TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 358, Number 8, Pages 3535–3570
S 0002-9947(06)03978-X
Article electronically published on March 1, 2006

NONNEGATIVE SOLVABILITY OF LINEAR EQUATIONS IN CERTAIN ORDERED RINGS

PHILIP SCOWCROFT

ABSTRACT. In the integers and in certain densely ordered rings that are not fields, projections of the solution set of finitely many homogeneous weak linear inequalities may be defined by finitely many congruence inequalities, where a congruence inequality combines a weak inequality with a system of congruences. These results extend well-known facts about systems of weak linear inequalities over ordered fields and imply corresponding analogues of Farkas' Lemma on nonnegative solvability of systems of linear equations.

1. INTRODUCTION

In the fall of 2002 I found a simple model-theoretic proof of Weyl's theorem ([11], p. 4) on convex polyhedral cones and a simple reduction to this result of Farkas' Lemma ([4], p. 5). Though I have since discovered how to eliminate all traces of mathematical logic from the proof, its structure encouraged me to search for contexts, not so easily simplified, in which my original argument might bear fruit. This paper describes the results of that search, which starts from the simplified proof of

Farkas' Lemma. *Let F be an ordered field, A an m-by-n matrix over F, and $b \in F^m$. The following conditions are equivalent:*
(i) *$b = Az$ for some $z \geq 0$ in F^n.*
(ii) *For all $y \in F^m$, if $y^{\mathrm{T}} A \geq 0$, then $y^{\mathrm{T}} b \geq 0$.*

(Here and in what follows, a matrix is nonnegative just in case its entries are nonnegative, and $^{\mathrm{T}}$ stands for transpose.)

The argument from (i) to (ii) is immediate: if $z \geq 0$ and $b = Az$, then $y^{\mathrm{T}} b = y^{\mathrm{T}}(Az) = (y^{\mathrm{T}} A)z \geq 0$.

The argument from (ii) to (i) proceeds with the help of

Proposition 1. *Let $E(y_1, \ldots, y_m, z_1, \ldots, z_n)$ be a finite system of weak homogeneous linear inequalities, in the $m + n$ variables $y_1, \ldots, y_m, z_1, \ldots, z_n$, with coefficients from F. There is a finite system $G(y_1, \ldots, y_m)$ of weak homogeneous linear inequalities, in the m variables $y_1, \ldots, y_m$ and with coefficients from F, such that for all $y \in F^m$*

$$y \text{ obeys } G \text{ just in case there is } z \in F^n \text{ such that } y, z \text{ obey } E.$$

Received by the editors July 19, 2004.
2000 *Mathematics Subject Classification.* Primary 03C64; Secondary 06F20, 15A39.

Apply Proposition 1 to the system $E(y, z) =$

$$y = Az \text{ and } z \geq 0,$$

which one may view as a system of weak homogeneous linear inequalities because an identity is equivalent to a pair of weak inequalities. The resulting finite system $G(y)$ of weak homogeneous linear inequalities may be written in the form

$$Cy \geq 0,$$

where C has as many rows as there are inequalities in G. Assuming (ii), one may establish (i) by showing that

$$Cb \geq 0;$$

i.e., that

$$c^{\mathrm{T}} b \geq 0 \text{ for each row } c^{\mathrm{T}} \text{ of } C.$$

By (ii), this conclusion will hold if

$$c^{\mathrm{T}} A \geq 0 \text{ for each row } c^{\mathrm{T}} \text{ of } C;$$

i.e., if

$$CA \geq 0,$$

or if

$$Ca \geq 0 \text{ for each column } a \text{ of } A.$$

By the choice of C, this conclusion holds just in case for each column a of A,

$$a = Az \text{ for some } z \geq 0.$$

The ith column of A is A times the ith standard basis vector, which is nonnegative; so the argument is complete.

Proposition 1 also has an easy proof. Since the variables z may be eliminated one at a time, one may assume that $n = 1$ and that $z_1 = z$. In each inequality of $E(y, z)$, place the y's on one side and z on the other, and divide both sides by the coefficient of z if this coefficient is nonzero (the sense of the inequality may change). In this way one may view $E(y, z)$ as a system of inequalities

$$t_i(y) \geq 0, u_j(y) \geq z, \text{ and } z \geq v_k(y),$$

where the t's, u's, and v's are linear forms in the y's, and i, j, k range over the finite sets I, J, K, respectively. One may now let $G(y)$ consist of all inequalities

$$t_i(y) \geq 0 \text{ and } u_j(y) \geq v_k(y)$$

for $i \in I$, $j \in J$, and $k \in K$ (where if $J = \emptyset$ or $K = \emptyset$, only inequalities of the first kind appear).

This proof of Proposition 1 exploits "Fourier-Motzkin elimination" ([2], pp. 84–85) and, as used in the proof of Farkas' Lemma, establishes Weyl's theorem ([11], p. 4) that a convex polyhedral cone is a finite intersection of halfspaces. Once Weyl's theorem is available, Farkas' Lemma reduces to the manipulation of linear inequalities written in matrix form. The simplicity of this part of the argument suggests that one apply it to other ordered rings obeying versions of Weyl's theorem, and this paper will follow this strategy to obtain analogues of Farkas' Lemma for many such rings.

The most interesting example is the ring of integers, but certain dense subrings of $\mathbb{R}$ will receive attention first because they fall victim to a simpler version of the argument handling the integers. Since the focus is on linear inequalities, the analogues of Proposition 1 proved below will concern systems of inequalities in ordered groups of special kinds, just as Proposition 1 really deals with systems of inequalities in ordered vector spaces over F. When the ordered groups are not ordered vector spaces, one must pay attention to congruences modulo a given integer, ring element, or finitely generated ideal, and inequalities are replaced by conditions combining inequalities with congruences: congruence inequalities. Proposition 3.1, for example, is a version of Proposition 1 in which F becomes a dense regular group ([9], p. 59), and the inequalities $t \leq u$ are replaced by congruence inequalities $t \leq_k u$ stating that between t and u lies an element divisible by the positive integer k. Similarly, Proposition 4 is a version of Proposition 1 in which F becomes $\mathbb{Z}$ and the inequalities $t \leq u$ are replaced by congruence inequalities stating that between t and u lie elements, partially ordered in a certain way, that together with t and u obey a particular system of congruences. Propositions 3.1 and 4 in turn yield versions of Farkas' Lemma in which the inequalities appearing in (ii) are replaced by congruence inequalities of the appropriate kind.

While the proof of Proposition 1 gives a recipe for building the new system $G(y)$ from the given system $E(y, z)$, the proofs of Propositions 3.1 and 4 provide only nonconstructive arguments for G's existence. Because G appears only in the proof of Farkas' Lemma, these nonconstructive arguments will not obscure the statement of the new results. Yet questions raised by the present results, and mentioned in the Conclusion, might be more easily answered if one knew how to build G from E.

Techniques from mathematical logic help to prove results like Proposition 1 because they concern different ways in which a subset of m-space may be defined. After Section 2 establishes the model-theoretic test permitting proofs of results like Proposition 1, Section 3 applies the test to obtain versions of Farkas' Lemma for dense subrings of $\mathbb{R}$. Section 4 follows a similar strategy to obtain a version for the integers, and Section 5 seeks to strengthen the results of the previous two sections. The techniques from model theory exploited below are all presented in [1].

2. A model-theoretic test

The analogues of Proposition 1 all rest on the following model-theoretic characterization of conjunctions of atomic formulas.

Lemma 2.1. *Let $\mathcal{L}$ be a language with at least one constant symbol, let T be a set of $\mathcal{L}$-sentences, and let $\varphi(x_1, \ldots, x_n)$ be an $\mathcal{L}$-formula, with free variables among those displayed, such that $T \models \exists \overline{x} \varphi(\overline{x})$. The following conditions are equivalent:*

(i) *$\varphi(\overline{x})$ is equivalent, modulo T, to a conjunction of atomic formulas.*

(ii) *Suppose that for all i in the nonempty set I, there is an n-tuple $\overline{a}_i$ from $\mathcal{M}_i \models T$ with $\mathcal{M}_i \models \varphi[\overline{a}_i]$. If $\mathcal{N} \subseteq \prod_{i \in I} \mathcal{M}_i$, $\overline{a} = (\overline{a}_i)_{i \in I}$ belongs to N^n, and $g : \mathcal{N} \to \mathcal{H} \models T$ is a homomorphism, then $\mathcal{H} \models \varphi[g(\overline{a})]$.*

Proof. The model-theoretic condition is clearly necessary. Conversely, assume the condition, and let Γ be the set of atomic $\mathcal{L}$-formulas, with free variables among $x_1, \ldots, x_n$, that are implied by $\varphi(\overline{x})$, modulo T. If $T \cup \Gamma$ implies $\varphi(\overline{x})$, the compactness theorem gives the result desired.

Let Γ' be the set of all atomic $\mathcal{L}$-formulas, with free variables among $x_1, \ldots, x_n$, that do not belong to Γ.

Suppose first that $\Gamma' \neq \emptyset$. If $T \cup \Gamma \not\models \varphi$, there are $\mathcal{H} \models T$ and $\overline{q} \in H^n$ such that

$$\mathcal{H} \models (\Gamma \cup \{\neg\varphi\})[\overline{q}].$$

For each θ in the nonempty set Γ' there are $\mathcal{M}_\theta \models T$ and $\overline{b}_\theta \in M_\theta^n$ with

$$\mathcal{M}_\theta \models (\varphi \ \wedge \ \neg\theta)[\overline{b}_\theta].$$

Let $\mathcal{N} \subseteq \prod_{\theta\in\Gamma'} \mathcal{M}_\theta$ be generated by $\overline{b} = (\overline{b}_\theta)_{\theta\in\Gamma'}$. If $\delta(\overline{x})$ is an atomic $\mathcal{L}$-formula with $\mathcal{N} \models \delta[\overline{b}]$, then $\prod_{\theta\in\Gamma'} \mathcal{M}_\theta \models \delta[\overline{b}]$ because δ is quantifier-free, and $\mathcal{M}_\theta \models \delta[\overline{b}_\theta]$ for every $\theta \in \Gamma'$ because δ is atomic. Thus $\delta \neq \theta$ for all $\theta \in \Gamma'$, $\delta \in \Gamma$, and $\mathcal{H} \models \delta[\overline{q}]$ whenever $\mathcal{N} \models \delta[\overline{b}]$. So there is a homomorphism $g : \mathcal{N} \to \mathcal{H}$ that sends $\overline{b}$ to $\overline{q}$. Because $\mathcal{H} \not\models \varphi[\overline{q}]$, this conclusion violates the model-theoretic condition; so $T \cup \Gamma \models \varphi$ if $\Gamma' \neq \emptyset$.

If $\Gamma' = \emptyset$, then $T \cup \{\varphi\}$ implies every atomic $\mathcal{L}$-formula with free variables among $x_1, \ldots, x_n$. If d is a constant symbol of $\mathcal{L}$, then

$$T \models \varphi(\overline{x}) \to \bigwedge_{i=1}^{n} x_i = d.$$

Because $T \models \exists\overline{x}\varphi(\overline{x})$, $T \models \varphi(\overline{d})$ as well and

$$T \models \bigwedge_{i=1}^{n} x_i = d \to \varphi(\overline{x}).$$

Thus $\varphi(\overline{x})$ is equivalent, modulo T, to $\bigwedge_{i=1}^{n} x_i = d$. □

Note that if $n = 0$, one may replace $\bigwedge_{i=1}^{n} x_i = d$ by $d = d$ in the last part of the argument. One needs some hypothesis like "$T \models \exists\overline{x}\varphi(\overline{x})$" because any formula $\varphi(\overline{x})$ inconsistent with T will obey the model-theoretic condition of the lemma.

It is inspired by van den Dries' test for formulas that are equivalent, modulo T, to positive, quantifier-free formulas ([3]). Though he is not trying to find formulas of the kind considered here, van den Dries can obtain such a formula in one of his examples because it concerns a theory of integral domains, in which a disjunction of identities is equivalent to an identity.

3. Dense regular groups

A first generalization of Proposition 1 handles systems of weak inequalities in dense regular groups ([9], p. 59). In the language $\mathcal{L} = \{+, -, \leq, 0\}$ appropriate for ordered Abelian groups, one may build a set T of universal-existential axioms for dense regular groups. Expand $\mathcal{L}$ to $\mathcal{L}'$ by adding, for each integer $k \geq 2$, a binary relation symbol $\leq_k$, and expand T to T' by adding the new axioms

$$\forall x, y(x \leq_k y \leftrightarrow \exists z(x \leq kz \leq y))$$

for all $k \geq 2$. Call any atomic $\mathcal{L}'$-formula

$$t \leq_k u$$

a congruence inequality of modulus k.[1] Modulo T', $x = y$ is equivalent to $x \leq y \ \wedge \ y \leq x$, and $x \leq y$ is equivalent to $kx \leq_k ky$; so every atomic $\mathcal{L}'$-formula is equivalent modulo T' to a conjunction of congruence inequalities. When $k, l \geq 2$,

[1] Conditions like these, but with strict inequalities and 0 at the left, figure in ([8], p. 138).

$x \leq_k y$ is equivalent modulo T' to $lx \leq_{kl} ly$; so any conjunction of atomic $\mathcal{L}'$-formulas is equivalent modulo T' to a conjunction of congruence inequalities, all with the same modulus. One may now state

Proposition 3.1. *Modulo T', every existential quantification of a conjunction of atomic formulas is equivalent to a conjunction of congruence inequalities.*

So in a dense regular group, any projection of the solution set of finitely many weak inequalities may be defined by a finite system of congruence inequalities, all with the same modulus.

Proof. Let $\varphi(\overline{x}, \overline{y})$ be a conjunction of congruence inequalities in the variables $\overline{x} = (x_1, \ldots, x_m)$ and $\overline{y} = (y_1, \ldots, y_n)$. Because $T' \models \exists \overline{y} \varphi(\overline{0}, \overline{y})$, one may invoke Lemma 2.1 to show that $\exists \overline{y} \varphi(\overline{x}, \overline{y})$ is equivalent modulo T' to a conjunction of atomic formulas and so to a conjunction of congruence inequalities. Suppose, therefore, that for all $i \in I$ ($\neq \emptyset$), $\mathcal{M}_i \models T'$, $\overline{a}_i \in M_i^m$, $\mathcal{M}_i \models \exists \overline{y} \varphi[\overline{a}_i]$, $\mathcal{N} \subseteq \prod_{i \in I} \mathcal{M}_i$, $\overline{a} = (\overline{a}_i)_{i \in I} \in N^m$, and $f : \mathcal{N} \to \mathcal{H} \models T'$; the goal is to show that $\mathcal{H} \models \exists \overline{y} \varphi[f(\overline{a})]$. Without loss of generality $N \neq \{0\}$ and $\mathcal{H}$ is $|\mathcal{M}|^+$-saturated. Since $\varphi(\overline{x}, \overline{y})$ is a conjunction of atomic formulas, the desired result holds if f extends to a homomorphism of $\mathcal{M}$ into $\mathcal{H}$. By Zorn's lemma there is a pair $(\mathcal{N}', g)$, with $\mathcal{N} \subseteq \mathcal{N}' \subseteq \mathcal{M}$, $g : \mathcal{N}' \to \mathcal{H}$, and $f \subseteq g$, maximal with respect to inclusion (in both coordinates), and one wants to show that $\mathcal{N}' = \mathcal{M}$.

If $c \in M$ and $rc \in N'$ for some positive integer r, then for every $d \in N' + \mathbb{Z}c$, $rd \in N'$ and

$$rd \leq_r rd.$$

So

$$g(rd) \leq_r g(rd)$$

in $\mathcal{H} \models T'$, and there is a unique $e \in H$ with

$$re = g(rd).$$

One may therefore define $h : N' + \mathbb{Z}c \to H$ by

$$h(d) = e.$$

If $d \in N'$, then

$$re = g(rd) = rg(d)$$

and $h(d) = e = g(d)$; so h extends g. If $h(d_1) = e_1$ and $h(d_2) = e_2$, then

$$re_i = g(rd_i)$$

for $i = 1, 2$, and

$$r(e_1 \pm e_2) = g(rd_1 \pm rd_2) = g(r(d_1 \pm d_2));$$

so

$$h(d_1 \pm d_2) = h(d_1) \pm h(d_2).$$

If $d_1 \leq_k d_2$ ($d_1 \leq d_2$), then $rd_1 \leq_{rk} rd_2$ ($rd_1 \leq rd_2$),

$$re_1 = g(rd_1) \leq_{rk} g(rd_2) = re_2$$

($re_1 = g(rd_1) \leq g(rd_2) = re_2$), and $e_1 \leq_k e_2$ ($e_1 \leq e_2$). Thus h is a homomorphism, extending g, of the substructure of $\mathcal{M}$ with domain $N' + \mathbb{Z}c$ into $\mathcal{H}$, and $c \in N'$ by the maximality of $(\mathcal{N}', g)$. So if $c \in M - N'$, then $rc \notin N'$ for all $r > 0$ (and so for all $r \neq 0$).

