AN ELIMINATION THEOREM FOR MIXED REAL-INTEGER SYSTEMS

MATTHIAS ASCHENBRENNER

ABSTRACT. An elimination result for mixed real-integer systems of linear equations is established, and used to give a short proof for an adaptation of Farkas' Lemma by Köppe and Weismantel [4]. An extension of the elimination theorem to a quantifier elimination result is indicated.

Let A be an $m \times n$ -matrix with real entries and $b \in \mathbb{R}^m$. (In the following, we think of elements of the various euclidean spaces \mathbb{R}^k as column vectors.) If b is not contained in the closed convex cone C generated by the columns of A, then b can be separated from C by a hyperplane. More precisely, the following are equivalent:

- (1) There is no column vector $x = (x_1, \ldots, x_n)^{t} \in \mathbb{R}^n$ with Ax = b and $x \ge 0$ (i.e., $x_i \ge 0$ for every i = 1, ..., n). (2) There is some $y \in \mathbb{R}^m$ such that $y^{\mathrm{t}}A \ge 0$ and $y^{\mathrm{t}}b < 0$.

That is, b is contained in $C = \{Ax : x \in \mathbb{R}^n, x \ge 0\}$ if and only if $y^{t}b \ge 0$ for all $y \in \mathbb{R}^m$ with $y^{\mathrm{t}} A \geq 0$. This statement about linear inequalities, known as Farkas' Lemma [3], underlies the duality theorem of linear programming, and plays an important role in game theory (zero-sum two-person games) and nonlinear programming (Kuhn-Tucker theorem); see [14]. As befits such a fundamental fact, many proofs of Farkas' Lemma are known, but it is still considered a "pedagogical annoyance" because some parts of it are easy to verify while the main result cannot be proved in an elementary way ([2], p. 503). In [9], however, Scowcroft gave such an elementary proof, rendering it an immediate application of the Fourier-Motzkin elimination algorithm for systems of linear inequalities in ordered vector spaces over ordered fields. The methods of elimination theory find their most general setting in model theory. Indeed, one of the main results of [9], obtained by employing model-theoretic techniques, is a variant of Farkas' Lemma over the integers, giving a necessary and sufficient condition (of "Farkas' Lemma type") for the existence of a solution $x \in \mathbb{N}^n$ of the system Ax = b. Here A and b are assumed to have integer entries. (Later, Scowcroft also found a constructive proof [10].)

Now, the literature already contains other variants of "Farkas' Lemma for the integers," most notably the following fact, which plays a role in integer programming analogous to Farkas' Lemma in linear programming (see [17]):

Proposition 1 (Kronecker [6]). Assume that A and b have rational entries. Suppose that the implication $y^{t}A \in \mathbb{Z}^{n} \Rightarrow y^{t}b \in \mathbb{Z}$ holds for every $y \in \mathbb{Q}^{m}$. Then there is some $x \in \mathbb{Z}^n$ such that Ax = b.

Date: April 26, 2007.

²⁰⁰⁰ Mathematics Subject Classification. Primary 13J05; Secondary 11G50, 13P10.

The author was partially supported by NSF grant DMS DMS-0556197. He would also like to thank Philip Scowcroft for remarks which corrected and improved an earlier version of this note.

While reviewing [9] for *Mathematical Reviews*, I noticed that an adaptation of the argument used for Farkas' Lemma in [9] also gives rise to a short proof, reproduced below, of the proposition above. In fact, one also easily obtains the following "mixed real-integer version" of Farkas' Lemma, which was first shown (in slightly weaker form) in [4]. Here and below, we let $d \in \{0, ..., n\}$.

Theorem 2. Suppose A and b have rational entries. The following are equivalent:

- (1) There is $x \in \mathbb{Q}^n$ with $x_1, \ldots, x_d \in \mathbb{Z}$ such that Ax = b.
- (2) There is $x \in \mathbb{R}^n$ with $x_1, \ldots, x_d \in \mathbb{Z}$ such that Ax = b.
- (3) For every $y \in \mathbb{R}^m$, if $y^{\mathrm{t}}A \in \mathbb{Z}^d \times \{0\}^{n-d}$, then $y^{\mathrm{t}}b \in \mathbb{Z}$.
- (4) For every $y \in \mathbb{Q}^m$, if $y^t A \in \mathbb{Z}^d \times \{0\}^{n-d}$, then $y^t b \in \mathbb{Z}$.

