MATHEMATICS OF OPERATIONS RESEARCH
Vol. 27, No. 3, August 2002, pp. 470–484
Printed in U.S.A.

COMBINING PROBLEM STRUCTURE WITH BASIS REDUCTION TO SOLVE A CLASS OF HARD INTEGER PROGRAMS

QUENTIN LOUVEAUX AND LAURENCE A. WOLSEY

Recently Aardal et al. (2000) have successfully solved some small, difficult, equality-constrained integer programs by using basis reduction to reformulate the problems as inequality-constrained integer programs in a different space. Here, we adapt their method to solve integer programs that are larger but have special structure. The practical problem motivating this work is a variant of the market share problem. More formally, the problem can be viewed as finding a matrix $X \in \mathbb{Z}_+^{mn}$ satisfying $XA = C$, $BX = D$, where A, B, C, D are matrices of compatible dimensions, and the approach requires us to find a reduced basis of the lattice $\mathscr{L} = \{X \in \mathbb{Z}^{m\times n} : XA = 0, BX = 0\}$.

The main topic of this paper is a study of the lattice $\mathscr{L}$. It is shown that an integer basis of $\mathscr{L}$ can be obtained by taking the Kronecker product of vectors from integer bases of two much smaller lattices. Furthermore, the resulting basis is a reduced basis if the integer bases of the two small lattices are reduced bases and a suitable ordering is chosen.

Finally, some limited computational results are presented showing the benefits of making use of the problem structure.

1. Introduction. Consider a banker who must establish a certain number of portfolios for his clients. Client i's portfolio must consist of d_i shares, and the banker holds a_j shares of type j, whose estimated profit per share is p_j. The banker's problem is to divide up the $\sum_j a_j$ shares among the clients so that the expected profit per share of each client is as close as possible to the average value. Mathematically, he has the problem of finding a solution of

$$(1)\qquad \begin{cases} \sum_j x_{ij} = d_i & 1 \le i \le m \\ \sum_i x_{ij} = a_j & 1 \le j \le n \\ \frac{1}{d_i}\left(\sum_j p_j x_{ij}\right) \simeq \bar{c} & 1 \le i \le m \\ x \in \mathbb{Z}_+^{mn}, & \end{cases}$$

where $\bar{c}$ is the average expected profit $\left(\sum_i \sum_j p_{ij} x_{ij}\right) / \sum_{ij} x_{ij}$ and $\simeq$ means that we want to be as close as possible to equality. One natural way to attempt to solve this problem is to introduce nonnegative slack variables s_i^+ and s_i^-, write $(1/d_i)\sum_j p_j x_{ij} + s_i^+ - s_i^- = \bar{c}$, take as objective function $\min \sum_i s_i^+ + \sum_i s_i^-$, and then solve the resulting mixed-integer program with a commercial system such as Cplex or Xpress. However, this does not work. Even for small problems with $m = 6$ clients and $n = 15$ share types, an optimal solution cannot be found within hours.

The banker's problem is a variant with integer variables of the market share problem (Williams 1993). An alternative viewpoint is to see it as a closest vector problem. Specifically, we have to find a nonnegative integer combination of the vectors $(\underline{e}_i, \underline{e}_j, p_j \underline{e}_i)^T$ that is as close as possible to the vector $(\underline{d}, \underline{a}, \bar{c}\underline{d})^T$.

Received November 14, 2000; revised December 7, 2001.
MSC 2000 subject classification. Primary: 90C10.
OR/MS subject classification. Primary: Programming/integer.
Key words. Integer programming, basis reduction, lattices, market share problem.

0364-765X/02/2703/0470/$05.00
1526-5471 electronic ISSN, © 2002, INFORMS

We now develop another approach allowing us to tackle the problem. Consider the problem of finding feasible solutions of equality-constrained integer programs or, more specifically, of finding points in the set

$$Z = \{x \in \mathbb{Z}_+^N : Ax = b\},$$

where $A \in \mathbb{Z}^{M\times N}$ and $b \in \mathbb{Z}^M$. For this problem, Aardal et al. (2000) have recently developed a successful two-step approach based on basis reduction (Lenstra et al. 1982). In Step 1, they use basis reduction on the associated lattice

$$\begin{pmatrix} I & 0 \\ 0 & 1 \\ A & -b \end{pmatrix}$$

of dimension $N+M+1$ to construct an alternative representation of the feasible set Z of the form

$$Z = \{x : x = q + P\lambda,\ \lambda \in \mathbb{Z}^{N-M},\ x \geq 0\}, \tag{2}$$

where q is an integer vector and P an integer matrix, $Aq = b$, P is an integral basis of the null space of A and due to the basis reduction algorithm, the vector q and the columns of P are "short." In Step 2, they apply a mixed-integer programming (MIP) system to the reformulated set Z with $\lambda \in \mathbb{Z}^{N-M}$ as the variables. For small instances of the banker's problem, this approach works, whereas the original MIP approach does not.