Suppose now that $c \in M - N'$ and there are $a \leq b$ in N' with $a \leq c \leq b$ and $g(a) = g(b)$. The result of the last paragraph implies that every element of $N' + \mathbb{Z}c$ has a unique representation

$$n + rc$$

with $n \in N'$ and $r \in \mathbb{Z}$. One may therefore define $h : N' + \mathbb{Z}c \to H$ by

$$h(n + rc) = g(n) + rg(a) = g(n) + rg(b).$$

Clearly h is a group homomorphism extending g. If

$$n_1 + r_1 c \leq_k n_2 + r_2 c$$

with each $n_i \in N'$ and each $r_i \in \mathbb{Z}$, let

$$c_1 = \begin{cases} a & \text{if } r_1 \geq 0, \\ b & \text{if } r_1 < 0, \end{cases} \quad \text{and } c_2 = \begin{cases} b & \text{if } r_2 \geq 0, \\ a & \text{if } r_2 < 0. \end{cases}$$

Then $c_i \in \{a, b\}$ for $i = 1, 2$, and

$$n_1 + r_1 c_1 \leq n_1 + r_1 c \leq_k n_2 + r_2 c \leq n_2 + r_2 c_2.$$

Because T' implies the Horn sentence

$$\forall x, y, z, w (x \leq y \ \wedge \ y \leq_k z \ \wedge \ z \leq w \to x \leq_k w),$$

it holds in every product of models of T', and so in $\mathcal{M}$. Thus

$$n_1 + r_1 c_1 \leq_k n_2 + r_2 c_2$$

in $\mathcal{M}$ and in $\mathcal{N}' \subseteq \mathcal{M}$, and

$$g(n_1 + r_1 c_1) \leq_k g(n_2 + r_2 c_2).$$

Yet since each

$$g(n_i + r_i c_i) = g(n_i) + r_i g(c_i) = g(n_i) + r_i g(a) = h(n_i + r_i c),$$

h preserves congruence inequalities, and a similar argument shows that h preserves inequalities. So h is a homomorphism into $\mathcal{N}$, extending g, of the substructure of $\mathcal{M}$ with domain $N' + \mathbb{Z}c$, and $(\mathcal{N}', g)$ is not maximal. This contradiction implies that if $c \in M - N'$, $a \leq b$ in $\mathcal{N}'$, and $a \leq c \leq b$, then $g(a) \neq g(b)$, and thus $g(a) < g(b)$. Equivalently, if $a \leq b$ in $\mathcal{N}'$ and $g(a) = g(b)$, then N' contains the interval $[a, b]$ of $\mathcal{M}$.

Now let $c \in M$. If there is $d \in H$ realizing the images under g of all atomic formulas, with parameters from N', realized by c in $\mathcal{M}$, then g extends to a homomorphism into $\mathcal{H}$ of the substructure of $\mathcal{M}$ with domain $\mathcal{N}' + \mathbb{Z}c$, and $c \in N'$ by the maximality of $(\mathcal{N}', g)$. Because $\mathcal{H}$ is $|\mathcal{M}|^+$-saturated, one need show merely that for any finite collection of atomic formulas, with parameters from N', realized by c in $\mathcal{M}$, there is $d \in H$ realizing the images under g of these formulas. Without loss of generality the formulas realized by c are congruence inequalities, say

$$a_j + r_j x \leq_{k_j} b_j + s_j x,$$

where j belongs to the finite index set J, the a's and b's belong to N', and the r's and s's are integers. One aims to find $d \in H$ with

$$g(a_j) + r_j d \leq_{k_j} g(b_j) + s_j d$$

for all $j \in J$.

Let

$$\begin{aligned} K &= \{i \in J : g(a_i) < g(b_i) \text{ or } r_i \neq s_i\}, \\ L &= J - K = \{i \in J : g(a_i) \geq g(b_i) \text{ and } r_i = s_i\}. \end{aligned}$$

Lemma 3.2. *There are $p < q$ in H for which*

$$g(a_i) + r_i d < g(b_i) + s_i d$$

whenever $p < d < q$ and $i \in K$.

Note that since $\mathcal{H}$ is dense regular, Lemma 3.2 implies that

$$g(a_i) + r_i d \leq_{k_i} g(b_i) + s_i d$$

whenever $p < d < q$ and $i \in K$.

Proof. Let $K = K_- \cup K_= \cup K_+$, where

$$\begin{aligned} K_- &= \{i \in K : r_i < s_i\}, \\ K_= &= \{i \in K : r_i = s_i\}, \\ K_+ &= \{i \in K : r_i > s_i\}. \end{aligned}$$

Then for $i \in K_=$,

$$g(a_i) < g(b_i) \text{ and } r_i = s_i,$$

for $i \in K_-$,

$$a_i - b_i \leq (s_i - r_i)c \text{ and } s_i - r_i > 0,$$

and for $i \in K_+$,

$$(r_i - s_i)c \leq b_i - a_i \text{ and } r_i - s_i > 0.$$

If $K_+ = \emptyset$, one may let

$$p = \max(\{g(a_i - b_i) : \ i \in K_-\} \cup \{0\})$$

and q be any element of H bigger than p. If $K_- = \emptyset$, one may let

$$q = \min(\{g(b_i - a_i) : \ i \in K_+\} \cup \{0\})$$

and p be any element of H less than q. Assume, therefore, that $K_\pm \neq \emptyset$, and let

$$P = \prod_{i \in K_- \cup K_+} |r_i - s_i|$$

and

$$P_i = P/|r_i - s_i| \text{ for } i \in K_- \cup K_+.$$

Then for $i \in K_-$

$$P_i(a_i - b_i) \leq Pc,$$

and for $j \in K_+$

$$Pc \leq P_j(b_j - a_j).$$

Since one may as well suppose that $c \notin N'$, $Pc \notin N'$, and by an earlier result

$$g(P_i(a_i - b_i)) < g(P_j(b_j - a_j))$$

when $i \in K_-$ and $j \in K_+$. Since $\mathcal{H}$ is dense regular, there are $p < q$ in H with

$$g(P_i(a_i - b_i)) < Pp < Pq < g(P_j(b_j - a_j))$$

whenever $i \in K_-$ and $j \in K_+$. So when $i \in K_-$, $j \in K_+$, and $p < d < q$,

$$g(P_i(a_i - b_i)) < Pd < g(P_j(b_j - a_j)),$$
$$P_i(g(a_i) - g(b_i)) < Pd < P_j(g(b_j) - g(a_j)),$$
$$g(a_i) - g(b_i) < (s_i - r_i)d \text{ and } (r_j - s_j)d < g(b_j) - g(a_j),$$

and

$$g(a_i) + r_i d < g(b_i) + s_i d \text{ and } g(a_j) + r_j d < g(b_j) + s_j d.$$

For $i \in K_=$,

$$g(a_i) + r_i d < g(b_i) + r_i d = g(b_i) + s_i d$$

for any d in H; so the argument is complete. □

When t and u are $\mathcal{L}'$-terms, let

$$t \equiv_k u \text{ abbreviate } t - u \leq_k t - u.$$

In an ordered group, $t \equiv_k u$ just in case t is congruent to u modulo k. Call any formula $t \equiv_k u$ a congruence with modulus k.

Lemma 3.3. *If $r_1, \dots, r_l$ are nonzero integers, then*

$$\exists z(\bigwedge_{i=1}^{l} x_i + r_i z \leq_{k_i} y_i + r_i z)$$

is equivalent modulo T' to

$$\exists u_1 \dots \exists u_l(\bigwedge_{i=1}^{l} x_i \leq u_i \leq y_i \ \wedge \ H(\overline{u})),$$

where $H(\overline{u})$ is a conjunction of congruences in the variables $\overline{u} = (u_1, \dots, u_l)$.

Proof. Modulo T', the given formula is equivalent to

$$\exists z \exists v_1 \dots \exists v_l(\bigwedge_{i=1}^{l} x_i + r_i z \leq k_i v_i \leq y_i + r_i z),$$

to

$$\exists z \exists v_1 \dots \exists v_l(\bigwedge_{i=1}^{l} x_i \leq k_i v_i - r_i z \leq y_i),$$

to

$$\exists z \exists u_1 \dots \exists u_l(\bigwedge_{i=1}^{l} x_i \leq u_i \leq y_i \ \wedge \ r_i z + u_i \equiv_{k_i} 0),$$

and to

$$\exists u_1 \dots \exists u_l(\bigwedge_{i=1}^{l} x_i \leq u_i \leq y_i \ \wedge \ \exists z(\bigwedge_{j=1}^{l} r_j z + u_j \equiv_{k_j} 0)).$$

The formula

$$\exists z(\bigwedge_{j=1}^{l} r_j z + u_j \equiv_{k_j} 0)$$

is equivalent modulo T' to

$$\exists z(\bigwedge_{r_j > 0} u_j \equiv_{k_j} |r_j|(-z) \ \wedge \ \bigwedge_{r_j < 0} -u_j \equiv_{k_j} |r_j|(-z)).$$

So if $R = \prod_{j=1}^{l} |r_j|$ and $R_j = R/|r_j|$ for each j, then this last formula is equivalent modulo T' to

$$\exists z(\bigwedge_{r_j>0} R_j u_j \equiv_{R_j k_j} R(-z) \ \wedge \ \bigwedge_{r_j<0} -R_j u_j \equiv_{R_j k_j} R(-z))$$

and to

$$\exists w(\bigwedge_{r_j>0} R_j u_j \equiv_{R_j k_j} w \ \wedge \ \bigwedge_{r_j<0} -R_j u_j \equiv_{R_j k_j} w \ \wedge \ w \equiv_R 0)$$

(where the last conjunct may be omitted if $R = 1$). The Chinese Remainder Theorem ([5], pp. 292–293) makes this last formula equivalent modulo T' to $(*) =$

$$\begin{array}{ll} \bigwedge_j & R_j u_j \equiv_{(R_j k_j, R)} 0 \\ \wedge \ \bigwedge_{r_j r_m>0} & R_j u_j \equiv_{(R_j k_j, R_m k_m)} R_m u_m \\ \wedge \ \bigwedge_{r_j r_m<0} & R_j u_j \equiv_{(R_j k_j, R_m k_m)} -R_m u_m \end{array}$$

(where one may drop any congruence with modulus 1). Thus the original formula is equivalent modulo T' to

$$\exists u_1 \ldots \exists u_l(\bigwedge_{i=1}^{l} x_i \leq u_i \leq y_i \ \wedge \ (*)).$$

$\square$

One may now establish

Lemma 3.4. *There is $d \in H$ realizing all formulas*

$$g(a_i) + r_i x \leq_{k_i} g(b_i) + s_i x$$

with $i \in L$.

Proof. When $i \in L$, $g(a_i) \geq g(b_i)$ and $r_i = s_i$; so since $a_i + r_i c \leq_{k_i} b_i + s_i c$, $a_i \leq b_i$ as well, and thus $g(a_i) \leq g(b_i)$ and $g(a_i) = g(b_i)$. Without loss of generality $r_i \neq 0$ for all $i \in L$. Apply Lemma 3.3 to the formula

$$\exists z(\bigwedge_{i \in L} x_i + r_i z \leq_{k_i} y_i + r_i z)$$

to obtain the formula $(\#) =$

$$\exists (u_i)_{i \in L}(\bigwedge_{i \in L} x_i \leq u_i \leq y_i \ \wedge \ H(\overline{u})).$$

Because $\mathcal{M}$ is a direct product of models of T' there are, for $i \in L$, elements $c_i \in M$ with

$$\bigwedge_{i \in L} a_i \leq c_i \leq b_i \ \wedge \ H(\overline{c})$$

in $\mathcal{M}$. Because each $g(a_i) = g(b_i)$, an earlier result implies that each $c_i \in N'$; so since the homomorphism g must preserve congruences,

$$\bigwedge_{i \in L} g(a_i) \leq g(c_i) \leq g(b_i) \ \wedge \ H(g(\overline{c}))$$

in $\mathcal{H}$. So by the choice of $(\#)$ one reaches the desired conclusion. $\square$

One may now finish the proof of Proposition 3.1. If P is $\prod_{i\in L} k_i$, then any $d' \in H$ congruent to d modulo P will also satisfy the formulas of Lemma 3.4. So since $\mathcal{H}$ is dense regular, the interval (p, q) from Lemma 3.2 contains a d' congruent to d modulo P, and d' satisfies

$$g(a_i) + r_i x \leq_{k_i} g(b_i) + s_i x$$

for all $i \in J$. □

Corollary 3.5. *Let D be a dense subring of $\mathbb{R}$ and A an m-by-n matrix over $\mathbb{Z}$. There is an integer $k \geq 2$ such that the following conditions are equivalent for any $b \in D^m$:*

(i) *$b = Az$ for some $z \geq 0$ in D^n.*

(ii) *For all $y, w \in D^m$, if $y^{\mathrm{T}}A \geq_k w^{\mathrm{T}}A$, then $y^{\mathrm{T}}b \geq_k w^{\mathrm{T}}b$.*

Here matrices are related by $\geq_k$ just in case all corresponding entries are so related. Note that (ii) is stronger than the condition

$$\text{for all } y \in D^m, \text{ if } y^{\mathrm{T}}A \geq_k 0, \text{ then } y^{\mathrm{T}}b \geq_k 0$$

because congruence inequalities of modulus k are preserved, not under arbitrary translations, but only under translations by elements divisible by k.

Proof. (i) implies (ii) for every $k \geq 2$ because congruence inequalities are preserved under multiplication by nonnegative elements of D and may be added. If $z \geq 0$, $b = Az$, and $y^{\mathrm{T}}A \geq_k w^{\mathrm{T}}A$, then for all i, the ith entry $(y^{\mathrm{T}}A)_i$ of $y^{\mathrm{T}}A$ bears $\geq_k$ to the ith entry $(w^{\mathrm{T}}A)_i$ of $w^{\mathrm{T}}A$, and so each

$$(y^{\mathrm{T}}A)_i z_i \geq_k (w^{\mathrm{T}}A)_i z_i$$

and

$$\sum_{i=1}^{n} (y^{\mathrm{T}}A)_i z_i \geq_k \sum_{i=1}^{n} (w^{\mathrm{T}}A)_i z_i;$$

the left-hand side is $(y^{\mathrm{T}}A)z = y^{\mathrm{T}}(Az) = y^{\mathrm{T}}b$, and the right-hand side is $(w^{\mathrm{T}}A)z = w^{\mathrm{T}}b$.

To obtain a $k \geq 2$ for which (ii) implies (i), view D as an ordered Abelian group with respect to addition. D will then be a model of T', and one may apply Proposition 3.1 and the introductory remarks on congruence inequalities to the $\mathcal{L}'$-formula $(*)$ =

$$\exists z_1 \ldots \exists z_n \Big(\bigwedge_{j=1}^{n} z_j \geq 0 \ \wedge \ \bigwedge_{i=1}^{m} x_i = \sum_{j=1}^{n} a_{ij} z_j\Big),$$

where a_{ij} is the ij-entry of A. So there are $k \geq 2$ and vectors $c_i, d_i \in \mathbb{Z}^m$, for $1 \leq i \leq q$, making $(*)$ equivalent to

$$\bigwedge_{i=1}^{q} c_i^{\mathrm{T}} x \geq_k d_i^{\mathrm{T}} x$$

in D. Now assume that $b \in D^m$ obeys (ii). b will obey (i) just in case

$$\bigwedge_{i=1}^{q} c_i^{\mathrm{T}} b \geq_k d_i^{\mathrm{T}} b.$$

With the help of (ii), one sees that this condition holds if

$$\bigwedge_{i=1}^{q} c_i^{\mathrm{T}} A \geq_k d_i^{\mathrm{T}} A;$$

i.e., just in case each column a of A obeys (i). But since the lth column of A is A times the lth standard basis vector, which is nonnegative, the argument is complete. $\square$

The congruence inequalities in (ii) cannot in general be replaced by congruences and inequalities separately; i.e., (ii) is in general not equivalent to

$$\begin{aligned}&\text{for all } y, w \in D^m, \text{ if } y^{\mathrm{T}} A \equiv_k w^{\mathrm{T}} A, \text{ then } y^{\mathrm{T}} b \equiv_k w^{\mathrm{T}} b,\\ &\qquad\qquad\text{and if } y^{\mathrm{T}} A \geq w^{\mathrm{T}} A, \text{ then } y^{\mathrm{T}} b \geq w^{\mathrm{T}} b\end{aligned}$$

or to the equivalent

$$\begin{aligned}&\text{for all } y \in D^m, \text{ if } y^{\mathrm{T}} A \equiv_k 0, \text{ then } y^{\mathrm{T}} b \equiv_k 0,\\ &\qquad\qquad\text{and if } y^{\mathrm{T}} A \geq 0, \text{ then } y^{\mathrm{T}} b \geq 0.\end{aligned}$$

For an example, consider the condition

$$x \leq_2 y,$$

which is equivalent in D to

$$\exists rstu \geq 0 \left(\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 & -2 & -1 & 0 \\ 2 & -2 & 0 & 1 \end{pmatrix} \begin{pmatrix} r \\ s \\ t \\ u \end{pmatrix} \right).$$

Every condition

$$\forall vw \left(\begin{pmatrix} v & w \end{pmatrix} \begin{pmatrix} 2 & -2 & -1 & 0 \\ 2 & -2 & 0 & 1 \end{pmatrix} \equiv_k 0 \rightarrow \begin{pmatrix} v & w \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \equiv_k 0 \right)$$

is trivially satisfied in D, while the condition

$$\forall vw \left(\begin{pmatrix} v & w \end{pmatrix} \begin{pmatrix} 2 & -2 & -1 & 0 \\ 2 & -2 & 0 & 1 \end{pmatrix} \geq 0 \rightarrow \begin{pmatrix} v & w \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \geq 0 \right)$$

is equivalent in D to $x \leq y$. Yet $x \leq y$ and $x \leq_2 y$ are not equivalent in D unless every element of D is divisible by two.