The implications from (1) to (2) and from (3) to (4) are trivial, and (2) \Rightarrow (3) is equally immediate: if $x \in \mathbb{R}^n$ with $x_1, \ldots, x_d \in \mathbb{Z}$ satisfies Ax = b and $y \in \mathbb{R}^m$ satisfies $y^t A \in \mathbb{Z}^d \times \{0\}^{n-d}$, then $y^t b = y^t (Ax) = (y^t A)x \in \mathbb{Z}$. Thus we only really need to prove that (4) implies (1). As in [9], for this we use an elimination result, which may be seen as an analogue of Fourier-Motzkin elimination for mixed real-integer systems of linear equations, and which might be of independent interest. More generally, let (V, M) range over all pairs consisting of a \mathbb{Q} -linear space V and an arbitrary distinguished subgroup M of V; the result will be applied below to $(V, M) = (\mathbb{Q}, \mathbb{Z})$ (but might also be useful, for instance, in the case $V = \mathbb{R}^m$ and M = an arbitrary lattice in \mathbb{R}^m).

Proposition 3. There is an algorithm which, given a finite system $\Phi(X,Y)$ of conditions of the form

$$f(X,Y) \in aM$$

where f(X,Y) is a homogeneous linear form in the tuples of indeterminates $X = (X_1, \ldots, X_n)$, $Y = (Y_1, \ldots, Y_k)$ with rational coefficients and a is an integer (possibly zero), constructs a system $\Gamma(Y)$ consisting of finitely many conditions of the form

 $g(Y) \in aM$

where g(Y) is a homogeneous linear form in Y with rational coefficients and a is an integer (again, possibly zero), with the property that for all (V, M) and $y \in V^k$:

y satisfies Γ if and only if

there is an $x \in V^n$ with $x_1, \ldots, x_d \in M$ such that (x, y) satisfies Φ .

Thus, in the system Φ the indeterminates x have been *eliminated*. In mathematical logic, results such as these go under the name of *quantifier elimination*.

To see how (4) \Rightarrow (1) in Theorem 2 follows, suppose that statement (4) holds, i.e., $y^{t}A \in \mathbb{Z}^{d} \times \{0\}^{n-d} \Rightarrow y^{t}b \in \mathbb{Z}$, for every $y \in \mathbb{Q}^{m}$. Note that then $y^{t}A = 0 \Rightarrow y^{t}b = 0$, for every $y \in \mathbb{Q}^{m}$. (This is because the set of rational numbers of the form $y^{t}b$ for some $y \in \mathbb{Q}^{m}$ with $y^{t}A = 0$ is a \mathbb{Q} -linear subspace of \mathbb{Q} , and hence trivial since it is contained in \mathbb{Z} , by (4).) Applying Proposition 3 to the system Φ given by Ax = y and the pair $(V, M) = (\mathbb{Q}, \mathbb{Z})$, we obtain an $r \times m$ -matrix C (for some r) and an $s \times m$ -matrix D (for some s) with rational entries, such that for any $y \in \mathbb{Z}^{m}$:

(*) there is $x \in \mathbb{Q}^n$ with $x_1, \ldots, x_d \in \mathbb{Z}$ such that Ax = y

if and only if $Cy \in \mathbb{Z}^r$ and Dy = 0.

We now want to prove that there is some $x \in \mathbb{Q}^n$ solving the system

$$Ax = b \& x_1, \dots, x_d \in \mathbb{Z}.$$

By (*), this means that we need to show $Cb \in \mathbb{Z}^r$ and Db = 0, that is, $c^t b \in \mathbb{Z}$ and $d^t b = 0$ for every row c^t of C and every row d^t of D. By assumption this holds provided $c^t A \in \mathbb{Z}^d \times \{0\}^{n-d}$ and $d^t A = 0$ for every such c^t and d^t ; equivalently, with $a_1, \ldots, a_n \in \mathbb{Z}^m$ denoting the columns of A, if

- (1) $Ca_i \in \mathbb{Z}^r$, $Da_i = 0$ for $i = 1, \ldots, d$, and
- (2) $Ca_i = 0, Da_i = 0$ for i = d + 1, ..., n.

