+r\vec{u}+s\vec{v}$ where $r,s\in\mathbb{Q}$, and $\vec{u}$, $\vec{v}$ are the unit basis vectors for L. In other words, we are always referring to the coordinate system of the lattice L.

Lemma 1.4 (A$'$). *Let L be a lattice, and w be a point having rational coordinates with respect to L. Let P be a (countable) set of points containing w, all of which have rational coordinates with respect to L, and satisfying the following: for all integers d, i, j, a, b, there are infinitely many points of P which have coordinates with respect to L of the form $(\frac{i}{d}+k,\frac{j}{d}+l)$, where k, l are integers with $k\equiv a \mod d$, $l\equiv b \mod d$. Then there is a set S satisfying:*

(1) *For every rational translation L' of L we have $S\cap L'\neq\emptyset$.*
(2) *For all distinct $z_1,z_2\in S$ we have $\rho(z_1,z_2)^2\notin\mathbb{Z}$.*
(3) *$w\in S$.*
(4) *$S\subseteq P$.*

Note that lemma A$'$ immediately implies lemma A taking P to be the set of all points having rational coordinates with respect to L.

The second lemma is a result in pure plane geometry, which arises in carrying out the hull construction mentioned above.

Lemma 1.5 (B). *Let c_1,c_2,c_3 be three distinct points in the plane, and let r_1, r_2, $r_3>0$ be real numbers. Let C_1 be the circle in the plane with center at c_1 and radius r_1, and likewise for C_2 and C_3. Let a,b,c be three distinct points in the plane. Then, except for the exceptional case described afterwards, there are only finitely many triples of points (p_1,p_2,p_3) in the plane such that*

(1) *$p_1\in C_1$, $p_2\in C_2$, and $p_3\in C_3$.*
(2) *The triangle $p_1p_2p_3$ is isometric with the triangle abc (we allow the degenerate case where the points a,b,c are collinear).*

The exceptional case is when $r_1=r_2=r_3$ and the triangle abc is isometric with $c_1c_2c_3$.

In §2 we give the proof of theorem 1.2 assuming lemmas A$'$ and B. In §3 we prove lemma A$'$, and in §4 we prove lemma B. §§3, 4 are self-contained and may be read independently.

2. The Main Theorem

In this section we prove theorem 1.2 assuming lemmas A$'$ and B. Throughout, "lattice" will mean an isometric copy of $\mathbb{Z}^2$. ω denotes the first infinite ordinal, we which identify with the set of natural numbers.

Recall that by a "rational translation" of a lattice L we are referring to the coordinate system of the lattice L. By a rational rotation of $\mathbb{Z}^2$ we mean an operation of the form $\mathbb{Z}^2 \to R(\mathbb{Z}^2)$, where R is a rotation of the plane whose corresponding matrix $M_R = \begin{pmatrix} r_{11} & r_{12} \\ r_{21} & r_{22} \end{pmatrix}$ has rational entries. In this case, M_R must be of the form $\begin{pmatrix} \frac{a}{d} & -\frac{b}{d} \\ \frac{b}{d} & \frac{a}{d} \end{pmatrix}$ where a, b, d are integers and $a^2 + b^2 = d^2$. For a general lattice L, a rational rotation means a rotation about a point of L which is rational in the coordinate system of L.

Definition 2.1. Two lattices are equivalent $L_1 \sim L_2$, if L_2 can be obtained from L_1 by rational rotations and translations.

This is equivalent to saying that in the coordinate system determined by L_1, the isometry moving L_1 to L_2 is of the form

$$\begin{pmatrix} x \\ y \end{pmatrix} \to \begin{pmatrix} q_1 & q_2 \\ q_3 & q_4 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} q_5 \\ q_6 \end{pmatrix},$$

where all of the q_i are rational. Equivalently, $L_1 \sim L_2$ iff all of the points of L_2 have rational coordinates with respect to the coordinate system determined by L_1 (and vice-versa). This is easily an equivalence relation, with each equivalence class countable.

We first prove a lemma which will help us deal with rotations.

Lemma 2.2. *Let L_1 be a lattice, and L_2 obtained from L_1 by a rational rotation. Let $S \subseteq \mathbb{R}^2$ satisfy the following:*

1. *For every lattice L which is a rational translation of L_1, $S \cap L \neq \emptyset$.*
2. *For all distinct z_1, $z_2 \in S$, $\rho(z_1, z_2)^2 \notin \mathbb{Z}$.*

Then for every lattice L' which is a rational translation of L_2 we have $S \cap L' \neq \emptyset$.

Proof. Without loss of generality we may assume $L_1 = \mathbb{Z}^2$. Let the rational rotation R correspond to the matrix $M = \begin{pmatrix} \frac{a}{d} & -\frac{b}{d} \\ \frac{b}{d} & \frac{a}{d} \end{pmatrix}$, where a, b, $d \in \mathbb{Z}$, $d > 1$, and $a^2 + b^2 = d^2$. $L_2 = R(\mathbb{Z}^2)$ has standard basis vectors $\vec{u} = (\frac{a}{d}, \frac{b}{d})$ and $\vec{v} = (-\frac{b}{d}, \frac{a}{d})$. It suffices to show that for any positive integer e such that $d|e$, and any rationals of the form $r = \frac{m}{e}$, $s = \frac{n}{e}$ (m, n integers), that $S \cap L'_{r,s} \neq \emptyset$, where $L'_{r,s} = L_2 + r\vec{u} + s\vec{v}$ is the rational translation of L_2 by (r, s). Fix a positive integer e with $d|e$. Consider the e^2 set of points of the form $\frac{m}{e}\vec{u} + \frac{n}{e}\vec{v}$, where $0 \leq m, n < e$. For each such point p, we must show that there are integers $k = k_p$, $l = l_p$ such that $p + k\vec{u} + l\vec{v} \in S$.

We require the following technical lemma whose proof we give below.

Lemma 2.3. *Let e be a positive integer, and R the rational rotation with matrix $M = \begin{pmatrix} \frac{a}{d} & -\frac{b}{d} \\ \frac{b}{d} & \frac{a}{d} \end{pmatrix}$, where $d|e$. Let $L'_2 = \frac{1}{e}R(\mathbb{Z}^2)$. Then there are exactly e^2 points of the scaled lattice L'_2 which are of the form (x, y) with $0 \leq x, y < 1$.*

Granting the lemma, we finish the proof of lemma 2.2. Let T denote the e^2 set of points in L_2' of the form (x, y) with $0 \leq x, y < 1$. Note that each of these points has coordinates (x, y) with x and y rational (in fact, their denominators can be taken to be de). By property (1) of S, for each such point (x, y) there are integers (k', l') such that $(x, y) + (k', l') \in S$. For each such (x, y), let $(x', y') = (x, y) + (k', l')$ denote the corresponding point in S. Clearly the map $f(x, y) = (x', y')$ from T into S is one-to-one. Thus $f[T]$ is a subset of S of size exactly e^2. Note also that in the coordinate system determined by L_2, each point of $f[T]$ has coordinates in $\frac{1}{e}\mathbb{Z}^2$ (since this is true of the points in T, and (k', l') has coordinates with respect to L_2 which have denominators d and $d|e$). For each point $(x', y') \in f[T]$, let k'', l'' be integers such that $(x'', y'') \doteq (x', y') + k''\vec{u} + l''\vec{v}$ has coordinates with respect to L_2 of the form $(\frac{m}{e}, \frac{n}{e})$, where $0 \leq m, n < e$. Let g be the function defined on $f[T]$ sending (x', y') to (x'', y''). Note that g is one-to-one, or else we would violate property (2) of S. Thus, $(g \circ f)[T]$ consists of e^2 points which in the L_2 coordinate system all have coordinates of the form $(\frac{m}{e}, \frac{n}{e})$ where $0 \leq m, n < e$. Since there are only e^2 such points, $(g \circ f)[T]$ exhausts this set. By definition of g, we thus have for any point p having L_2 coordinates of the form $(\frac{m}{e}, \frac{n}{e})$, $0 \leq m, n < e$, there are integers $k = -k''$, $l = -l''$ such that $p + k\vec{u} + l\vec{v} \in S$. This completes the proof of lemma 2.2. □

Proof of lemma 2.3. Scaling by e, the lemma follows immediately from the following well-known more general fact about lattices: Suppose $v_1, \dots, v_d$ are linearly independent vectors in $\mathbb{Z}^d$. Let $D = \det(v_1, \dots, v_d)$. Then there are exactly D points of $\mathbb{Z}^d$ of the form $a_1v_1 + \dots a_dv_d$ where $0 \leq a_1, \dots, a_d < 1$. To see this, let R be the fundamental domain for the lattice determined by the v_i. That is, $R = \{a_1v_1 + \dots a_dv_d : 0 \leq a_1, \dots, a_d < 1, a_i \in \mathbb{R}\}$. Suppose there are D' points of $\mathbb{Z}^d$ in R. Clearly any translation of R of the form $R + n_1v_1 + \cdots + n_dv_d$, where the n_i are integers, also contains exactly D' points of $\mathbb{Z}^d$. Thus, $nR = \{a_1v_1 + \dots a_dv_d : 0 \leq a_1, \dots, a_d < n, a_i \in \mathbb{R}\}$ contains exactly $(D')n^d$ points of $\mathbb{Z}^d$. On the other hand, a volume argument shows this number to be of the form $(D + o(1))n^d$. □

Lemma 2.4. *Let L be a lattice and $z \in \mathbb{R}^2$. Suppose z has coordinates (x, y) with respect to the lattice L, where at least one of x, y is irrational. Then there is a line $l = l(z, L)$ such that if w has rational coordinates with respect to L and $w \notin l$, then $\rho(w, z)^2 \notin \mathbb{Q}$.*

Proof. Without loss of generality, suppose $L = \mathbb{Z}^2$. Suppose $z = (x, y)$ with at least one of x, y irrational and $w = (a, b) \in \mathbb{Q}^2$. If $\rho(w, z)^2 \in \mathbb{Q}$, then $(x-a)^2 + (y-b)^2 \in \mathbb{Q}$, and so

$$x^2 + y^2 - 2ax - 2yb \in \mathbb{Q}.$$

If $w_1 = (a_1, b_1)$ and $w_2 = (a_2, b_2)$ were two such points, then subtracting the corresponding equations we would have

$$2(a_1 - a_2)x + 2(b_1 - b_2)y \in \mathbb{Q}. \tag{1}$$

If $w_3 = (a_3, b_3)$ were a third such point, then we likewise have

$$2(a_1 - a_3)x + 2(b_1 - b_3)y \in \mathbb{Q}. \tag{2}$$

If w_1, w_2, w_3 were not collinear, then we could solve equations (1), (2) for x and y, and these numbers would both be rational, a contradiction. Thus, all such points w (if any) must lie on a single line. □

Lemma 2.5. *Let L_1, L_2 be lattices which are not equivalent. Then there is at most one point which has rational coordinates with respect to both L_1 and L_2.*

Proof. Assume without loss of generality that $L_1 = \mathbb{Z}^2$. If there were two points in $\mathbb{Q}^2$ having rational coordinates with respect to L_2, then the standard basis vectors $\vec{u}$, $\vec{v}$ of L_2 would also have rational coordinates. Since one point of L_2 has rational coordinates, it follows that all of the points of L_2 have rational coordinates, that is, $L_1 \sim L_2$. □

We now turn to the proof of theorem 1.2.

If $L \subseteq \mathbb{R}^2$ is an isometric copy of $\mathbb{Z}^2$, let $[L]$ denote the equivalence class of L under the equivalence relation $\sim$ of definition 2.1. Let $\mathfrak{L}$ denote the family of all equivalence classes. By AC, let $\mathcal{L} \to L(\mathcal{L})$ be a function which picks for each equivalence class $\mathcal{L}$ a member $L(\mathcal{L}) \in \mathcal{L}$.

To carry out the main construction, we first describe a particular enumeration of the equivalence classes of the lattices. Let $\kappa(\emptyset) = 2^\omega$, and let $\{M_{\alpha_0} : \alpha_0 < \kappa(\emptyset)\}$, be a continuous increasing chain of elementary substructures of a large V_κ ($V_{\omega+1}$ will actually suffice) with $|M_{\alpha_0}| < \kappa(\emptyset)$ for all $\alpha_0 < \kappa(\emptyset)$ and such that every equivalence class of lattices is in some M_{α_0}. Assume also $M_0 = \emptyset$. Let $N_{\alpha_0} = M_{\alpha_0+1} - M_{\alpha_0}$. In general, suppose that $M_{\vec{\alpha}}$ is defined for $\vec{\alpha}$ in a certain subtree of $\mathrm{ON}^{<\omega}$. If $M_{\alpha_0,\ldots,\alpha_k}$ is defined, we assume also that $\kappa(\alpha_0,\ldots,\alpha_{k-1})$ has been defined and is an uncountable cardinal. Furthermore, we assume in this case that $M_{\alpha_0,\ldots,\alpha_{k-1},\beta}$ is defined iff $\beta < \kappa(\alpha_0,\ldots,\alpha_{k-1})$. We let $N_{\alpha_0,\ldots,\alpha_k}$ denote $M_{\alpha_0,\ldots,\alpha_k+1} - M_{\alpha_0,\ldots,\alpha_k}$.

Suppose now that $M_{\alpha_0,\ldots,\alpha_k}$ is defined. If $N_{\alpha_0,\ldots,\alpha_k}$ contains only countably many equivalence classes of lattices, let $\mathcal{L}_{\alpha_0,\ldots,\alpha_k;n}$ enumerate them. In this case, $(\alpha_0,\ldots,\alpha_k)$ is a terminal node in the tree of indices $\vec{\alpha}$ for which $M_{\vec{\alpha}}$ is defined. Otherwise, let $\kappa(\alpha_0,\ldots,\alpha_k) = |N_{\alpha_0,\ldots,\alpha_k} \cap \mathfrak{L}|$ and write

$$N_{\alpha_0,\ldots,\alpha_k} = \bigcup_{\alpha_{k+1} < \kappa(\alpha_0,\ldots,\alpha_k)} M_{\alpha_0,\ldots,\alpha_k,\alpha_{k+1}},$$

as a continuous, increasing union, where each $M_{\alpha_0,\ldots,\alpha_k,\alpha_{k+1}}$ is the intersection of $N_{\alpha_0,\ldots,\alpha_k}$ with an elementary substructure of V_κ, and each $M_{\alpha_0,\ldots,\alpha_k,\alpha_{k+1}}$ contains fewer than $\kappa(\alpha_0,\ldots,\alpha_k)$ many equivalence classes of lattices. Assume also $M_{\alpha_0,\ldots,\alpha_k,0} = \emptyset$. Easily, the tree of indices is well-founded (since the $\kappa_{\vec{\alpha}}$ are decreasing along any branch).

If $\vec{\alpha}$ is incompatible with $\vec{\beta}$, then $N_{\vec{\alpha}}$ and $N_{\vec{\beta}}$ have no equivalence class of lattices in common. Furthermore, every equivalence class occurs as some $\mathcal{L}_{\alpha_0,\ldots,\alpha_k;n}$. Thus, the $\mathcal{L}_{\alpha_0,\ldots,\alpha_k;n}$ precisely enumerate the equivalence classes of lattices. We consider the indices to be (well) ordered lexicographically.

The following simple lemma will be used.

Lemma 2.6. *Suppose $\vec{\alpha}$ is an index for which $M_{\vec{\alpha}}$ is defined. Let $a_1,\ldots,a_m \in M_{\vec{\alpha}}$ and suppose b is definable from $a_1,\ldots,a_m$ in V_κ. Then $b \in \bigcup_{\vec{\beta} \leq \vec{\alpha}} M_{\vec{\beta}}$.*

Proof. Let $\vec{\alpha} = (\alpha_0,\ldots,\alpha_k)$ and assume $b \notin \bigcup_{\vec{\beta} \leq \vec{\alpha}} M_{\vec{\beta}}$. Since $M_{\alpha_0,\ldots,\alpha_k}$ is relatively closed under the skolem functions of V_κ inside of $N_{\alpha_0,\ldots,\alpha_{k-1}}$, it follows that $b \notin N_{\alpha_0,\ldots,\alpha_{k-1}}$. Since $b \notin M_{\alpha_0,\ldots,\alpha_{k-1}}$ by assumption, we thus have $b \notin M_{\alpha_0,\ldots,\alpha_{k-1}+1}$. Continuing, we eventually have $b \notin M_{\alpha_0+1}$, a contradiction since M_{α_0+1} is a substructure of V_k containing the a_i. □

Fix now a terminal index $\vec{\alpha} = (\alpha_0, \dots, \alpha_k)$. Assume inductively we have defined for each terminal index $\vec{\beta} < \vec{\alpha}$ a set $S_{\vec{\beta}} \subseteq \mathbb{R}^2$ which satisfy the following:

(1) If $\vec{\beta}_1 < \vec{\beta}_2 < \vec{\alpha}$, then $S_{\vec{\beta}_1} \subseteq S_{\vec{\beta}_2}$.
(2) For every terminal index $\vec{\beta}$ less than $\vec{\alpha}$, $S_{\vec{\beta}}$ meets every lattice in every equivalence class $\mathcal{L}_{\vec{\beta};n}$.
(3) Every point of $S_{\vec{\beta}} - \bigcup_{\vec{\gamma}<\vec{\beta}} S_{\vec{\gamma}}$ lies on some lattice of the form $\mathcal{L}_{\vec{\beta};n}$.
(4) For all distinct $z_1, z_2 \in S_{\vec{\beta}}$, $\rho(z_1, z_2)^2 \notin \mathbb{Z}$.
(5) Suppose $\vec{\beta}_1 < \vec{\beta}_2 < \vec{\alpha}$, $x \in S_{\vec{\beta}_1}$, and $y \in S_{\vec{\beta}_2} - \bigcup_{\vec{\gamma}<\vec{\beta}_2} S_{\vec{\gamma}}$. Then if $\rho(x,y)^2 \in \mathbb{Q}$ then x, y both have rational coordinates with respect to some lattice of the form $\mathcal{L}_{\vec{\beta}_2;n}$.

Let $S_{<\vec{\alpha}} = \bigcup_{\vec{\beta}<\vec{\alpha}} S_{\vec{\beta}}$. We show how to extend $S_{<\vec{\alpha}}$ to a set $S_{\vec{\alpha}}$ also satisfying 4, 5 and such that $S_{\vec{\alpha}}$ meets every lattice in each equivalence class $\mathcal{L}_{\vec{\alpha},n}$. This suffices to prove theorem 1.2.

To ease notation, let $\mathcal{L}_n = \mathcal{L}_{\vec{\alpha};n}$, and let $L_n = L(\mathcal{L}_n)$. From lemma 2.2, it suffices to maintain property 4, have property 5 when $\vec{\beta}_2 = \vec{\alpha}$, and have $S_{\vec{\alpha}}$ meet every rational translation of each L_n (recall a rational translation of L_n refers to a motion which is a translation in the coordinate system of L_n).

For integers n, d, i, j, let $L_n^{d,i,j}$ denote the translation of L_n by the amount $(\frac{i}{d}, \frac{j}{d})$ (in the coordinate system of L_n).

Note for the following the simple fact that if two distinct points y, z lie on a lattice L, then L is definable from y and z. In fact, there are only finitely many lattices containing both y and z. More generally, if y, z both have rational coordinates with respect to L, then L is definable from y and z.

Claim 2.7. For each n and rationals $\frac{i}{d}, \frac{j}{d}$, there is a finite set of lines $G_n(\frac{i}{d}, \frac{j}{d})$ with the following property: if $c \in S_{<\vec{\alpha}}$ does not have rational coordinates with respect to L_n, if $z \in L_n^{d,i,j}$, and if $\rho(c,z)^2 \in \mathbb{Q}$, then $z \in \cup G_n(\frac{i}{d}, \frac{j}{d})$.

Proof. Suppose there is a $z_1 \in L_n^{d,i,j}$ and a $c_1 \in S_{<\vec{\alpha}}$ not rational with respect to L_n such that $\rho(z_1, c_1)^2 \in \mathbb{Q}$ (otherwise there is nothing to prove). Let $l_1 = l(c_1, L_n^{d,i,j})$ be the line (necessarily through z_1) given by lemma 2.4. Suppose there is a $z_2 \notin l_1$, $z_2 \in L_n^{d,i,j}$, and a $c_2 \in S_{<\vec{\alpha}}$ not rational with respect to L_n with $\rho(z_2, c_2)^2 \in \mathbb{Q}$ (necessarily $c_2 \neq c_1$). Let $l_2 = l(c_2, L_n^{d,i,j})$ be given by lemma 2.4. Continuing, construct $z_m \in L_n^{d,i,j}$, $c_m \in S_{<\vec{\alpha}}$ if possible so that $z_m \notin l_1 \cup \cdots \cup l_{m-1}$ and $\rho(z_m, c_m)^2 \in \mathbb{Q}$. If the construction fails at some point, then the claim is proved. Assume toward a contradiction that we continue to produce an infinite sequence $z_1, c_1, z_2, c_2, \dots$. Note that the c_i are distinct. Let $\vec{\beta}^m = (\beta_0^m, \dots, \beta_l^m)$ be the terminal index (where l depends on m) such that $c_m \in N_{\vec{\beta}^m}$. Thus, $\vec{\beta}^m < \vec{\alpha}$. Easily, there is a $k' \leq k$ such that for infinitely many m we have $\beta_0^m = \alpha_0, \dots, \beta_{k'-1}^m = \alpha_{k'-1}$, and $\beta_{k'}^m < \alpha_{k'}$ (we allow $k' = 0$, in which case we have $\beta_0^m < \alpha_0$). Let $\vec{\gamma} = (\alpha_0, \dots, \alpha_{k'})$. Thus $\vec{\gamma} \leq \vec{\alpha}$, and for these infinitely many m we have $c_m \in M_{\vec{\gamma}}$. Let m_1, m_2, m_3 be three such m. Let $r_1 = \rho(c_{m_1}, z_{m_1})$, and similarly for r_2, r_3. We apply lemma B to the circles with centers at c_{m_i} of radii r_i and the points z_{m_i}. Note that we are not in the exceptional case of lemma B, as otherwise we would have $\rho(z_{m_1}, z_{m_2}) = \rho(c_{m_1}, c_{m_2})$. This contradicts the fact that $\rho(c_{m_1}, c_{m_2})^2 \notin \mathbb{Z}$ as they lie in $S_{<\vec{\alpha}}$ (note that $\rho(z_{m_1}, z_{m_2})^2 \in \mathbb{Z}$ as z_{m_1}, z_{m_2} lie in $L_n^{d,i,j}$). From lemma B, the points z_{m_1}, z_{m_2}, z_{m_3} are definable from c_{m_1}, c_{m_2}, and c_{m_3}. Since

L_n is definable from z_{m_1}, z_{m_2}, z_{m_3} (in fact, from any two of them), L_n is definable from c_{m_1}, c_{m_2}, and c_{m_3}. It follows from lemma 2.6 that L_n lies in some $M_{\vec{\beta}}$, for $\vec{\beta} \leq \vec{\alpha}$. This contradicts $L_n \in N_{\vec{\alpha}}$. □

We next construct a sequence of points $\{x_m\}_{m\in\omega}$, which we view as "potential points" to be added to the set $S_{<\vec{\alpha}}$ to form $S_{\vec{\alpha}}$. We will in fact have $S_{\vec{\alpha}} - S_{<\vec{\alpha}} \subseteq \{x_m : m \in \omega\}$.