A defect in Corollary 3.5 is that A's entries are integers, rather than arbitrary elements of D. One may relax this restriction if D is a subring of $\mathbb{Q}$, since the condition

$$b = Az \text{ for some } z \geq 0$$

is equivalent, for any positive integer N, to

$$Nb = (NA)z \text{ for some } z \geq 0,$$

and for suitable N, NA has integer entries which may be represented in $\mathcal{L}$-formulas. More generally, one may carry out a version of the earlier argument in any dense subring of the reals that obeys the Chinese Remainder Theorem; i.e., in any dense subring of the reals that is a Prüfer domain (see [5], pp. 292–293, 296).[2] Because such rings need not be principal ideal domains, an expansion of the class of congruence inequalities seems necessary. If D is a Prüfer domain that is dense in $\mathbb{R}$, let $\mathcal{L}^I$ be the expansion of $\mathcal{L}$ by binary relation symbols $\leq_{k_1,\ldots,k_l}$—where l is a positive integer and $k_1, \ldots, k_l \in D - \{0\}$—and unary function symbols $k\cdot$ for each $k \in D$. Expand T to T^I by adjoining axioms for unital torsion-free ordered D-modules and, for $k_1, \ldots, k_l \in D - \{0\}$, axioms

$$\forall x, y \left(x \leq_{k_1,\ldots,k_l} y \leftrightarrow \exists z_1 \ldots \exists z_l \left(x \leq \sum_{i=1}^{l} k_i \cdot z_i \leq y \right) \right)$$

and

$$\forall x, y\, (x < y \to x \leq_{k_1,\ldots,k_l} y)\,.$$

So $x \leq_{k_1,\ldots,k_l} y$ says that an element of the ideal $(k_1, \ldots, k_l)$ of D lies between x and y, and one easily verifies that D, viewed as an ordered D-module, satisfies T^I. Any formula

$$t \leq_{k_1,\ldots,k_l} u$$

is called a congruence inequality modulo $k_1, \ldots, k_l$, and any formula

$$t - u \leq_{k_1,\ldots,k_l} t - u$$

is called a congruence modulo $k_1, \ldots, k_l$, and may be written

$$t \equiv_{k_1,\ldots,k_l} u.$$

If $\varphi(\overline{x}, y)$ is a conjunction of congruences in the variables $\overline{x} = (x_1, \ldots, x_m)$ and y, then one may use the Chinese Remainder Theorem to show that $\exists y \varphi(\overline{x}, y)$ is equivalent over D to a conjunction $\psi(\overline{x})$ of congruences in the variables $\overline{x}$. Expand T^I to T^C by adding all sentences

$$\forall \overline{x} (\exists y \varphi(\overline{x}, y) \leftrightarrow \psi(\overline{x}))$$

obtained in this way. By making slight changes in the proof of Proposition 3.1 one may establish

Proposition 3.6. *Modulo T^C, every existential quantification of a conjunction of atomic formulas is equivalent to a conjunction of congruence inequalities.*

So in a dense subring of the reals that is a Prüfer domain, any projection of the solution set of finitely many weak linear inequalities may be defined by a finite system of congruence inequalities of the new kind. A familiar argument now yields

Corollary 3.7. *Let D be a Prüfer domain dense in $\mathbb{R}$. If A is an m-by-n matrix over D, there are $k_{ij} \in D - \{0\}$ $(1 \leq i \leq q,\ 1 \leq j \leq l_i)$ such that for all $b \in D^m$, the following conditions are equivalent:*

(i) *$b = Az$ for some $z \geq 0$ in D^n.*

(ii) *For all $y, z \in D^m$, if $y^{\mathrm{T}} A \geq_{k_{i1},\ldots,k_{il_i}} w^{\mathrm{T}} A$, then $y^{\mathrm{T}} b \geq_{k_{i1},\ldots,k_{il_i}} w^{\mathrm{T}} b$ (for all i, $1 \leq i \leq q$).*

---

[2]The Chinese Remainder Theorem allows one to show that an existential quantification of a conjunction of congruences is equivalent to a conjunction of congruences that has a special form. The present argument still works if an existential quantification of a conjunction of congruences is equivalent to some conjunction of congruences, whether or not this new system has the special form provided by the Chinese Remainder Theorem. I do not know whether this weaker condition on congruences allows one to handle dense subrings of $\mathbb{R}$ that are not Prüfer domains.

As usual, (i) implies (ii) for any $\geq_{k_1,\ldots,k_l}$, and not just the $\geq_{k_{i1},\ldots,k_{il_i}}$'s with $1 \leq i \leq q$.

4. The integers

To obtain results for the integers analogous to the results of the last section, one again exploits Lemma 2.1 to show that $A\mathbb{N}^n$ may be defined by a conjunction of formulas combining inequalities with congruences. But the congruence inequalities used here are more complex, and their manipulation is more difficult, because the division of labor represented by Lemmas 3.2 and 3.4 no longer exists. Nonempty open intervals in $\mathbb{Z}$ may be finite, and not contain solutions to systems of congruences solvable elsewhere in $\mathbb{Z}$; so even if one obtains partial solutions, as in Lemmas 3.2 and 3.4, one may not be able to combine them to obtain a complete solution.

Let $\mathcal{L} = \{+, -, \leq, 0\}$ be as in Section 3 and let $T_{\mathbb{Z}}$ be the $\mathcal{L}$-theory of $\mathbb{Z}$-groups ([9], pp. 54–55). This theory is usually formulated in a language featuring a constant symbol for the least positive element, but by doing without such a constant symbol one obtains atomic formulas that are homogeneous. Let $\mathcal{L}_{\text{con}}$ be the expansion of $\mathcal{L}$ by binary relation symbols $\equiv_k$ for integers $k \geq 2$, and let T_{con} be the expansion of $T_{\mathbb{Z}}$ by axioms

$$\forall x, y(x \equiv_k y \leftrightarrow \exists z(x = y + kz))$$

for all $k \geq 2$. An atomic formula

$$t \equiv_k u$$

is called a congruence of modulus k. Whenever $\overline{x}=(x_1, \ldots, x_m)$ and $\overline{y}=(y_1, \ldots, y_n)$ are disjoint lists of distinct variables, and $D(\overline{x})$ and $H(\overline{x};\overline{y})$ are $\mathcal{L}_{\text{con}}$-formulas, described below, with free variables among those shown, add a corresponding $n+2$–place relation symbol $\leq^{D,H}$ to $\mathcal{L}_{\text{con}}$, and let $\mathcal{L}_{\text{in}}$ be the resulting language. $D(\overline{x})$ will always be a conjunction, possibly empty, of inequalities $x_i \leq x_j$, with the property that the directed graph

$$\{(i,j) : x_i \leq x_j \text{ is a conjunct of } D\}$$

contains no cycles. This condition ensures that in $T_{\mathbb{Z}}$, $D(\overline{x})$ does not imply $x_i = x_j$ unless $i = j$. $H(\overline{x};\overline{y})$ will be a conjunction, possibly empty, of congruences. And T_{in} will be the expansion of T_{con} by axioms

$$\forall u, v, \overline{y}(u \leq_{\overline{y}}^{D,H} v \leftrightarrow \exists \overline{x}(u \leq \overline{x} \leq v \ \wedge \ D(\overline{x}) \ \wedge \ H(\overline{x};\overline{y})))$$

for all D, H as above ($u \leq \overline{x} \leq v$ abbreviates $\bigwedge_{i=1}^m u \leq x_i \leq v$, and the semicolon in $H(\overline{x};\overline{y})$ separates the variables $\overline{x}$ to which $\exists$ is applied from the variables $\overline{y}$ that appear as arguments in $u \leq_{\overline{y}}^{D,H} v$). If $\leq^{D,H}$ belongs to $\mathcal{L}_{\text{in}} - \mathcal{L}_{\text{con}}$, call (D, H) a basic pair, and call an atomic formula

$$r \leq_{\overline{t}}^{D,H} s$$

a congruence inequality between r and s with parameters $\overline{t}$.[3] The principal result of this section is the following.

[3]Conditions like these, but with strict inequalities, 0 at the left, and more than one possible right-hand side to the inequalities, appear in ([10], p. 238).

Proposition 4.1. [4] *Modulo T_{in}, every existential quantification of a conjunction of atomic formulas is equivalent to a conjunction of congruence inequalities.*

So in the integers, any projection of the solution set of finitely many weak linear inequalities may be defined by a finite system of congruence inequalities.

Before giving the long proof of this result one may apply it to obtain a version of Farkas' Lemma, and the application becomes easier to understand if preceded by a brief discussion of congruence inequalities. If one applies Proposition 4 to a formula $\exists\overline{z}\varphi(\overline{w},\overline{z})$ to obtain a formula $\psi(\overline{w})$, where $\overline{w}$ consists of p distinct variables $w_1,\dots,w_p$, then the conjuncts of $\psi(\overline{w})$ are congruence inequalities

$$r^{\mathrm{T}}\overline{w} \leq^{D,H}_{M\overline{w}} s^{\mathrm{T}}\overline{w} \tag{1}$$

in which $r, s \in \mathbb{Z}^p$ and M is an n-by-p matrix over $\mathbb{Z}$ ($\overline{w}$ is viewed as a column). (1) is equivalent modulo T_{in} to

$$\exists\overline{x}(r^{\mathrm{T}}\overline{w} \leq \overline{x} \leq s^{\mathrm{T}}\overline{w} \ \wedge\ D(\overline{x}) \ \wedge\ H(\overline{x}; M\overline{w})).$$

If one lets $K(\overline{x};\overline{w})$ be $H(\overline{x}; M\overline{w})$, then (1) is equivalent modulo T_{in} to

$$r^{\mathrm{T}}\overline{w} \leq^{D,K}_{\overline{w}} s^{\mathrm{T}}\overline{w}, \tag{2}$$

where the arguments are linear forms in the (distinct) parameters $\overline{w}$; one may write

$$r^{\mathrm{T}}\overline{w} \leq^{D,K} s^{\mathrm{T}}\overline{w} \tag{3}$$

for (2).

Congruence inequalities (3) may be added as follows: if $r^{\mathrm{T}}\overline{w}_1 \leq^{D,K} s^{\mathrm{T}}\overline{w}_1$ and $r^{\mathrm{T}}\overline{w}_2 \leq^{D,K} s^{\mathrm{T}}\overline{w}_2$, then $r^{\mathrm{T}}(\overline{w}_1+\overline{w}_2) \leq^{D,K} s^{\mathrm{T}}(\overline{w}_1+\overline{w}_2)$. Also, $\overline{0}$ obeys any congruence inequality (3). So if $r^{\mathrm{T}}\overline{w} \leq^{D,K} s^{\mathrm{T}}\overline{w}$ and n is a natural number, then $r^{\mathrm{T}}(n\overline{w}) \leq^{D,K} s^{\mathrm{T}}(n\overline{w})$. Finally, (3) is equivalent modulo T_{in} to

$$0 \leq^{D,L} (s-r)^{\mathrm{T}}\overline{w},$$

where $L(\overline{x};\overline{w})$ is

$$K(x_1 + r^{\mathrm{T}}\overline{w}, \dots, x_m + r^{\mathrm{T}}\overline{w}; \overline{w}).$$

A congruence inequality

$$0 \leq^{D,L} v^{\mathrm{T}}\overline{w}$$

defines a subset S of $\mathbb{Z}^p$ closely related to the subset H of $\mathbb{Q}^p$ defined by

$$0 \leq v^{\mathrm{T}}\overline{w}$$

(a halfspace, unless $v = 0$). The remarks of the last paragraph show that S contains the origin and is closed under addition, and certainly $S \subseteq H$. If N is the product of the moduli of the congruences in L, then

$$0 \leq^{D,L} v^{\mathrm{T}}(N\overline{w}) \text{ iff } 0 \leq v^{\mathrm{T}}(N\overline{w}),$$

and the intersection of S with the lattice $N\mathbb{Z}^p$ looks exactly like the intersection of H with $N\mathbb{Z}^p$.

---

[4] Added in proof. I have recently discovered that Proposition 4 continues to hold when $T_{\mathbb{Z}}$ is replaced by the $\mathcal{L}$-theory of ordered Abelian groups. An account of the proof, and of a corresponding generalization of Corollary 4.2, will appear elsewhere.

Now one may apply Proposition 4 to obtain

Corollary 4.2. *Let A be an m-by-n matrix over $\mathbb{Z}$. There are finitely many basic pairs (D_i, H_i) $(1 \le i \le l)$ such that for any $b \in \mathbb{Z}^m$ the following conditions are equivalent:*

(i) *$b = Az$ for some $z \ge 0$ in $\mathbb{Z}^n$.*

(ii) *For all $y \in \mathbb{Z}^m$, if $y^{\mathrm{T}} A \ge^{D_i,H_i} 0$, then $y^{\mathrm{T}} b \ge^{D_i,H_i} 0$ (for all i, $1 \le i \le l$).*

Proof. Let $a_1, \dots, a_n$ be the columns of A.

(i) implies (ii) for every (D, H). For if $b = Az$, $z \ge 0$, and $y^{\mathrm{T}} A \ge^{D,H} 0$, then each $y^{\mathrm{T}} a_i \ge^{D,H} 0$, each $y^{\mathrm{T}}(a_i z_i) \ge^{D,H} 0$ because the ith entry z_i of z is nonnegative,

$$y^{\mathrm{T}}(\sum_{i=1}^{n} a_i z_i) \ge^{D,H} 0$$

by the additivity property of congruence inequalities, and $y^{\mathrm{T}} b \ge^{D,H} 0$ because $b = Az = \sum_{i=1}^{n} a_i z_i$.

To obtain the pairs for which (ii) implies (i), apply Proposition 4 and the remarks on congruence inequalities to the $\mathcal{L}$-formula $(*)$ =

$$\exists z_1 \dots \exists z_n (\bigwedge_{j=1}^{n} z_j \ge 0 \ \wedge \ \bigwedge_{i=1}^{m} x_i = \sum_{j=1}^{n} a_{ij} z_j),$$

where a_{ij} is the ij-entry of A. So there are pairs (D_i, H_i) and vectors $c_i \in \mathbb{Z}^m$ making $(*)$ equivalent modulo T_{in} to

$$\bigwedge_{i=1}^{q} c_i^{\mathrm{T}} \overline{x} \ge^{D_i,H_i} 0.$$

Now assume (ii) for these pairs (D_i, H_i). b will obey (i) just in case

$$\bigwedge_{i=1}^{q} c_i^{\mathrm{T}} b \ge^{D_i,H_i} 0.$$

With the help of (ii) one sees that this condition holds if

$$\bigwedge_{i=1}^{q} c_i^{\mathrm{T}} A \ge^{D_i,H_i} 0,$$

i.e., just in case each a_j obeys (i). The argument ends as before. $\square$

The proof of Proposition 4 begins as does the proof of Proposition 3.1. Let $\varphi(\overline{w}, \overline{z})$ be a conjunction of atomic formulas. Since $T_{\mathrm{in}} \models \exists \overline{z} \varphi(\overline{0}, \overline{z})$, one may use Lemma 2.1 to show that $\exists \overline{z} \varphi(\overline{w}, \overline{z})$ is equivalent modulo T_{in} to a conjunction of atomic formulas (and so to a conjunction of congruence inequalities, since each identity, inequality, and congruence is equivalent modulo T_{in} to a conjunction of congruence inequalities). So suppose that for all $i \in I$ $(\ne \emptyset)$, $\mathcal{M}_i \models T_{\mathrm{in}}$, $\overline{a}_i \in M_i^q$, $\mathcal{M}_i \models \exists \overline{z} \varphi[\overline{a}_i]$, $\mathcal{N} \subseteq \prod_{i \in I} \mathcal{M}_i = \mathcal{M}$, $\overline{a} = (\overline{a}_i)_{i \in I} \in N^q$, and $f : \mathcal{N} \to \mathcal{H} \models T_{\mathrm{in}}$; the goal is to show that $\mathcal{H} \models \exists \overline{z} \varphi[f(\overline{a})]$. Without loss of generality $N \ne \{0\}$ and $\mathcal{H}$ is $|\mathcal{M}|^+$-saturated; since $\varphi(\overline{w}, \overline{z})$ is a conjunction of atomic formulas, the desired result holds if f extends to a homomorphism of $\mathcal{M}$ into $\mathcal{H}$. By Zorn's lemma there is a pair $(\mathcal{N}', g)$, with $\mathcal{N} \subseteq \mathcal{N}' \subseteq \mathcal{M}$, $g : \mathcal{N}' \to \mathcal{H}$, and $f \subseteq g$, maximal with respect to inclusion (in both coordinates), and one wants to show that $\mathcal{N}' = \mathcal{M}$. If $U \in M$, U will belong to N' if g extends to a homomorphism into

$\mathcal{H}$ of the substructure of $\mathcal{M}$ with domain $N' + \mathbb{Z}U$. Such an extension will exist if some $\mathbb{U} \in H$ realizes the images, under g, of all congruence inequalities, over N', satisfied by U in $\mathcal{N}'$. Because $\mathcal{N}$ is $|\mathcal{M}|^+$-saturated, one need find such a $\mathbb{U}$ only for finitely many congruence inequalities at once. So, suppose that for all j in the finite set J, U satisfies

$$A_j + r_j u \leq^{D_j, H_j}_{\overline{P_j + t_j u}} B_j + s_j u$$

in $\mathcal{N}'$, where the A's, B's, and P's come from $\mathcal{N}'$ and the r's, s's, and t's are integers ($\overline{P_j + t_j u}$ is a tuple $(P_{j1} + t_{j1}u, P_{j2} + t_{j2}u, \dots)$).[5] The goal is to find $\mathbb{U} \in H$ satisfying each congruence inequality

$$g(A_j) + r_j u \leq^{D_j, H_j}_{\overline{g(P_j) + t_j u}} g(B_j) + s_j u$$

in $\mathcal{H}$.