Clearly (1) follows from (*), since $Ae_i = a_i$, where e_i is the *i*th standard basis vector of \mathbb{Q}^n . So if d = n (the case of Proposition 1) we are already done. In general, to show (2) use the same argument, with (*) replaced by

(**)
$$CAx = 0$$
 and $DAx = 0$ for all $x \in \mathbb{Q}^n$ with $x_1 = \cdots = x_d = 0$.

To see (**) note that by (*) the \mathbb{Q} -linear subspace of \mathbb{Q}^r consisting of all vectors of the form CAx with $x \in \mathbb{Q}^n$ and $x_1 = \cdots = x_d = 0$ is contained in \mathbb{Z}^r , hence trivial.

We now prove Proposition 3. First, by multiplying both sides of every condition $f(X, Y) \in a\mathbb{Z}$ in Φ , where $f \neq 0$, with a common denominator of all nonzero coefficients of f, we may achieve that every f has integer coefficients. Next successively eliminate from Φ the conditions $f(X, Y) \in aM$ with nonzero a by iterating the following step: if Φ contains such a condition, introduce a new indeterminate X_0 and replace the condition $f(X, Y) \in a\mathbb{Z}$ in Φ by the equation $f(X, Y) - aX_0 = 0$; then for any $x \in V^n$ and $y \in V^k$ with $x_1, \ldots, x_d \in M^d$, the tuple (x, y) satisfies Φ if and only if there is $x_0 \in M$ such that (x', y), where $x' = (x_0, \ldots, x_n)$, satisfies the new system Φ' . Now rename the indeterminates X_0, \ldots, X_n into resp. X_1, \ldots, X_{n+1} in Φ' , and replace Φ by Φ' and d by d + 1.

Hence we may assume that Φ is given by AX = CY where A is an $m \times n$ matrix and C is an $m \times k$ -matrix, both having integer entries. (Here we think of X and Y as column vectors of indeterminates.) It is well-known that one can construct an $m \times m$ -matrix P and an $n \times n$ -matrix Q, both having integer entries and being invertible over \mathbb{Z} , such that $D := PAQ \in \mathbb{Z}^{m \times n}$ is a diagonal matrix (Smith normal form). Thus for every $y \in V^k$, the existence of $x \in V^n$ such that Ax = Cy is equivalent to the existence of $z \in V^n$ such that Dz = (PC)y, and similarly with " M^n " in place of " V^n ". Thus in both the case where d = 0 (no integrality requirements on the x_i) or d = n (all x_i are required to be integral) we may, after replacing (A, C) by (D, PC), reduce to the case that A is a diagonal matrix. Suppose for a moment that indeed d = 0 or d = n, and A is diagonal, with diagonal entries a_1, \ldots, a_μ (where $\mu := \min\{m, n\}$). Let also c_1^t, \ldots, c_m^t be the rows of C. Then the *i*th equation of Φ has the form

$$\begin{cases} c_i^{\mathsf{t}} Y = a_i X_i & \text{if } i \in \{1, \dots, \mu\}, \\ c_i^{\mathsf{t}} Y = 0 & \text{if } i \in \{\mu + 1, \dots, m\} \end{cases}$$

Thus in the case d = 0, the system Γ obtained from Φ by deleting all equations of the form $c_i^t Y = a_i X_i$ with nonzero a_i does the job. For d = n, which is the case used in the proof of Kronecker's theorem (Proposition 1), a system Γ with the required property may be obtained from Φ by simply replacing each condition $c_i^t Y = a_i X_i$ by $c_i^t Y \in a_i M$. Thus we have shown Proposition 3 in both the cases d = 0 and d = n. The general case now follows by first eliminating the variables X_{d+1}, \ldots, X_n from Φ , using the case d = 0, and then eliminating the integral variables X_1, \ldots, X_n from the resulting system, using the case d = n.

It is clear from the proof just given that Proposition 3 remains true if \mathbb{Z} is replaced by a principal ideal domain R, \mathbb{Q} with its fraction field, and (V, M) ranges over all pairs consisting of a K-linear space V and an R-submodule M of V. (This is because the only relevant property of \mathbb{Z} used in the proof of Proposition 3 is that every matrix over \mathbb{Z} is equivalent to a diagonal matrix, and this continues to hold over principal ideal domains.) Thus Theorem 2 remains true if \mathbb{Z} is replaced by a principal ideal domain which is not a field, \mathbb{Q} with its fraction field K, and \mathbb{R} with any K-linear space extending K.