Let $(n,d,i,j,a,b,p) \to \langle n,d,i,j,a,b,p\rangle \in \omega$ be a fixed bijection between ω^7 and ω. For $m \in \omega$, let $(m)_0$, $(m)_1, \ldots$ be the "decoding functions" for our bijection, that is, $m = \langle (m)_0, (m)_1, \ldots, (m)_6\rangle$. If the integer m is understood, we will write n for $(m)_0$, d for $(m)_1$, etc. Let $M_n^{d,i,j,a,b} \subseteq L_n^{d,i,j}$ be the sublattice of points whose coordinates in the L_n system are of the form $(\frac{i}{d}+k, \frac{j}{d}+l)$, where $k \equiv a$, $l \equiv b$ mod d.

We inductively construct the x_m to satisfy the following (here n denotes $(m)_0$, d denotes $(m)_1$, etc.).

(1) $x_m \in M_n^{d,i,j,a,b}$.
(2) If $m_1 \neq m_2$, then $x_{m_1} \neq x_{m_2}$.
(3) Suppose $m_1 < m_2$. If x_{m_1} does not have rational coordinates with respect to L_{n_2} ($= L_{(m_2)_0}$), then $x_{m_2} \notin l(x_{m_1}, L_{n_2})$, where $l(x_{m_1}, L_{n_2})$ is as in lemma 2.4.
(4) $x_m \notin \cup G_n(\frac{i}{d}, \frac{j}{d})$.

Since at each step there are only finitely many points and lines to avoid, there is no problem defining the sequence $\{x_m\}$.

Claim 2.8. For each n, there is at most one point in $S_{<\vec{\alpha}} \cup \{x_m | (m)_0 \neq n\}$ having rational coordinates with respect to L_n.

Proof. Suppose y and z were two such points. Suppose first both y and z were in $S_{<\vec{\alpha}}$. Say $y \in S_{\vec{\beta}_1} - \bigcup_{\vec{\gamma}<\vec{\beta}_1} S_{\vec{\gamma}}$, $z \in S_{\vec{\beta}_2} - \bigcup_{\vec{\gamma}<\vec{\beta}_2} S_{\vec{\gamma}}$ where $\vec{\beta}_1 \leq \vec{\beta}_2$. If $\vec{\beta}_1 = \vec{\beta}_2$, then each of y, z lies on a lattice in $N_{\vec{\beta}_2}$. Since L_n is definable from y and z, L_n is definable from two points which lie in some $M_{\vec{\beta}}$ for some $\vec{\beta} \leq \vec{\alpha}$. From lemma 2.6 it follows that $L_n \in \bigcup_{\vec{\gamma}\leq\vec{\alpha}} M_{\vec{\gamma}}$, a contradiction. If $\vec{\beta}_1 < \vec{\beta}_2$ then from inductive property 5 we have either $\rho(y,z)^2 \notin \mathbb{Q}$ which is impossible (as both y, z have rational coordinates with respect to L_n), or else y, z both have rational coordinates with respect to some lattice L in $N_{\vec{\beta}_2}$. This would again imply that $L_n \in \bigcup_{\vec{\gamma}\leq\vec{\alpha}} M_{\vec{\gamma}}$, a contradiction. Suppose next that $y \in S_{<\vec{\alpha}}$ and $z = x_m$ where $(m)_0 \neq n$. Since y and z are rational with respect to L_n we have $\rho(y,z)^2 \in \mathbb{Q}$. Since $x_m \notin \cup G_{(m)_0}(\frac{i}{d}, \frac{j}{d})$ (where $d = (m)_1$, $i = (m)_2$, $j = (m)_3$), we must have that y is rational with respect to $L_{(m)_0}$ (as otherwise $\rho(y,z)^2 \notin \mathbb{Q}$). Thus, both y and z have rational coordinates with respect to both L_n and $L_{(m)_0}$, a contradiction to lemma 2.5. Suppose now $y = x_{m_1}$, $z = x_{m_2}$, where $(m_1)_0, (m_2)_0 \neq n$. Let $n_1 = (m_1)_0$, $n_2 = (m_2)_0$, and assume without loss of generality that $m_1 < m_2$. Again, $\rho(y,z)^2 \in \mathbb{Q}$, as both are rational with respect to L_n. From the definition of x_{m_2}, we must have that x_{m_1} is rational with respect to L_{n_2} (as otherwise $\rho(y,z)^2 \notin \mathbb{Q}$). Thus, both y and z are rational with respect to L_n and L_{n_2}, a contradiction. □

Let w_n, if it exists, be the unique point having rational coordinates with respect to L_n which is either in $S_{<\vec{\alpha}}$ or of the form x_m for some m with $(m)_0 \neq n$.

By induction on n we define sets $T_n \subseteq \{x_m : (m)_0 = n\}$. Assume $T_0, \dots, T_{n-1}$ have been defined, and for $i < n$, $T_i \subseteq \{x_m : (m)_0 = i\}$. Let $P_1 = \{x_m : (m)_0 = n\}$. Let $P_2 = P_1 - \{w_i : i < n\}$. If w_n exists and $w_n \in S_{<\vec{\alpha}} \cup \bigcup_{i<n} T_i$, let $w = w_n$ and $P = P_2 \cup \{w\}$. If w_n exists, but $w_n \notin S_{<\vec{\alpha}} \cup \bigcup_{i<n} T_i$, let $P = P_2 - \{w_n\}$ and let w be some point in P. If w_n does not exist, let $P = P_2$ and let w be some point in P. Apply now lemma A$'$ to the lattice L_n, the set P, and the point w. Let T_n be the set produced from lemma A$'$.

Let $S_{\vec{\alpha}} = S_{<\vec{\alpha}} \cup \bigcup_n T_n$. Clearly $S_{\vec{\alpha}}$ meets each lattice in each $\mathcal{L}_n$, and $S_{\vec{\alpha}} \subseteq \bigcup_{\vec{\beta} \leq \vec{\alpha}, k} \cup \mathcal{L}_{\vec{\beta}, k}$. Thus, inductive property 2 is still satisfied. Properties 1 and 3 are trivially satisfied. By construction, if $z \in S_{\vec{\alpha}} - S_{<\alpha}$ (say $z \in T_n - \bigcup_{m<n} T_m$) and $y \in S_{<\vec{\alpha}}$, then either $\rho(y,z)^2 \notin \mathbb{Q}$ or y, z are both rational with respect to L_n. Thus property 5 continues to hold.

To complete the proof, we show that for any y, $z \in S_{\vec{\alpha}}$ that $\rho(y,z)^2 \notin \mathbb{Z}$. By induction, we may assume y, z do not both lie in $S_{<\vec{\alpha}}$. Suppose first that $y \in S_{<\vec{\alpha}}$ and $z \in T_n - \bigcup_{i<n} T_i$. Say $z = x_m$. Note that $(m)_0 = n$ as otherwise $z = w_n$, and this is impossible since from the construction $w_n \in T_n$ implies $w_n \in \bigcup_{i<n} T_i$. If y does not have rational coordinates with respect to L_n, then since $x_m \in P$ (P as in the definition of T_n) and $P \cap (\cup G_n(\frac{i}{d}, \frac{j}{d})) = \emptyset$, we would have $\rho(y,z)^2 \notin \mathbb{Q}$. So, assume y is rational with respect to L_n, and hence $y = w_n$. In defining T_n in this case, we took $w = w_n$ in applying lemma A$'$. Since $z \in T_n$, we therefore have $\rho(y,z)^2 \notin \mathbb{Z}$. Suppose next that y first appears in T_{n_1}, and z first appears in T_{n_2}. From the construction it again follows that $y = x_{m_1}$ where $(m_1)_0 = n_1$ and $z = x_{m_2}$ where $(m_2)_0 = n_2$ (in fact, $y \neq w_{n_1}$ and $z \neq w_{n_2}$). If $n_1 = n_2$ then from the definition of T_{n_1} we have $\rho(y,z)^2 \notin \mathbb{Z}$. Assume without loss of generality that $n_1 < n_2$. If $x_{m_1} = w_{n_2}$, then by definition of T_{n_2} we have $\rho(y,z)^2 \notin \mathbb{Z}$, so assume $y = x_{m_1} \neq w_{n_2}$. By construction, $z = x_{m_2} \neq w_{n_1}$, as $n_1 < n_2$ (w_{n_1} cannot first get into T_{n_2} as $n_1 < n_2$; recall the definition of P_2). Thus, y does not have rational coordinates with respect to L_{n_2}, and z does not have rational coordinates with respect to L_{n_1}. If say $m_1 > m_2$ (the other case being identical), it now follows from the definition of x_{m_1} that $\rho(x_{m_1}, x_{m_2})^2 \notin \mathbb{Q}$.

This completes the proof of theorem 1.2, assuming lemmas A$'$ and B.

3. Proof of Lemma A$'$

Our goal in this section is to prove lemma A$'$. Actually, we concentrate on proving lemma A, as a minor adjustment to this proof will prove lemma A$'$.

Throughout we use the following notation. For $a, b \in \mathbb{Z}$ we write $a|b$ for "a divides b." If $b > 0$, we write $a \mod b$ for the unique $0 \leq a' < b$ with $a' \equiv a \mod b$. For rationals r, s, let $L_{r,s} = \mathbb{Z}^2 + (r,s)$ be the rational translation of $\mathbb{Z}^2$ by (r,s).

Recall the statement of lemma A:

Lemma 3.1 (A)**.** *Then there is a set $S \subseteq \mathbb{R}^2$ satisfying the following.*

(1) *For every rationals r, s, $S \cap L_{r,s} \neq \emptyset$.*
(2) *For all distinct $z_1, z_2 \in S$, $\rho(z_1, z_2)^2 \notin \mathbb{Z}$.*

Let $R = \mathbb{Q}^2 \cap ([0,1) \times [0,1))$. For each positive integer d let $R_d \subseteq R$ be defined by $R_d = \{(\frac{i}{d}, \frac{j}{d}) : 0 \leq i, j < d\}$.

We may reformulate lemma A as follows. For all $(r,s) \in R$, there are integers $k = k(r,s)$ and $l = l(r,s)$ such that if $S = \{(r + k(r,s), s + l(r,s)) : r, s \in \mathbb{Q}\}$, then for all distinct $z_1, z_2 \in S$, $\rho(z_1, z_2)^2 \notin \mathbb{Z}$ (property 2 of lemma A). Thus, our problem is to define the integer valued functions $k(r, s)$ and $l(r, s)$ satisfying property 2.

Our plan for defining these functions is to proceed inductively as follows. Assume we have defined the values $k(r, s)$, $l(r, s)$ for all $(r, s) \in R_d$ for some $d > 1$. Assume that the partial functions k, l so far defined satisfy property 2, more precisely, assume:

$(*)_d$: For any distinct $(\frac{i_1}{d}, \frac{j_1}{d})$, $(\frac{i_2}{d}, \frac{j_2}{d})$ in R_d, if $z_1 = (\frac{i_1}{d} + k_1, \frac{j_1}{d} + l_1)$, $z_2 = (\frac{i_2}{d} + k_2, \frac{j_2}{d} + l_2)$ where $k_1 = k(\frac{i_1}{d}, \frac{j_1}{d})$, $l_1 = l(\frac{i_1}{d}, \frac{j_1}{d}))$ and similarly for k_2, l_2, then $\rho(z_1, z_2)^2 \notin \mathbb{Z}$.

Let p be a prime, and $d' = pd$. We then show that we can extend the k, l functions to rational pairs in $R_{d'}$, maintaining property 2. This clearly suffices to prove lemma A.

We note that in this inductive step of the proof, it is important that we assume that the k, l functions are defined on *all* of the points $(\frac{i}{d}, \frac{j}{d})$ in R_d (and satisfy property 2, of course). It is not true in general that functions k, l which are defined on a subset of $R_{d'}$ (and satisfy property 2) can be extended to functions defined on all of $R_{d'}$ also satisfying property 2.

We make the following simple general observation. If $x = (\frac{i_1}{d} + k_1, \frac{j_1}{d} + l_1)$, $y = (\frac{i_2}{d} + k_2, \frac{j_2}{d} + l_2)$, then $\rho(x, y)^2 \in \mathbb{Z}$ iff

$$(i_1 - i_2)^2 + (j_1 - j_2)^2 + 2d[(i_1 - i_2)(k_1 - k_2) + (j_1 - j_2)(l_1 - l_2)] \in d^2\mathbb{Z}. \tag{3}$$

We use this frequently below. We will also frequently let a denote $i_1 - i_2$ and let b denote $j_1 - j_2$, in which case our equation becomes

$$(a^2 + b^2) + 2d[a(k_1 - k_2) + b(l_1 - l_2)] \in d^2\mathbb{Z}. \tag{4}$$

3.1. **A Special Case.** Since the general inductive step is somewhat technical, we feel it helps to illustrate the main points involved by considering a special case. Thus, we first show how to define the k, l functions on the points in R_{p^n}, for p a prime, and then show how to extend the functions from R_{p^n} to $R_{p^{n+1}}$. [We could start with $n = 1$, but this does not really simplify the argument, and would cause us to repeat part of the argument.] These arguments are not necessary for the general case, and the reader may choose to skip down to the general argument.

So, let $d = p^n$. Consider two points of the form $z_1 = (\frac{i_1}{p^n} + k_1, \frac{j_1}{p^n} + l_1)$, $z_2 = (\frac{i_2}{p^n} + k_2, \frac{j_2}{p^n} + l_2)$, where $0 \le i_1, i_2, j_1, j_2 < p^n$ and k_1, k_2, l_1, l_2 are integers. Substituting into equation 4, we see that $\rho(z_1, z_2)^2 \notin \mathbb{Z}$ unless

$$(a^2 + b^2) + 2p^n[a(k_1 - k_2) + b(l_1 - l_2)] \equiv 0 \mod p^{2n}. \tag{5}$$

First note that if $p = 2$ or $p \equiv 3 \mod 4$, then we may define the k, l values arbitrarily and equation 5 will have no solutions. For clearly if equation 4 holds then we must have $p^n | a^2 + b^2$. Since $0 \le i_1, i_2 < p^n$, p^n does not divide a, and likewise p^n does not divide b. Say $a = p^e u$, $b = p^f u$, where $e, f < n$ and u, v are prime to p. Suppose w.l.o.g. that $e \le f$. Dividing equation 5 through by p^{2e} we get $u^2 + p^{2f-2e}v^2 \equiv 0 \mod p$. This implies $e = f$. Hence, $u^2 + v^2 \equiv 0 \mod p$. Thus, $(\frac{v}{u})^2 \equiv -1 \mod p$, a contradiction if $p \equiv 3 \mod 4$, since -1 is not a square mod p in this case. If $p = 2$, then since u, v are both odd, $u^2 + v^2 \equiv 2 \mod 4$. Dividing equation 5 through by p^{2e} gives

$$(u^2 + v^2) + 2p^{n-e}[u(k_1 - k_2) + v(l_1 - l_2)] \equiv 0 \mod p^{2(n-e)}.$$

This is impossible, however, as 4 divides the remaining terms in this equation. Thus, if $p = 2$ or $p \equiv 3 \mod 4$, we may define the k, l functions arbitrarily on R_{p^n} and property 2 will be satisfied. For the rest of the special case we therefore assume $p \equiv 1 \mod 4$.

Recall that if $p \equiv 1 \mod 4$, then there are exactly two square roots of $-1 \mod p^m$ for any m. Let λ, μ, with $0 < \lambda, \mu < p^n$ be the two square roots of $-1 \mod p^n$. Note that $\lambda \equiv -\mu \mod p^n$. Note also that for any $k < n$, $(\lambda \mod p^k)$ and $(\mu \mod p^k)$ are the two square roots of $-1 \mod p^k$.

As we remarked above, if equation 5 holds, we must have $p^n | a^2 + b^2$. In this case, if $(p, a) = 1$ (and hence also $(p, b) = 1$), this gives $(\frac{b}{a})^2 \equiv -1 \mod p^n$, and hence either $b \equiv \lambda a \mod p^n$, or $b \equiv \mu a \mod p^n$. Suppose now $p|a$ (and hence $p|b$, or else equation 5 cannot hold). Say $a = p^e u$, $b = p^f v$, where e, $f < n$, and $(p, u) = (p, v) = 1$. Assuming $e \leq f$ (the other case being similar), putting these into equation 5, and dividing through by p^{2e} we have

$$(u^2 + p^{2f-2e}v^2) + p^{n-e}[u(k_1 - k_2) + p^{f-e}v(l_1 - l_2)] \in p^{2n-2e}\mathbb{Z}.$$

This clearly implies $e = f$. Also, using a previous remark, $v \equiv \lambda u \mod p^{n-e}$ or $v \equiv \mu u \mod p^{n-e}$. Multiplying through by p^e, we conclude that in all cases for equation 5 to hold, we must have either $b \equiv \lambda a \mod p^n$, or $b \equiv \mu a \mod p^n$.

Suppose, for example, that equation 5 holds and $b \equiv \lambda a \mod p^n$. Let $\tilde{\jmath}$ be the integer, $0 \leq \tilde{\jmath} < p^n$, such that $\tilde{\jmath} + \lambda i_1 \equiv j_1 \mod p^n$. Note that $\tilde{\jmath} + \lambda i_2 \equiv j_2 \mod p^n$ as well. Let $\bar{\jmath}_1 = \tilde{\jmath} + \lambda i_1$, and let m_1 be such that $\bar{\jmath}_1 = j_1 + p^n m_1$. Likewise define $\bar{\jmath}_2$ and m_2. Note that $\bar{\jmath}_1 - \bar{\jmath}_2 = \lambda(i_1 - i_2)$. Also, we may express the points z_1, z_2 now as

$$z_1 = (\frac{i_1}{p^n} + k_1, \frac{\bar{\jmath}_1}{p^n} + (l_1 - m_1)), \quad z_2 = (\frac{i_2}{p^n} + k_2, \frac{\bar{\jmath}_2}{p^n} + (l_2 - m_2)).$$

Substituting into equation 3, and dividing through by p^n we obtain:

$$(i_1 - i_2)^2 \left(\frac{1 + \lambda^2}{p^n}\right) + 2(i_1 - i_2)[(k_1 - k_2) + \lambda(l_1 - l_2 - m_1 + m_2)] \equiv 0 \mod p^n.$$

Note that this makes sense as $p^n | (1 + \lambda^2)$. Let $r < n$ be such that $i_1 - i_2 = p^r u$, where $(p, u) = 1$. This equation is then equivalent to

$$(i_1 - i_2)(\frac{1}{2}) \left(\frac{1 + \lambda^2}{p^n}\right) + [(k_1 - k_2) + \lambda(l_1 - l_2 - m_1 + m_2)] \equiv 0 \mod p^{n-r}.$$

Rearranging, this becomes

$$\begin{aligned} &(k_1 + \lambda l_1) + i_1(\frac{1}{2}) \left(\frac{1 + \lambda^2}{p^n}\right) - \lambda m_1 \equiv \\ &(k_2 + \lambda l_2) + i_2(\frac{1}{2}) \left(\frac{1 + \lambda^2}{p^n}\right) - \lambda m_2 \mod p^{n-r}. \end{aligned} \tag{6}$$

This suggests the following definition.

Definition 3.2. A *good* permutation $\pi = (\pi(0), \pi(1), \ldots, \pi(p^n - 1))$ of length p^n is a permutation of the integers $(0, 1, \ldots, p^n - 1)$ such that for all $i_1 \neq i_2$ with $0 \leq i_1, i_2 < p^n$, if $i_1 - i_2 = p^r u$ where $(p, u) = 1$, then $\pi(i_1) - \pi(i_2) \not\equiv 0 \mod p^{n-r}$.

We use the following simple fact.

Fact 1. There is a good permutation of length p^n.

Proof. If $n=1$, let $\pi=(0,1,2,\dots,p-1)$. For $n>1$, suppose $i=b_0+b_1p+b_2p^2+\cdots+b_{n-1}p^{n-1}$ where $0\le b_i<p$. Set $\pi(i)=b_0p^{n-1}+b_1p^{n-2}+\cdots+b_{n-1}$. This easily works. $\square$

With the above arguments as motivation, we are now in a position to state precisely and prove two lemmas which complete the analysis for the special case $d=p^n$ we are considering.