By considering special cases first one may introduce the various tricks making the general argument succeed, but even this gradual approach ends with a very complicated case.

Lemma 4.3. *If $r_j = s_j = 0$ for all $j \in J$, then a suitable $\mathbb{U}$ exists.*

Proof. In $\mathcal{M}$ there are, for $j \in J$, $\overline{X}_j$ with

$$\bigwedge_{j \in J} A_j \leq \overline{X}_j \leq B_j \ \wedge \ D_j(\overline{X}_j) \ \wedge \ H_j(\overline{X}_j; \overline{P_j + t_j U}).$$

The Chinese Remainder Theorem provides a conjunction $K(\overline{x}_j; \overline{p}_j)_{j \in J}$ of congruences such that in any $\mathbb{Z}$-group

$$K(\overline{x}_j; \overline{p}_j)_{j \in J} \leftrightarrow \exists u \bigwedge_{i \in J} H_i(\overline{x}_i; \overline{p_i + t_i u})$$

(here the subscript "$j \in J$" indicates that the free variables of K are among the variables in $\overline{x}_j, \overline{p}_j$ as j varies over J). This equivalence holds in any direct product of $\mathbb{Z}$-groups, and so in $\mathcal{M}$; thus

$$\bigwedge_{i \in J} A_i \leq \overline{X}_i \leq B_i \ \wedge \ D_i(\overline{X}_i) \ \wedge \ K(\overline{X}_j; \overline{P}_j)_{j \in J}. \tag{4}$$

If one can show that

$$\exists (\overline{x}_i)_{i \in J} \bigwedge_{i \in J} g(A_i) \leq \overline{x}_i \leq g(B_i) \ \wedge \ D_i(\overline{x}_i) \ \wedge \ K(\overline{x}_j; g(\overline{P}_j))_{j \in J}$$

is true in $\mathcal{H} \models T_{\text{in}}$, then there are $\overline{\mathbb{X}}_j$ $(j \in J)$ and $\mathbb{U}$ from H with

$$\bigwedge_{i \in J} g(A_i) \leq \overline{\mathbb{X}}_i \leq g(B_i) \ \wedge \ D_i(\overline{\mathbb{X}}_i) \ \wedge \ H_i(\overline{\mathbb{X}}_i; \overline{g(P_i) + t_i \mathbb{U}}),$$

and Lemma 4.3 follows.

(4) implies that

$$\bigwedge_{i \in J} 0 \leq \overline{X}_i - A_i \leq B_i - A_i \ \wedge \ D_i(\overline{X}_i - A_i) \ \wedge \ K((\overline{X}_j - A_j) + A_j; \overline{P}_j)_{j \in J},$$

[5] This proof manipulates large systems of congruences and inequalities. To make them easier to understand, I will use lower-case letters for (sequences of) variables or integers, corresponding upper-case letters for elements of M that replace the variables, and corresponding upper-case boldface letters for elements of H that replace the variables. Thus the variable x may be replaced by $X \in M$ or $\mathbb{X} \in H$.

where $\overline{X}_i - A_i$ is the tuple $(X_{i1} - A_i, X_{i2} - A_i, \dots)$. So if one writes

$$K'(\overline{x}_j; \overline{p}_j, a_j)_{j\in J}$$

for

$$K(\overline{x}_j + a_j; \overline{p}_j)_{j\in J},$$

one has

$$\bigwedge_{i\in J} 0 \le \overline{X}_i - A_i \le B_i - A_i \ \wedge\ D_i(\overline{X}_i - A_i) \ \wedge\ K'(\overline{X}_j - A_j; \overline{P}_j, A_j)_{j\in J}.$$

$g(A_i) \le g(B_i)$ for all $i \in J$; let

$$\begin{aligned} J_\infty &= \{i \in J : g(B_i) - g(A_i) \text{ is infinite}\}, \\ J_{<\infty} &= J - J_\infty. \end{aligned}$$

The Chinese Remainder Theorem provides a conjunction $K''(\overline{x}_l; \overline{p}_m, a_m)_{\substack{l\in J_{<\infty}\\ m\in J}}$ of congruences such that in any $\mathbb{Z}$-group

$$K''(\overline{x}_l; \overline{p}_m, a_m)_{l\in J_{<\infty}, m\in J} \leftrightarrow \exists (\overline{x}_j)_{j\in J_\infty} K'(\overline{x}_l; \overline{p}_l, a_l)_{l\in J}.$$

So this equivalence holds in $\mathcal{M}$, a direct product of $\mathbb{Z}$-groups, and by letting each $\overline{X}_i - A_i = \widetilde{X}_i$ one obtains

$$\bigwedge_{i\in J_{<\infty}} 0 \le \widetilde{X}_i \le B_i - A_i \ \wedge\ D_i(\widetilde{X}_i) \ \wedge\ K''(\widetilde{X}_l; \overline{P}_m, A_m)_{l\in J_{<\infty}, m\in J}.$$

Let $\Delta = \sum_{i\in J_{<\infty}} (B_i - A_i)$ and $\Delta_i = \Delta - (B_i - A_i)$ for $i \in J_{<\infty}$. Then

$$\bigwedge_{i\in J_{<\infty}} 0 \le \widetilde{X}_i \le \widetilde{X}_i + \Delta_i \le \Delta \ \wedge\ D_i(\widetilde{X}_i) \ \wedge\ K''(\widetilde{X}_l; \overline{P}_m, A_m)_{l\in J_{<\infty}, m\in J}.$$

$M = g(\Delta)$ is a natural number. For each $i \in J_{<\infty}$ let $\overline{x}'_i$ be a sequence of new variables of the same length as $\overline{x}_i$, let δ_i be another new variable, let $D(\overline{x}_i, \overline{x}'_i)_{i\in J_{<\infty}}$ be the formula

$$\bigwedge_{i\in J_{<\infty}} D_i(\overline{x}_i) \ \wedge\ \overline{x}_i \le \overline{x}'_i,$$

and let $H(\overline{x}_i, \overline{x}'_i; \overline{p}_m, a_m, \delta_i)_{i\in J_{<\infty}, m\in J}$ be the formula

$$K''(\overline{x}_l; \overline{p}_m, a_m)_{l\in J_{<\infty}, m\in J} \ \wedge \bigwedge_{i\in J_{<\infty}} \overline{x}_i + \delta_i \equiv_{M+2} \overline{x}'_i$$

(where $\overline{x}_i + \delta_i \equiv_{M+2} \overline{x}'_i$ means that for corresponding entries x_{ij} of $\overline{x}_i$ and x'_{ij} of $\overline{x}'_i$, $x_{ij} + \delta_i \equiv_{M+2} x'_{ij}$). Then

$$\begin{aligned} \bigwedge_{i\in J_{<\infty}} 0 \le \widetilde{X}_i, \widetilde{X}_i + \Delta_i \le \Delta \ \wedge\ & D(\widetilde{X}_l, \widetilde{X}_l + \Delta_l)_{l\in J_{<\infty}} \\ & \wedge\ H(\widetilde{X}_l, \widetilde{X}_l + \Delta_l; \overline{P}_m, A_m, \Delta_l)_{l\in J_{<\infty}, m\in J} \end{aligned}$$

and so

$$0 \le^{D,H}_{(\overline{P}_m, A_m, \Delta_i)_{i\in J_{<\infty}, m\in J}} \Delta.$$

Because g is a homomorphism

$$0 \le^{D,H}_{(g(\overline{P}_m), g(A_m), g(\Delta_i))_{i\in J_{<\infty}, m\in J}} g(\Delta)$$

in $\mathcal{H}$, and there are $\overline{\mathbb{X}}_i, \overline{\mathbb{X}}_i'$ from H with

$$\bigwedge_{i \in J_{<\infty}} 0 \leq \overline{\mathbb{X}}_i, \overline{\mathbb{X}}_i' \leq g(\Delta) \ \wedge \ D_i(\overline{\mathbb{X}}_i) \ \wedge \ \overline{\mathbb{X}}_i \leq \overline{\mathbb{X}}_i'$$

$$\wedge \ K''(\overline{\mathbb{X}}_l; g(\overline{P}_m), g(A_m))_{l \in J_{<\infty}, m \in J} \ \wedge \ \overline{\mathbb{X}}_i + g(\Delta_i) \equiv_{M+2} \overline{\mathbb{X}}_i'.$$

$M = g(\Delta)$, each $g(B_i) - g(A_i) \geq 0$, and for $i \in J_{<\infty}$

$$0 \leq \overline{\mathbb{X}}_i \leq \overline{\mathbb{X}}_i' \leq g(\Delta);$$

so

$$0 \leq \overline{\mathbb{X}}_i' - \overline{\mathbb{X}}_i \leq M, \ -M \leq -g(\Delta_i) \leq 0,$$

and

$$-M \leq \overline{\mathbb{X}}_i' - (\overline{\mathbb{X}}_i + g(\Delta_i)) \leq M$$

when $i \in J_{<\infty}$. Because the middle terms are divisible by $M+2$, they are zero, and

$$\overline{\mathbb{X}}_i + g(\Delta_i) \leq g(\Delta) = g(\Delta_i) + (g(B_i) - g(A_i))$$

and

$$\overline{\mathbb{X}}_i \leq g(B_i) - g(A_i)$$

for $i \in J_{<\infty}$. Thus

$$\bigwedge_{i \in J_{<\infty}} 0 \leq \overline{\mathbb{X}}_i \leq g(B_i) - g(A_i) \ \wedge \ D_i(\overline{\mathbb{X}}_i) \ \wedge \ K''(\overline{\mathbb{X}}_l; g(\overline{P}_m), g(A_m))_{l \in J_{<\infty}, m \in J}.$$

By the choice of K'' there are $\overline{\mathbb{X}}_l$ from H, for $l \in J_\infty$, such that

$$K'(\overline{\mathbb{X}}_i; g(\overline{P}_i), g(A_i))_{i \in J}.$$

The truth of K' depends only on the congruence classes of its entries, modulo the product of the moduli of the congruences in K'. When $i \in J_\infty$, $g(B_i) - g(A_i) > 0$ is infinite; so one may assume that $0 \leq \overline{\mathbb{X}}_i \leq g(B_i) - g(A_i)$. Since the graph corresponding to $D_i(\overline{x}_i)$ is cycle-free, $D_i(\overline{x}_i)$ does not imply that $x_k = x_l$ if $k \neq l$; so for $i \in J_\infty$ one may assume that $D_i(\overline{\mathbb{X}}_i)$. Thus

$$\bigwedge_{i \in J} 0 \leq \overline{\mathbb{X}}_i \leq g(B_i) - g(A_i) \ \wedge \ D_i(\overline{\mathbb{X}}_i) \ \wedge \ K'(\overline{\mathbb{X}}_j; g(\overline{P}_j), g(A_j))_{j \in J},$$

and by the choice of K'

$$\bigwedge_{i \in J} g(A_i) \leq \overline{\mathbb{X}}_i + g(A_i) \leq g(B_i) \ \wedge \ D_i(\overline{\mathbb{X}}_i + g(A_i)) \ \wedge \ K(\overline{\mathbb{X}}_j + g(A_j); g(\overline{P}_j))_{j \in J}.$$

Thus the argument for Lemma 4.3 is complete. $\square$

More generally, one may state

Lemma 4.4. *If every $r_i = s_i$, then a suitable $\mathbb{U}$ exists.*

Proof. In $\mathcal{M}$ there are $\overline{X}_i$, for $i \in J$, with

$$\bigwedge_{i \in J} A_i + r_i U \leq \overline{X}_i \leq B_i + r_i U \ \wedge \ D_i(\overline{X}_i) \ \wedge \ H_i(\overline{X}_i; \overline{P_i + t_i U}),$$

and so

$$\bigwedge_{i \in J} A_i \leq \overline{X}_i - r_i U \leq B_i \ \wedge \ D_i(\overline{X}_i - r_i U) \ \wedge \ H_i((\overline{X}_i - r_i U) + r_i U; \overline{P_i + t_i U}).$$

Writing

$$H_i'(\overline{x}_i;\overline{p}_i,u)$$

for

$$H_i(\overline{x}_i+r_iu;\overline{p_i+t_iu}),$$

one finds that

$$\bigwedge_{i\in J} A_i \leq^{D_i,H_i'}_{\overline{P}_i,U} B_i.$$

So Lemma 4.3 provides $\mathbb{U}\in H$ with

$$\bigwedge_{i\in J} g(A_i) \leq^{D_i,H_i'}_{g(\overline{P}_i),\mathbb{U}} g(B_i),$$

and for $i\in J$ there are $\overline{\mathbb{X}}_i$ from H with

$$\bigwedge_{i\in J} g(A_i)\leq \overline{\mathbb{X}}_i \leq g(B_i) \ \wedge\ D_i(\overline{\mathbb{X}}_i) \ \wedge\ H_i'(\overline{\mathbb{X}}_i;g(\overline{P}_i),\mathbb{U}).$$

Thus

$$\bigwedge_{i\in J} g(A_i)+r_i\mathbb{U}\leq \overline{\mathbb{X}}_i+r_i\mathbb{U} \leq g(B_i)+r_i\mathbb{U} \ \wedge\ D_i(\overline{\mathbb{X}}_i+r_i\mathbb{U})$$
$$\wedge\ H_i(\overline{\mathbb{X}}_i+r_i\mathbb{U};\overline{g(P_i)+t_i\mathbb{U}}),$$

and the argument is complete. □

Still more generally one may state

Lemma 4.5. *If no two r_i-s_i's have strictly different signs, then a suitable $\mathbb{U}$ exists.*

Proof. Without loss of generality every $r_i-s_i\geq 0$, and by Lemma 4.4 one may assume that at least one $r_i-s_i>0$. Let

$$\begin{aligned} J_+ &= \{i\in J : r_i>s_i\},\\ J_= &= J-J_+=\{i\in J: r_i=s_i\}. \end{aligned}$$

In $\mathcal{M}$ there are $\overline{X}_i$, for $i\in J$, with

$$A_i+r_iU\leq \overline{X}_i\leq B_i+r_iU \ \wedge\ D_i(\overline{X}_i) \ \wedge\ H_i(\overline{X}_i;\overline{P_i+t_iU})$$

for all $i\in J_=$ and

$$A_i+(r_i-s_i)U\leq \overline{X}_i-s_iU\leq B_i \ \wedge\ D_i(\overline{X}_i-s_iU) \ \wedge\ H_i((\overline{X}_i-s_iU)+s_iU;\overline{P_i+t_iU})$$

for all $i\in J_+$. Use the Chinese Remainder Theorem to find a conjunction $K(\overline{p}_i,u)_{i\in J_+}$ of congruences such that in any $\mathbb{Z}$-group

$$K(\overline{p}_i,u)_{i\in J_+}\leftrightarrow \exists(\overline{x}_l)_{l\in J_+}\bigwedge_{l\in J_+} H_l(\overline{x}_l+s_lu;\overline{p_l+t_lu}).$$

Since $\mathcal{M}$ is a direct product of $\mathbb{Z}$-groups,

$$\bigwedge_{i\in J_=} A_i+r_iU\leq \overline{X}_i\leq B_i+r_iU \ \wedge\ D_i(\overline{X}_i) \ \wedge\ H_i(\overline{X}_i;\overline{P_i+t_iU})$$
$$\wedge\ K(\overline{P}_l,U)_{l\in J_+}.$$

So if $H_i'(\overline{x}_i;\overline{p}_i,\overline{p}_l,u)_{l\in J_+}$ is $H_i(\overline{x}_i;\overline{p_i+t_iu}) \ \wedge\ K(\overline{p}_l,u)_{l\in J_+}$,

$$\bigwedge_{i\in J_=} A_i+r_iU \leq^{D_i,H_i'}_{(\overline{P}_i,\overline{P}_l,U)_{l\in J_+}} B_i+r_iU.$$