Proposition 3 may also be generalized in a different direction. In order to explain this, we first define:

Definition 4. A real-integer system of linear conditions in X with d integral variables (short: a real-integer system) is a finite collection $\Phi = \Phi(X)$ of conditions either of the type

$$(\diamond) \qquad f(X) \in aM \quad \text{or} \quad f(X) \notin aM$$

where f(X) is a homogeneous linear form in $X = (X_1, \ldots, X_n)$ with integer coefficients, and a is an integer (with a = 0 allowed). A solution of such a real-integer system Φ in a given pair (V, M) is a tuple $x = (x_1, \ldots, x_n)$ where $x_1, \ldots, x_d \in M$ and $x_{d+1}, \ldots, x_n \in V$, satisfying each of the conditions specified in Φ .

Proposition 3 deals exclusively with *positive* real-integer systems, i.e., systems E as above in which no conditions (\diamond) of the form $f(X) \notin aM$ appear. It may be rephrased as saying: given a positive real-integer system Φ in (X, Y) with d integral variables X_1, \ldots, X_d , one can constructively obtain a positive real-integer system Γ in Y with no integral variables such that for any (V, M), a tuple $y \in V^k$ can be expanded to a solution (x, y) to the system Φ if and only if y is a solution to Γ . An analogue of this fact for general real-integer systems holds. However, we have to place some restrictions on the admissible pairs (V, M): for example, consider the system $\Phi = \Phi(X)$ with n = d > 1 and k = 0 given by

$$(1/n)(X_i - X_j) \notin M$$
 for $1 \le i < j \le n$,

which has a solution in (\mathbb{Q}, \mathbb{Z}) , but not in the trivial pair (0, 0). This turns out to be the only obstruction:

Definition 5. We call (V, M) a real-integer structure if |M/pM| = p for every prime number p.

Clearly (\mathbb{Q}, \mathbb{Z}) and (\mathbb{R}, \mathbb{Z}) are real-integer structures. More exotic examples may be obtained as follows: let V be a nontrivial \mathbb{Q} -linear space, v an arbitrary nonzero vector in V, and W a \mathbb{Q} -linear subspace of V with $\mathbb{Q}v \cap W = \{0\}$; then (V, M)where $M = \mathbb{Z}v \oplus W$ is a real-integer structure. Every torsion-free abelian group Mwith |M/pM| = p arises as the distinguished subgroup of a real-integer structure (V, M) (take V = the divisible hull of M). It is easy to see that if (V, M) is a real-integer structure, then |aM/bM| = a/b for all nonzero integers a, b with b|a. Note also that $V \neq M$ (since the abelian group V is divisible, whereas M isn't) and M is infinite (since a finite abelian group is p-divisible for every prime p not dividing its order). For later use, we also observe:

Lemma 6. Let $a \in \mathbb{Q}^n$ be nonzero and $q \in \mathbb{Q}$. Then for every real-integer structure (V, M) and $v \in V$ there exist infinitely many $x \in V^n$ such that $a^{t}x \notin v + qM$.

Proof. It is enough to show this for n = 1, a = 1. The case q = 0 is clear, and if $q \neq 0$, then for every real-integer structure (V, M), the set $V \setminus (v + qM)$ is in bijection with the infinite set $V \setminus M$.

Here now is the promised version of Proposition 3 for real-integer systems:

Proposition 7. There is an algorithm which computes, upon input of a real-integer system Φ in (X, Y) with d integral variables, finitely many real-integer systems $\Gamma_1, \ldots, \Gamma_r$ in Y with no integral variables, such that for every real-integer structure (V, M) and every $y \in V^k$, the following are equivalent:

- (1) There is some $x \in V^n$ such that (x, y) is a solution of Φ in (V, M);
- (2) there is some $i \in \{1, ..., r\}$ such that y is a solution of Γ_i in (V, M).