Lemma 3.3. *Let p be a prime and $n\ge 1$. There are integer functions k, l defined on R_{p^n} such that for all distinct $(\frac{i_1}{p^n},\frac{j_1}{p^n})$, $(\frac{i_2}{p^n},\frac{j_2}{p^n})\in R_{p^n}$ we have $\rho(z_1,z_2)^2\notin\mathbb{Z}$, where $z_1=(\frac{i_1}{p^n}+k_1,\frac{j_1}{p^n}+l_1)$, $z_2=(\frac{i_2}{p^n}+k_2,\frac{j_2}{p^n}+l_2)$, and $k_1=k(\frac{i_1}{p^n},\frac{j_1}{p^n})$, $l_1=l(\frac{i_1}{p^n},\frac{j_1}{p^n})$, and similarly for k_2, l_2.*

Proof. If $p=2$ or $p\equiv 3 \mod 4$, the result is trivial (that is, we may define the k, l functions arbitrarily) as shown above. So assume $p\equiv 1 \mod 4$, and let λ, μ be the two square roots of $-1 \mod p^n$. Let $\pi=(\pi(0),\dots,\pi(p^n-1))$ be a good permutation of length p^n.

Suppose now $0\le i,j<p^n$, and we define the k, l values for the corresponding point $(\frac{i}{p^n},\frac{j}{p^n})$. Let $\tilde{\jmath}$ be such that $\tilde{\jmath}+\lambda i\equiv j \mod p^n$, and $0\le\tilde{\jmath}<p^n$. Let $\bar{\jmath}=\tilde{\jmath}+\lambda i$. Let m be the integer such that $\bar{\jmath}=j+p^n m$. Consider then the equation

$$k+\lambda l\equiv \pi(i)+\lambda m-\frac{1}{2}\left(\frac{1+\lambda^2}{p^n}\right)i \mod p^n. \tag{7}$$

Similarly, let $\tilde{\tilde{\jmath}}$ be such that $\tilde{\tilde{\jmath}}+\mu i\equiv j \mod p^n$, and let $\bar{\bar{\jmath}}=\tilde{\tilde{\jmath}}+\mu i$. Let m' be such that $\bar{\bar{\jmath}}=j+m'p^n$. Consider also the equation

$$k+\mu l\equiv \pi(i)+\mu m'-\frac{1}{2}\left(\frac{1+\mu^2}{p^n}\right)i \mod p^n. \tag{8}$$

Equations 7 and 8 form a non-singular system $\mod p^n$, and we let (k,l) be a solution (to be specific, say the unique solution with $0\le k,l<p^n$). This completes the definition of the k, l functions on R_{p^n}.

Suppose now that $(\frac{i_1}{p^n},\frac{j_1}{p^n})$, and $(\frac{i_2}{p^n},\frac{j_2}{p^n})$ are given with $0\le i_1,i_2,j_1,j_2<p^n$. Let (k_1,l_1) and (k_2,l_2) be the corresponding values as defined above. Let $z_1=(\frac{i_1}{p^n}+k_1,\frac{j_1}{p^n}+l_1)$ and similarly for z_2. We must show that $\rho(z_1,z_2)^2\notin\mathbb{Z}$.

Again let $a=i_1-i_2$ and $b=j_1-j_2$. From equation 4, we must show that

$$(a^2+b^2)+2p^n[a(k_1-k_2)+b(l_1-l_2)]\not\equiv 0 \mod p^{2n}.$$

As we have already noted, this inequality is immediate unless $b\equiv\lambda a \mod p^n$ or $b\equiv\mu a \mod p^n$. Assume $b\equiv\lambda a \mod p^n$, the other case being similar. Let $\tilde{\jmath}$ be such that $\tilde{\jmath}+\lambda i_1\equiv j_1 \mod p^n$. Let $\bar{\jmath}_1=\tilde{\jmath}+\lambda i_1$, and let m_1 be such that $\bar{\jmath}_1=j_1+p^n m_1$. Since $b\equiv\lambda a \mod p^n$, we also have that $\tilde{\jmath}+\lambda i_2\equiv j_2 \mod p^n$. Let $\bar{\jmath}_2=\tilde{\jmath}+\lambda i_2$, and let m_2 be such that $\bar{\jmath}_2=j_2+p^n m_2$. Note that $\bar{\jmath}_1-\bar{\jmath}_2=\lambda(i_1-i_2)$. If we let $r<n$ be such that $i_1-i_2=p^r u$ where $(p,u)=1$, then as we showed above, this equation reduces to

$$(k_1+\lambda l_1)+i_1(\frac{1}{2})(\left(\frac{1+\lambda^2}{p^n}\right)-\lambda m_1\not\equiv(k_2+\lambda l_2)+i_2(\frac{1}{2})(\left(\frac{1+\lambda^2}{p^n}\right)-\lambda m_2 \mod p^{n-r}. \tag{9}$$

Substituting in the definitions of k_1, l_1, k_2, l_2 (c.f. equation 7; note that this equation holds mod p^n, and so mod p^{n-r}) this becomes $\pi(i_1)\not\equiv\pi(i_2) \mod p^{n-r}$. This, however, follows immediately from the definition of r and the fact that π is good. $\square$

The following remark on the proof just given will be used in the following arguments.

Remark 3.4. Although we used a single permutation π in the proof of lemma 3.3, a somewhat more general construction could have been used. Namely, suppose that for each of the two square roots λ, μ of $-1 \mod p^n$, and for each $\tilde{\jmath}$ with $0 \leq \tilde{\jmath} < p^n$, good permutations $\pi^\lambda_{\tilde{\jmath}}$ and $\pi^\mu_{\tilde{\jmath}}$ of length p^n are given. Then in defining $k(i,j)$, $l(i,j)$, we could have used the analogs to equations 7, 8 where in equation 7 for $\pi(i)$ we use $\pi^\lambda_{\tilde{\jmath}}(i)$, and likewise for equation 8 (here $\tilde{\jmath}$ is as in the definition of m). This follows since in the non-trivial case in the proof of lemma 3.3, the points $(\frac{i_1}{p^n}, \frac{j_1}{p^n})$, $(\frac{i_2}{p^n}, \frac{j_2}{p^n})$ have the same value of $\tilde{\jmath}$, and thus the analogs of equation 7 for these two points are referring to the same permutation (and likewise for equation 8).

The following lemma gives a sort of converse to the argument used in the proof of lemma 3.3, and of remark 3.4.

Lemma 3.5. *Suppose to all $0 \leq i,j < p^n$ we have assigned a pair of integers $(k,l) = (k(i,j), l(i,j))$ such that for any pair of distinct points of the form $z_1 = (\frac{i_1}{p^n} + k(i_1,j_1), \frac{j_1}{p^n} + l(i_1,j_1))$, $z_2 = (\frac{i_2}{p^n} + k(i_2,j_2), \frac{j_2}{p^n} + l(i_2,j_2))$ we have $\rho(z_1,z_2)^2 \notin \mathbb{Z}$. For each of the two square roots λ, μ of $-1 \mod p^n$, for each $0 \leq \tilde{\jmath} < p^n$, and each $0 \leq i < p^n$, define $0 \leq \pi^\lambda_{\tilde{\jmath}}(i) < p^n$ to be the integer such that*

$$\pi^\lambda_{\tilde{\jmath}}(i) \equiv (k(i,j) + \lambda l(i,j)) - \lambda m + \frac{1}{2}\left(\frac{1+\lambda^2}{p^n}\right) i \mod p^n.$$

Here $0 \leq j < p^n$ is the integer such that $\tilde{\jmath} + \lambda i \equiv j \mod p^n$, and also $\tilde{\jmath} + \lambda i = j + mp^n$. Then, $\pi^\lambda_{\tilde{\jmath}}$ is a good permutation of p^n.

Proof. Fix one of the roots, say λ, and a value of $\tilde{\jmath}$. Let i_1, i_2 be distinct integers with $0 \leq i_1, i_2 < p^n$. Let j_1, j_2 be as in the statement of the lemma for i_1, i_2 respectively. Let $z_1 = (\frac{i_1}{p^n} + k(i_1,j_1), \frac{j_1}{p^n} + l(i_1,j_1))$, and $z_2 = (\frac{i_2}{p^n} + k(i_2,j_2), \frac{j_2}{p^n} + l(i_2,j_2))$. Note that if $a = i_1 - i_2$ and $b = j_1 - j_2$, then we are in the case where $b \equiv \lambda a \mod p^n$. Let $\bar{\jmath}_1 = \tilde{\jmath} + \lambda i_1$, and $\bar{\jmath}_2 = \tilde{\jmath} + \lambda i_2$. Since $\rho(x,y)^2 \notin \mathbb{Z}$, equation 3 becomes:

$$\begin{aligned}&(i_1 - i_2)^2 + (\lambda(i_1 - i_2) - p^n(m_1 - m_2))^2 + \\ &\quad 2p^n[(i_1 - i_2)(k_1 - k_2) + (\lambda(i_1 - i_2) - p^n(m_1 - m_2))(l_1 - l_2)] \not\equiv 0 \mod p^{2n}.\end{aligned}$$

Dividing through by p^n, this is equivalent to:

$$\begin{aligned}&(i_1 - i_2)^2 \left(\frac{1+\lambda^2}{p^n}\right) - 2\lambda(i_1 - i_2)(m_1 - m_2) + \\ &\qquad 2[(i_1 - i_2)(k_1 - k_2) + \lambda(i_1 - i_2)(l_1 - l_2)] \not\equiv 0 \mod p^n.\end{aligned}$$

Suppose now $i_1 - i_2 = p^r u$ where $r < n$ and $(p,u) = 1$. Dividing through by $2(i_1 - i_2)$ we have:

$$(i_1 - i_2)\frac{1}{2}\left(\frac{1+\lambda^2}{p^n}\right) - \lambda(m_1 - m_2) + [(k_1 - k_2) + \lambda(l_1 - l_2)] \not\equiv 0 \mod p^{n-r}.$$

Using the definitions of $\pi^\lambda_{\tilde{\jmath}}(i_1)$ and $\pi^\lambda_{\tilde{\jmath}}(i_2)$, this becomes $\pi^\lambda_{\tilde{\jmath}}(i_1) \not\equiv \pi^\lambda_{\tilde{\jmath}}(i_2) \mod p^{n-r}$, and we are done. ∎

Suppose now the k, l functions have been defined at all points of R_{p^n} and satisfy $(*)_{p^n}$. We now show how to extend these functions to $R_{p^{n+1}}$ satisfying $(*)_{p^{n+1}}$. We again assume $p \equiv 1 \mod 4$, as otherwise the extension is arbitrary. Again let λ, μ denote the square roots of $-1 \bmod p^n$. Let λ', μ' denote the square roots of $-1 \bmod p^{n+1}$, chosen so that $\lambda \equiv \lambda' \mod p^n$, and $\mu \equiv \mu' \mod p^n$. For each $0 \leq \tilde{j} < p^n$, let $\pi_{\tilde{j}}^{\lambda}$, $\pi_{\tilde{j}}^{\mu}$ be the good permutations of length p^n from lemma 3.5.

For each $0 \leq \tilde{j} < p^{n+1}$ we define good permutations $\sigma_{\tilde{j}}^{\lambda'}$, $\sigma_{\tilde{j}}^{\mu'}$ of length p^{n+1}. If p does not divide $\tilde{j}$, let these be arbitrary good permutations of length p^{n+1}. It remains to define the permutations $\sigma_{p\tilde{j}}^{\lambda'}$, $\sigma_{p\tilde{j}}^{\mu'}$ for $0 \leq \tilde{j} < p^n$.

First, for any $0 \leq i < p^n$, we define $\sigma_{p\tilde{j}}^{\lambda'}(pi)$. This is defined as in the statement of lemma 3.5, using p^{n+1}. To be specific, let $0 \leq \sigma_{p\tilde{j}}^{\lambda'}(pi) < p^{n+1}$ be such that

$$\sigma_{p\tilde{j}}^{\lambda'}(pi) \equiv (k + \lambda' l) - \lambda' m' + (\frac{1}{2}) \left(\frac{1 + \lambda'^2}{p^{n+1}} \right) pi \mod p^{n+1}, \tag{10}$$

where k, l are the values of the functions at the point $(\frac{pi}{p^{n+1}}, \frac{pj}{p^{n+1}})$, $pj \equiv p\tilde{j} + \lambda'(pi) \mod p^{n+1}$, and $p\tilde{j} + \lambda'(pi) = pj + p^{n+1}m'$. Since we also have $j \equiv \tilde{j} + \lambda i \mod p^n$, we also have

$$\pi_{\tilde{j}}^{\lambda}(i) \equiv (k + \lambda l) - \lambda m + (\frac{1}{2}) \left(\frac{1 + \lambda^2}{p^n} \right) i \mod p^n,$$

where these are the same k, l values, and $\tilde{j} + \lambda i = j + p^n m$. Say $\lambda' = \lambda + ep^n$. Then $pj + p^{n+1}m' = p\tilde{j} + \lambda'(pi) = p(\tilde{j} + \lambda i + ep^n i) = pj + p^{n+1}m + ep^{n+1}i$. Hence, $m' = m + ei$. Thus we have

$$\begin{aligned} \sigma_{p\tilde{j}}^{\lambda'}(pi) &\equiv (k + \lambda l) - \lambda(m + ei) + (\frac{1}{2}) \left(\frac{1 + \lambda^2 + 2e\lambda p^n}{p^{n+1}} \right) pi \mod p^n \\ &\equiv (k + \lambda l) - \lambda m + (\frac{1}{2}) \left(\frac{1 + \lambda^2}{p^n} \right) i \mod p^n \\ &\equiv \pi_{\tilde{j}}^{\lambda}(i) \mod p^n. \end{aligned} \tag{11}$$

We say a map σ from the integers i, $0 \leq i < p^{n+1}$, which are divisible by p to the integers mod p^{n+1} is a *partial good* permutation if whenever $0 \leq i_1, i_2 < p^{n+1}$ are distinct integers with $i_1 - i_2 = p^r u$ and $(p, u) = 1$, then $\sigma(i_1) \not\equiv \sigma(i_2) \mod p^{n+1-r}$. Since $\pi_{\tilde{j}}^{\lambda}$ is a good permutation of length p^n, it follows now easily from the above equation that $\sigma_{p\tilde{j}}^{\lambda'}$ is a partial good permutation.

Lemma 3.6. *If σ is a partial good permutation on p^{n+1}, then there is a good permutation of length p^{n+1} extending σ.*

Proof. For i of the form $i = i_0 + pm$ where $0 \leq i_0 < p$, extend σ by defining $\sigma(i) = \sigma(pm) + i_0 p^n$. This easily works. □

Extend now each $\sigma_{\tilde{j}}^{\lambda'}$ to a good permutation of length p^{n+1}. Likewise we define the good permutations $\sigma_{\tilde{j}}^{\mu'}$. Using these good permutations, remark 3.4 shows that we may define k, l functions on $R_{p^{n+1}}$ which satisfy $(*)_{p^{n+1}}$. Furthermore, for points of the form $(\frac{pi}{p^{n+1}}, \frac{pj}{p^{n+1}})$, we may take the k, l values already defined on R_{p^n}, since by definition of the (partial) permutations $\sigma_{p\tilde{j}}^{\lambda'}$, $\sigma_{p\tilde{j}}^{\mu'}$, these values will be a solution to the two equations for $k + \lambda' l$ and $k + \mu' l$ (the equation defining $k + \lambda' l$, for example, is just equation 10 rearranged). Thus, we have extended k, l functions satisfying $(*)_{p^n}$ to functions defined on all of $R_{p^{n+1}}$ and satisfying $(*)_{p^{n+1}}$. This completes the arguments for the special case $d = p^n$.

3.2. **The General Case.** We now give the general proof of lemma A, and note at the end how the proof also shows lemma A$'$. The following lemma, whose proof occupies the rest of this section, embodies what must be shown.

Lemma 3.7. *Let $d > 1$, and suppose functions k, l have been defined on R_d and satisfy $(*)_d$. Let p be a prime, and $d' = pd$. Then these functions may be extended to $R_{d'}$ so as to satisfy $(*)_{d'}$.*

The proof will use the following definition and lemma, which generalize definition 3.2 and lemma 3.6.

Definition 3.8. Let $d > 1$ and $d = p_1^{a_1} \cdots p_n^{a_n}$ be its prime decomposition. We say a permutation $\pi = (\pi(0), \dots, \pi(d-1))$ of the set $(0, 1, \dots, d-1)$ is a d-good permutation if whenever $0 \leq i_1, i_2 < d$ are distinct and $i_1 - i_2 = p_1^{b_1} \dots p_n^{b_n} v$ where $(v, d) = 1$, then $\pi(i_1) \not\equiv \pi(i_2) \mod p_1^{\eta(a_1-b_1)} \cdots p_n^{\eta(a_n-b_n)}$. Here, $\eta(m)$ is defined to be m if $m \geq 0$, and 0 otherwise.

Note that the goodness condition is equivalent to saying that if $i_1 - i_2 = uv$ where u is a product of powers of primes dividing d and $(v, d) = 1$, then $\pi(i_1) \not\equiv \pi(i_2) \mod \frac{d}{u}$, where in writing $\frac{d}{u}$ we adopt the convention that if any prime divides u to a higher power that d, then that prime is removed completely from both the numerator and denominator. We adopt also this convention for the proof of the following lemma.

Suppose $d > 1$, p is a prime, and $d' = pd$. Suppose $0 \leq i_d < p$, and by the *distinguished class* we mean those $0 \leq i < d'$ with $i \equiv i_d \mod p$. If $\pi(i)$ is defined on the distinguished class and satisfies $\pi(i_1) \not\equiv \pi(i_2) \mod \frac{d'}{u}$ whenever $i_1 \neq i_2$ are in the distinguished class (recall here our convention above) and $i_1 - i_2 = uv$ where $(v, d') = 1$, then we say π is partially d'-good.

The next lemma is a general extension lemma which allows us to extend partially d'-good permutations to good permutations.

Lemma 3.9. *Let $d > 1$, p be a prime, and $d' = pd$. Let $0 \leq i_d < p$ represent a distinguished class mod p. Let π be defined on the distinguished class and be partially d'-good. Let u be defined by $d' = up^n$, where $(u, p) = 1$. Let $s \colon d' \to d'$ be a function satisfying the following:*

(1) If $i_1 \equiv i_2 \mod p$, then $s(i_1) = s(i_2)$.

(2) $s(i)$ is divisible by u for all i.

(3) For i in the distinguished class, $s(i) = 0$.

(4) For all i, $i + s(i) \equiv i_d \mod p$.

Define σ by $\sigma(i) = \pi(i + s(i) \mod d') + \frac{s(i)}{u} d \mod d'$. Then σ extends π and is d'-good.

Proof. From (3) it is clear that σ extends π. To show goodness, suppose $0 \leq i_1, i_2 < d'$. Let $i_1' = i_1 + s(i_1) \mod d'$, $i_2' = i_2 + s(i_2) \mod d'$. Suppose first that $i_1 \equiv i_2 \mod p$. Then by (1), $i_1' - i_2' \equiv i_1 - i_2 \mod d'$. Also, from the definition of σ, $\sigma(i_1) - \sigma(i_2) \equiv \pi(i_1') - \pi(i_2') \mod d'$. Since π is partially d'-good, the result follows.

Suppose now $i_1 - i_2$ is not divisible by p. Say, $i_1 - i_2 = u_1 v$ where $(v, d') = 1$ and $(u_1, p) = 1$. Consider first the case where $i'_1 = i'_2$, with i'_1, i'_2 as above. Then $\sigma(i_1) - \sigma(i_2) \equiv \frac{s(i_1)-s(i_2)}{u} d$. Since $s(i_1) - s(i_2) \not\equiv 0 \mod p$ in this case, we have $\sigma(i_1) \not\equiv \sigma(i_2) \mod p^n$ (note: $d = up^{n-1}$). Since p^n divides $\frac{d'}{u_1}$ (using our conventions), the result follows. Suppose finally that $i'_1 \neq i'_2$. From (2) it follows that $u_1 | (i'_1 - i'_2)$. Also, $p | (i'_1 - i'_2)$. So by partial goodness, $\sigma(i'_1) \not\equiv \sigma(i'_2) \mod \frac{d'}{pu_1} = \frac{d}{u_1}$. Since $\sigma(i_1) \equiv \sigma(i'_1) \mod d$, and likewise for i_2, it follows that $\sigma(i_1) \not\equiv \sigma(i_2) \mod \frac{d'}{pu_1}$, and hence are not equivalent mod $\frac{d'}{u_1}$. □

Let us say that a prime is trivial if $p = 2$ or $p \equiv 3 \mod 4$. Otherwise, we say p is non-trivial. The next lemma shows that we need only consider the non-trivial primes.