By Lemma 4.4, therefore, there is $\mathbb{U} \in H$ for which

$$\bigwedge_{i \in J_=} g(A_i) + r_i\mathbb{U} \leq^{D_i, H_i'}_{(g(\overline{P}_i), g(\overline{P}_l), \mathbb{U})_{l \in J_+}} B_i + r_i\mathbb{U};$$

so there are $\overline{\mathbb{X}}_i$ from H, for $i \in J_=$, with

$$\bigwedge_{i \in J_=} g(A_i) + r_i\mathbb{U} \leq \overline{\mathbb{X}}_i \leq g(B_i) + r_i\mathbb{U} \ \wedge \ D_i(\overline{\mathbb{X}}_i) \ \wedge \ H_i(\overline{\mathbb{X}}_i; \overline{g(P_i) + t_i\mathbb{U}})$$
$$\wedge \ K(g(\overline{P}_l), \mathbb{U})_{l \in J_+}.$$

Since $\mathcal{H}$ is a $\mathbb{Z}$-group, there are $\overline{\mathbb{X}}_l$ from H, for $l \in J_+$, with

$$\bigwedge_{l \in J_+} H_l(\overline{\mathbb{X}}_l + s_l\mathbb{U}; \overline{g(P_l) + t_l\mathbb{U}}).$$

The truth of all the congruences above depends only on the congruence classes of their entries modulo P, the product of the moduli of the congruences. For $i \in J_+$, $r_i - s_i > 0$. So by the saturation assumption on $\mathcal{H}$ there is $\mathbb{F} \in H$ for which

$$(r_i - s_i)\mathbb{V} + g(A_i) - g(B_i) = g(A_i) + r_i\mathbb{V} - (g(B_i) + s_i\mathbb{V})$$

is negative infinite whenever $\mathbb{V} < \mathbb{F}$ in $\mathcal{H}$. If one picks $\mathbb{V} < \mathbb{F}$ with $\mathbb{V} \equiv_P \mathbb{U}$, then

$$g(A_i) + r_i\mathbb{V} \leq \overline{\mathbb{X}}_i + r_i(\mathbb{V} - \mathbb{U}) \leq g(B_i) + r_i\mathbb{V} \ \wedge \ D_i(\overline{\mathbb{X}}_i + r_i(\mathbb{V} - \mathbb{U}))$$
$$\wedge \ H_i(\overline{\mathbb{X}}_i + r_i(\mathbb{V} - \mathbb{U}); \overline{g(P_i) + t_i\mathbb{V}})$$

whenever $i \in J_=$, and

$$g(A_i) + r_i\mathbb{V} - (g(B_i) + s_i\mathbb{V}) \text{ is negative infinite } \ \wedge \ H_i(\overline{\mathbb{X}}_i + s_i\mathbb{V}; \overline{g(P_i) + t_i\mathbb{V}})$$

whenever $i \in J_+$. When $i \in J_+$, the graph corresponding to D_i contains no cycles, and $g(A_i) + r_i\mathbb{V} - (g(B_i) + s_i\mathbb{V})$ is negative infinite; so one may assume that

$$g(A_i) + r_i\mathbb{V} \leq \overline{\mathbb{X}}_i + s_i\mathbb{V} \leq g(B_i) + s_i\mathbb{V} \ \wedge \ D_i(\overline{\mathbb{X}}_i + s_i\mathbb{V})$$

whenever $i \in J_+$. Thus the desired conclusion holds. □

The last case is treated in

Lemma 4.6. *If at least two $r_i - s_i$'s have strictly different signs, then a suitable $\mathbb{U}$ exists.*

Proof. Here a multiple of U is forced to be in an interval with endpoints in N'. If the image under g of this interval is infinite, one follows the strategy applied to J_∞ in the proof of Lemma 4.3: eliminate U from the congruences with the help of the Chinese Remainder Theorem, solve a system of congruences in $\mathcal{H}$, and then shift the solution to a congruent one, in the infinite interval, that is ordered in the required way. If the image under g of this interval is finite, one follows the strategy applied to $J_{<\infty}$ in the proof of Lemma 4.3: collapse the system of congruence inequalities to a single one by replacing certain identities by congruences modulo a number related to the length of the finite interval; transfer this congruence inequality to $\mathcal{H}$; and then recover the images of the original congruence inequalities. Because inequalities constrain U in this case, it cannot be eliminated merely by applying the Chinese Remainder Theorem, and the details grow more complex.

Let

$$\begin{aligned} J_+ &= \{i \in J : r_i > s_i\}\ (\neq \emptyset), \\ J_= &= \{i \in J : r_i = s_i\}, \\ J_- &= \{i \in J : r_i < s_i\}\ (\neq \emptyset). \end{aligned}$$

For $i \in J_- \cup J_+$ there are $\widetilde{X}_i$ from M with

$$\begin{aligned} &\bigwedge_{i\in J_-} A_i \leq \widetilde{X}_i - r_iU \leq B_i + (s_i - r_i)U \ \wedge\ D_i(\widetilde{X}_i) \ \wedge\ H_i(\widetilde{X}_i; \overline{P_i + t_iU}) \\ \wedge &\bigwedge_{j\in J_+} A_j + (r_j - s_j)U \leq \widetilde{X}_j - s_jU \leq B_j \ \wedge\ D_j(\widetilde{X}_j) \ \wedge\ H_j(\widetilde{X}_j; \overline{P_j + t_jU}), \end{aligned}$$

where $s_i - r_i > 0$ ($r_j - s_j > 0$) when $i \in J_-$ ($j \in J_+$). Multiplying these relations by suitable positive integers and making corresponding changes to the moduli of congruences, one may assume that

$$s_i - r_i = r_j - s_j = N > 0 \text{ for all } i \in J_- \text{ and } j \in J_+.$$

The same trick allows one to assume that the congruence inequalities for $i \in J_=$ have the form

$$A_i + r_iNU \leq^{D_i,H_i}_{\overline{P_i+t_iNU}} B_i + r_iNU.$$

So one concludes that

$$\begin{aligned} &\bigwedge_{i\in J_-} A_i - B_i \leq \widetilde{X}_i - (B_i + r_iU) \leq NU \ \wedge\ D_i(\widetilde{X}_i - (B_i + r_iU)) \\ &\qquad\qquad \wedge\ H_i((\widetilde{X}_i - (B_i + r_iU)) + (B_i + r_iU); \overline{P_i + t_iU}) \\ \wedge &\bigwedge_{i\in J_+} NU \leq \widetilde{X}_i - (A_i + s_iU) \leq B_i - A_i \ \wedge\ D_i(\widetilde{X}_i - (A_i + s_iU)) \\ &\qquad\qquad \wedge\ H_i((\widetilde{X}_i - (A_i + s_iU)) + (A_i + s_iU); \overline{P_i + t_iU}) \\ \wedge &\bigwedge_{i\in J_=} A_i + r_iNU \leq^{D_i,H_i}_{\overline{P_i+t_iNU}} B_i + r_iNU. \end{aligned}$$

For $(i,j) \in J_- \times J_+$ let $Q_{(i,j)} = A_i - B_i$ and $R_{(i,j)} = B_j - A_j$; then

$$Q_{(i,j)} \leq NU \leq R_{(k,l)}$$

for all $(k,l) \in J_- \times J_+$, and so

$$\mathfrak{m} = \max_{(i,j)\in J_-\times J_+} g(Q_{(i,j)}) \leq \min_{(i,j)\in J_-\times J_+} g(R_{(i,j)}) = \mathfrak{M}$$

in $\mathcal{H}$.

If $\mathfrak{M} - \mathfrak{m}$ is infinite, use the Chinese Remainder Theorem to find a conjunction $K(\overline{x}_i; \overline{p}_j, a_j, b_j, u)_{i\in J_=, j\in J}$ of congruences equivalent to

$$\begin{aligned} \exists(\overline{x}_l)_{l\in J_-\cup J_+}(&\bigwedge_{j\in J_-} H_j(\overline{x}_j + (b_j + r_ju); \overline{p_j + t_ju}) \\ \wedge &\bigwedge_{j\in J_+} H_j(\overline{x}_j + (a_j + s_ju); \overline{p_j + t_ju}) \\ \wedge &\bigwedge_{j\in J_=} H_j(\overline{x}_j; \overline{p_j + t_jNu})) \end{aligned}$$

in any $\mathbb{Z}$-group, and so in any product of $\mathbb{Z}$-groups. When $i \in J_=$, there is $\widetilde{X}_i$ from $\mathcal{M}$ with

$$A_i + r_i NU \leq \widetilde{X}_i \leq B_i + r_i NU \ \wedge \ D_i(\widetilde{X}_i) \ \wedge \ H_i(\widetilde{X}_i; \overline{P_i + t_i NU});$$

so

$$\bigwedge_{i \in J_=} A_i + r_i NU \leq \widetilde{X}_i \leq B_i + r_i NU \ \wedge \ D_i(\widetilde{X}_i)$$
$$\wedge \ K(\widetilde{X}_j; \overline{P}_l, A_l, B_l, U)_{j \in J_=, l \in J}.$$

By the proofs of Lemmas 4.3 and 4.4 there are $\mathbb{U}$ and $\overline{\mathbb{X}}_i$ from $\mathcal{H}$, for $i \in J_=$, with

$$\bigwedge_{i \in J_=} g(A_i) + r_i N\mathbb{U} \leq \overline{\mathbb{X}}_i \leq g(B_i) + r_i N\mathbb{U} \ \wedge \ D_i(\overline{\mathbb{X}}_i)$$
$$\wedge \ K(\overline{\mathbb{X}}_j; g(\overline{P}_l), g(A_l), g(B_l), \mathbb{U})_{j \in J_=, l \in J}.$$

So by the choice of K there are $\overline{\mathbb{X}}_i$ from $\mathcal{H}$, for $i \in J_- \cup J_+$, with

$$\bigwedge_{j \in J_-} H_j(\overline{\mathbb{X}}_j + (g(B_j) + r_j \mathbb{U}); \overline{g(P_j) + t_j \mathbb{U}})$$
$$\wedge \ \bigwedge_{j \in J_+} H_j(\overline{\mathbb{X}}_j + (g(A_j) + s_j \mathbb{U}); \overline{g(P_j) + t_j \mathbb{U}})$$
$$\wedge \ \bigwedge_{j \in J_=} H_j(\overline{\mathbb{X}}_j; \overline{g(P_j) + t_j N\mathbb{U}}).$$

The truth of these congruences depends only on the congruence classes of their entries, modulo the product of the moduli of the congruences. Since $\mathfrak{M} - \mathfrak{m}$ is infinite and the graph corresponding to each D_i is cycle-free, one may assume that for $(k, l) \in J_- \times J_+$

$$\mathfrak{m} \leq \overline{\mathbb{X}}_k \leq N\mathbb{U} \leq \overline{\mathbb{X}}_l \leq \mathfrak{M} \ \wedge \ D_k(\overline{\mathbb{X}}_k) \ \wedge \ D_l(\overline{\mathbb{X}}_l);$$

note that if the original $\mathbb{U}$ is shifted to a congruent element, corresponding shifts in the $\overline{\mathbb{X}}_i$ for $i \in J_=$ will preserve the conditions

$$\bigwedge_{i \in J_=} g(A_i) + r_i N\mathbb{U} \leq \overline{\mathbb{X}}_i \leq g(B_i) + r_i N\mathbb{U} \ \wedge \ D_i(\overline{\mathbb{X}}_i).$$

So for $i \in J_-$, $D_i(\overline{\mathbb{X}}_i + g(B_i) + r_i \mathbb{U})$ and

$$\begin{aligned} g(A_i) + r_i \mathbb{U} &= g(A_i) - g(B_i) + g(B_i) + r_i \mathbb{U} \\ &\leq \mathfrak{m} + g(B_i) + r_i \mathbb{U} \\ &\leq \overline{\mathbb{X}}_i + g(B_i) + r_i \mathbb{U} \\ &\leq N\mathbb{U} + g(B_i) + r_i \mathbb{U} = g(B_i) + s_i \mathbb{U}. \end{aligned}$$

A similar argument shows that when $i \in J_+$, $D_i(\overline{\mathbb{X}}_i + g(A_i) + s_i \mathbb{U})$ and $g(A_i) + r_i \mathbb{U} \leq \overline{\mathbb{X}}_i + g(A_i) + s_i \mathbb{U} \leq g(B_i) + s_i \mathbb{U}$. One thus reaches the desired conclusion when $\mathfrak{M} - \mathfrak{m}$ is infinite.

Now assume that $\mathfrak{M} - \mathfrak{m}$ is finite. Let $\mathfrak{P} = J_- \times J_+$ and

$$\begin{aligned} \mathfrak{L} &= \{i \in \mathfrak{P} : g(Q_i) - g(R_j) \text{ is finite for some } j \in \mathfrak{P}\}, \\ \mathfrak{U} &= \{j \in \mathfrak{P} : g(Q_i) - g(R_j) \text{ is finite for some } i \in \mathfrak{P}\}. \end{aligned}$$

Then

$$\{(i,j) \in \mathfrak{P}^2 : g(Q_i) - g(R_j) \text{ is finite}\} = \mathfrak{L} \times \mathfrak{U} \neq \emptyset,$$

and if $(i,j),(m,n) \in \mathfrak{L} \times \mathfrak{U}$, $i' \in \mathfrak{P} - \mathfrak{L}$, and $j' \in \mathfrak{P} - \mathfrak{U}$, then $g(Q_i) - g(Q_m)$ and $g(R_j) - g(R_n)$ are finite and $g(Q_i) - g(Q_{i'})$ and $g(R_{j'}) - g(R_j)$ are positive infinite. Let

$$\begin{aligned} J^{\infty} &= \{i \in J_= : g(B_i) - g(A_i) \text{ is infinite}\}, \\ J^{<\infty} &= J_= - J^{\infty}, \end{aligned}$$

and let B be a positive integer at least as large as the natural number

$$\sum_{(i,j)\in\mathfrak{L}\times\mathfrak{U}} (g(R_j) - g(Q_i)) + \sum_{i,m\in\mathfrak{L}} |g(Q_i) - g(Q_m)| \\ + \sum_{j,n\in\mathfrak{U}} |g(R_j) - g(R_n)| + \sum_{i\in J^{<\infty}} g(B_i) - g(A_i)$$

(absolute value in $\mathcal{H}$ is defined in the obvious way). For $i \in J_-$ let $H_i^*(\overline{x}_i, v; \overline{p}_i, w_i)$ result from

$$H_i(\overline{x}_i + w_i + r_i u; \overline{p_i + t_i u})$$

when u is replaced by v/N and then every congruence (and modulus) is multiplied by N. When $i \in J_+$, obtain $H_i^*(\overline{x}_i, v; \overline{p}_i, w_i)$ from $H_i(\overline{x}_i + w_i + s_i u; \overline{p_i + t_i u})$ in similar fashion, and for $i \in J_=$ let $H_i^*(\overline{x}_i, v; \overline{p}_i, w_i)$ be $H_i(\overline{x}_i + w_i + r_i v; \overline{p_i + t_i v})$. For $i \in J_=$ pick $\widetilde{X}_i$ from $\mathcal{M}$ with

$$A_i + r_i NU \leq \widetilde{X}_i \leq B_i + r_i NU \ \wedge \ D_i(\widetilde{X}_i) \ \wedge \ H_i(\widetilde{X}_i; \overline{P_i + t_i NU}).$$

Letting

$$\begin{aligned} \overline{X}_i &= \begin{cases} \widetilde{X}_i - (B_i + r_i U) & \text{if } i \in J_-, \\ \widetilde{X}_i - (A_i + s_i U) & \text{if } i \in J_+, \\ \widetilde{X}_i - (A_i + r_i NU) & \text{if } i \in J_=, \end{cases} \\ V &= NU, \\ W_i &= \begin{cases} A_i & \text{if } i \in J_+ \cup J_=, \\ B_i & \text{if } i \in J_-, \end{cases} \end{aligned}$$

one sees that

$$\begin{aligned} \bigwedge_{(i,j)\in\mathfrak{P}} & Q_{(i,j)} \leq \overline{X}_i \leq V \leq \overline{X}_j \leq R_{(i,j)} \ \wedge \ D_i(\overline{X}_i) \ \wedge \ D_j(\overline{X}_j) \\ & \wedge \ H_i^*(\overline{X}_i, V; \overline{P}_i, W_i) \ \wedge \ H_j^*(\overline{X}_j, V; \overline{P}_j, W_j) \\ & \wedge \ V \equiv_N 0 \\ \wedge \bigwedge_{k\in J_=} & 0 \leq \overline{X}_k \leq B_k - A_k \ \wedge \ D_k(\overline{X}_k) \ \wedge \ H_k^*(\overline{X}_k, V; \overline{P}_k, W_k). \end{aligned}$$

Let $\pi_- : \mathfrak{P} \to J_-$ and $\pi_+ : \mathfrak{P} \to J_+$ be the projections on the first and second coordinates. For $(i,j) \in \mathfrak{L} \times \mathfrak{U}$ let $\overline{x}^{(i,j)}_{\pi_-(i)}$ $(\overline{x}^{(i,j)}_{\pi_+(j)})$ be a tuple of new variables of the same length as $\overline{x}_{\pi_-(i)}$ ($\overline{x}_{\pi_+(j)}$) and let v_i and q_i be new variables. Let

$$\begin{aligned}\overline{X}^{(i,j)}_{\pi_-(i)} &= \overline{X}_{\pi_-(i)} - Q_i \text{ if } (i,j) \in \mathfrak{L} \times \mathfrak{U},\\ \overline{X}^{(i,j)}_{\pi_+(j)} &= \overline{X}_{\pi_+(j)} - Q_i \text{ if } (i,j) \in \mathfrak{L} \times \mathfrak{U},\\ V_i &= V - Q_i \text{ if } i \in \mathfrak{L}.\end{aligned}$$