This result is at the same time more general and less precise than Proposition 3: it applies to arbitrary real-integer systems (rather than only positive ones); however, this comes at the cost of having to restrict to solvability in real-integer structures (rather than arbitrary pairs (V, M)), and possibly having to introduce more than one system Γ_i . It is a variation of a classical result due to Szmielew [13] (with a simpler proof for the special case required here in [18]):

Proposition 8. Given a real-integer system Φ in the n+k integral variables (X, Y), one can construct finitely many real-integer systems $\Gamma_1, \ldots, \Gamma_r$ in the k integral variables Y such that the statements (1) and (2) in Proposition 7 are equivalent for every real-integer structure (V, M) and every $y \in M^k$.

To show how this implies Proposition 7, we may assume, as in the beginning of the proof of Proposition 3, that Φ is given to us in the form

 $AX = CY \quad \& \quad f_1(X) + g_1(Y) \notin d_1M \quad \& \cdots \& \quad f_l(X) + g_l(Y) \notin d_lM$

where A is an $m \times n$ -matrix, C is an $m \times k$ -matrix (for some m), both with integer entries, the f_j , g_j are homogeneous linear forms with integer coefficients, and $d_j \in \mathbb{Z}$. Moreover, as in the proof of Proposition 3, it is enough to show two special cases, formulated in the next two lemmas, in the situation where A is a diagonal matrix. Let a_1, \ldots, a_{μ} , where $\mu := \min\{m, n\}$, be the diagonal entries of A, and let c_1^1, \ldots, c_m^t be the rows of C.

Lemma 9. Proposition 7 holds provided we restrict to real-integer systems Φ with no integral variables.

Proof. After replacing, for every *i* with $a_i \neq 0$, each occurrence of X_i in the conditions $f_j(X) + g_j(Y) \notin d_j M$ by $(1/a_i)c_i^{t}Y$, we may reduce to A = the zero matrix. After reordering, we may also assume that $f_1, \ldots, f_s \neq 0$ and $f_{s+1} = \cdots = f_l = 0$. Then, by Lemma 6, a single system Γ_i , namely

$$Cy = 0$$
 & $g_1(Y) \notin d_1M$ & \cdots & $g_s(Y) \notin d_sM$,

does the job.

Lemma 10. Proposition 7 holds for Φ with d = n integral variables.

Proof. For every i with $a_i \neq 0$, replace each occurrence of X_i in the conditions $f_j(X) + g_j(Y) \notin d_j M$ by $(1/a_i)c_i^{t}Y$, and each equation $a_i X_i = c_i^{t}Y$ in the system AX = CY by the condition $c_i^{t}Y \in a_i M$. The resulting real-integer system has the same solutions in every real-integer structure as the original system Φ . After changing notation, we may assume it has the form

 $\Psi(Y) \quad \& \quad f_1(X) + g_1(Y) \notin d_1M \quad \& \cdots \& \quad f_l(X) + g_l(Y) \notin d_lM$

where Ψ is a real-integer system in Y. Now let $Z = (Z_1, \ldots, Z_l)$ be a tuple of new indeterminates, and let J range over subsets of $\{1, \ldots, l\}$. Let $\Psi_J(X, Z)$ be the real-integer system (with n integral variables) consisting of the conditions

$$f_j(X) + Z_j \notin d_j M \qquad (j \in J)$$

Applying Proposition 8, we find real-integer systems

 $\Psi_{J,1}(Z), \ldots, \Psi_{J,t_J}(Z)$ (for some integer $t_J \ge 0$)

with the following property: for each real-integer structure (V, M) and $z \in M^l$,

z is a solution to one of $\Psi_{J,1}, \ldots, \Psi_{J,t_J}$ if and only if

there is an $x \in M^n$ such that (x, z) is a solution to Ψ_J .

Now for each J and $s = 1, ..., t_J$ let $\Gamma_{J,s}(Y)$ be the real-integer system (without integral variables) consisting of the following conditions:

(1) $\Psi(Y)$, (2) $g_j(Y) \notin M \ (j \in \{1, \dots, l\} \setminus J)$, (3) $g_j(Y) \in M \ (j \in J)$, and (4) $\Phi_{J,s}(g_1(Y), \dots, g_l(Y))$.

It is easily seen that the systems $\Gamma_{J,s}$ have the required property.