Lemma 3.10. *If lemma 3.7 holds for all d which are divisible by only non-trivial primes, then the lemma holds for all d.*

Proof. Let $d = p_1^{a_1} \cdots p_n^{a_n} q_1^{c_1} \cdots q_m^{c_m}$, where the p_i are non-trivial, and the q_i are trivial. We assume the k, l functions are defined on R_d and satisfy $(*)_d$. Let $d' = pd$, and assume first that p is non-trivial. Let $P = p_1^{a_1} \cdots p_n^{a_n}$, $P' = pP$, and $Q = q_1^{c_1} \cdots q_m^{c_m}$. Let G be the subgroup of $\mathbb{Q}/\mathbb{Z} \times \mathbb{Q}/\mathbb{Z}$ of elements of the form $(\frac{i}{d} + \mathbb{Z}, \frac{j}{d} + \mathbb{Z})$, and likewise define G' using d'. Let H be the subgroup of G consisting of elements of the form $(\frac{i}{P} + \mathbb{Z}, \frac{j}{P} + \mathbb{Z})$, and likewise define H' using P'. Let K be the subgroup of elements of the form $(\frac{i}{Q} + \mathbb{Z}, \frac{j}{Q} + \mathbb{Z})$. Note that the given k, l functions may be viewed as selector functions on the group G, that is functions on G with $(k(r + \mathbb{Z}, s + \mathbb{Z}), l(r + \mathbb{Z}, s + \mathbb{Z})) \in (r + \mathbb{Z}, s + \mathbb{Z})$. We extend these selector functions to the group G'. The cosets of H' in G' are exactly enumerated as $H' + (r + \mathbb{Z}, s + \mathbb{Z})$, where $r + \mathbb{Z}, s + \mathbb{Z} \in K/\mathbb{Z}$. Consider such a coset of H' in G', say $C' = H' + (r + \mathbb{Z}, s + \mathbb{Z})$. The k, l functions are already defined on the corresponding coset $C = H + (r + \mathbb{Z}, s + \mathbb{Z})$ of H. Since C, C' are translations of H, H', we may by assumption extend the k, l functions from C to functions k', l' on C' so as to satisfy $(*)$ on C' (that is, for any distinct cosets $x = (r_1 + \mathbb{Z}, s_1 + \mathbb{Z})$, $y = (r_2 + \mathbb{Z}, s_2 + \mathbb{Z}) \in C'$, $\rho(z_1, z_2)^2 \notin \mathbb{Z}$, where $z_1 = (k'(x), l'(x))$, $z_2 = (k'(y), l'(y))$). Doing this for each coset of H' in G' defines the k', l' functions on G'.

To see this works, let $x = (r_1 + \mathbb{Z}, s_1 + \mathbb{Z}), y = (r_2 + \mathbb{Z}, s_2 + \mathbb{Z})$ be distinct elements of G'. Let $z_1 = (k'(x), l'(x))$, $z_2 = (k'(y), l'(y))$, and we show that $\rho(z_1, z_2)^2 \notin \mathbb{Z}$. We may assume that x, y are in distinct cosets of H'. Thus $(a, b) \doteq z_1 - z_2 \notin H'$. The result now follows from the fact that if $a, b \in \mathbb{Q}$ and $a^2 + b^2 \in \mathbb{Z}$, then a, b (when reduced) have denominators divisible only by non-trivial primes.

The case where p is trivial is similar but easier. Briefly, view G' now as a union of cosets of H, with H as above. For those cosets which are subsets of G, the k, l functions are already defined, and for the other cosets they are defined easily using the fact that these cosets are translations of H (we do not use in this case our assumption that the result holds for d divisible by only non-trivial primes). As above, the resulting k', l' functions satisfy $(*)_{d'}$. □

Returning to the proof of lemma 3.7, by lemma 3.10 be may assume that d and d' are divisible by only non-trivial primes. We make this standing assumption for the remainder of the proof of lemma 3.7.

Let $d = p_1^{a_1} \cdots p_n^{a_n}$, where all of the p_i are non-trivial primes. We prove two lemmas which characterize the existence of the functions k, l on R_d satisfying $(*)_d$ in terms of the existence of a family of permutations satisfying certain properties.

Suppose k, l functions are given on R_d. Since all of the p_i are non-trivial primes, there are exactly 2^n classes λ mod d such that $\lambda^2 \equiv -1 \mod d$. We refer to such a λ as a d-root. For each d-root λ, each $0 \leq \tilde{j} < d$, and each $0 \leq i < d$, define

$$\pi_{\tilde{j}}^{\lambda}(i) = (k + \lambda l) - \lambda m + \frac{1}{2}\left(\frac{1+\lambda^2}{d}\right)(i) \mod d, \tag{12}$$

where (k, l) are the values associated to $(\frac{i}{d}, \frac{j}{d})$, where $0 \leq j < d$, and j, m are defined by

$$j = \tilde{j} + \lambda i - md.$$

We introduce two conditions on the $\pi_{\tilde{j}}^{\lambda}$.

(d-goodness) For each $0 \leq \tilde{j} < d$, and each d-root λ, $\pi_{\tilde{j}}^{\lambda}$ is a d-good permutation.

(d-consistency) Suppose $0 \leq \tilde{j}_1, \tilde{j}_2 < d$ and λ_1, λ_2 are both d-roots. Suppose p^a is one of the prime factors $p_1^{a_1}, \ldots, p_n^{a_n}$ and $\lambda_1 \equiv \lambda_2 \mod p^a$. Then

$$\pi_{\tilde{j}_1}^{\lambda_1}(i) - \pi_{\tilde{j}_2}^{\lambda_2}(i) \equiv -\frac{\lambda(\tilde{j}_1 - \tilde{j}_2)}{d} \mod p^a \tag{13}$$

for any $0 \leq i < d$ such that

$$i(\lambda_1 - \lambda_2) \equiv -(\tilde{j}_1 - \tilde{j}_2) \mod d \tag{14}$$

(in equation 13, λ could be either λ_1 or λ_2; note that this expression makes sense since $p^a | (\tilde{j}_1 - \tilde{j}_2)$).

Note that the values of i satisfying equation 14 are precisely those $0 \leq i < d$ such that if we define $0 \leq j_1, j_2 < d$ (and m_1, m_2) by

$$\begin{aligned} j_1 &= \tilde{j}_1 + \lambda_1 i - m_1 d \\ j_2 &= \tilde{j}_2 + \lambda_2 i - m_2 d, \end{aligned}$$

then $j_1 = j_2$.

Lemma 3.11. *Let $d = p_1^{a_1} \cdots p_n^{a_n}$ where each p_i is non-trivial. Assume the k, l functions are defined on R_d and satisfy $(*)_d$, and the $\pi_{\tilde{j}}^{\lambda}$ are defined by equation 12. Then the $\pi_{\tilde{j}}^{\lambda}$ satisfy the d-goodness and d-consistency conditions.*

Proof. Fix $0 \leq \tilde{j} < d$ and a d-root λ. We show that $\pi_{\tilde{j}}^{\lambda}$ defined by equation 12 is d-good. Let $0 \leq i_1, i_2 < d$ be distinct. Let $0 \leq j_1, j_2 < d$ and m_1, m_2 be defined by

$$\begin{aligned} j_1 &= \tilde{j} + \lambda i_1 - m_1 d \\ j_2 &= \tilde{j} + \lambda i_2 - m_2 d. \end{aligned} \tag{15}$$

Let k_1, l_1 be the values associated to the point $w_1 = (\frac{i_1}{d}, \frac{j_1}{d})$, and k_2, l_2 the values associated to $w_2 = (\frac{i_2}{d}, \frac{j_2}{d})$. If $z_1 = w_1 + (k_1, l_1)$ and $z_2 = w_2 + (k_2, l_2)$, then since $\rho(z_1, z_2)^2 \notin \mathbb{Z}$ we have

$$(i_1 - i_2)^2 + (j_1 - j_2)^2 + 2d[(i_1 - i_2)(k_1 - k_2) + (j_1 - j_2)(l_1 - l_2)] \not\equiv 0 \mod d^2.$$

Substituting from equation 15 we have

$$\begin{aligned}(16)\qquad &(i_1-i_2)^2(1+\lambda^2)-2(i_1-i_2)(m_1-m_2)d\lambda\\ &+2d[(i_1-i_2)(k_1-k_2)+\lambda(i_1-i_2)(l_1-l_2)]\not\equiv 0 \mod d^2.\end{aligned}$$

Since d divides $1+\lambda^2$, we may divide through by d to get

$$\begin{aligned}(17)\qquad &(i_1-i_2)^2\left(\frac{1+\lambda^2}{d}\right)-2(i_1-i_2)(m_1-m_2)\lambda\\ &+2[(i_1-i_2)(k_1-k_2)+\lambda(i_1-i_2)(l_1-l_2)]\not\equiv 0 \mod d.\end{aligned}$$

Say $i_1-i_2=p_1^{b_1}\cdots p_n^{b_n}u$, where $(u,d)=1$. Dividing through by $2(i_1-i_2)$ we have

$$(i_1-i_2)\left(\frac{1+\lambda^2}{2d}\right)-(m_1-m_2)\lambda+[(k_1-k_2)+\lambda(l_1-l_2)]\not\equiv 0 \mod p_1^{\eta(a_1-b_1)}\cdots p_n^{\eta(a_n-b_n)},$$

where we recall $\eta(r)=r$ if $r\geq 0$, and $\eta(r)=0$ for $r<0$. Since $p_1^{\eta(a_1-b_1)}\cdots p_n^{\eta(a_n-b_n)}$ divides d, we have

$$\begin{aligned}(18)\qquad \pi_{\tilde{j}}^{\lambda}(i_1)&\equiv(k_1+\lambda l_1)-\lambda m_1+\left(\frac{1+\lambda^2}{2d}\right)i_1 \mod p_1^{\eta(a_1-b_1)}\cdots p_n^{\eta(a_n-b_n)}\\ &\not\equiv(k_2+\lambda l_2)-\lambda m_2+\left(\frac{1+\lambda^2}{2d}\right)i_2 \mod p_1^{\eta(a_1-b_1)}\cdots p_n^{\eta(a_n-b_n)}\\ &\equiv\pi_{\tilde{j}}^{\lambda}(i_2) \mod p_1^{\eta(a_1-b_1)}\cdots p_n^{\eta(a_n-b_n)}.\end{aligned}$$

Thus, $\pi_{\tilde{j}}^{\lambda}$ is d-good.

To verify d-consistency, suppose λ_1 and λ_2 are both d-roots, and $\lambda_1\equiv\lambda_2 \mod p^a$, where p^a is one of the prime powers occurring in d. Let $0\leq\tilde{j}_1,\tilde{j}_2<d$, and $0\leq i<d$ be such that $i(\lambda_1-\lambda_2)\equiv-(\tilde{j}_1-\tilde{j}_2) \mod d$. If we let $0\leq j_1,j_2<d$ and m_1, m_2 be defined by

$$\begin{aligned}j_1&=\tilde{j}_1+\lambda_1 i-m_1 d\\ j_2&=\tilde{j}_2+\lambda_2 i-m_2 d,\end{aligned}$$

then $j_1=j_2$, which we now denote by j. Say $\lambda_2=\lambda_1+ep^a$. Thus,

$$\tilde{j}_1-\tilde{j}_2=-i(\lambda_1-\lambda_2)+d(m_1-m_2)=iep^a+d(m_1-m_2).$$

Let k, l be the values associated to the point $(\frac{i}{d},\frac{j}{d})$. From the definition of the $\pi_{\tilde{j}}^{\lambda}$ we have:

$$\begin{aligned}k+\lambda_1 l&\equiv\pi_{\tilde{j}_1}^{\lambda_1}(i)+\lambda_1 m_1-\frac{1}{2}\left(\frac{1+\lambda_1^2}{d}\right)i \mod p^a\\ k+\lambda_2 l&\equiv\pi_{\tilde{j}_2}^{\lambda_2}(i)+\lambda_2 m_2-\frac{1}{2}\left(\frac{1+\lambda_2^2}{d}\right)i \mod p^a\\ &\equiv\pi_{\tilde{j}_2}^{\lambda_2}(i)+\lambda_1 m_2-\frac{1}{2}\left(\frac{1+\lambda_2^2}{d}\right)i \mod p^a\\ &\equiv\pi_{\tilde{j}_2}^{\lambda_2}(i)+\lambda_1 m_1+\lambda_1\left(\frac{iep^a}{d}-\frac{\tilde{j}_1-\tilde{j}_2}{d}\right)-\frac{1}{2}\left(\frac{1+(\lambda_1+ep^a)^2}{d}\right)i \mod p^a\\ &\equiv\pi_{\tilde{j}_2}^{\lambda_2}(i)+\lambda_1 m_1-\frac{1}{2}\left(\frac{1+\lambda_1^2}{d}\right)i-\frac{\lambda_1(\tilde{j}_1-\tilde{j}_2)}{d} \mod p^a\end{aligned}$$

Note that p^a divides $\tilde{j}_1 - \tilde{j}_2$, so the last two equations make sense. Thus, we have:

$$\pi^{\lambda_1}_{\tilde{j}_1}(i) - \pi^{\lambda_2}_{\tilde{j}_2}(i) \equiv -\frac{\lambda_1(\tilde{j}_1 - \tilde{j}_2)}{d} \mod p^a.$$

This verifies d-consistency. □

We now establish a converse to lemma 3.11. Suppose that for each d-root λ, and each $0 \le \tilde{j} < d$, a d-good permutation $\pi^{\lambda}_{\tilde{j}}$ is given, and these permutations satisfy the d consistency condition. We show how to define the k, l functions on R_d so as to satisfy $(*)_d$. Fix a point $(\frac{i}{d}, \frac{j}{d})$, where $0 \le i, j < d$, and we define the values of k, l associated to that point. Let p^a be one of the prime powers occurring in d. For any d-root λ, $\lambda_{p^a} \doteq \lambda \mod p^a$ is one of the two square roots of $-1 \bmod p^a$. Fix for the moment such a λ and λ_{p^a}. Define $0 \le \tilde{j} < d$ and m by

$$j = \tilde{j} + \lambda i - md.$$

Consider the following mod p^a equation

$$k + \lambda_{p^a} l \equiv \pi^{\lambda}_{\tilde{j}}(i) + \lambda_{p^a} m - \frac{1}{2}\left(\frac{1+\lambda^2}{d}\right) i \mod p^a. \tag{19}$$

We claim that the right-hand side of this equation depends only on λ_{p^a}. For let $\lambda_1 = \lambda$, and suppose λ_2 is also a d-root with $\lambda_2 \equiv \lambda_1 \mod p^a$. Say, $\lambda_2 = \lambda_1 + ep^a$. Let $\tilde{j}_1$, m_1 be the values using λ_1, and $\tilde{j}_2$, m_2 the values using λ_2. Since

$$j = \tilde{j}_1 + \lambda_1 i - m_1 d = \tilde{j}_2 + \lambda_2 i - m_2 d,$$

we have $i(\lambda_1 - \lambda_2) \equiv -(\tilde{j}_1 - \tilde{j}_2) \mod d$. Therefore, by consistency we have

$$\pi^{\lambda_1}_{\tilde{j}_1}(i) - \pi^{\lambda_2}_{\tilde{j}_2}(i) \equiv -\frac{\lambda_1(\tilde{j}_1 - \tilde{j}_2)}{d} \mod p^a.$$

Thus

$$\begin{aligned}
&\pi^{\lambda_1}_{\tilde{j}_1}(i) + \lambda_{p^a} m_1 - \left(\frac{1+\lambda_1^2}{2d}\right) i \\
&\equiv \pi^{\lambda_2}_{\tilde{j}_2}(i) - \frac{\lambda_1(\tilde{j}_1 - \tilde{j}_2)}{d} + \lambda_{p^a}(m_2 + \frac{\tilde{j}_1 - \tilde{j}_2}{d} + i\frac{\lambda_1 - \lambda_2}{d}) \\
&\quad - \left(\frac{1 + (\lambda_2 - ep^a)^2}{2d}\right) i \mod p^a \\
&\equiv \pi^{\lambda_2}_{\tilde{j}_2}(i) + \lambda_{p^a} m_2 - i\lambda_{p^a}\frac{ep^a}{d} - \left(\frac{1 + (\lambda_2 - ep^a)^2}{2d}\right) i \mod p^a \\
&\equiv \pi^{\lambda_2}_{\tilde{j}_2}(i) + \lambda_{p^a} m_2 - \left(\frac{1+\lambda_2^2}{2d}\right) i \mod p^a.
\end{aligned} \tag{20}$$

This verifies the claim. Thus, for each of the two square roots λ_{p^a}, $-\lambda_{p^n}$ of -1 mod p^a we have unambiguous values, say v_1 and v_2, for the right-hand sides of equation 19. For each prime factor p^a, and each of the two roots $\pm\lambda_{p^a} \mod p^a$, we solve the system

$$\begin{aligned}
k + \lambda_{p^a} l &\equiv v_1 \mod p^a \\
k - \lambda_{p^a} l &\equiv v_2 \mod p^a
\end{aligned}$$

From the Chinese remainder theorem, we may choose (k, l) so that all of these systems for the various p^a are simultaneously satisfied. This completes the definition of the k, l functions.

To verify $(*)_d$, let $0 \le i_1, j_1, i_2, j_2 < d$, and let $w_1 = (\frac{i_1}{d}, \frac{j_1}{d})$, $w_2 = (\frac{i_2}{d}, \frac{j_2}{d})$. let $z_1 = w_1 + (k_1, l_1)$, $z_2 = w_2 + (k_2, l_2)$, where k_1, l_1 are the values as defined above for w_1, and similarly for k_2, l_2. We must show $\rho(z_1, z_2)^2 \notin \mathbb{Z}$. Toward a contradiction, assume $\rho(z_1, z_2)^2 \in \mathbb{Z}$, which becomes as usual

$$(i_1 - i_2)^2 + (j_1 - j_2)^2 + 2d[(i_1 - i_2)(k_1 - k_2) + (j_1 - j_2)(l_1 - l_2)] \equiv 0 \mod d^2. \tag{21}$$

Consider for the moment one of the prime powers p^a of d such that if p^e is the exact power of p dividing $i_1 - i_2$, then $e < a$ (such a factor must clearly exist as $|i_1 - i_2| < d$). Write $i_1 - i_2 = p^e u$ where $(u, p) = 1$. Let f be the exact power of p dividing $j_1 - j_2$, and write $j_1 - j_2 = p^f v$, where $(v, p) = 1$. Since $e < a$, it follows easily from equation 21 that $e = f$. Dividing through by p^{2e} shows that $u^2 + v^2 \equiv 0 \mod p^{a-e}$. Thus, there is a square root $\bar\lambda$ of $-1 \mod p^{a-e}$ such that $v \equiv \bar\lambda u \mod p^{a-e}$. There is a square root λ_{p^a} of $-1 \mod p^a$ such that $\lambda \equiv \bar\lambda \mod p^{a-e}$. Thus, $v \equiv \lambda_{p^a} u \mod p^{a-e}$ as well. Hence $j_1 - j_2 \equiv \lambda_{p^a}(i_1 - i_2) \mod p^a$.

If p^a is a prime power occurring in d for which $e \ge a$, equation 21 implies that $f \ge a$ as well (using the notation above). Thus, for any square root λ_{p^n} of $-1 \mod p^a$ the equation $j_1 - j_2 \equiv \lambda_{p^a}(i_1 - i_2) \mod p^a$ holds trivially.

Let now λ be a d-root such that for any prime power p^a occurring in d, $\lambda \equiv \lambda_{p^n} \mod p^a$, with λ_{p^a} as in the cases above. It follows that $j_1 - j_2 \equiv \lambda(i_1 - i_2) \mod d$.

Let $0 \le \tilde{\jmath} < d$ and m_1 be defined by

$$j_1 = \tilde{\jmath} + \lambda i_1 - m_1 d. \tag{22}$$

Since $j_1 - j_2 \equiv \lambda(i_1 - i_2) \mod d$, it follows that there is an m_2 such that

$$j_2 = \tilde{\jmath} + \lambda i_2 - m_2 d. \tag{23}$$

From the definitions of k_1, l_1 (in which we use the above values of $\tilde{\jmath}$, λ; this is permissible by d-consistency) we have

$$k_1 + \lambda l_1 \equiv \pi_{\tilde{\jmath}}^{\lambda}(i_1) + \lambda m_1 - \left(\frac{1+\lambda^2}{2d}\right) i_1 \mod d, \tag{24}$$

since this equation holds mod each prime power $p_i^{a_i}$ occurring in d. Likewise,

$$k_2 + \lambda l_2 \equiv \pi_{\tilde{\jmath}}^{\lambda}(i_2) + \lambda m_2 - \left(\frac{1+\lambda^2}{2d}\right) i_2 \mod d. \tag{25}$$

Substituting equations 22, 23 into equation 21 and dividing through by $2d$ we obtain

$$(i_1-i_2)^2 \left(\frac{1+\lambda^2}{2d}\right) - \lambda(i_1-i_2)(m_1-m_2) + [(i_1-i_2)(k_1-k_2) + \lambda(i_1-i_2)(l_1-l_2)] \equiv 0 \mod d. \tag{26}$$

Dividing through by $i_1 - i_2$ gives

$$(i_1-i_2)\left(\frac{1+\lambda^2}{2d}\right) - \lambda(m_1-m_2) + [(k_1-k_2) + \lambda(l_1-l_2)] \equiv 0 \mod p_1^{\eta(a_1-b_1)} \cdots p_n^{\eta(a_n-b_n)}, \tag{27}$$

where $i_1 - i_2 = p_1^{b_1} \cdots p_n^{b_n} u$ and $(u, d) = 1$. Substituting equations 24 and 25 now gives $\pi_{\tilde{\jmath}}^{\lambda}(i_1) - \pi_{\tilde{\jmath}}^{\lambda}(i_2) \equiv 0 \mod p_1^{\eta(a_1-b_1)} \cdots p_n^{\eta(a_n-b_n)}$. This, however, contradicts the assumed d-goodness of the $\pi_{\tilde{\jmath}}^{\lambda}$.

Summarizing, we have shown the following converse to lemma 3.11.

Lemma 3.12. *Let $d = p_1^{a_1} \cdots p_n^{a_n}$ be a product of non-trivial primes. Assume that for each $0 \le \tilde{\jmath} < d$ and each d-root λ a d-good permutation $\pi_{\tilde{\jmath}}^{\lambda}$ is given, and these permutations satisfy the d-consistency condition. Then we may associate to each $(\frac{i}{d}, \frac{j}{d})$, $0 \le i, j < d$, integer values k, l such that for all d-roots λ, and all $0 \le \tilde{\jmath} < d$ satisfying $j \equiv \tilde{\jmath} + \lambda i \mod d$ (say $j = \tilde{\jmath} + \lambda i - md$), we have*

$$k + \lambda l \equiv \pi_{\tilde{\jmath}}^{\lambda}(i) + \lambda m - \left(\frac{1+\lambda^2}{2d}\right) i \mod d$$

Furthermore, these k, l functions satisfy $(*)_d$.