Fix $j_0 \in \mathfrak{L}$, and let S be the product of the moduli in H^*_i for all $i \in J$. When the free variables in the following formula are replaced by their upper-case versions, one obtains a statement true in $\mathcal{M}$:

$$\begin{aligned}\exists(\overline{x}_i)_{i \in J_- \cup J_+ \cup J^\infty}\Big(&\bigwedge_{j \in J} H^*_j(\overline{x}_j, v_{j_0} + q_{j_0}; \overline{p}_j, w_j)\\ &\wedge \bigwedge_{l,l' \in \mathfrak{L}} v_l + q_l \equiv_{2B+1} v_{l'} + q_{l'} \;\wedge\; v_l + q_l \equiv_N 0\\ &\wedge \bigwedge_{\substack{(l,m),(l',m') \in \mathfrak{L}\times\mathfrak{U}\\ \pi_-(l)=\pi_-(l')}} \overline{x}^{(l,m)}_{\pi_-(l)} + q_l \equiv_{2B+1} \overline{x}^{(l',m')}_{\pi_-(l')} + q_{l'}\\ &\qquad \wedge\; \overline{x}^{(l,m)}_{\pi_-(l)} + q_l \equiv_S \overline{x}_{\pi_-(l)}\\ &\wedge \bigwedge_{\substack{(l,m),(l',m') \in \mathfrak{L}\times\mathfrak{U}\\ \pi_+(m)=\pi_+(m')}} \overline{x}^{(l,m)}_{\pi_+(m)} + q_l \equiv_{2B+1} \overline{x}^{(l',m')}_{\pi_+(m')} + q_{l'}\\ &\qquad \wedge\; \overline{x}^{(l,m)}_{\pi_+(m)} + q_l \equiv_S \overline{x}_{\pi_+(m)}\Big).\end{aligned}$$

By the Chinese Remainder Theorem there is a conjunction

$$K(\overline{x}^{(l,m)}_{\pi_-(l)}, \overline{x}^{(l,m)}_{\pi_+(m)}, \overline{x}_i, v_l; \overline{p}_j, w_j, q_l)_{(l,m)\in\mathfrak{L}\times\mathfrak{U}, i \in J^{<\infty}, j \in J}$$

of congruences equivalent to the last displayed formula in any $\mathbb{Z}$-group, and so in any product of $\mathbb{Z}$-groups. If $D(\overline{x}^{(l,m)}_{\pi_-(l)}, \overline{x}^{(l,m)}_{\pi_+(m)}, \overline{x}_i, v_l)_{(l,m)\in\mathfrak{L}\times\mathfrak{U}, i\in J^{<\infty}}$ is the formula

$$\bigwedge_{(l,m)\in\mathfrak{L}\times\mathfrak{U}} D_{\pi_-(l)}(\overline{x}^{(l,m)}_{\pi_-(l)}) \;\wedge\; \overline{x}^{(l,m)}_{\pi_-(l)} \le v_l \le \overline{x}^{(l,m)}_{\pi_+(m)} \;\wedge\; D_{\pi_+(m)}(\overline{x}^{(l,m)}_{\pi_+(m)})$$
$$\wedge \bigwedge_{i \in J^{<\infty}} D_i(\overline{x}_i),$$

then one obtains a statement true in $\mathcal{M}$ when the variables are replaced by their uppercase versions, and the corresponding graph is cycle-free. Let

$$\Delta = \sum_{(l,m)\in\mathfrak{L}\times\mathfrak{U}} (R_m - Q_l) + \sum_{i \in J^{<\infty}} B_i - A_i,$$

and for $(l,m) \in \mathfrak{L} \times \mathfrak{U}$ and $i \in J^{<\infty}$ let

$$\begin{aligned}\Delta_{(l,m)} &= \Delta - (R_m - Q_l),\\ \Delta_i &= \Delta - (B_i - A_i).\end{aligned}$$

For $(l,m) \in \mathfrak{L} \times \mathfrak{U}$ and $i \in J^{<\infty}$ introduce tuples $\overline{x}^{(l,m),+}_{\pi_-(l)}$, $\overline{x}^{(l,m),+}_{\pi_+(m)}$, $\overline{x}^+_i$ of new variables—of the same lengths as $\overline{x}^{(l,m)}_{\pi_-(l)}$, $\overline{x}^{(l,m)}_{\pi_+(m)}$, $\overline{x}_i$, respectively—as well as new variables $v^+_{(l,m)}$, and let

$$\begin{aligned}\overline{X}^{(l,m),+}_{\pi_-(l)} &= \overline{X}^{(l,m)}_{\pi_-(l)} + \Delta_{(l,m)},\\ \overline{X}^{(l,m),+}_{\pi_+(m)} &= \overline{X}^{(l,m)}_{\pi_+(m)} + \Delta_{(l,m)},\\ \overline{X}^+_i &= \overline{X}_i + \Delta_i,\\ V^+_{(l,m)} &= V_l + \Delta_{(l,m)}.\end{aligned}$$

Then

$$0 \le \overline{X}^{(l,m)}_{\pi_-(l)}, \overline{X}^{(l,m),+}_{\pi_-(l)}, \overline{X}^{(l,m)}_{\pi_+(m)}, \overline{X}^{(l,m),+}_{\pi_+(m)}, \overline{X}_i, \overline{X}^+_i, V_l, V^+_{(l,m)} \le \Delta.$$

For $(l,m) \in \mathfrak{L} \times \mathfrak{U}$ and $i \in J^{<\infty}$ let $\delta_{(l,m)}$ and δ_i be new variables, and let

$$K^+(\overline{x}^{(l,m)}_{\pi_-(l)}, \overline{x}^{(l,m),+}_{\pi_-(l)}, \overline{x}^{(l,m)}_{\pi_+(m)}, \overline{x}^{(l,m),+}_{\pi_+(m)}, \overline{x}_i, \overline{x}^+_i, v_l, v^+_{(l,m)}; \overline{p}_j, w_j, q_l, \delta_{(l,m)}, \delta_i)_{\substack{(l,m)\in\mathfrak{L}\times\mathfrak{U}\\ i\in J^{<\infty}, j\in J}}$$

be the formula

$$\begin{aligned}&K(\overline{x}^{(l,m)}_{\pi_-(l)}, \overline{x}^{(l,m)}_{\pi_+(m)}, \overline{x}_i, v_l; \overline{p}_j, w_j, q_l)_{(l,m)\in\mathfrak{L}\times\mathfrak{U}, i\in J^{<\infty}, j\in J}\\ &\wedge \bigwedge_{(l,m)\in\mathfrak{L}\times\mathfrak{U}} \overline{x}^{(l,m)}_{\pi_-(l)} + \delta_{(l,m)} \equiv_{2B+1} \overline{x}^{(l,m),+}_{\pi_-(l)} \;\wedge\; v_l + \delta_{(l,m)} \equiv_{2B+1} v^+_{(l,m)}\\ &\qquad\qquad\qquad\qquad\qquad\qquad \wedge\; \overline{x}^{(l,m)}_{\pi_+(m)} + \delta_{(l,m)} \equiv_{2B+1} \overline{x}^{(l,m),+}_{\pi_+(m)}\\ &\wedge \bigwedge_{i\in J^{<\infty}} \overline{x}_i + \delta_i \equiv_{2B+1} \overline{x}^+_i.\end{aligned}$$

When the variables are replaced by their upper-case versions, one obtains a statement true in $\mathcal{M}$. So in $\mathcal{N}' \subseteq \mathcal{M}$

$$0 \le^{D,K^+}_{(\overline{P}_j, W_j, Q_l, \Delta_{(l,m)}, \Delta_i)_{(l,m)\in\mathfrak{L}\times\mathfrak{U}, i\in J^{<\infty}, j\in J}} \Delta.$$

Because g is a homomorphism

$$0 \le^{D,K^+}_{(g(\overline{P}_j), g(W_j), g(Q_l), g(\Delta_{(l,m)}), g(\Delta_i))_{(l,m)\in\mathfrak{L}\times\mathfrak{U}, i\in J^{<\infty}, j\in J}} g(\Delta)$$

in $\mathcal{H}$, and for $(l,m) \in \mathfrak{L} \times \mathfrak{U}$ and $i \in J^{<\infty}$ there are elements

$$\overline{\mathbb{X}}^{(l,m)}_{\pi_-(l)}, \overline{\mathbb{X}}^{(l,m),+}_{\pi_-(l)}, \overline{\mathbb{X}}^{(l,m)}_{\pi_+(m)}, \overline{\mathbb{X}}^{(l,m),+}_{\pi_+(m)}, \overline{\mathbb{X}}_i, \overline{\mathbb{X}}^+_i, \mathbb{V}_l, \mathbb{V}^+_{(l,m)}$$

in $\mathcal{H}$, between 0 and $g(\Delta) \le B$, which satisfy D and K^+ in $\mathcal{H}$. Since $0 \le g(\Delta_{(l,m)}), g(\Delta_i) \le g(\Delta) \le B$ for all $(l,m) \in \mathfrak{L} \times \mathfrak{U}$ and $i \in J^{<\infty}$, the congruences in K^+ connecting $\overline{x}^{(l,m)}_{\pi_-(l)}$ with $\overline{x}^{(l,m),+}_{\pi_-(l)}$, $\overline{x}^{(l,m)}_{\pi_+(m)}$ with $\overline{x}^{(l,m),+}_{\pi_+(m)}$, $\overline{x}_i$ with $\overline{x}^+_i$, and v_l with $v^+_{(l,m)}$ imply that

$$\begin{aligned}\overline{\mathbb{X}}^{(l,m),+}_{\pi_-(l)} &= \overline{\mathbb{X}}^{(l,m)}_{\pi_-(l)} + g(\Delta_{(l,m)})\\ \overline{\mathbb{X}}^{(l,m),+}_{\pi_+(m)} &= \overline{\mathbb{X}}^{(l,m)}_{\pi_+(m)} + g(\Delta_{(l,m)})\\ \overline{\mathbb{X}}^+_i &= \overline{\mathbb{X}}_i + g(\Delta_i)\\ \mathbb{V}^+_{(l,m)} &= \mathbb{V}_l + g(\Delta_{(l,m)}).\end{aligned}$$

So for $(l,m) \in \mathfrak{L} \times \mathfrak{U}$

$$\overline{\mathbb{X}}^{(l,m)}_{\pi_-(l)} = \overline{\mathbb{X}}^{(l,m),+}_{\pi_-(l)} - g(\Delta_{(l,m)}) \le g(\Delta) - g(\Delta_{(l,m)}) = g(R_m) - g(Q_l),$$

and one similarly concludes that

$$\overline{\mathbb{X}}^{(l,m)}_{\pi_+(m)} \leq g(R_m) - g(Q_l),\ \mathbb{V}_l \leq g(R_m) - g(Q_l),$$

and

$$\overline{\mathbb{X}}_i \leq g(B_i) - g(A_i)$$

when $i \in J^{<\infty}$. By the truth of K in $\mathcal{H}$ there are, for $i \in J_- \cup\ J_+ \cup J^\infty$, tuples $\overline{\mathbb{X}}_i$ from $\mathcal{H}$ such that

$$\begin{aligned}
&\bigwedge_{j\in J} H^*_j(\overline{\mathbb{X}}_j, \mathbb{V}_{j_0} + g(Q_{j_0}); g(\overline{P}_j), g(W_j)) \\
\wedge &\bigwedge_{l,l'\in\mathfrak{L}} \mathbb{V}_l + g(Q_l) \equiv_{2B+1} \mathbb{V}_{l'} + g(Q_{l'})\ \wedge\ \mathbb{V}_l + g(Q_l) \equiv_N 0 \\
\wedge &\bigwedge_{\substack{(l,m),(l',m')\in\mathfrak{L}\times\mathfrak{U}\\ \pi_-(l)=\pi_-(l')}} \overline{\mathbb{X}}^{(l,m)}_{\pi_-(l)} + g(Q_l) \equiv_{2B+1} \overline{\mathbb{X}}^{(l',m')}_{\pi_-(l')} + g(Q_{l'}) \\
&\qquad \wedge\ \overline{\mathbb{X}}^{(l,m)}_{\pi_-(l)} + g(Q_l) \equiv_S \overline{\mathbb{X}}_{\pi_-(l)} \\
\wedge &\bigwedge_{\substack{(l,m),(l',m')\in\mathfrak{L}\times\mathfrak{U}\\ \pi_+(m)=\pi_+(m')}} \overline{\mathbb{X}}^{(l,m)}_{\pi_+(m)} + g(Q_l) \equiv_{2B+1} \overline{\mathbb{X}}^{(l',m')}_{\pi_+(m')} + g(Q_{l'}) \\
&\qquad \wedge\ \overline{\mathbb{X}}^{(l,m)}_{\pi_+(m)} + g(Q_l) \equiv_S \overline{\mathbb{X}}_{\pi_+(m)}.
\end{aligned}$$

When $l, l' \in \mathfrak{L}$, $g(Q_l) - g(Q_{l'})$ is between $-B$ and B, as is $\mathbb{V}_{l'} - \mathbb{V}_l$ and every entry of $\overline{\mathbb{X}}^{(l',m')}_{\pi_-(l')} - \overline{\mathbb{X}}^{(l,m)}_{\pi_-(l)}$ and $\overline{\mathbb{X}}^{(l',m')}_{\pi_+(m')} - \overline{\mathbb{X}}^{(l,m)}_{\pi_+(m)}$. So by the congruences just displayed

$$\begin{aligned}
&\bigwedge_{l,l'\in\mathfrak{L}} \mathbb{V}_l + g(Q_l) = \mathbb{V}_{l'} + g(Q_{l'}) \equiv_N 0 \\
\wedge &\bigwedge_{\substack{(l,m),(l',m')\in\mathfrak{L}\times\mathfrak{U}\\ \pi_-(l)=\pi_-(l')}} \overline{\mathbb{X}}^{(l,m)}_{\pi_-(l)} + g(Q_l) = \overline{\mathbb{X}}^{(l',m')}_{\pi_-(l')} + g(Q_{l'}) \equiv_S \overline{\mathbb{X}}_{\pi_-(l)} \\
\wedge &\bigwedge_{\substack{(l,m),(l',m')\in\mathfrak{L}\times\mathfrak{U}\\ \pi_+(m)=\pi_+(m')}} \overline{\mathbb{X}}^{(l,m)}_{\pi_+(m)} + g(Q_l) = \overline{\mathbb{X}}^{(l',m')}_{\pi_+(m')} + g(Q_{l'}) \equiv_S \overline{\mathbb{X}}_{\pi_+(m)}.
\end{aligned}$$

Let the common value of the $\mathbb{V}_l + g(Q_l)$'s be $N\mathbb{U}$. Since the truth of $H^*_{\pi_-(l)}$ and $H^*_{\pi_+(m)}$ depends only on the congruence classes of their entries modulo S, and $\pi_-(\mathfrak{L}) \subseteq J_-$ and $\pi_+(\mathfrak{U}) \subseteq J_+$, one may assume that

$$\bigwedge_{(l,m)\in\mathfrak{L}\times\mathfrak{U}} \overline{\mathbb{X}}_{\pi_-(l)} = \overline{\mathbb{X}}^{(l,m)}_{\pi_-(l)} + g(Q_l)\ \wedge\ \overline{\mathbb{X}}_{\pi_+(m)} = \overline{\mathbb{X}}^{(l,m)}_{\pi_+(m)} + g(Q_l).$$

Since

$$0 \leq \overline{\mathbb{X}}^{(l,m)}_{\pi_-(l)} \leq g(R_m) - g(Q_l)$$

when $(l, m) \in \mathfrak{L} \times \mathfrak{U}$,

$$g(Q_l) \leq \overline{\mathbb{X}}_{\pi_-(l)} \leq g(R_m);$$

similarly

$$g(Q_l) \leq \overline{\mathbb{X}}_{\pi_+(m)} \leq g(R_m).$$

Also,

$$\overline{\mathbb{X}}_{\pi_-(l)} = \overline{\mathbb{X}}^{(l,m)}_{\pi_-(l)} + g(Q_l) \leq \mathbb{V}_l + g(Q_l)(= N\mathbb{U}) \leq \overline{\mathbb{X}}^{(l,m)}_{\pi_+(m)} + g(Q_l) = \overline{\mathbb{X}}_{\pi_+(m)}$$

when $(l,m) \in \mathfrak{L} \times \mathfrak{U}$. For $i \in J^{<\infty}$

$$g(A_i) \leq \overline{\mathbb{X}}_i + g(A_i) \leq g(B_i).$$

When $i \in J^\infty$, $g(B_i) - g(A_i)$ is infinite. So since the graph corresponding to $D_i(\overline{x}_i)$ is cycle-free, one may replace the $\overline{\mathbb{X}}_i$ by elements, between 0 and $g(B_i) - g(A_i)$, that are arranged in the proper order and congruent to the original elements modulo S, and without loss of generality

$$0 \leq \overline{\mathbb{X}}_i \leq g(B_i) - g(A_i) \ \wedge\ D_i(\overline{\mathbb{X}}_i) \ \wedge\ H^*_i(\overline{\mathbb{X}}_i, N\mathbb{U}; g(\overline{P}_i), g(W_i)).$$