By Proposition 7 (applied in the case k = 0) there is an algorithm which decides, upon input of a real-integer system ϕ in X, whether Φ has a solution in some (or equivalently, every) real-integer structure. This should be contrasted with [1], which shows that no analogous result holds if (V, M) ranges over *arbitrary* abelian groups V with distinguished subgroup M.

Proposition 7 also has a completely model-theoretic proof (we won't give it here) which avoids manipulations with real-integer systems and replaces them with proofs of extension statements for morphisms of real-integer structures. For other model-theoretic aspects of *torsion-free* abelian groups with distinguished subgroup see [5] (with simplifications in [8]).

An elimination theorem for mixed real-integer systems incorporating (possibly inhomogeneous) inequalities was first proved by Skolem [11] (see also [12], III.4, Exercise 15), and later independently rediscovered by Miller [7] and Weispfenning [15]. For other applications of a related elimination result (for Presburger arithmetic) to integer programming see [16].

References

- W. Baur, Undecidability of the theory of Abelian groups with a subgroup, Proc. Amer. Math. Soc. 55 (1976), 125–129.
- 2. A. Dax, An elementary proof of Farkas' lemma, SIAM Rev. 39 (1997), no. 3, 503-507.
- J. Farkas, Über die Theorie der einfachen Ungleichungen, J. Reine Angew. Math. 124 (1902), 1–27.

- M. Köppe and R. Weismantel, *Cutting planes from a mixed integer Farkas lemma*, Oper. Res. Lett. **32** (2004), no. 3, 207–211.
- 5. G. T. Kozlov and A. I. Kokorin, The elementary theory of Abelian groups without torsion with a predicate selecting a subgroup, Algebra and Logic 8 (1969), 182–190.
- L. Kronecker, Näherungsweise ganzzahlige Auflösung linearer Gleichungen, Monatsberichte Königl. Preuss. Akad. Wiss. Berlin (1884), 1179–1193 and 1271–1299.
- C. Miller, Expansions of dense linear orders with the intermediate value property, J. Symbolic Logic 66 (2001), no. 4, 1783–1790.
- P. H. Schmitt, The elementary theory of torsionfree Abelian groups with a predicate specifying a subgroup, Z. Math. Logik Grundl. Math. 28 (1982), 323–329.
- P. Scowcroft, Nonnegative solvability of linear equations in certain ordered rings, Trans. Amer. Math. Soc. 358 (2006), no. 8, 3535–3570 (electronic).
- 10. _____, Generalized halfspaces in dimension groups, preprint, 2007.
- T. Skolem, Über einige Satzfunktionen in der Arithmetik, Skr. Norske Vidensk. Akad., Oslo, Math.-naturwiss. Kl. 7 (1931), 1–28.
- 12. C. Smoryński, *Logical Number Theory*, I, An Introduction, Universitext, Springer-Verlag, Berlin, 1991.
- 13. W. Szmielew, Elementary properties of Abelian groups, Fund. Math. 41 (1955), 203-271.
- R. V. Vohra, The ubiquitous Farkas Lemma, in: F. B. Alt et al. (eds.), Perspectives in Operations Research, Operations Research/Computer Science Interfaces Series vol. 36, pp. 199–210, Springer-Verlag, New York, 2006.
- V. Weispfenning, Mixed real-integer linear quantifier elimination, in: Proceedings of the 1999 International Symposium on Symbolic and Algebraic Computation (Vancouver, BC), 129–136 (electronic), ACM, New York, 1999.
- H. P. Williams, Fourier-Motzkin elimination extension to integer programming problems, J. Combinatorial Theory Ser. A 21 (1976), no. 1, 118–123.
- 17. _____, The equivalence of two theorems of integer programming, Bull. London Math. Soc. 28 (1996), no. 3, 311–316.
- E. Zakon, Model-completeness and elementary properties of torsion free abelian groups, Canad. J. Math. 26 (1974), 829–840.

E-mail address: maschenb@math.uic.edu URL: http://www.math.uic.edu/~maschenb

DEPARTMENT OF MATHEMATICS, STATISTICS, AND COMPUTER SCIENCE, UNIVERSITY OF ILLINOIS AT CHICAGO, 851 S. MORGAN ST. (M/C 249), CHICAGO, IL 60607-7045, U.S.A.