To unify notation, let us write now $d = p_1^{a_1} \cdots p_n^{a_n}$, and $d' = p_1^{a_1+1} p_2^{a_2} \cdots p_n^{a_n}$ (thus we do not assume these primes are in increasing order, and we allow $a_1 = 0$). The case $a_1 = 0$ differs in only trivial notational ways from the case $a_1 \ge 1$, so we assume below all of the a_i are positive. Recall we are assuming the k, l functions have been defined on R_d and satisfy $(*)_d$, and we must extend them to functions k', l' on $R_{d'}$ satisfying $(*)_{d'}$.

For each $0 \le \tilde{\jmath} < d$, and each d-root λ, let $\pi_{\tilde{\jmath}}^{\lambda}$ be as in lemma 3.11 using the given k, l functions. Thus, each $\pi_{\tilde{\jmath}}^{\lambda}$ is a d-good permutation, and this family satisfies the d-consistency condition.

For each $\tilde{\jmath}$ with $0 \le p_1\tilde{\jmath} < d'$, each d'-root λ' (that is, ${\lambda'}^2 \equiv -1 \mod d'$), and each i with $0 \le p_1 i < d'$, define

$$\sigma_{p_1\tilde{\jmath}}^{\lambda'}(p_1 i) = (k + \lambda' l) - \lambda' m + \frac{1}{2}\left(\frac{1+{\lambda'}^2}{d'}\right)(p_1 i) \mod d' \tag{28}$$

where (k, l) are the values already assigned to the pair $(\frac{i}{d}, \frac{j}{d}) = (\frac{p_1 i}{d'}, \frac{p_1 j}{d'})$, and j, m are defined by

$$p_1 j = p_1 \tilde{\jmath} + \lambda'(p_1 i) - md'. \tag{29}$$

This makes sense since the right-hand side is divisible by p_1. Thus, each $\sigma_{p_1\tilde{\jmath}}^{\lambda'}$ is a partial function in that it is only defined on the $0 \le i < d'$ which are divisible by p_1. We will momentarily extend these to fully d'-good permutations satisfying the d'-consistency condition, but first we catalog the properties satisfied by these partial functions.

First note that if $\lambda = \lambda' \mod d$, then $\sigma_{p_1\tilde{\jmath}}^{\lambda'}(p_1 i) \equiv \pi_{\tilde{\jmath}}^{\lambda}(i) \mod d$. To see this, let $\lambda' = \lambda + ed$. Thus, $j = \tilde{\jmath} + \lambda' i - md = \tilde{\jmath} + \lambda i - (m - ei)d$. Hence, if k, l are the values associated to the pair $(\frac{i}{d}, \frac{j}{d})$ then

$$\begin{aligned}
\sigma_{p_1\tilde{\jmath}}^{\lambda'}(p_1 i) &= (k + \lambda' l) - \lambda' m + \frac{1}{2}\left(\frac{1+{\lambda'}^2}{d'}\right)(p_1 i) \mod d' \\
&\equiv (k + \lambda l) - \lambda m + \frac{1}{2}\left(\frac{1+{\lambda'}^2}{d'}\right)(p_1 i) \mod d \\
&\equiv (k + \lambda l) - \lambda(m - ei) - ie\lambda + \frac{1}{2}\left(\frac{1+(\lambda+ed)^2}{d}\right) i \mod d \\
&\equiv (k + \lambda l) - \lambda(m - ei) + \frac{1}{2}\left(\frac{1+\lambda^2}{d}\right) i \mod d \\
&\equiv \pi_{\tilde{\jmath}}^{\lambda}(i) \mod d.
\end{aligned} \tag{30}$$

We introduce now the following "partial" goodness and consistency conditions for the $\sigma^{\lambda'}_{p_1\tilde{\jmath}}$.

(partial d'-goodness) If $0 \le p_1\tilde{\jmath} < d'$, $0 \le p_1 i_1, p_1 i_2 < d'$ and $(p_1 i_1 - p_1 i_2) = p_1^{b_1} \cdots p_n^{b_n} v$, where $(v, d') = 1$, then $\sigma^{\lambda'}_{p_1\tilde{\jmath}}(p_1 i_1) \not\equiv \sigma^{\lambda'}_{p_1\tilde{\jmath}}(p_1 i_2) \mod p_1^{\eta(a_1+1-b_1)} \cdots p_n^{\eta(a_n-b_n)}$.

(partial d'-consistency) If $0 \le p_1\tilde{\jmath}_1, p_1\tilde{\jmath}_2 < d'$, λ'_1, λ'_2 are d'-roots with $\lambda'_1 \equiv \lambda'_2 \mod p^a$ where p^a is one of the prime factors $p_1^{a_1+1}, \ldots, p_n^{a_n}$ of d', then for any $0 \le p_1 i < d'$ with $(p_1 i)(\lambda'_1 - \lambda'_2) \equiv -(p_1\tilde{\jmath}_1 - p_1\tilde{\jmath}_2) \mod d'$ we have

$$\sigma^{\lambda'_1}_{p_1\tilde{\jmath}_1}(p_1 i) - \sigma^{\lambda'_2}_{p_1\tilde{\jmath}_2}(p_1 i) \equiv -\frac{\lambda'(p_1\tilde{\jmath}_1 - p_1\tilde{\jmath}_2)}{d'} \mod p^a.$$

Lemma 3.13. *The partial functions $\sigma^{\lambda'}_{p_1\tilde{\jmath}}$ satisfy the d'-partial goodness and d'-partial consistency conditions.*

Proof. The proof is essentially identical to that of lemma 3.11. For example, to verify partial d'-consistency, let j, m'_1, m'_2 be defined by

$$\begin{aligned} p_1 j &= p_1\tilde{\jmath}_1 + \lambda'_1(p_1 i) - m'_1 d' \\ &= p_1\tilde{\jmath}_2 + \lambda'_2(p_1 i) - m'_2 d' \end{aligned}$$

Let (k, l) be the values associated to $(\frac{p_1 i}{d'}, \frac{p_1 j}{d'})$, and let $\lambda'_2 = \lambda'_1 + e p^a$. Then we have:

$$\begin{aligned} \sigma^{\lambda'_1}_{p_1\tilde{\jmath}_1}(p_1 i) &\equiv (k + \lambda'_1 l) - \lambda'_1 m_1 + \frac{1}{2}\left(\frac{1 + {\lambda'_1}^2}{d'}\right)(p_1 i) \mod p^a \\ &\equiv (k + \lambda'_2 l) - \lambda'_2 m_2 - \lambda'_2 \frac{p_1(\tilde{\jmath}_1 - \tilde{\jmath}_2) + (\lambda'_1 - \lambda'_2)(p_1 i)}{d'} \\ &\quad + \frac{1}{2}\left(\frac{1 + (\lambda'_2 - e p^a)^2}{d'}\right)(p_1 i) \mod p^a \\ &\equiv (k + \lambda'_2 l) - \lambda'_2 m_2 + \frac{1}{2}\left(\frac{1 + {\lambda'_2}^2}{d'}\right)(p_1 i) - \frac{\lambda'_2(p_1\tilde{\jmath}_1 - p_1\tilde{\jmath}_2)}{d'} \mod p^a \\ &\equiv \sigma^{\lambda'_2}_{p_1\tilde{\jmath}_2}(p_1 i) - \frac{\lambda'_2(p_1\tilde{\jmath}_1 - p_1\tilde{\jmath}_2)}{d'} \mod p^a \end{aligned}$$

□

We now define the permutations $\sigma^{\lambda'}_{\tilde{\jmath}}(i)$ for all $0 \le \tilde{\jmath} < d'$, all d'-roots λ', and all $0 \le i < d'$, and which extend the partial permutations so far defined (the $\sigma^{\lambda'}_{p_1\tilde{\jmath}}(p_1 i)$). Since we do not need to refer to the d-roots anymore, we will henceforth use λ to refer to the d' roots. Also, we refer to the $i, j, \tilde{\jmath}$ which are divisible by p_1 as "old," and the other $i, j, \tilde{\jmath}$ as "new." Thus, $\sigma^{\lambda}_{\tilde{\jmath}}(i)$ is currently defined for the old $\tilde{\jmath}$ and i, and we wish to extend to the new values.

We introduce two families of functions, $r^{\lambda}_{\tilde{\jmath}}$ and $s^{\lambda}_{\tilde{\jmath}}$, from d' to d'. These "shift" functions will tell us how to extend certain partially defined permutations to fully good permutations. These functions are defined for each d' root λ. The r functions are defined for old $\tilde{\jmath}$, and the s functions for new $\tilde{\jmath}$. Actually, for the construction below it suffices (though it is not necessary) to take $r^\lambda_{\tilde{\jmath}}$ functions which are independent of $\tilde{\jmath}$ and λ, that is, we have a single function $r: d' \to d'$. In general, the properties we desire of the r and s functions are described in the following lemma.

Definition 3.14. Let λ be a root mod d', and $0 \le \tilde{\jmath} < d'$. By the $\lambda, \tilde{\jmath}$-distinguished class we mean the equivalence class mod p_1 of $0 \le i < d'$ satisfying $i(\lambda - \bar{\lambda}) \equiv -\tilde{\jmath} \mod p_1$, where $\bar{\lambda}$ is a root not equivalent to λ mod p_1 (so, $\bar{\lambda} \equiv -\lambda \mod p_1$).

Note that for a given $\tilde{\jmath}$, there are really only two distinguished classes, one for each of the two possible values of a root mod p_1, and each of these classes is the negative of the other, mod p_1.

Lemma 3.15. *There are functions r, $s^\lambda_{\tilde{\jmath}}: d' \to d'$ satisfying the following:*

1. *For each $0 \le i < d'$, $i + r(i)$ is divisible by p_1. Further, if $p_1 | i$, then $r(i) = 0$.*
2. *For each root λ, new $\tilde{\jmath}$, and $0 \le i < d'$, $i + s^\lambda_{\tilde{\jmath}}(i)$ is in the $\lambda, \tilde{\jmath}$-distinguished class. Further, if i is in the $\lambda, \tilde{\jmath}$- distinguished class, then $s^\lambda_{\tilde{\jmath}}(i) = 0$.*
3. *$r(i)$, $s^\lambda_{\tilde{\jmath}}(i)$ only depend on the classes of $\tilde{\jmath}$ and i mod p_1.*
4. *$s^\lambda_{\tilde{\jmath}}(i)$ depends only on the class of $\lambda \mod p_1$.*
5. *$r(i)$, $s^\lambda_{\tilde{\jmath}}(i)$ are divisible by u (recall $u = p_2^{a_2} \cdots p_n^{a_n}$).*

   For the remaining statements we fix some notation. Let $0 \le \tilde{\jmath}_1, \tilde{\jmath}_2 < d'$, with $\tilde{\jmath}_1$, $\tilde{\jmath}_2$ new. Let λ_1, λ_2 be d' roots with $\lambda_1 \equiv -\lambda_2 \mod p_1$. Let $0 \le i < d'$. Suppose $i(\lambda_1 - \lambda_2) \equiv -(\tilde{\jmath}_1 - \tilde{\jmath}_2) \mod p_1$.
6. *$s^{\lambda_1}_{\tilde{\jmath}_1}(i) + r(i + s^{\lambda_1}_{\tilde{\jmath}_1}(i)) = s^{\lambda_2}_{\tilde{\jmath}_2}(i) + r(i + s^{\lambda_2}_{\tilde{\jmath}_2}(i)) \mod d'$.*
7. *$s^{\lambda_1}_{\tilde{\jmath}_1}(i) = r(i + s^{\lambda_2}_{\tilde{\jmath}_2}(i))$.*

With the notation as fixed in the statement of the lemma, if we let s_1 abbreviate $s^{\lambda_1}_{\tilde{\jmath}_1}(i)$, $r_2 = r(i + s^{\lambda_1}_{\tilde{\jmath}_1}(i))$, $s_2 = s^{\lambda_2}_{\tilde{\jmath}_2}(i)$, and $r_1 = r(i + s^{\lambda_2}_{\tilde{\jmath}_2}(i))$, then the last two statements become

(6) $s_1 + r_2 = s_2 + r_1$

(7) $s_1 = r_1$.

Of course, we also have in this case that $s_2 = r_2$.

Proof. We give an algorithm for constructing the r, $s^\lambda_{\tilde{\jmath}}$ functions. First, let $r(i) = (-\frac{i}{u} \mod p_1)u$, where $u = p_2^{a_2} \cdots p_n^{a_n}$. Clearly (1) is satisfied.

Suppose that λ is a root and $\tilde{\jmath}$ is new. Let $0 \le i_d < p_1$ represent the $\lambda, \tilde{\jmath}$-distinguished class. Let $s^\lambda_{\tilde{\jmath}}(i)$ be the unique value in $\{r(0), \dots, r(p_1 - 1)\}$ such that $i + s^\lambda_{\tilde{\jmath}}(i) \equiv i_d \mod p_1$.

This completes the definition of the r and $s^\lambda_{\tilde{\jmath}}$ functions. Property (2) is clear, and (3) is also since the $\lambda, \tilde{\jmath}$-distinguished class depends on the class of $\tilde{\jmath} \mod p_1$. Likewise, this class depends only the value of $\lambda \mod p_1$, and so (4) follows. (5) is immediate from the definitions.

To see (6), fix $i, \tilde{\jmath}_1, \tilde{\jmath}_2, \lambda_1, \lambda_2$ with $\lambda_1 \equiv -\lambda_2 \mod p_1$ and $i(\lambda_1 - \lambda_2) \equiv -(\tilde{\jmath}_1 - \tilde{\jmath}_2) \mod p_1$. Let s_1, r_2, s_2, r_1 be as above. Let $i_1 = i + s_1 \mod d'$, so i_1 is in the $\lambda_1, \tilde{\jmath}_1$-distinguished class. Likewise, let $i_2 = i + s_2 \mod d'$, which is in the $\lambda_2, \tilde{\jmath}_2$-distinguished class. Since i_1 is in the distinguished class we have $i_1(\lambda_1 - \lambda_2) \equiv -\tilde{\jmath}_1 \mod p_1$, and likewise we have $i_2(\lambda_2 - \lambda_1) \equiv -\tilde{\jmath}_2$. Subtracting these equations gives

$$(i_1 + i_2)(\lambda_1 - \lambda_2) \equiv -(\tilde{\jmath}_1 - \tilde{\jmath}_2) \equiv i(\lambda_1 - \lambda_2) \mod p_1.$$

Thus, $i \equiv i_1 + i_2 \mod p_1$. Also, by definition of the r function we have $r_2 \equiv -i_1 \mod p_1$, and $r_1 \equiv -i_2 \mod p_1$. Thus, $i + r_2 \equiv i - i_1 \equiv i_2 \mod p_1$. From the definition of s_2 it now follows that $s_2 = r_2$. Similarly, $r_1 \equiv -i_2 \mod p_1$ and so $i + r_1 \equiv i - i_2 \equiv i_1 \mod p_1$ from which it follows that $s_1 = r_1$. This verifies (7) as well. $\square$

We now define the $\sigma^\lambda_{\tilde{\jmath}}$. First assume that $\tilde{\jmath}$ is old. In this case, $\sigma^\lambda_{\tilde{\jmath}}(i)$ is already defined for the old i. We extend the partial function $\sigma^\lambda_{\tilde{\jmath}}$ to all values of i using lemma 3.9 and the r function. Thus,

$$\sigma^\lambda_{\tilde{\jmath}}(i) = \sigma^\lambda_{\tilde{\jmath}}(i + r(i) \mod d') + (\frac{r(i)}{u})d \mod d'.$$

It is immediate from lemma 3.9 that $\sigma^\lambda_{\tilde{\jmath}}$ is d'-good.

Suppose now $\tilde{\jmath}$ is new. Let i_d represent the congruence class mod p_1 of the distinguished class. We first define $\sigma^\lambda_{\tilde{\jmath}}(i)$ for $i \equiv i_d \mod p_1$, that is, in the distinguished class. Fix such an i, and we define $\sigma^\lambda_{\tilde{\jmath}}(i)$ by defining its congruence class mod $p_1^{a_1+1}, \ldots, p_n^{a_n}$. Consider one of these prime powers p^a, and suppose first that $p \neq p_1$. Let λ_2 be a root with $\lambda_2 \equiv \lambda \mod p^a$ and $\lambda_2 \equiv -\lambda \mod p_1$. Define $\tilde{\jmath}_2$ by $i(\lambda - \lambda_2) \equiv -(\tilde{\jmath} - \tilde{\jmath}_2) \mod d'$. Note that since i is in the distinguished class, $p_1|\tilde{\jmath}_2$, that is, $\tilde{\jmath}_2$ is old. Define then

$$\sigma^\lambda_{\tilde{\jmath}}(i) \equiv \sigma^{\lambda_2}_{\tilde{\jmath}_2}(i) - \frac{\lambda(\tilde{\jmath} - \tilde{\jmath}_2)}{d'} \mod p^a.$$

We check that this is well-defined, that is, it does not depend on the choice of λ_2. Suppose λ_3 is another root with $\lambda_3 \equiv \lambda \mod p^a$ and $\lambda_3 \equiv -\lambda \mod p_1$, so $\lambda_3 \equiv \lambda_2 \mod p_1^{a_1+1}$ as well. Let $\tilde{\jmath}_3$ be such that $i(\lambda - \lambda_3) \equiv -(\tilde{\jmath} - \tilde{\jmath}_3) \mod d'$. Since

$$i(\lambda - \lambda_2) \equiv -(\tilde{\jmath} - \tilde{\jmath}_2) \quad \text{and} \quad i(\lambda - \lambda_3) \equiv -(\tilde{\jmath} - \tilde{\jmath}_3) \mod d',$$

it follows that

$$i(\lambda_2 - \lambda_3) \equiv -(\tilde{\jmath}_2 - \tilde{\jmath}_3) \mod d'.$$

Let $i' = i + r(i) \mod d'$. Then we also have $i'(\lambda_2 - \lambda_3) \equiv -(\tilde{\jmath}_2 - \tilde{\jmath}_3) \mod d'$ since $(i - i')(\lambda_2 - \lambda_3)$ is divisible by d' (recall $r(i)$ is divisible by u). Since i', $\tilde{\jmath}_2$, $\tilde{\jmath}_3$ are old, by partial d'-consistency we therefore have

$$\sigma^{\lambda_2}_{\tilde{\jmath}_2}(i') - \sigma^{\lambda_3}_{\tilde{\jmath}_3}(i') \equiv -\frac{\lambda(\tilde{\jmath}_2 - \tilde{\jmath}_3)}{d'} \mod p^a.$$

Since $\sigma^{\lambda_2}_{\tilde{\jmath}_2}(i) - \sigma^{\lambda_3}_{\tilde{\jmath}_3}(i) \equiv \sigma^{\lambda_2}_{\tilde{\jmath}_2}(i') - \sigma^{\lambda_3}_{\tilde{\jmath}_3}(i') \mod d'$, it follows that

$$\sigma^{\lambda_2}_{\tilde{\jmath}_2}(i) - \sigma^{\lambda_3}_{\tilde{\jmath}_3}(i) \equiv -\frac{\lambda(\tilde{\jmath}_2 - \tilde{\jmath}_3)}{d'} \mod p^a.$$

Consequently, $\sigma^{\lambda_2}_{\tilde{\jmath}_2}(i) - \frac{\lambda(\tilde{\jmath} - \tilde{\jmath}_2)}{d'} \equiv \sigma^{\lambda_3}_{\tilde{\jmath}_3}(i) - \frac{\lambda(\tilde{\jmath} - \tilde{\jmath}_3)}{d'} \mod p^a$, and we are done.

For i still in the $\lambda, \tilde{\jmath}$-distinguished class, we now define $\sigma^\lambda_{\tilde{\jmath}}(i) \mod p_1^{a_1+1}$. Let π be a fixed good permutation of length $p_1^{a_1}$. For i in the distinguished class let $i' = \frac{i - (i \mod p_1)}{p_1}$. Define then $\sigma^\lambda_{\tilde{\jmath}}(i) \equiv \pi(i') - \frac{\lambda(\tilde{\jmath} - (\tilde{\jmath} \mod p_1^{a_1+1}))}{d'} \mod p_1^{a_1+1}$.

This defines $\sigma^\lambda_{\tilde{\jmath}}(i)$ for i in the distinguished class. We extend this to a full permutation using the $s^\lambda_{\tilde{\jmath}}$ function. Thus,

$$\sigma^\lambda_{\tilde{\jmath}}(i) \equiv \sigma^\lambda_{\tilde{\jmath}}(i + s^\lambda_{\tilde{\jmath}}(i) \mod d') + (\frac{s^\lambda_{\tilde{\jmath}}(i)}{u})d \mod d'.$$

This completes the definition of the $\sigma^\lambda_{\tilde{\jmath}}$ functions. It remains to verify that they satisfy the goodness and consistency conditions.

Lemma 3.16. *The $\sigma_{\tilde{j}}^{\lambda}$ satisfy the d'-goodness condition.*

Proof. We have already observed that this is the case for old $\tilde{j}$, so assume $\tilde{j}$ is new. It is enough to check that $\sigma_{\tilde{j}}^{\lambda}$ restricted to the distinguished class is a partially good function. To see this, suppose i_1, i_2 are in the distinguished class (in particular, $i_1 \equiv i_2 \mod p_1$). Let $i_1 - i_2 = p_1^{b_1} \dots p_n^{b_n} v$ where $(v, d') = 1$. Suppose first that $b_1 < a_1 + 1$. Let i_1', i_2' correspond to i_1, i_2 as in the definition of $\sigma_{\tilde{j}}^{\lambda} \mod p_1^{a_1+1}$. So, $i_1' - i_2' = \frac{(i_1 - i_2)}{p_1}$. By goodness of π, $\pi(i_1') \not\equiv \pi(i_2') \mod p_1^{a_1-(b_1-1)} = p_1^{(a_1+1)-b_1}$, and so $\sigma_{\tilde{j}}^{\lambda}(i_1) \not\equiv \sigma_{\tilde{j}}^{\lambda}(i_2) \mod p_1^{a_1+1-b_1}$, and thus also inequivalent mod $p_1^{\eta(a_1+1-b_1)} \cdots p_n^{\eta(a_n-b_n)}$.