Summing up, so far, one may state that

$$\begin{aligned}
&\bigwedge_{(l,m)\in\mathfrak{L}\times\mathfrak{U}} g(Q_l) \leq \overline{\mathbb{X}}_{\pi_-(l)} \leq N\mathbb{U} \leq \overline{\mathbb{X}}_{\pi_+(m)} \leq g(R_m)\\
&\qquad \wedge\ D_{\pi_-(l)}(\overline{\mathbb{X}}_{\pi_-(l)}) \ \wedge\ D_{\pi_+(m)}(\overline{\mathbb{X}}_{\pi_+(m)})\\
&\qquad \wedge\ H^*_{\pi_-(l)}(\overline{\mathbb{X}}_{\pi_-(l)}, N\mathbb{U}; g(\overline{P}_{\pi_-(l)}), g(W_{\pi_-(l)}))\\
&\qquad \wedge\ H^*_{\pi_+(m)}(\overline{\mathbb{X}}_{\pi_+(m)}, N\mathbb{U}; g(\overline{P}_{\pi_+(m)}), g(W_{\pi_+(m)}))\\
&\wedge \bigwedge_{i\in(J_- - \pi_-(\mathfrak{L}))\cup(J_+ - \pi_+(\mathfrak{U}))} H^*_i(\overline{\mathbb{X}}_i, N\mathbb{U}; g(\overline{P}_i), g(W_i))\\
&\wedge \bigwedge_{i\in J_=} g(A_i) \leq \overline{\mathbb{X}}_i + g(A_i) \leq g(B_i) \ \wedge\ D_i(\overline{\mathbb{X}}_i) \ \wedge\ H^*_i(\overline{\mathbb{X}}_i, N\mathbb{U}; g(\overline{P}_i), g(W_i)).
\end{aligned}$$

If $i \in J_- - \pi_-(\mathfrak{L})$, and one picks any j from the nonempty set $\mathfrak{L}$, then $(i, \pi_+(j)) \in \mathfrak{P} - \mathfrak{L}$, and so $g(Q_j) - g(Q_{(i,\pi_+(j))})$ is positive infinite by the remarks following the definitions of $\mathfrak{L}$ and $\mathfrak{U}$. Because $g(Q_j) \leq N\mathbb{U}$,

$$N\mathbb{U} - g(Q_{(i,\pi_+(j))}) = N\mathbb{U} - g(A_i - B_i)$$

is positive infinite, and as above one may without loss of generality assume that

$$g(A_i - B_i) \leq \overline{\mathbb{X}}_i \leq N\mathbb{U} \ \wedge\ D_i(\overline{\mathbb{X}}_i).$$

A similar argument shows that when $i \in J_+ - \pi_+(\mathfrak{U})$, one may assume that

$$N\mathbb{U} \leq \overline{\mathbb{X}}_i \leq g(B_i - A_i) \ \wedge\ D_i(\overline{\mathbb{X}}_i).$$

Since $Q_l = A_{\pi_-(l)} - B_{\pi_-(l)}$ and $R_m = B_{\pi_+(m)} - A_{\pi_+(m)}$ when $(l,m) \in \mathfrak{L} \times \mathfrak{U}$, one concludes that

$$\begin{aligned}
&\bigwedge_{i\in J_-} g(A_i - B_i) \leq \overline{\mathbb{X}}_i \leq N\mathbb{U} \ \wedge\ D_i(\overline{\mathbb{X}}_i)\\
&\qquad\qquad\qquad \wedge\ H^*_i(\overline{\mathbb{X}}_i, N\mathbb{U}; g(\overline{P}_i), g(W_i))\\
&\wedge \bigwedge_{i\in J_+} N\mathbb{U} \leq \overline{\mathbb{X}}_i \leq g(B_i - A_i) \ \wedge\ D_i(\overline{\mathbb{X}}_i)\\
&\qquad\qquad\qquad \wedge\ H^*_i(\overline{\mathbb{X}}_i, N\mathbb{U}; g(\overline{P}_i), g(W_i))\\
&\wedge \bigwedge_{i\in J_=} g(A_i) \leq \overline{\mathbb{X}}_i + g(A_i) \leq g(B_i) \ \wedge\ D_i(\overline{\mathbb{X}}_i)\\
&\qquad\qquad\qquad \wedge\ H^*_i(\overline{\mathbb{X}}_i, N\mathbb{U}; g(\overline{P}_i), g(W_i)).
\end{aligned}$$

If $i \in J_-$, the definition of H_i^* implies that

$$H_i(\overline{\mathbb{X}}_i + g(W_i) + r_i\mathbb{U}; \overline{g(P_i) + t_i\mathbb{U}});$$

so since $W_i = B_i$,

$$H_i(\overline{\mathbb{X}}_i + g(B_i) + r_i\mathbb{U}; \overline{g(P_i) + t_i\mathbb{U}}).$$

Since the proof of this lemma started by arranging that $N = s_i - r_i$,

$$\begin{aligned} g(A_i) + r_i\mathbb{U} = g(A_i - B_i) + g(B_i) + r_i\mathbb{U} &\le \overline{\mathbb{X}}_i + g(B_i) + r_i\mathbb{U} \\ &\le N\mathbb{U} + g(B_i) + r_i\mathbb{U} = g(B_i) + s_i\mathbb{U}. \end{aligned}$$

So since $D_i(\overline{\mathbb{X}}_i + g(B_i) + r_i\mathbb{U})$,

$$g(A_i) + r_i\mathbb{U} \le^{D_i,H_i}_{g(P_i)+t_i\mathbb{U}} g(B_i) + s_i\mathbb{U}$$

when $i \in J_-$. Much the same argument reaches this conclusion when $i \in J_+$, though in this case $W_i = A_i$ and $N = r_i - s_i$. Finally, when $i \in J_=$ the definition of H_i^* implies that

$$H_i(\overline{\mathbb{X}}_i + g(W_i) + r_iN\mathbb{U}; \overline{g(P_i) + t_iN\mathbb{U}});$$

so since $W_i = A_i$,

$$H_i(\overline{\mathbb{X}}_i + g(A_i) + r_iN\mathbb{U}; \overline{g(P_i) + t_iN\mathbb{U}}),$$

where

$$g(A_i) + r_iN\mathbb{U} \le \overline{\mathbb{X}}_i + g(A_i) + r_iN\mathbb{U} \le g(B_i) + r_iN\mathbb{U} = g(B_i) + s_iN\mathbb{U}$$

and $D_i(\overline{\mathbb{X}}_i + g(A_i) + r_iN\mathbb{U})$, and

$$g(A_i) + r_iN\mathbb{U} \le^{D_i,H_i}_{g(P_i)+t_iN\mathbb{U}} g(B_i) + s_iN\mathbb{U}.$$

Thus the proofs of Lemma 4.6 and of Proposition 4 are complete. □

5. Conditional congruence inequalities

Both Corollary 3.5 and Corollary 4.2 focus on the solvability condition (i) =

$$\exists x \ge 0(b = Ax)$$

and show that it is equivalent to a system (ii) of implications between congruence inequalities built in a special way from A. But in many applications of Farkas' Lemma one starts with an implication (ii) and exploits the nonnegative solvability of a system (i) obtained from (ii). The results of Sections 3 and 4 do not lend themselves to such applications because the congruence inequalities appearing in (ii) depend in an as yet unknown way on A. The earlier results do not show, for example, that a system (ii) of implications—of conditional congruence inequalities—built with randomly selected congruence inequalities is equivalent to a solvability condition (i).

This section will prove results of this kind. The idea behind the proof for the integers is that if one starts with an implication $(*)$ =

$$\forall y(y^{\mathrm{T}}A \ge^{D,H} 0 \to y^{\mathrm{T}}b \ge^{D,H} 0),$$

one looks at the set S of all y obeying $(**)$ =

$$y^{\mathrm{T}}A \ge^{D,H} 0$$

and shows that S is the nonnegative linear span of certain integer vectors $d_1, \ldots, d_k$. The set T of all z obeying

$$\bigwedge_{i=1}^{k} d_i^{\mathrm{T}} z \geq^{D,H} 0$$

is also the nonnegative linear span of certain vectors $e_1, \ldots, e_l$, and by the definition of S one may assume that the columns of A are among the e's. So without loss of generality the matrix whose columns are the e's is $(A\ C)$ for some matrix C. Finally, one shows that

$$\exists w \geq 0 (b = (A\ C)w)$$

is equivalent to $(*)$.

One reason this argument does not work as it stands is that $(**)$ contains parameters and is thus not symmetric between the row y^{T} and the n columns a_j of A. The unabbreviated version of $(**)$ says that

$$\bigwedge_{j=1}^{n} y^{\mathrm{T}} a_j \geq_{a_j}^{D,H} 0.$$

So the entries of a_j may appear as arguments of the congruences in H, and when A is fixed, the condition may not define the nonnegative linear span of finitely many vectors; for example, 0 may not obey the condition.

One may overcome this difficulty by first proving a refinement of Corollary 4.2 in which the congruence inequalities appearing in (ii) enjoy a symmetry between rows and columns. Then one follows the plan sketched above to show that in this refinement of Corollary 4.2, every system (ii) of conditional congruence inequalities arises from a solvability condition (i).

The especially symmetric congruence inequalities may be isolated as follows. Suppose that $\overline{u} = (u_1, \ldots, u_k)$, $\overline{v} = (v_1, \ldots, v_k)$, and $\overline{x} = (x_1, \ldots, x_m)$ are disjoint lists of distinct variables. If $(D(\overline{x}), H(\overline{x}; \overline{u}, \overline{v}))$ is a basic pair in which the variables in H come from $\overline{u}$, $\overline{v}$, and $\overline{x}$, then $(\#) =$

$$\sum_{i=1}^{k} u_i \preccurlyeq^{D,H} \sum_{i=1}^{k} v_i$$

abbreviates the congruence inequality

$$\sum_{i=1}^{k} u_i \leq_{\overline{u},\overline{v}}^{D,H} \sum_{i=1}^{k} v_i.$$

Any formula

$$\sum_{i=1}^{k} t_i \preccurlyeq^{D,H} \sum_{i=1}^{k} w_i$$

obtained from $(\#)$ by replacing the free variables $\overline{u}$, $\overline{v}$ by $\mathcal{L}$-terms $\overline{t}$, $\overline{w}$ may be called a special congruence inequality.

Lemma 5.1. *If $\overline{y} = (y_1, \ldots, y_k)^{\mathrm{T}}$ is a column of distinct variables, $a, b \in \mathbb{Z}^k$, and C is an integer matrix with k columns, then any congruence inequality*

$$a^{\mathrm{T}} \overline{y} \leq_{C\overline{y}}^{D,H} b^{\mathrm{T}} \overline{y}$$

is equivalent modulo T_{in} *to a special congruence inequality*

$$\sum_{i=1}^{k} f_i y_i \preccurlyeq^{D,K} \sum_{i=1}^{k} g_i y_i.$$

Proof. First one may assume that for each j, a_j or b_j is not 0: for if $a_j = b_j = 0$, then the given congruence inequality, equivalent modulo T_{in} to

$$\exists \overline{x}(a^{\mathrm{T}}\overline{y} \le \overline{x} \le b^{\mathrm{T}}\overline{y} \ \wedge \ D(\overline{x}) \ \wedge \ H(\overline{x}; C\overline{y})),$$

is equivalent to

$$\exists \overline{x}(a^{\mathrm{T}}\overline{y} + y_j \le \overline{x} + y_j \le b^{\mathrm{T}}\overline{y} + y_j \ \wedge \ D(\overline{x} + y_j) \ \wedge \ H((\overline{x} + y_j) - y_j; C\overline{y})),$$

and so to a congruence inequality

$$a^{\mathrm{T}}\overline{y} + y_j \le_{C'\overline{y}}^{D,H'} b^{\mathrm{T}}\overline{y} + y_j.$$

Under this new assumption one may multiply the congruences in H and their moduli by suitable positive integers, and perhaps introduce some minus signs, to obtain a conjunction $K(\overline{x}; \overline{u}, \overline{v})$ of congruences making $H(\overline{x}; C\overline{y})$ equivalent to

$$K(\overline{x}; a_1 y_1, \ldots, a_k y_k, b_1 y_1, \ldots, b_k y_k)$$

modulo T_{in}. D and K yield a special congruence inequality equivalent modulo T_{in} to the given congruence inequality. □

Now one may state a new version of Corollary 4.2.

Corollary 5.2. *Let A be an m-by-n matrix over $\mathbb{Z}$. There are finitely many basic pairs (D_i, H_i) $(1 \le i \le l)$ such that for any $b \in \mathbb{Z}^m$ the following conditions are equivalent:*

(i) *$b = Az$ for some $z \ge 0$ in $\mathbb{Z}^n$.*

(ii) *For all $y, w \in \mathbb{Z}^m$, if $y^{\mathrm{T}}A \preccurlyeq^{D_i,H_i} w^{\mathrm{T}}A$, then $y^{\mathrm{T}}b \preccurlyeq^{D_i,H_i} w^{\mathrm{T}}b$ (for all i, $1 \le i \le l$).*

In (ii), $y^{\mathrm{T}}A \preccurlyeq^{D_i,H_i} w^{\mathrm{T}}A$ means that for each j, the jth column a_j of A obeys $y^{\mathrm{T}}a_j \preccurlyeq^{D_i,H_i} w^{\mathrm{T}}a_j$; i.e., $\sum_{i=1}^m y_i a_{ij} \preccurlyeq^{D_i,H_i} \sum_{i=1}^m w_i a_{ij}$.

Proof. If $b = Az$, where $z \ge 0$, then each

$$b_i = \sum_{j=1}^{n} a_{ij} z_j.$$

So if

$$\sum_{i=1}^{m} y_i a_{ij} \preccurlyeq^{D,H} \sum_{i=1}^{m} w_i a_{ij}$$

for every j, then

$$\sum_{i=1}^{m} y_i a_{ij} z_j \preccurlyeq^{D,H} \sum_{i=1}^{m} w_i a_{ij} z_j$$

for every j, and

$$\sum_{i=1}^{m} y_i b_i = \sum_{i=1}^{m} y_i \sum_{j=1}^{n} a_{ij} z_j \preccurlyeq^{D,H} \sum_{i=1}^{m} w_i \sum_{j=1}^{n} a_{ij} z_j = \sum_{i=1}^{m} w_i b_i.$$

To obtain the finitely many pairs for which (ii) implies (i), apply Proposition 4 and Lemma 5.1 to obtain a formula

$$\bigwedge_i \sum_{k=1}^m p_{ik}x_k \preccurlyeq^{D_i,H_i} \sum_{k=1}^m q_{ik}x_k$$

equivalent to $(*) =$

$$\exists z \geq 0(x = Az)$$

modulo T_{in}. Assume that $b \in \mathbb{Z}^m$ obeys (ii) for these pairs (D_i, H_i). To show that b obeys (i), one must show that

$$\bigwedge_i \sum_{k=1}^m p_{ik}b_k \preccurlyeq^{D_i,H_i} \sum_{k=1}^m q_{ik}b_k.$$

By (ii), one need show merely that

$$\bigwedge_{i,j} \sum_{k=1}^m p_{ik}a_{kj} \preccurlyeq^{D_i,H_i} \sum_{k=1}^m q_{ik}a_{kj};$$

i.e., that for every j, the jth column $a_j = (a_{1j}, \ldots, a_{mj})^{\mathrm{T}}$ of A obeys $(*)$. The argument ends as before. □

Now one may state

Proposition 5.3. *Let A be an m-by-n matrix over $\mathbb{Z}$ and, for each i with $1 \leq i \leq l$, let $(D_i(\overline{x}_i), H_i(\overline{x}_i; (u_1, \ldots, u_m), (v_1, \ldots, v_m)))$ be a basic pair as in the definition of special congruence inequality. There is a matrix C over $\mathbb{Z}$ such that for any $b \in \mathbb{Z}^m$ the following conditions are equivalent:*

(i) *$b = (A\ C)z$ for some integer vector $z \geq 0$.*

(ii) *For all $y, w \in \mathbb{Z}^m$, if $y^{\mathrm{T}}A \preccurlyeq^{D_i,H_i} w^{\mathrm{T}}A$, then $y^{\mathrm{T}}b \preccurlyeq^{D_i,H_i} w^{\mathrm{T}}b$ (for all i, $1 \leq i \leq l$).*

Call a subset S of $\mathbb{Z}^k$ an integer cone just in case it is the nonnegative span of finitely many vectors in $\mathbb{Z}^k$; i.e., just in case $S = B\mathbb{N}^m$ for some k-by-m matrix B over $\mathbb{Z}$. The first lemma in the proof of Proposition 5.3 states

Lemma 5.4. *If E is an m-by-k matrix over $\mathbb{Z}$, then $\{x \in \mathbb{N}^k : Ex = 0\}$ is an integer cone.*

Proof. See [6], pp. 102–105. □

An easy corollary is

Lemma 5.5. *If F is an m-by-$k + n$ matrix over $\mathbb{Z}$, then*

$$S = \{x \in \mathbb{Z}^k : \exists w \in \mathbb{Z}^n F \begin{pmatrix} x \\ w \end{pmatrix} \geq 0\}$$

is an integer cone.