Assume next that $b_1 \geq a_1 + 1$. We must show that $\sigma_{\tilde{j}}^{\lambda}(i_1) \not\equiv \sigma_{\tilde{j}}^{\lambda}(i_2) \mod w \doteq p_2^{\eta(a_2-b_2)} \cdots p_n^{\eta(a_n-b_n)}$. Let λ_2 be the root with $\lambda_2 \equiv -\lambda \mod p_1^{a_1+1}$, but $\lambda_2 \equiv \lambda \mod p_i^{a_i}$ for $i \geq 2$. Let $\tilde{j}_2$ be defined by $i_1(\lambda - \lambda_2) \equiv -(\tilde{j} - \tilde{j}_2) \mod d'$. Note then that we also have $i_2(\lambda - \lambda_2) \equiv -(\tilde{j} - \tilde{j}_2) \mod d'$, as $p_1^{a_1+1}$ divides $i_1 - i_2$. By the well-definedness noted above, we may use λ_2 and $\tilde{j}_2$ in the definitions of both $\sigma_{\tilde{j}}^{\lambda}(i_1)$ and $\sigma_{\tilde{j}}^{\lambda}(i_2)$ modulo any of the powers $p_i^{a_i}$, $i \geq 2$. Let p^a denote one of these powers. From the definition of the $\sigma_{\tilde{j}}^{\lambda}$ we have

$$\sigma_{\tilde{j}}^{\lambda}(i_1) \equiv \sigma_{\tilde{j}_2}^{\lambda_2}(i_1) - \frac{\lambda(\tilde{j} - \tilde{j}_2)}{d'} \mod p^a,$$

and

$$\sigma_{\tilde{j}}^{\lambda}(i_2) \equiv \sigma_{\tilde{j}_2}^{\lambda_2}(i_2) - \frac{\lambda(\tilde{j} - \tilde{j}_2)}{d'} \mod p^a,$$

and thus

$$\sigma_{\tilde{j}}^{\lambda}(i_1) - \sigma_{\tilde{j}}^{\lambda}(i_2) \equiv \sigma_{\tilde{j}_2}^{\lambda_2}(i_1) - \sigma_{\tilde{j}_2}^{\lambda_2}(i_2) \mod p^a.$$

Since this is true for each of the prime powers p^a, we also have

$$\sigma_{\tilde{j}}^{\lambda}(i_1) - \sigma_{\tilde{j}}^{\lambda}(i_2) \equiv \sigma_{\tilde{j}_2}^{\lambda_2}(i_1) - \sigma_{\tilde{j}_2}^{\lambda_2}(i_2) \mod u,$$

where $u = p_2^{a_2} \cdots p_n^{a_n}$. Hence it is enough to show that $\sigma_{\tilde{j}_2}^{\lambda_2}(i_1) \not\equiv \sigma_{\tilde{j}_2}^{\lambda_2}(i_2) \mod w$. Since $i_1 \equiv i_2 \mod p_1$, $r(i_1) = r(i_2)$. If i_1^* denotes $i_1 + r(i_1) \mod d'$ and likewise for i_2^*, then $i_1^* - i_2^* \equiv i_1 - i_2 \mod d'$, and also $\sigma_{\tilde{j}_2}^{\lambda_2}(i_1) - \sigma_{\tilde{j}_2}^{\lambda_2}(i_2) \equiv \sigma_{\tilde{j}_2}^{\lambda_2}(i_1^*) - \sigma_{\tilde{j}_2}^{\lambda_2}(i_2^*) \mod d'$ from the definition of $\sigma_{\tilde{j}}^{\lambda}$ for the old $\tilde{j}$. So, it is enough to show that $\sigma_{\tilde{j}_2}^{\lambda_2}(i_1^*) \not\equiv \sigma_{\tilde{j}_2}^{\lambda_2}(i_2^*) \mod w$. This, however follows immediately from the partial goodness of $\sigma_{\tilde{j}_2}^{\lambda_2}$ and the fact that $i_1^* - i_2^* \equiv i_1 - i_2 \mod d'$.

We have now shown that $\sigma_{\tilde{j}}^{\lambda}$ restricted to the distinguished class is partially good. The goodness of the full function $\sigma_{\tilde{j}}^{\lambda}$ now follows immediately from the extension lemma 3.9. □

Lemma 3.17. *The $\sigma_{\tilde{j}}^{\lambda}$ functions satisfy the d' consistency conditions.*

Proof. Fix i, $\tilde{j}_1$, $\tilde{j}_2$, λ_1, λ_2 with $i(\lambda_1 - \lambda_2) \equiv -(\tilde{j}_1 - \tilde{j}_2) \mod d'$. Let p^a be a prime power with $\lambda_1 \equiv \lambda_2 \mod p^a$. We may assume that $\tilde{j}_1$, $\tilde{j}_2$ are not both old, and without loss of generality that $\tilde{j}_1$ is new. For if $\tilde{j}_1$, $\tilde{j}_2$ are both old, then as in an argument above we would have $i'(\lambda_1 - \lambda_2) \equiv -(\tilde{j}_1 - \tilde{j}_2) \mod d'$ and $\sigma_{\tilde{j}_1}^{\lambda_1}(i') - \sigma_{\tilde{j}_2}^{\lambda_2}(i') \equiv \sigma_{\tilde{j}_1}^{\lambda_1}(i) - \sigma_{\tilde{j}_2}^{\lambda_2}(i) \mod d'$, where $i = i + r(i) \mod d'$. The result then follows.

Assume first that $\tilde{j}_2$ is old. In this case we must have i is new and $\lambda_2 \equiv -\lambda_1 \mod p_1$. In particular, $p \neq p_1$. From well-definedness, we may use $\tilde{j}_2$, λ_2 in the definition of $\sigma_{\tilde{j}_1}^{\lambda_1}(i) \mod p^a$. However, it is then immediate that

$$\sigma_{\tilde{j}_1}^{\lambda_1}(i) - \sigma_{\tilde{j}_2}^{\lambda_2}(i) \equiv -\frac{\lambda(\tilde{j}_1 - \tilde{j}_2)}{d'} \mod p^a,$$

where λ denotes either λ_1 or λ_2.

Assume henceforth that $\tilde{j}_1$, $\tilde{j}_2$ are both new. Consider first the case $p = p_1$. Thus, $\lambda_1 \equiv \lambda_2 \mod p_1^{a_1+1}$, and so $\tilde{j}_1 \equiv \tilde{j}_2 \mod p_1^{a_1+1}$. Thus, $s_{\tilde{j}_1}^{\lambda_1} = s_{\tilde{j}_2}^{\lambda_2} = s$, say. Let $i' = i + s(i) \mod d'$. Then i' is in the $\lambda_1, \tilde{j}_1$-distinguished class, which is the same as the $\lambda_2, \tilde{j}_2$-distinguished class. From the definition of the permutation extension, it follows that

$$\sigma_{\tilde{j}_1}^{\lambda_1}(i) - \sigma_{\tilde{j}_2}^{\lambda_2}(i) \equiv \sigma_{\tilde{j}_1}^{\lambda_1}(i') - \sigma_{\tilde{j}_2}^{\lambda_2}(i') \mod d'.$$

Thus, it suffices to show that $\sigma_{\tilde{j}_1}^{\lambda_1}(i') - \sigma_{\tilde{j}_2}^{\lambda_2}(i') \equiv -\frac{\lambda(\tilde{j}_1 - \tilde{j}_2)}{d'} \mod p_1^{a_1+1}$. Let $i^* = \frac{i-(i \mod p_1)}{p_1}$. Then

$$\sigma_{\tilde{j}_1}^{\lambda_1}(i') \equiv \pi(i^*) - \frac{\lambda(\tilde{j}_1 - (\tilde{j}_1 \mod p_1^{a_1+1}))}{d'} \mod p_1^{a_1+1},$$

where again λ denotes either λ_1 or λ_2. Likewise

$$\sigma_{\tilde{j}_2}^{\lambda_2}(i') \equiv \pi(i^*) - \frac{\lambda(\tilde{j}_2 - (\tilde{j}_2 \mod p_1^{a_1+1}))}{d'} \mod p_1^{a_1+1},$$

and so $\sigma_{\tilde{j}_1}^{\lambda_1}(i') - \sigma_{\tilde{j}_2}^{\lambda_2}(i') \equiv -\frac{\lambda(\tilde{j}_1 - \tilde{j}_2)}{d'} \mod p_1^{a_1+1}$.

Consider finally the case $p \neq p_1$. First, we argue that we may assume $\lambda_1 \not\equiv \lambda_2 \mod p_1^{a_1+1}$. For assume we can prove consistency in this case, and suppose $\lambda_1 \equiv \lambda_2 \mod p_1^{a_1+1}$. Let $\lambda_3 \equiv \lambda_1 \equiv \lambda_2 \mod p^a$, but $\lambda_3 \equiv -\lambda_1 \equiv -\lambda_2 \mod p_1$. Define $\tilde{j}_3$ by $i(\lambda_1 - \lambda_3) \equiv -(\tilde{j}_1 - \tilde{j}_3) \mod d'$. Since $i(\lambda_1 - \lambda_2) \equiv -(\tilde{j}_1 - \tilde{j}_2) \mod d'$, it also follows that $i(\lambda_2 - \lambda_3) \equiv -(\tilde{j}_2 - \tilde{j}_3) \mod d'$. By assumption we can show that that

$$\sigma_{\tilde{j}_1}^{\lambda_1}(i) - \sigma_{\tilde{j}_3}^{\lambda_3}(i) \equiv -\frac{\lambda(\tilde{j}_1 - \tilde{j}_3)}{d'} \mod p^a,$$

and also

$$\sigma_{\tilde{j}_2}^{\lambda_2}(i) - \sigma_{\tilde{j}_3}^{\lambda_3}(i) \equiv -\frac{\lambda(\tilde{j}_2 - \tilde{j}_3)}{d'} \mod p^a.$$

Subtracting, it follows that

$$\sigma_{\tilde{j}_1}^{\lambda_1}(i) - \sigma_{\tilde{j}_2}^{\lambda_2}(i) \equiv -\frac{\lambda(\tilde{j}_1 - \tilde{j}_2)}{d'} \mod p^a.$$

So, we may assume $\lambda_1 \equiv -\lambda_2 \mod p_1$. Consider first the definition of $\sigma_{\tilde{j}_1}^{\lambda_1}(i)$. Let $s_1 = s_{\tilde{j}_1}^{\lambda_1}(i)$. Let $i_1 = i + s_1 \mod d'$. Thus,

$$\sigma_{\tilde{j}_1}^{\lambda_1}(i) \equiv \sigma_{\tilde{j}_1}^{\lambda_1}(i_1) + (\frac{s_1}{u})d \mod d'.$$

Recall i_1 is in the $\lambda_1, \tilde{j}_1$-distinguished class. In defining $\sigma_{\tilde{j}_1}^{\lambda_1}(i_1) \mod p^a$, we may use the root λ_2 as $\lambda_2 \equiv \lambda_1 \mod p^a$ and $\lambda_2 \equiv -\lambda_1 \mod p_1^{a_1+1}$. Let $\tilde{j}_3$ be defined by $i_1(\lambda_1 - \lambda_2) \equiv -(\tilde{j}_1 - \tilde{j}_3) \mod d'$. We then have

$$\sigma_{\tilde{j}_1}^{\lambda_1}(i_1) - \sigma_{\tilde{j}_3}^{\lambda_2}(i_1) \equiv -\frac{\lambda(\tilde{j}_1 - \tilde{j}_3)}{d'} \mod p^a,$$

where again λ denotes either λ_1 or λ_2. Note that $\tilde{\jmath}_3$ is old. Let $r_2 = r(i_1)$. Let $i' = i_1 + r_1 \mod d'$. Then again by definition we have

$$\sigma^{\lambda_2}_{\tilde{\jmath}_3}(i_1) - \sigma^{\lambda_2}_{\tilde{\jmath}_3}(i') \equiv (\frac{r_2}{u})d \mod d'.$$

Combining these, we get

$$\sigma^{\lambda_1}_{\tilde{\jmath}_1}(i) \equiv \sigma^{\lambda_2}_{\tilde{\jmath}_3}(i') + (\frac{s_1 + r_2}{u})d - \frac{\lambda(\tilde{\jmath}_1 - \tilde{\jmath}_3)}{d'} \mod p^a.$$

Now consider $\sigma^{\lambda_2}_{\tilde{\jmath}_2}(i)$. Let $s_2 = s^{\tilde{\jmath}_2}_{\lambda_2}(i)$, and $i_2 = i + s_2 \mod d'$. So,

$$\sigma^{\lambda_2}_{\tilde{\jmath}_2}(i) - \sigma^{\lambda_2}_{\tilde{\jmath}_2}(i_2) \equiv (\frac{s_2}{u})d \mod d'.$$

In defining $\sigma^{\lambda_2}_{\tilde{\jmath}_2}(i_2)$, we may use λ_1 as the auxiliary root. Let $\tilde{\jmath}_4$ be defined by $i_2(\lambda_2 - \lambda_1) \equiv -(\tilde{\jmath}_2 - \tilde{\jmath}_4) \mod d'$. Thus we have

$$\sigma^{\lambda_2}_{\tilde{\jmath}_2}(i_2) - \sigma^{\lambda_1}_{\tilde{\jmath}_4}(i_2) \equiv -\frac{\lambda(\tilde{\jmath}_2 - \tilde{\jmath}_4)}{d'} \mod p^a.$$

Let $r_1 = r(i_2)$. Let $i'' = i_2 + r_1 \mod d'$. Since $i' \equiv i + s_1 + r_2 \mod d'$, and $i'' \equiv i + s_2 + r_1 \mod d'$, from (6) of lemma 3.15 it follows that $i' = i''$. We therefore have

$$\sigma^{\lambda_1}_{\tilde{\jmath}_4}(i_2) - \sigma^{\lambda_1}_{\tilde{\jmath}_4}(i') \equiv (\frac{r_1}{u})d \mod d'.$$

Combining, we get

$$\sigma^{\lambda_2}_{\tilde{\jmath}_2}(i) \equiv \sigma^{\lambda_1}_{\tilde{\jmath}_4}(i') - \frac{\lambda(\tilde{\jmath}_2 - \tilde{\jmath}_4)}{d'} + (\frac{s_2 + r_1}{u})d \mod p^a.$$

Thus,

$$\sigma^{\lambda_1}_{\tilde{\jmath}_1}(i) - \sigma^{\lambda_2}_{\tilde{\jmath}_2}(i) \equiv \sigma^{\lambda_2}_{\tilde{\jmath}_3}(i') - \sigma^{\lambda_1}_{\tilde{\jmath}_4}(i') + \frac{\lambda(\tilde{\jmath}_3 - \tilde{\jmath}_4)}{d'} - \frac{\lambda(\tilde{\jmath}_1 - \tilde{\jmath}_2)}{d'} \mod p^a.$$

We now claim that i' satisfies the hypothesis of the consistency condition for $\lambda_2, \tilde{\jmath}_3$ and $\lambda_1, \tilde{\jmath}_4$, that is, we claim that $i'(\lambda_2 - \lambda_1) \equiv -(\tilde{\jmath}_3 - \tilde{\jmath}_4) \mod d'$. If so, then by partial consistency (note: i', $\tilde{\jmath}_3$, $\tilde{\jmath}_4$ are old) we have

$$\sigma^{\lambda_2}_{\tilde{\jmath}_3}(i') - \sigma^{\lambda_1}_{\tilde{\jmath}_4}(i') \equiv -\frac{\lambda(\tilde{\jmath}_3 - \tilde{\jmath}_4)}{d'} \mod p^a,$$

and it then follows that

$$\sigma^{\lambda_1}_{\tilde{\jmath}_1}(i) - \sigma^{\lambda_2}_{\tilde{\jmath}_2}(i) \equiv -\frac{\lambda(\tilde{\jmath}_1 - \tilde{\jmath}_2)}{d'} \mod p^a,$$

and we are done.

It remains to show the claim. Collecting the above definitions we have (all the following equations are mod d'):

$$\begin{aligned}
&i(\lambda_1 - \lambda_2) \equiv -(\tilde{\jmath}_1 - \tilde{\jmath}_2) \\
&i_1(\lambda_1 - \lambda_2) \equiv -(\tilde{\jmath}_1 - \tilde{\jmath}_3) \\
&i_2(\lambda_2 - \lambda_1) \equiv -(\tilde{\jmath}_2 - \tilde{\jmath}_4) \\
&i_1 \equiv i + s_1 \\
&i_2 \equiv i + s_2 \\
&i' \equiv i + s_1 + r_2 \equiv i + s_2 + r_1
\end{aligned}$$

Thus,

$$i'(\lambda_2-\lambda_1) \equiv (i+s_2+r_1)(\lambda_2-\lambda_1) \equiv (\tilde{\jmath}_1-\tilde{\jmath}_2)+(s_2+r_1)(\lambda_2-\lambda_1).$$

On the other hand,

$$\begin{aligned}-(\tilde{\jmath}_3-\tilde{\jmath}_4) &\equiv -\left[\tilde{\jmath}_1+i_1(\lambda_1-\lambda_2)-\tilde{\jmath}_2-i_2(\lambda_2-\lambda_1)\right]\\ &\equiv -(\tilde{\jmath}_1-\tilde{\jmath}_2)-(i_1+i_2)(\lambda_1-\lambda_2)\\ &\equiv -(\tilde{\jmath}_1-\tilde{\jmath}_2)-(2i+s_1+s_2)(\lambda_1-\lambda_2) \mod d'.\end{aligned}$$

Thus,

$$\begin{aligned}&i'(\lambda_2-\lambda_1)+(\tilde{\jmath}_3-\tilde{\jmath}_4)\\ &\quad\equiv 2(\tilde{\jmath}_1-\tilde{\jmath}_2)-(s_2+r_1)(\lambda_1-\lambda_2)+(2i+s_1+s_2)(\lambda_1-\lambda_2)\\ &\quad\equiv -2i(\lambda_1-\lambda_2)-(s_2+r_1)(\lambda_1-\lambda_2)+(2i+s_1+s_2)(\lambda_1-\lambda_2)\\ &\quad\equiv (\lambda_1-\lambda_2)(s_1-r_1) \mod d'\end{aligned}$$

From (7) of lemma 3.15 we have $s_1=r_1$, and so $i'(\lambda_2-\lambda_1)+(\tilde{\jmath}_3-\tilde{\jmath}_4)\equiv 0 \mod d'$, which gives the claim. □

We now summarize and finish the proof of lemma 3.7. Let $d=p_1^{a_1}\cdots p_n^{a_n}$, and $d'=p_1d$. Assume the k, l functions are defined on R_d and satisfy $(*)_d$. From lemma 3.10, we may assume all of the p_i are non-trivial (congruent to 1 mod 4). By lemma 3.11, we get d-good permutations $\pi_{\tilde{\jmath}}^{\lambda}$ for all $0\le\tilde{\jmath}<d$ and d-roots λ which satisfy the d-consistency condition. From lemmas 3.16, 3.17, the family $\sigma_{\tilde{\jmath}}^{\lambda'}$ for $0\le\tilde{\jmath}<d'$, λ' a d'-root, satisfies the d'-goodness and d'-consistency conditions. From lemma 3.12, we have functions k', l' defined on $R_{d'}$ which satisfy $(*)_{d'}$. Finally, without loss of generality, we may assume the k', l' functions extend the k, l functions. This follows from d'-consistency, since for points of the form $(\frac{i}{d},\frac{j}{d})=(\frac{p_1i}{d'},\frac{p_1j}{d'})$, by definition of the $\sigma_{p_1\tilde{\jmath}}^{\lambda'}$ the given values of k, l for this point satisfy the defining equations for $k'+\lambda'l'$ mod each prime power of d'. More specifically, for any d' root λ', the definition of the $\sigma_{p_1\tilde{\jmath}}^{\lambda'}$, equation 28, rewritten becomes

$$(k+\lambda'l)\equiv\sigma_{p_1\tilde{\jmath}}^{\lambda'}(p_1i)+\lambda'm-\frac{1}{2}\left(\frac{1+\lambda'^2}{d'}\right)(p_1i) \mod d', \tag{31}$$

where $\tilde{\jmath}$ and m are such that $0\le\tilde{\jmath}<d$ and $p_1j=p_1\tilde{\jmath}+\lambda'p_1i-md'$. If p^a is a prime power occurring in d', and $\lambda'_{p^a}=\lambda' \mod p^a$, then

$$(k+\lambda'_{p^a}l)\equiv\sigma_{p_1\tilde{\jmath}}^{\lambda'}(p_1i)+\lambda'_{p^a}m-\frac{1}{2}\left(\frac{1+\lambda'^2}{d'}\right)(p_1i) \mod p^a, \tag{32}$$

and this is precisely equation 19 (with $\sigma_{p_1\tilde{\jmath}}^{\lambda'}$ replacing $\pi_{\tilde{\jmath}}^{\lambda}$, and λ' replacing λ), which is a typical defining equation for k', l'.

This completes the proof of lemma 3.7, and of lemma A. We now indicate the minor adjustments necessary to get lemma A′. There are two differences between lemma A and lemma A′. First, in lemma A′ there is a distinguished point $(r,s)\in\mathbb{Q}^2\cap R$ for which there are prescribed values for the k, l functions. Secondly, in lemma A′ we must arrange that all of the points $z+(k(z),l(z))$ for $z\in\mathbb{Q}^2\cap R$ lie in the set P as in the statement of lemma A′.

Fix i, j, d such that $r=\frac{i}{d}$, $s=\frac{j}{d}$. Let k_d, l_d be functions on R_d satisfying $(*)_d$. If we add constant values k_0, l_0 to the k_d, l_d functions respectively, the new functions

k'_d, l'_d also satisfy $(*)_d$. We choose k_0, l_0 so that k'_d, l'_d take the prescribed values at (r,s). Inspecting equation 3, we see that if functions k''_d, l''_d satisfy $k''_d(z) \equiv k'_d \mod d$, $l''_d(z) \equiv l'_d \mod d$ for all $z \in R_d$, then k''_d, l''_d also satisfy $(*)_d$. From the assumed property of P, we may choose k''_d, l''_d so that $z + (k''_d(z), l''_d(z)) \in P$ for all $z \in R_d$. Similarly, at each step when we extend the k, l functions from R_d to $R_{d'}$, only the values of the extended functions mod d' matter in determining $(*)_{d'}$. We may therefore adjust these values mod d' so that $z + (k(z), l(z)) \in P$ for all $z \in R_{d'}$. This completes the proof of lemma A$'$.

4. Proof of lemma B

In this section we prove lemma B, which completes the proof of theorem 1.2. First, we note that a weaker version of lemma B due to Komjáth (lemma 1.1 of [13]) would suffice for our main theorem. Specifically,

Lemma 4.1. (Komjáth) *There is bound $s \in \omega$ such that if $c_1, \dots, c_s$ are points in the plane with $\rho(c_i, c_j)^2 \notin \mathbb{Z}$ for distinct c_i, c_j, and if $z_1, \dots, z_s$ are* colinear *points with $\rho(c_i, z_i)^2 \in \mathbb{Q}$ and $\rho(z_i, z_j)^2 \in \mathbb{Z}$, then the z_i are definable from $\{c_1, \dots, c_s\}$; in fact, for fixed $c_1, \dots, c_s$, distances $\rho(c_i, z_i)$ and $\rho(z_i, z_j)$, there are only finitely many such $\{z_1, \dots, z_s\}$.*

To see this suffices, consider (in the notation of claim 2.7) The set E_n of points z having rational coordinates with respect to L_n such that for some $c \in S_{<\vec{\alpha}}$, $\rho^2(c, z) \in \mathbb{Q}$, where c is not rational respect to L_n. Using lemma 4.1 it is easy to see that E_n is *semi-small* respect to L_n. By this we mean that for any rational translation L of L_n, there is a finite set F of lines such that for any line $l \notin F$, $l \cap L \cap E_n$ is finite. Then at each stage in the construction of the points x_m (following claim 2.7) we must have x_m avoid a certain semi-small set, which is no problem.

As we mentioned earlier, lemma B is implicit in the analysis of Gibson-Newstead [8], although it is not explicitly stated there. Newstead (private communication) pointed out the following argument. Consider the coupler curve traced out by the point p_3, where triangle $\triangle p_1 p_2 p_3$ is rigid, and p_1, p_2 are constrained to lie on circles C_1, C_2 respectively. From [8], the complexification of this curve is a degree 6 curve C in the complex projective plane. They show it is the projection of a higher dimensional curve (the "residual curve") also of degree 6, whose singularities they analyze. Thus, the irreducible components of C precisely correspond to those of R. The components of R are analyzed in [8]. The list on pp. 119, 120 gives two cases where R (and thus C) can have a component of degree two, namely:

(i) $c_1 c_2 p_2 p_1$ is a parallelogram.

(ii) $p_1 = c_2$ or $p_2 = c_1$.

The second case forces $c_3 = c_2$ or $c_3 = c_1$, which is forbidden as we require c_1, c_2, c_3 be distinct. The first case is our exceptional case of lemma B.

We now present two elementary proofs of lemma B. The first is a short algebraic proof using some computer algebra, and the second a purely geometric argument.

4.1. An Algebraic Proof.

The following algebraic computations were performed using *Maple*.

We assume without loss of generality that C_1 is the circle centered at $c_1 = (0,0)$ of radius 1, C_2 is the circle centered at $c_2 = (a, 0)$ of radius r, and C_3 is the circle centered at (b, c) of radius s. Let $p_1 = (x, y)$ be a point on C_1. If we let d denote the fixed distance between p_1 and the point p_2 on C_2, then we may coordinatize $p_2 = (x_2, y_2)$ by

$$\begin{aligned} x_2 &= x + d\cos(\theta) \\ y_2 &= y + d\sin(\theta), \end{aligned} \tag{33}$$

where θ denotes the angle p_1p_2 makes with the horizontal, measured in the usual way. Let α denote the fixed angle of the triangle $p_1p_2p_3$, and let $e = \rho(p_1, p_3)$. Thus, the coordinates of p_3 are of the form

$$\begin{aligned} x_3 &= x + e\cos(\alpha+\theta) = x + u\cos(\theta) - v\sin(\theta) \\ y_3 &= y + e\sin(\alpha+\theta) = y + v\cos(\theta) + u\sin(\theta), \end{aligned} \tag{34}$$

where we let $u = e\cos(\alpha)$ and $v = e\sin(\alpha)$. Since p_1, p_2, p_3 lie on C_1, C_2, C_3 we have

$$\begin{aligned} &x^2 + y^2 - 1 = 0 \\ &(x_2 - a)^2 + y_2^2 - r^2 = 0 \\ &(x_3 - b)^2 + (y_3 - c)^2 - s^2 = 0. \end{aligned} \tag{35}$$

Subtracting the second, third equations from the first gives two linear equations for x, y in terms of θ:

(36)

$$\begin{aligned} &-1 - 2\,x\,d\cos(\theta) + 2\,x\,a + 2\,d\cos(\theta)\,a - a^2 - 2\,y\,d\sin(\theta) - d^2 + r^2 = 0 \\ &-1 - 2\cos(\theta)\,u\,x + 2\cos(\theta)\,u\,b - v^2 + 2\sin(\theta)\,v\,x - 2\sin(\theta)\,v\,b + 2\,x\,b - b^2 - u^2 \\ &\quad - 2\sin(\theta)\,u\,y + 2\sin(\theta)\,u\,c - 2\cos(\theta)\,v\,y + 2\cos(\theta)\,v\,c + 2\,y\,c - c^2 + s^2 = 0. \end{aligned}$$

Solving these two equations for x, y gives:

(37)

$$\begin{aligned} x = &-\frac{1}{2}(-d\sin(\theta) - \cos(\theta)\,v\,r^2 + \cos(\theta)\,v\,d^2 + \cos(\theta)\,v\,a^2 - c - v^2\,d\sin(\theta) + \sin(\theta)\,u \\ &+ \cos(\theta)\,v - \sin(\theta)\,u\,r^2 + \sin(\theta)\,u\,d^2 + \sin(\theta)\,u\,a^2 + s^2\,d\sin(\theta) - c^2\,d\sin(\theta) - \\ &u^2\,d\sin(\theta) - b^2\,d\sin(\theta) + 2\,c\,d\cos(\theta)\,a - c\,a^2 - c\,d^2 + c\,r^2 - 2\,v\,d\,a + \\ &2\cos(\theta)\,v\,c\,d\sin(\theta) - 2\sin(\theta)\,u\,d\cos(\theta)\,a + 2\,v\,d\,a\sin^2(\theta) - 2\sin^2(\theta)\,v\,b\,d + \\ &2\sin^2(\theta)\,u\,c\,d + 2\cos(\theta)\,u\,b\,d\sin(\theta))/(c\,a + b\,d\sin(\theta) - \sin(\theta)\,u\,a - \cos(\theta)\,v\,a \\ &- c\,d\cos(\theta) + v\,d) \end{aligned}$$

(38)

$$\begin{aligned} y = &\frac{1}{2}(-d\cos(\theta) + a - b + \cos(\theta)\,u - \sin(\theta)\,v - v\,d^2\sin(\theta) + v\,r^2\sin(\theta) - v\,a^2\sin(\theta) \\ &- \cos(\theta)\,u\,r^2 + d^2\cos(\theta)\,u + \cos(\theta)\,u\,a^2 - d\cos(\theta)\,c^2 - d\cos(\theta)\,b^2 - d\cos(\theta)\,u^2 \\ &+ d\cos(\theta)\,s^2 - d\cos(\theta)\,v^2 - 2\,a\sin(\theta)\,u\,c - 2\,u\,b\,d\sin^2(\theta) - 2\,v\,c\,d\sin^2(\theta) \\ &+ 2\sin^2(\theta)\,u\,d\,a - 2\,d\cos(\theta)\sin(\theta)\,v\,b - 2\,a\cos(\theta)\,u\,b - d^2\,b + a\,v^2 + a\,u^2 \\ &+ a\,c^2 - a\,s^2 - a^2\,b + r^2\,b + a\,b^2 - 2\,u\,d\,a + 2\,u\,b\,d + 2\,v\,c\,d + 2\,d\cos(\theta)\sin(\theta)\,u\,c \\ &+ 2\,d\cos(\theta)\,v\,a\sin(\theta) + 2\,a\sin(\theta)\,v\,b - 2\,a\cos(\theta)\,v\,c + 2\,d\cos(\theta)\,a\,b)/ \\ &(c\,a + b\,d\sin(\theta) - \sin(\theta)\,u\,a - \cos(\theta)\,v\,a - c\,d\cos(\theta) + v\,d) \end{aligned}$$

Substituting these expressions back into the equation x^2+y^2-1 now gives a large rational function of $\sin(\theta)$, $\cos(\theta)$. Setting the numerator of this expression to 0 now gives an equation of the form

(39)

$$z_{00}+z_{01}\sin(\theta)+z_{10}\cos(\theta)+z_{11}\cos(\theta)\sin(\theta)+z_{20}\cos^2(\theta)+z_{21}\cos^2(\theta)\sin(\theta) + z_{30}\cos^3(\theta)=0,$$

where all of the z_{ij} are polynomials in a, b, c, d, u, v, r, and s.

The exceptional case of lemma B corresponds to a motion of p_1, p_2, p_3 where θ remains constant. Assuming we are not in this case, there will be infinitely many values of θ satisfying equation 39. Thus, the function of equation 39 is identically 0. Since the trigonometric polynomials of equation 39 are linearly independent, this implies that all of the z_{ij} are 0.

In fact, just the last two equations $z_{21}=0$, $z_{30}=0$ suffice to finish the proof. These two expressions are:

(40)

$$\begin{aligned} z_{21} &= 8\,v\,a^2\,d^2\,b-16\,v\,a^2\,u\,b\,d+16\,a\,u\,c\,d^2\,b-8\,v^2\,d\,c\,a^2+8\,u^2\,d\,c\,a^2-8\,b^2\,d^2\,v\,a \\ &\quad -16\,c\,u^2\,d\,a\,b-8\,u\,a^2\,c\,d^2+8\,c^2\,d^2\,v\,a-16\,d\,u\,c^2\,a\,v+16\,d\,v\,b^2\,a\,u+16\,v^2\,d\,b\,a\,c \\ z_{30} &= -32\,v\,a\,u\,c\,b\,d+16\,c\,a\,v\,d^2\,b+8\,d\,c^2\,a\,u^2-8\,v\,a^2\,c\,d^2-8\,d\,v^2\,a^2\,b \\ &\quad +16\,u\,a^2\,v\,c\,d+8\,d\,v^2\,a\,b^2-8\,d\,c^2\,a\,v^2-8\,u\,a^2\,d^2\,b+8\,a^2\,u^2\,d\,b-8\,c^2\,d^2\,u\,a \\ &\quad -8\,d\,u^2\,a\,b^2+8\,d^2\,b^2\,u\,a \end{aligned}$$

Computing a list of reduced Gröbner bases for this pair of equations yields the following (this means that the variety determined by the system $z_{21}=z_{30}=0$ is the union of the subvarieties determined by the polynomials in each basis listed):

(41)

$$\begin{aligned} &[d],\ [a],\ [c\,u\,d\,a-a\,d\,v\,b-2\,c\,u\,b\,d+2\,d\,v\,b^2-u^2\,a\,c+2\,u\,a\,v\,b+v^2\,a\,c+2\,c\,u^2\,b \\ &\quad -4\,v\,b^2\,u-2\,v^2\,b\,c,\ a\,u\,b\,d+c\,a\,v\,d-2\,u\,b^2\,d-2\,b\,v\,c\,d-b\,a\,u^2-2\,v\,a\,u\,c+b\,a\,v^2 \\ &\quad +2\,u^2\,b^2+4\,v\,u\,c\,b-2\,v^2\,b^2,\ c^2+b^2],\ [v,\ c,\ b],\ [d-2\,u,\ c,\ b], \\ &\quad [u\,d\,a-v\,c\,d+2\,a\,v^2+2\,u\,v\,c,\ v\,d\,a+d\,u\,c-2\,u\,v\,a+2\,v^2\,c,\ u^2+v^2,\ b], \\ &\quad [d-u,\ v,\ b],\ [u\,d\,a-a\,u^2+u\,v\,c,\ v\,d\,a-u\,v\,a+v^2\,c,\ -u\,c-a\,v+c\,d,\ c^2+a^2,\ b], \\ &\quad [c\,u\,d\,a-c\,u\,b\,d-c^2\,d\,v+2\,v^2\,a\,c+2\,u\,c^2\,v-2\,v^2\,b\,c, \\ &\quad a\,u\,b\,d-u\,b^2\,d-b\,v\,c\,d+2\,b\,a\,v^2+2\,v\,u\,c\,b-2\,v^2\,b^2, \\ &\quad v\,d\,a+d\,u\,c-d\,v\,b-2\,u\,v\,a+2\,v\,u\,b+2\,v^2\,c,\ u^2+v^2],\ [u,\ v,\ c],\ [a-b,\ v,\ c], \\ &\quad [d-u,\ v,\ c],\ [d-u,\ v],\ [a\,u\,b\,d-u\,b^2\,d-b\,a\,u^2+v\,u\,c\,b+u^2\,b^2,\ v\,d\,a \\ &\quad -d\,v\,b+v\,u\,b-u\,v\,a+v^2\,c,\ -u\,c+v\,b-a\,v+c\,d,\ b^2-2\,a\,b+c^2+a^2] \end{aligned}$$

Recalling that $u^2+v^2=e^2$, inspecting the bases in this list shows that they imply, in succession: $d=0$, $a=0$, $b=c=0$, $b=c=0$, $b=c=0$, $e=0$, $e=0$, $b=c=0$, $e=0$, $e=0$, $b=a$ and $c=0$, $e=0$, $e=0$, $b=a$ and $c=0$. We have used here the fact that the equations $d=u$ and $v=0$ imply that $p_3=p_2$, and hence $e=0$. Since the centers c_1, c_2, c_3 are distinct, all of these cases are forbidden. This completes the algebraic proof of lemma B.

4.2. **A Geometric Proof.** Let C_1 be the circle with center c_1 and radius r_1, and C_2 the circle with center c_2 and radius r_2. Let p_1, p_2 be distinct points with $p_1 \in C_1$ and $p_2 \in C_2$. Let $f = \rho(p_1, p_2)$. By a "motion" of (p_1, p_2) we mean continuous functions $p_1(t)$, $p_2(t)$ for $0 \le t \le 1$ such that $p_1(0) = p_1$, $p_2(0) = p_2$, and for all t from 0 to 1 we have $p_1(t) \in C_1$, $p_2(t) \in C_2$, and $\rho(p_1(t), p_2(t)) = f$. We say (q_1, q_2) is in the motion of (p_1, p_2) if there is a motion from (p_1, p_2) to (q_1, q_2). We will also say q_1 is in the motion of p_1 (and likewise for p_2, q_2) if there is a motion from p_1, p_2 to some pair (q_1, q_2). For a given motion, let $\theta_1(t)$ (and likewise for $\theta_2(t)$) be the continuous function such that $\theta_1(0) \in [0, 2\pi)$, and $\theta_1(t) \mod 2\pi$ is the angle θ such that $p_1(t) = c_1 + (r_1 \cos(\theta), r_1 \sin(\theta))$.

We say a motion $(p_1(t), p_2(t))$ is analytic if the coordinate functions $p_1(t) = (x_1(t), y_1(t))$, $p_2(t) = (x_2(t), y_2(t))$ are analytic functions of t.

Definition 4.2. We say (q_1, q_2) is an extreme point in the motion of (p_1, p_2) for q_1 (and likewise for q_2) if it is in the motion of (p_1, p_2), and any motion of (q_1, q_2) has, for sufficiently small t, q_1 moving in at most one of the two possible tangential directions on C_1 (we refer to this side as the allowable side of q_1). We will also refer to q_1 as being an extreme point in the motion of p_1. We say an extreme point (q_1, q_2) is non-trivial if there is a non-constant motion from (q_1, q_2).

If (q_1, q_2) is an extreme point in the motion of (p_1, p_2) for q_1, then q_1q_2 must pass through c_2. In fact, the non-trivial extreme points can be characterized as those points (q_1, q_2) such that q_1q_2 passes through one of the centers c_1, c_2, but not the other.

Figure 1 illustrates a possible extreme configuration (it is also possible that q_2 lies on the other side of c_2 from q_1).

The following lemma is not required for the proof of lemma B, but it helps to put the above definition in perspective.

Lemma 4.3. *Suppose c_2 lies outside of the circle C_1, or c_1 lies outside C_2. Then except for the exceptional case where $r_1 = r_2$ and $\rho(p_1, p_2) = \rho(c_1, c_2)$, there must be an extreme point in the motion of (p_1, p_2).*

Proof. Without loss of generality we may assume $c_1 = (0, 0)$, and $c_2 = (c, 0)$ is on the x-axis and to the right of C_1 ($c > r_1$). First assume $r_1 > r_2$. We show there is an extreme point in the motion of p_1. If not, then there is a motion of p_1 to the point $(-r_1, 0)$, and also a motion to the point $(r_1, 0)$. Note that C_2 lies entirely to the right of the line $x = 0$. The fact that p_1 can be moved to $(-r_1, 0)$ shows that $f \ge c + r_1 - r_2$. The fact that p_1 can be moved to $(r_1, 0)$, however, shows that $f \le c + r_2 - r_1$, a contradiction. Assume next that $r_1 < r_2$, and we show there is an extreme point in the motion of p_2. Suppose not, so p_2 can be moved to both $(c + r_2, 0)$ and $(c - r_2, 0)$. From the first fact it follows that $f \ge c + r_2 - r_1$. If $c - r_2 \le 0$, then the second fact implies $f \le r_1 + r_2 - c$. Hence $c \le r_1$, a contradiction. If $c - r_2 > 0$, the second fact implies $f \le c - r_2 + r_1$. Hence $r_2 \le r_1$, also a contradiction. Finally, if $r_1 = r_2$, then the argument of the first case also gives a contradiction unless $f = c$, that is, $\rho(c_1, c_2) = \rho(p_1, p_2)$. This is the exceptional case of lemma B. $\square$

Definition 4.4. We say a point (q_1, q_2) in the motion of (p_1, p_2) is a double point for q_1 if for all q_1' in a one-sided neighborhood of q_1 on C_1 (which we call an allowable side; this may include both sides) except perhaps for q_1 itself, there are two distinct points q_2', q_2'' on C_2 such that $\rho(q_1', q_2') = f$, $\rho(q_1', q_2'') = f$ and there is an analytic motion from (q_1', q_2') to (q_1', q_2'').

If (q_1, q_2) is a non-trivial extreme point for q_1 in the motion of (p_1, p_2), then it is a double point for q_1. For if $q_1' \neq q_1$ is sufficiently close to q_1 and on the allowable side of q_1, then there will be two distinct q_2', q_2'' such that $\rho(q_1', q_2') = f$, $\rho(q_1', q_2'') = f$, with q_2', q_2'' close to q_2 and lying on opposite sides of q_2. If $q_2(t)$ is an analytic function moving from q_2' to q_2'' along C_2, then the corresponding motion of q_1 is also described by an analytic function $q_1(t)$. [In general, if $q_2(t)$ is an analytic motion along C_2, and $q_1(t)$ is a motion along C_1 such that $\rho(q_1(t), q_2(t)) = f$ for all t, then $q_1(t)$ is necessarily analytic provided $q_1(t)q_2(t)$ does not pass through c_1 for all t.]

Note that in the definition of a double point, we do not require that in the analytic motion from (q_1', q_2') to (q_1', q_2'') the function $q_1(t)$ stay in a small neighborhood of q_1'. This is the case, however, if (q_1, q_2) is an extreme point in the motion of q_1, as the above argument shows.