Proof. Let

$$S' = \{(x, x', w, w', z) \in \mathbb{N}^{2k+2n+m} : F \begin{pmatrix} x - x' \\ w - w' \end{pmatrix} = z\}.$$

Lemma 5.4 provides a $2k + 2n + m$-by-q matrix G over $\mathbb{Z}$ with

$$S' = G\mathbb{N}^q.$$

If I is the k-by-k identity matrix and 0 is the k-by-$2n+m$ matrix of zeros,

$$\begin{aligned} S &= \{x - x' : \exists w, w', z((x, x', w, w', z) \in S')\} \\ &= (I \ \ -I \ \ 0)S' \\ &= (I \ \ -I \ \ 0)G\mathbb{N}^q, \end{aligned}$$

and S is an integer cone. □

Among integer cones are the sets defined by special congruence inequalities.

Lemma 5.6. *If $r_1, \ldots, r_k, t_1, \ldots, t_k$ are linear forms over $\mathbb{Z}$ in the variables $y = (y_1, \ldots, y_l)$, then $\{y \in \mathbb{Z}^l : \sum_{i=1}^k r_i \preccurlyeq^{D,H} \sum_{i=1}^k t_i\}$ is an integer cone.*

Proof. $\sum_{i=1}^k r_i \preccurlyeq^{D,H} \sum_{i=1}^k t_i$ is equivalent over $\mathbb{Z}$ to

$$\exists x_1 \ldots \exists x_m (\sum_{i=1}^k r_i \leq \overline{x} \leq \sum_{i=1}^k t_i \ \wedge \ D(\overline{x}) \ \wedge \ H(\overline{x}; \overline{r}, \overline{t})), \tag{1}$$

where $D(\overline{x})$ is a conjunction of inequalities

$$x_i \leq x_j \tag{2}$$

and $H(\overline{x}; \overline{u}, \overline{v})$ is a conjunction of congruences

$$c^{\mathrm{T}} \begin{pmatrix} \overline{x} \\ \overline{u} \\ \overline{v} \end{pmatrix} \equiv_q d^{\mathrm{T}} \begin{pmatrix} \overline{x} \\ \overline{u} \\ \overline{v} \end{pmatrix}. \tag{3}$$

One may rewrite the inequalities $\sum_{i=1}^k r_i \leq x_j$, $x_j \leq \sum_{i=1}^k t_i$, and (2) in the form

$$t \geq 0,$$

where t is a linear form with integer coefficients; and (3) holds just in case

$$\exists w \left(c - d^{\mathrm{T}} \begin{pmatrix} \overline{x} \\ \overline{u} \\ \overline{v} \end{pmatrix} - qw \geq 0 \ \wedge \ -c - d^{\mathrm{T}} \begin{pmatrix} \overline{x} \\ \overline{u} \\ \overline{v} \end{pmatrix} + qw \geq 0 \right).$$

So by rearranging inequalities and introducing new existentially quantified variables, one may convert (1) to an equivalent definition of the kind subject to Lemma 5.5. □

Note also that

Lemma 5.7. *The intersection of two integer cones is an integer cone.*

Proof. For $i = 1, 2$ let S_i be an integer cone defined by the k-by-q_i matrix A_i. Since

$$\begin{aligned} S_1 \cap S_2 &= \{x \in \mathbb{Z}^k : \exists y, z \geq 0 (x = A_1 y = A_2 z)\} \\ &= \{x \in \mathbb{Z}^k : \exists y, z (x - A_1 y, A_1 y - A_2 z, A_2 z - x, y, z \geq 0)\} \\ &= \{x \in \mathbb{Z}^k : \exists y, z \begin{pmatrix} I & -A_1 & 0 \\ 0 & A_1 & -A_2 \\ -I & 0 & A_2 \\ 0 & I & 0 \\ 0 & 0 & I \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} \geq 0\}, \end{aligned}$$

Lemma 5.5 implies that $S_1 \cap S_2$ is an integer cone. □

One may now prove a special case of Proposition 5.3: the case in which $l = 1$ and there is just one pair $(D_1, H_1) = (D, H)$. In (ii) the antecedent

$$\bigwedge_{j=1}^{n} \sum_{i=1}^{m} y_i a_{ij} \preccurlyeq^{D,H} \sum_{i=1}^{m} w_i a_{ij} \tag{4}$$

of the conditional is a conjunction of special congruence inequalities. By Lemma 5.6, each conjunct defines an integer cone in $\mathbb{Z}^{2m}$; so by Lemma 5.7, the conjunction defines an integer cone in $\mathbb{Z}^{2m}$. If this integer cone is defined by the $2m$-by-q matrix G, let its ith column be

$$\begin{pmatrix} e_i \\ f_i \end{pmatrix},$$

where $e_i, f_i \in \mathbb{Z}^m$. If $\overline{x} = (x_1, \ldots, x_m)$ is a sequence of m variables,

$$\bigwedge_{i=1}^{q} e_i^{\mathrm{T}} \overline{x} \preccurlyeq^{D,H} f_i^{\mathrm{T}} \overline{x} \tag{5}$$

is a conjunction of special congruence inequalities that defines an integer cone $S \subseteq \mathbb{Z}^m$. Since each column of G obeys (4), each column of A obeys (5); so there is an m by r matrix C over $\mathbb{Z}$ with

$$S = (A\ C)\mathbb{N}^{n+r}.$$

If $b \in S$, then for every (y, w) obeying (4),

$$\begin{pmatrix} y \\ w \end{pmatrix} = \sum_{i=1}^{q} n_i \begin{pmatrix} e_i \\ f_i \end{pmatrix}$$

for certain natural numbers $n_1, \ldots, n_q$. Therefore, since

$$\bigwedge_{i=1}^{q} e_i^{\mathrm{T}} b \preccurlyeq^{D,H} f_i^{\mathrm{T}} b,$$

addition of special congruence inequalities yields

$$\bigwedge_{i=1}^{q} (n_i e_i)^{\mathrm{T}} b \preccurlyeq^{D,H} (n_i f_i)^{\mathrm{T}} b$$

and

$$y^{\mathrm{T}} b = (\sum_{i=1}^{q} n_i e_i)^{\mathrm{T}} b \preccurlyeq^{D,H} (\sum_{i=1}^{q} n_i f_i)^{\mathrm{T}} b = w^{\mathrm{T}} b.$$

Conversely, if

$$\forall y, w (y^{\mathrm{T}} A \preccurlyeq^{D,H} w^{\mathrm{T}} A \to y^{\mathrm{T}} b \preccurlyeq^{D,H} w^{\mathrm{T}} b),$$

then one may show that $b \in S$ by showing that

$$\bigwedge_{i=1}^{q} e_i^{\mathrm{T}} b \preccurlyeq^{D,H} f_i^{\mathrm{T}} b.$$

By hypothesis, one need show merely that

$$\bigwedge_{i=1}^{q} e_i^{\mathrm{T}} A \preccurlyeq^{D,H} f_i^{\mathrm{T}} A,$$

and this claim holds because each column of A belongs to S.

Having established this special case, one combines it with Lemma 5.7 to obtain Proposition 5.3. Because each condition

$$\forall y, w(y^{\mathrm{T}}A \preccurlyeq^{D_i,H_i} w^{\mathrm{T}}A \to y^{\mathrm{T}}x \preccurlyeq^{D_i,H_i} w^{\mathrm{T}}x)$$

defines an integer cone $S_i \subseteq \mathbb{Z}^m$ that contains A's columns,

$$\bigwedge_{i=1}^{l} \forall y, w(y^{\mathrm{T}}A \preccurlyeq^{D_i,H_i} w^{\mathrm{T}}A \to y^{\mathrm{T}}x \preccurlyeq^{D_i,H_i} w^{\mathrm{T}}x)$$

defines $\bigcap_{i=1}^{l} S_i \subseteq \mathbb{Z}^m$, an integer cone that contains A's columns and so may be defined by a matrix $(A\ C)$.

A similar plan of attack will establish analogous theorems for dense subrings D of $\mathbb{R}$ obeying an analogue of Lemma 5.4; but what are these rings? If in light of Corollary 3.7 one concentrates on Prüfer domains D, one may show that for any m-by-k matrix E over D there is a k-by-q matrix F over D with

$$\{x \in D^k : Ex = 0\} = FD^q$$

(see Definition 5(vi) and Lemma 6 of [7], pp. 972–973 and Proposition 21.4(1) of [5], p. 301), but I do not know whether ordered Prüfer domains obey the obvious version of Lemma 5.4. Yet since dense subrings of $\mathbb{Q}$ inherit a version of Lemma 5.4 from $\mathbb{Z}$, they also obey a result that is to Corollary 3.5 as Proposition 5.3 is to Corollary 5.2:

Proposition 5.8. *Let D be a dense subring of $\mathbb{Q}$. If A is an m-by-n matrix over D and $k \geq 2$ is an integer, there is a matrix C over D such that the following conditions are equivalent for any $b \in D^m$:*

(i) *$b = (A\ C)z$ for some $z \geq 0$ from D.*

(ii) *For all $y, w \in D^m$, if $y^{\mathrm{T}}A \geq_k w^{\mathrm{T}}A$, then $y^{\mathrm{T}}b \geq_k w^{\mathrm{T}}b$.*

The proof of this result is just a simpler version of the proof of Proposition 5.3, once one has

Lemma 5.9. *If D is a dense subring of $\mathbb{Q}$ and E is an m-by-k matrix over D, then $\{x \in D^k : x \geq 0$ and $Ex = 0\}$ is a cone over D; i.e., a set BD_+^n, where B is a k-by-n matrix over D and $D_+ = \{x \in D : x \geq 0\}$.*

Proof. Since D is a dense subring of $\mathbb{Q}$, at least one prime of $\mathbb{Z}$ divides 1 in D. If $S \subseteq \mathbb{Z}$ is the multiplicative set generated by the primes of $\mathbb{Z}$ dividing 1 in D, then $S^{-1}\mathbb{Z}$, the ring of fractions of $\mathbb{Z}$ with respect to S, is a subring of D. In fact, $S^{-1}\mathbb{Z} = D$. For if $m/n \in D - \{0\}$, where m and n are relatively prime integers, then there are integers c and d with

$$cm + dn = 1,$$

and so

$$n\left(c\frac{m}{n} + d\right) = 1$$

in D. Thus every prime of $\mathbb{Z}$ dividing n in $\mathbb{Z}$ divides 1 in D and belongs to S, and $m/n \in S^{-1}\mathbb{Z}$.

So there is a positive N in S for which NE has integer entries, and by Lemma 5.4

$$\{x \in \mathbb{N}^k : NEx = 0\} = B\mathbb{N}^n$$

for some k-by-n integer matrix B. If $x \in D_+^k$ and $Ex = 0$, then there is $R > 0$ in S with $Rx \in \mathbb{N}^k$, and $NE(Rx) = NR(Ex) = 0$; so $Rx \in B\mathbb{N}^n$ and $x \in BD_+^n$. Conversely, if $x \in BD_+^n$, then there is $T > 0$ in S with $Tx \in B\mathbb{N}^n$; so $NE(Tx) = 0$ and $Ex = 0$. Thus

$$\{x \in D_+^n : Ex = 0\} = BD_+^n,$$

as desired. □

Note that if D is a dense subring of $\mathbb{R}$ which, as an ordered Abelian group, is elementarily equivalent to a dense subring of $\mathbb{Q}$, then matrices E with entries from $D \cap \mathbb{Q}$ will obey the conclusion of Lemma 5.9 and matrices A with entries from $D \cap \mathbb{Q}$ will obey the conclusion of Proposition 5.8. If H is a dense subring of $\mathbb{Q}$ and $a \in \mathbb{R}$ is transcendental, the elements of $\mathbb{Q}[a]$ with constant term from H provide an example of such a D. But since these examples, like the dense subrings of $\mathbb{Q}$, have Szmielew invariants at most one, many other examples are not touched by these results (see [9], p. 60).

6. Conclusion

Some of the questions left open by this paper concern possible improvements to Corollary 4.2. Can one replace its finitely many relations $\geq^{D_i,H_i}$ by a single relation $\geq^{D,H}$, just as one may express Corollary 3.5 with a single $\geq_k$? Though one may certainly suppose that all the congruences in all the H_i's have a common modulus, encoding all the different pairs (D_i, H_i) in a single (D, H) presents a greater challenge. A more basic question concerns the need for congruence inequalities $\geq^{D,H}$ more complex than the congruence inequalities $\geq_k$ of Section 3. While the example given there shows that over the integers one cannot get by with inequality conditions and congruence conditions separately, one might wonder whether the $\geq_k$'s must be replaced by the $\geq^{D,H}$'s. Suppose that there is a special congruence inequality

$$\sum_{i=1}^{m} u_i \preccurlyeq^{D,H} \sum_{i=1}^{m} v_i \tag{1}$$

not equivalent over $\mathbb{Z}$ to any conjunction

$$\bigwedge_{j=1}^{l} r_j \leq_k t_j, \tag{2}$$

where $k \geq 2$ and the r's and t's are linear forms over $\mathbb{Z}$ in the u's and v's. Under this assumption there is a formula

$$\exists z \geq 0 (x = Az) \tag{3}$$

not equivalent over $\mathbb{Z}$ to any formula

$$\forall y, w (y^{\mathrm{T}} A \geq_l w^{\mathrm{T}} A \rightarrow y^{\mathrm{T}} x \geq_l w^{\mathrm{T}} x). \tag{4}$$

For (1) defines an integer cone $S = A\mathbb{N}^q$, where A is a $2m$-by-q integer matrix. If this matrix makes (3) equivalent to (4) over $\mathbb{Z}$, the argument for Proposition 5.3—but with special congruence inequalities replaced by congruence inequalities $\geq_l$—shows that (3) is equivalent to a formula of shape (2); so (1) is also equivalent to (2). Though I think that the formula

$$\exists x, y (u \leq x, y \leq v \ \wedge\ x \leq y \ \wedge\ 3|x \ \wedge\ 2|y)$$

is a candidate for (1), I have not been able to show that it is not equivalent over $\mathbb{Z}$ to a formula (2).

The matrices C appearing in Propositions 5.3 and 5.8 deserve further study. The more control one has over C, the more useful these theorems may prove, and constructive proofs of these results might provide more information about C. Though Weispfenning's effective quantifier elimination in [10] may be relevant here, the problems on which he concentrates allow him to take disjunctions of formulas. Since disjunctions must be avoided here, new steps in effective quantifier elimination may be needed. The formal resemblance between Proposition 5.3 and Hilbert's Nullstellensatz suggests that the integer cone generated by $(A\ C)$ is to the integer cone generated by A as the radical of a polynomial ideal is to the ideal. One might also hope to develop duality theories for integer cones in which inequalities $\leq$ are replaced by relations $\preccurlyeq^{D,H}$; in both these projects the results obtained will depend on the pairs (D, H).

Finally, the generalization of Lemma 5.9 to other dense subrings of $\mathbb{R}$ would allow a similar generalization of Proposition 5.8.

References

[1] C. C. Chang and H. J. Keisler, *Model Theory*, North-Holland Publishing Co., Amsterdam, 1973. MR0409165 (53:12927)

[2] G. Dantzig, *Linear Programming and Extensions*, Princeton University Press, Princeton, 1998. MR1658673 (99g:90004)

[3] L. van den Dries, *Some applications of a model theoretic fact to (semi-)algebraic geometry*, Nederl. Akad. Wetensch. Indag. Math. **44** (1982), 397–401. MR0683527 (84m:14029)

[4] J. Farkas, *Theorie der einfachen Ungleichungen*, J. Reine Angew. Math. **124** (1902), 1–27.

[5] R. W. Gilmer, *Multiplicative ideal theory*, Queen's Papers in Pure and Applied Mathematics, No. 12, Queen's University, Kingston, 1968. MR0229624 (37:5198)

[6] J. H. Grace and A. Young, *The algebra of invariants*, University Press, Cambridge, 1903.

[7] P. Rothmaler, *Some model theory of modules. II. On stability and categoricity of flat modules*, J. Symbolic Logic **48** (1983), 970–985. MR0727787 (85e:03084)

[8] V. Weispfenning, *Elimination of quantifiers for certain ordered and lattice-ordered abelian groups*, Bull. Soc. Math. Belg. Sér. B **33** (1981), 131–155. MR0620968 (82h:03022)

[9] V. Weispfenning, *Model theory of abelian l-groups*. In A. M. W. Glass and W. C. Holland, eds., *Lattice-ordered groups*, Mathematics and its Applications, 48, Kluwer Academic Publishers, Dordrecht, 1989, pp. 41–79. MR1036073

[10] V. Weispfenning, *Existential equivalence of ordered abelian groups with parameters*, Arch. Math. Logic **29** (1990), 237–248. MR1062728 (91h:03044)

[11] H. Weyl, *The elementary theory of convex polyhedra*. In H. W. Kuhn and A. W. Tucker, eds., *Contributions to the Theory of Games, Volume I*, Annals of Mathematics Studies, No. 24, Princeton University Press, Princeton, 1950, pp. 3–18. MR0038088 (12:352g)

Department of Mathematics and Computer Science, Wesleyan University, Middletown, Connecticut 06459

E-mail address: pscowcroft@wesleyan.edu