We turn now to the proof of lemma B. Fix circles C_1, C_2 with centers at c_1, c_2 and radii r_1, r_2, and we assume $c_1 \neq c_2$. Fix $p_1 \in C_1$, $p_2 \in C_2$, and let $f = \rho(p_1, p_2)$ (we assume $f > 0$). Fix a triangle abc with $f = \rho(a, b)$. We henceforth assume we are not in the exceptional case of lemma B, so either $r_1 \neq r_2$ or $f \neq \rho(c_1, c_2)$. It suffices to show that for any analytic motion $p_1(t)$, $p_2(t)$ of (p_1, p_2), the corresponding motion $p_3(t)$ does not lie entirely on a circle C_3. Here $p_3(t)$ is the point such that the triangle $p_1(t)p_2(t)p_3(t)$ is congruent to abc. To see this, suppose (p_1^n, p_2^n, p_3^n) were infinitely many triples with $p_i \in C_i$ and $p_1^n p_2^n p_3^n$ congruent to abc. Let $p_1 \in C_1$, $p_2 \in C_2$, $p_3 \in C_3$, be such that (p_1, p_2, p_3) is a limit of a subsequence of the (p_1^n, p_2^n, p_3^n). Consider an analytic motion $p_1(t)$ on C_1 nearby p_1. If p_1p_2 does not pass through c_2, then the corresponding motions $p_2(t)$, $p_3(t)$ are uniquely determined and also analytic. Since $\rho(p_3(t), c_3)^2$ is analytic and has infinitely many zeros in a neighborhood of $t = 0$ (we assume $p_1(0) = p_1$), this function must then be identically zero, and thus $p_3(t)$ lies entirely on C_3. Suppose p_1p_2 passes through c_2. Let $p_1(t)$ be an analytic motion on C_1 nearby p_1 moving in a direction from p_1 such that there are infinitely many p_1^n in any interval $[p_1(0), p_1(t))$ for any $t > 0$. There at two analytic functions $p_2(t)$, $p_2'(t)$ such that $p_2(0) = p_2$ and $p_2(t) \in C_2$, $\rho(p_1(t), p_2(t)) = f$ for all t. Furthermore, all (q_1, q_2) close enough to (p_1, p_2) with q_1 on the appropriate side of p_1 and such that $q_1 \in C_1$, $q_2 \in C_2$, and $\rho(q_1, q_2) = f$ must be of the form $(p_1(t), p_2(t))$ or $(p_1(t), p_2'(t))$ for some t. Without loss of generality, assume for infinitely many n that $(p_1^n, p_2^n) = (p_1(t_n), p_2(t_n))$. Let $p_3(t)$ be the analytic function corresponding to $p_1(t)$, $p_2(t)$. Considering the function $\rho(p_3(t), c_3)^2$ as before now shows that $p_3(t)$ lies entirely on C_3.

We will consider several cases in the proof of lemma B.

Case I. There is a double point (q_1, q_2) in the motion of (p_1, p_2).

If $z_1 \in C_1$ is sufficiently close to q_1 and on an allowable side of q_1, then there are two points z_2, z_2' which lie on C_2 and satisfy $\rho(z_1, z_2) = \rho(z_1, z_2') = f$. Furthermore, there is an analytic motion from (q_1, q_2) to either (z_1, z_2) or (z_1, z_2'). Note that z_2, z_2' are symmetrical with respect to the line from z_1 to c_2. See figure 2. Let z_3, z_3' denote the corresponding values of z_3. Since z_3, z_3' both lie on C_3, clearly the line through z_1 which bisects the segment z_3z_3' passes through c_3. In other words, if $l(z_1)$ denotes the line through z_1 such that the angle between $l(z_1)$ and z_1c_2 is $\alpha \doteq$ the angle cab, then $l(z_1)$ must pass through c_3. To express this analytically, we coordinatize the circles by letting (without loss of generality) $c_1 = (0,0)$, $c_2 = (a,0)$, and $r_1 = 1$. Let $c_3 = (c,d)$, and $\gamma = \tan(\alpha)$. Let β be the angle between the segment z_1c_2 and the horizontal line from z_1. Let $z_1 = (\cos(\theta), \sin(\theta))$. Thus, $\tan(\beta) = \frac{\sin(\theta)}{a-\cos(\theta)}$. Note that $\alpha - \beta$ is the angle between the horizontal and the segment z_1c_3. If $m(\theta)$ denotes the slope of the line through z_1 and c_3, then we have

$$m(\theta) = \tan(\alpha - \beta) = \frac{\tan(\alpha) - \frac{\sin(\theta)}{a-\cos(\theta)}}{1 + (\tan(\alpha)\left(\frac{\sin(\theta)}{a-\cos(\theta)}\right)} = \frac{\gamma(a - \cos(\theta)) - \sin(\theta)}{(a - \cos(\theta)) + \gamma\sin(\theta)}.$$

Thus, the equation of the line $l(z_1)$ is

$$y = \frac{\gamma(a - \cos(\theta)) - \sin(\theta)}{(a - \cos(\theta)) + \gamma\sin(\theta)}x + \left[\sin(\theta) - (\cos(\theta))\frac{\gamma(a - \cos(\theta)) - \sin(\theta)}{(a - \cos(\theta)) + \gamma\sin(\theta)}\right].$$

Since all of these lines pass through (c,d), it follows that

$$\frac{\gamma(a - \cos(\theta)) - \sin(\theta)}{(a - \cos(\theta)) + \gamma\sin(\theta)}(c - \cos(\theta)) + \sin(\theta) - d$$

is identically 0 for θ in some interval. This simplifies to

$$(\gamma + \gamma ac - ad) + (a - c - \gamma d)\sin(\theta) + (-\gamma a - \gamma c + d)\cos(\theta) = 0.$$

Since 1, $\sin(\theta)$, $\cos(\theta)$ are linearly independent, we have

$$\begin{aligned} c\gamma a - ad + \gamma &= 0 \\ -c + a - \gamma d &= 0 \\ -c\gamma + d - \gamma a &= 0 \end{aligned} \tag{42}$$

From the first and third equations it follows that either $\gamma = 0$ or $a = 1$. If $\gamma = 0$, then from the second equation we have $c = a$. Since $\alpha = 0$ or π in this case, we must therefore have $d = 0$. That is, $c_3 = c_2$, a contradiction.

Assume now that $a = 1$. Solving the second and third equations for c and d gives $c = \frac{1-\gamma^2}{1+\gamma^2}$, $d = \frac{2\gamma}{1+\gamma^2}$. Thus, $c_3 = (c,d)$ lies on the circle C_1 of radius 1. Since $a = 1$, c_2 also lies on C_1. Recall $f = \rho(p_1, p_2)$, and let $e = \rho(p_1, p_3)$. Let $r = r_2$ be the radius of the second circle, and $s = r_3$ the radius of the third. Using

FIGURE 1

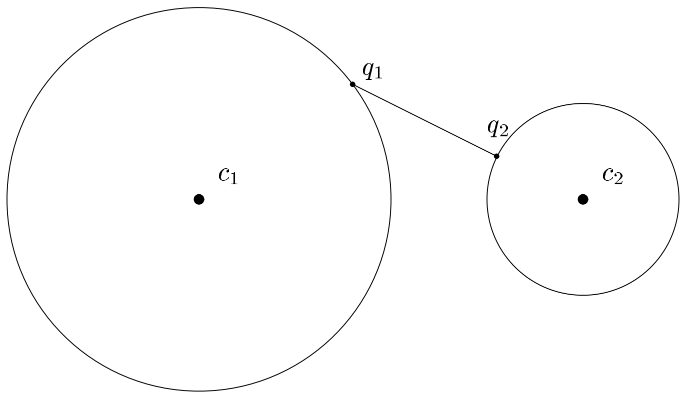
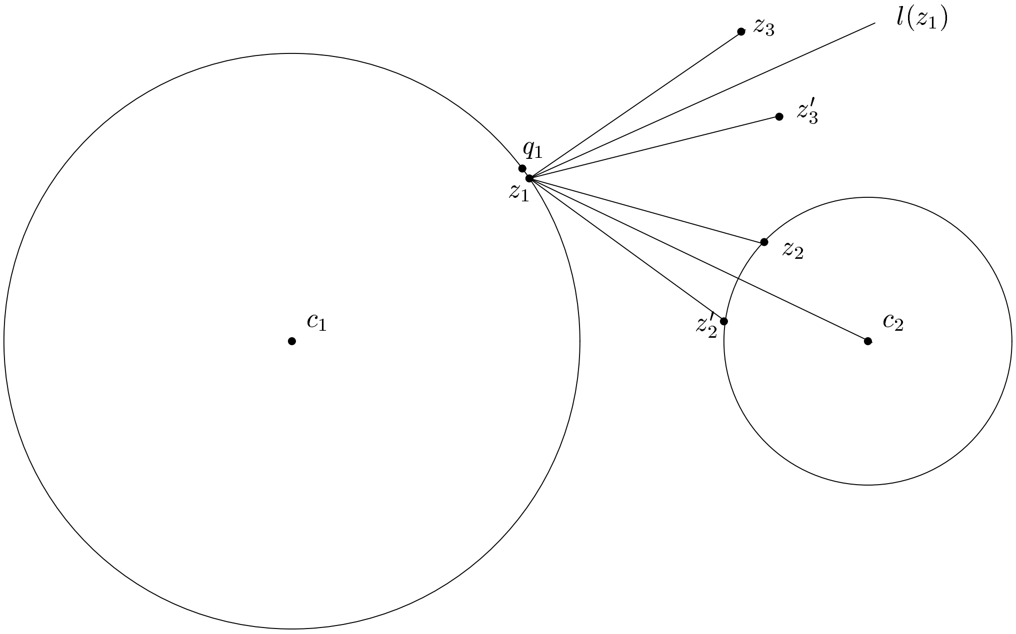


FIGURE 2



the same coordinatization and notation as above, except β now denotes the angle $\angle z_2 z_1 c_2 = \angle z_3 z_1 c_3$, the law of cosines gives

(43)

$$r^2 = f^2 + \sin^2(\theta) + (\cos(\theta) - a)^2 - 2f\sqrt{\sin^2(\theta) + (\cos(\theta) - a)^2}\cos(\beta)$$

$$s^2 = e^2 + (\sin(\theta - d)^2 + (\cos(\theta - c)^2 - 2e\sqrt{(\sin(\theta) - d)^2 + (\cos(\theta - c)^2)}\cos(\beta)$$

This becomes

$$\frac{u + a\cos(\theta)}{f\sqrt{\sin^2(\theta) + (\cos(\theta) - a)^2}} = \frac{v + d\sin(\theta) + c\cos(\theta)}{e\sqrt{(\sin(\theta) - d)^2 + (\cos(\theta) - c)^2}}, \tag{44}$$

where $2u = r^2 - f^2 - a^2 - 1$ and $2v = s^2 - e^2 - c^2 - d^2 - 1$. Substituting $a = 1$, cross-multiplying and squaring, this becomes

$$h_1 + h_2\cos(\theta) + h_3\cos^2(\theta) + h_4\cos^3(\theta) + h_5\sin(\theta) + h_6\sin(\theta)\cos(\theta) + h_7\sin(\theta)\cos^2(\theta) = 0,$$

where

$$\begin{aligned}
h_1 &= e^2\,u^2\,d^2 + e^2\,u^2\,c^2 - 2\,f^2\,v^2 - 2\,f^2\,d^2 + e^2\,u^2\\
h_2 &= 2\,f^2\,v^2 + 2\,e^2\,u + 2\,e^2\,u\,c^2 + 2\,e^2\,u\,d^2 + 2\,f^2\,d^2 - 4\,f^2\,v\,c - 2\,e^2\,u^2\,c\\
h_3 &= 2\,f^2\,d^2 - 4\,e^2\,u\,c - 2\,f^2\,c^2 + e^2\,c^2 + d^2\,e^2 + 4\,f^2\,v\,c + e^2\\
h_4 &= -2\,f^2\,d^2 - 2\,e^2\,c + 2\,f^2\,c^2\\
h_5 &= -4\,f^2\,v\,d - 2\,e^2\,u^2\,d\\
h_6 &= -4\,e^2\,u\,d - 4\,f^2\,d\,c + 4\,f^2\,v\,d\\
h_7 &= -2\,e^2\,d + 4\,f^2\,d\,c
\end{aligned} \tag{45}$$

By linear independence, $h_1 = \cdots = h_7 = 0$. From $h_7 = 0$ we have either $d = 0$, a contradiction as then $c_3 = c_2$, or $e^2 = 2f^2c$. Substituting into the fourth equation we have $f^2(c^2 + d^2) = 0$, hence $f = 0$, a contradiction.

This completes the proof of lemma B in case I.

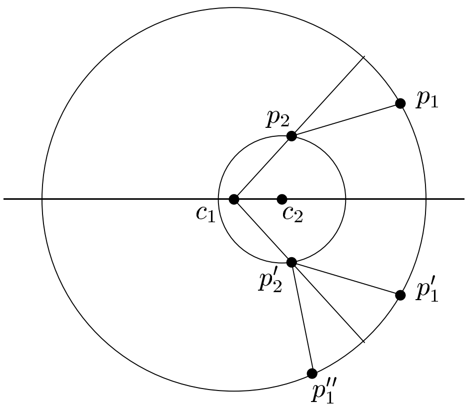
Case II. There is no point (q_1, q_2) in the motion of (p_1, p_2) such that q_1q_2 passes through both c_1 and c_2.

We may assume by case I that there is no double point, and hence no extreme point in the motion of (p_1, p_2). Let p_1', p_2' denote the reflections of p_1, p_2 about the x-axis, where we again assume $c_1 = (0, 0)$ and $c_2 = (a, 0)$. Let α denote the acute angle between p_1p_2 and the ray c_1p_2. See figure 3.

Consider an analytic $p_2(t)$ where $p_2(t)$ moves from p_2 to p_2'. Note that in any motion of (p_1, p_2) to a point (q_1, q_2), q_1q_2 cannot pass through either c_1 or c_2. For if it passed through exactly one of these, (q_1, q_2) would be a (non-trivial) extreme point in the motion of (p_1, p_2). Also, by the assumption of the case, q_1q_2 cannot pass through both centers. This implies that there is a uniquely determined analytic function $p_1(t)$ describing the corresponding motion of p_1. Let $\alpha(t)$ denote the angle between $p_2(t)p_1(t)$ and $c_1p_2(t)$ (so $\alpha(0) = \alpha$). Thus, $\alpha(t) \neq 0$ for all $t \in [0, 1]$. It follows that the terminal value of p_1, namely $p_1(1)$, is not the reflected point p_1', but rather the point p_1'' which is the reflection of p_1' about the line c_1p_2'. Thus, p_1'' is obtained from p_1 by two reflections, first about the x-axis, and then about the line c_1p_2'. Let $p_3(t)$ be the analytic function corresponding to $p_1(t)$, $p_2(t)$. Since the composition of two reflections is orientation preserving, it follows that $p_3(1)$ is obtained from $p_3(0)$ by the same two reflections. In particular, this shows that $p_3(0)$, $p_3(1)$ are equidistant from c_1. Let $l = l(p_1, p_2)$ be the perpendicular bisector of $p_3(0)p_3(1)$. Thus, l passes through $c_1 = (0, 0)$ as well as through c_3.

Consider now another point (q_1, q_2) in the motion of (p_1, p_2), and let $l(q_1, q_2)$ be the corresponding line. If $l(q_1, q_2) \neq l(p_1, p_2)$, then $c_3 = c_1$, a contradiction. Thus, $l(q_1, q_2) = l$ is independent of (q_1, q_2). This can be seen to be impossible. For example, we may argue as follows. By taking a motion of (p_1, p_2), we may assume p_2 is on the x-axis. It follows that l is the line through the origin and p_3. Since the composition of the two reflections described above is just a rotation about the origin, it follows that if we move (p_1, p_2) to any (q_1, q_2), then the angle that c_1q_3 makes with l is the same as q_2c_1 makes with the x-axis. Thus, if we

FIGURE 3



rotate triangle $q_1q_2q_3$ about the origin by this angle, the resulting triangle $q'_1q'_2q'_3$ will be such that q'_2 is on the x-axis, q'_1 is on C_1, and q'_3 is on l. This implies (for sufficiently small non-zero motions) that $(q'_1, q'_2, q'_3) = (p_1, p_2, p_3)$. In other words, (q_1, q_2, q_3) is obtained from (p_1, p_2, p_3) by a rotation about the origin. This shows that $c_2 = c_1 = (0, 0)$, a contradiction.

Case III. There is a point (q_1, q_2) in the motion of (p_1, p_2) such that q_1q_2 passes through both c_1 and c_2.

Again, we may assume that in any analytic motion of (p_1, p_2), there is no extreme point. Thus, as we take an analytic motion of p_1 to the point $q_1 = (1, 0)$, p_2 moves in an analytic manner to a point of intersection q_2 of C_2 with the x-axis. It suffices to show that no analytic motion $(q_1(t), q_2(t))$ of (q_1, q_2) can have the corresponding $q_3(t)$ lying entirely on a circle C_3. In fact, it clearly suffices to show that if $(q_1(t), q_2(t))$ is an analytic motion in which $q_1(t)$ moves at a uniform rate (say, $q_1(t) = (\cos(\pi t), \sin(\pi t))$) to the opposite point $(-1, 0)$, then $q_3(t)$ cannot lie entirely on C_3. The reader can also check that the only case where there is not an obvious extreme point in the motion of (q_1, q_2) occurs when $q_2 = a - r_2$ and $a - r_2 < 0$.

The analytic motion $(q_1(t), q_2(t))$ can be extended to $t < 0$ so that $(q_1(-t), q_2(-t))$ is the reflection of $(q_1(t), q_2(t))$ about the x-axis for $0 \leq t \leq 1$. Thus, for $0 \leq t \leq 1$, $q_1(t)$ moves counter-clockwise from $(1, 0)$ to $(-1, 0)$, and for t from 0 to -1, $q_1(t)$ moves clockwise from $(1, 0)$ to $(-1, 0)$. The two terminal positions of $q_2(t)$, namely, $q_2(1)$ and $q_2(-1)$ lie on C_2 and are reflections of each other about the x-axis. By continuity, for each q'_1 near $(-1, 0)$, there are points q'_2, q''_2 on C_2 with $\rho(q'_1, q'_2) = \rho(q'_1, q''_2) = f$, and such that there is an analytic motion from (q'_1, q'_2) to (q'_1, q''_2) (note that this motion involves moving q'_1 a full revolution around C_1). This shows that $(q_1(1), q_2(1))$ is a double point for $q_1(1)$, contrary to hypothesis.

5. Concluding Remarks and Questions

An immediate consequence of the existence of a Steinhaus set is the existence of an "n-point" Steinhaus set.

Theorem 5.1. *For each integer $n \geq 1$ there is a set $S_n \subseteq \mathbb{R}^2$ such that for every isometric copy L of $\mathbb{Z}^2$ we have $|S_n \cap L| = n$.*

Proof. Let $S_1 = S$ be the Steinhaus set from theorem 1.1. Let $z_1, \ldots, z_n$ be n distinct points in $\mathbb{Z}^2$. Let $S_n = \bigcup_{i=1}^n S + z_i$. Since S is a Steinhaus set, the sets $S + z_i$ are pairwise disjoint. Each lattice L clearly meets each $S + z_i$ in exactly one point, and the result follows. □

There are many problems about Steinhaus sets that remain open. As we mentioned in the introduction, a Steinhaus set $S \subseteq \mathbb{R}^2$ cannot be both bounded and measurable.

Question 1. Can a Steinhaus set $S \subseteq \mathbb{R}^2$ be bounded? Can it be measurable?

It is still unknown whether the analog of a Steinhaus set can exist in dimensions 3 or higher. That is,

Question 2. Does there exist a set $S \subseteq \mathbb{R}^n$ such that $|S \cap L| = 1$ for every isometric copy L of $\mathbb{Z}^n$? More generally, does there exist an $S \subseteq \mathbb{R}^n$ such that $|S \cap L| = 1$ for every copy L of $\mathbb{Z}^m$, where $m \leq n$?

One can also ask for which lattices L_0 (in $\mathbb{R}^2$ or $\mathbb{R}^n$) there is a corresponding Steinhaus set.

Question 3. For which lattices $L_0 \subseteq \mathbb{R}^n$ does there exist a set $S \subseteq \mathbb{R}^n$ such that $|S \cap L| = 1$ for every isometric copy L of L_0?

This question seems to be open even for the sublattice L_0 of $\mathbb{Z}^2$ with basis vectors $(2,0)$, $(0,1)$.

References

[1] J. Beck, On a lattice point problem of H. Steinhaus, Studia Sci. Math. Hung. 24 (1989), 263-268.
[2] H. T. Croft, Three lattice point problems of Steinhaus, Quart. J. Math. Oxford 33 (1982), 71-83.
[3] H. T. Croft, K. J. Falconer, and R. K. Guy, Unsolved Problems in Geometry, Springer-Verlag, New York, 1991.
[4] P. Erdős, P.M. Gruber, and J. Hammer, Lattice points, Longman Sci. Tech., Harlow, 1989.
[5] P. Erdős, Problems and results in combinatorial geometry, Discrete Geometry and Convexity, 44 (1985), New York Academy of Sciences, 1-10.
[6] P. Erdős, S. Jackson and R. D. Mauldin, On partitions of lines and space, Fund. Math. 145 (1994), 101-119.
[7] P. Erdős, S. Jackson and R. D. Mauldin, On infinite partitions of lines and space, Fund. Math. 152 (1997), 75-95.
[8] Gibson, C. G., and Newstead, P. E., On the Geometry of the Planar 4-Bar Mechanism, Acta Applicandae Mathematicae, 7 (1986), 113-135.
[9] S. Jackson and R. D. Mauldin, Sets meeting isometric copies of a lattice in exactly one point, Proceedings National Academy Sciences, submitted.
[10] K. H. Hunt, Kinematic Geometry of Mechanisms, Oxford Engineering Science Series, 7 Oxford Science Publications, The Clarendon Press, Oxford University press, New York, 1990
[11] M. N. Kolountzakis, A problem of Steinhaus: can all placements of a planar set contain exactly one lattice point?, Analytic number theory, Vol. 2 (Allerton Park, IL, 1995), 559-565, Progr. Math., 139, Birkhäuser Boston, Boston, MA, 1996.
[12] M. N. Kolountzakis and T. Wolff, On the Steinhaus tiling problem, Mathematika, 46 (1999), 253-280.
[13] P. Komjáth, A lattice point problem of Steinhaus, Quart. J. Math. Oxford 43 (1992), 235-241.
[14] W. Sierpiński, Sur un problème de H. Steinhaus concernant les ensembles de points sur le plan, Fund. Math. 46 (1958), 191-194.

Abstract. It is shown that there is a subset S of $\mathbb{R}^2$ such that each isometric copy of $\mathbb{Z}^2$ (the lattice points in the plane) meets S in exactly one point. This provides a positive answer to a problem of H. Steinhaus.

Department of Mathematics, University of North Texas, Denton, TX 76203
E-mail address: jackson@unt.edu

Department of Mathematics, University of North Texas, Denton, TX 76203
E-mail address: mauldin@unt.edu