However, difficulties arise when we try to solve larger instances by this approach. The dimension of the lattice to be reduced is $(M+N+1)$, and the basis reduction algorithm is $\mathcal{O}((M+N)^4)$ (Cohen 1996, Joux 1998). For $M+N$ greater than 300, the basis reduction algorithm becomes too time consuming. To overcome this difficulty, we propose to take advantage of the special structure of Z. Specifically, we consider sets of the form

$$Z = \{X \in \mathbb{Z}_+^{m\times n} : XA = C,\ BX = D\}, \tag{3}$$

where $A \in \mathbb{Z}^{n\times K}$, $B \in \mathbb{Z}^{L\times m}$, $C \in \mathbb{Z}^{m\times K}$, and $D \in \mathbb{Z}^{L\times n}$. Note that with

$$A = \begin{pmatrix} 1 & \cdots & 1 \\ p_1 & \cdots & p_n \end{pmatrix}^T$$

and $B = (1 \ \cdots \ 1)$, we obtain the system (1) arising in the banker's problem presented above.

For the system (3), the direct approach of Aardal et al. (2000) involves reducing a basis of dimension $(mn+Km+Ln+1)$, which is impractical. Instead, we work with the separate lattices $\mathcal{L}_A = \{\underline{x} \in \mathbb{Z}^n : \underline{x}A = \underline{0}\}$ and $\mathcal{L}_B = \{\underline{x} \in \mathbb{Z}^m : B\underline{x} = \underline{0}\}$, and we use the same approach to compute bases of $\mathcal{L}_A$ and $\mathcal{L}_B$ and use the resulting basis vectors to construct a reduced basis for the large lattice

$$\mathcal{L} = \{X \in \mathbb{Z}^{m\times n} : XA = \underline{\underline{0}}, BX = \underline{\underline{0}}\}.$$

In §2, we present the class of problems to be studied, and we show how its structure allows us to construct an integral basis of the large lattice $\mathcal{L}$ from integral bases of the two small lattices. In §3, we show that, when the bases of the small lattices are reduced bases, the basis constructed in §2 is also a reduced basis. In §4, we present computational results for the banker's problem with the original reduced basis approach and with our decomposition approach. Finally, in §5, we conclude and discuss some open questions, see Schrijver (1986) for some basics on lattices and reduced bases.

Notation. Throughout the paper, we use the following notation:

- An underlined letter $\underline{a}$ represents a vector (but of any dimension).
- a_i represents the ith component of the vector $\underline{a}$.

- $\underline{a}^p$ represents the pth vector of a collection of vectors.
- $\underline{a}_i^p$ represents the ith component of the pth vector of the collection.
- A capital letter A or a double underlined letter $\underline{\underline{a}}$ represents a matrix.

2. Constructing an integral basis for $\mathscr{L}$. The problem we address in this section is to find an alternative representation of

$$\mathscr{L} = \{X \in \mathbb{Z}^{m\times n} : XA = \underline{\underline{0}}, BX = \underline{\underline{0}}\}, \tag{4}$$

with given matrices $A \in \mathbb{Z}^{n\times K}$, with $K \le n$ of rank K, and $B \in \mathbb{Z}^{L\times m}$, with $L \le m$ of rank L.

Considering the second equation of (4), each column of X has to be a solution of the system $B\underline{x} = \underline{0}$. Let $\underline{\underline{\beta}} = (\underline{\beta}^1 \cdots \underline{\beta}^{m-L})$ denote an integral basis of the lattice $\mathscr{L}_B = \{x \in \mathbb{Z}^m : B\underline{x} = \underline{0}\}$. Thus, each matrix $X \in \mathscr{L}$ can be written

$$X = \underline{\underline{\beta}} \begin{pmatrix} \underline{\lambda}^1 \\ \vdots \\ \underline{\lambda}^{m-L} \end{pmatrix}, \tag{5}$$

with $\underline{\lambda}^1, \dots, \underline{\lambda}^{m-L} \in \mathbb{Z}^n$. Similarly, we can use an integer basis of the lattice $\mathscr{L}_A = \{x \in \mathbb{Z}^n : \underline{x}A = \underline{0}\}$ to describe the vectors of $\mathscr{L}$. Letting

$$\underline{\underline{\alpha}} = \begin{pmatrix} \underline{\alpha}^1 \\ \vdots \\ \underline{\alpha}^{n-K} \end{pmatrix}$$

be such an integral basis, each solution X of (4) can be written as

$$X = \big(\underline{\mu}^1 \cdots \underline{\mu}^{n-K}\big)\underline{\underline{\alpha}}, \tag{6}$$

where $\underline{\mu}^1, \dots, \underline{\mu}^{n-K} \in \mathbb{Z}^m$.

Now we can state the main result of this section.

THEOREM 2.1. *The matrices $X \in \mathscr{L}$ are precisely the matrices of the form*

$$X = \underline{\underline{\beta}}\Lambda\underline{\underline{\alpha}}, \tag{7}$$

with $\Lambda \in \mathbb{Z}^{(m-L)\times(n-K)}$.

To prove this theorem, we need several intermediate results.

OBSERVATION 2.2. For fixed unimodular matrices $M \in \mathbb{Z}^{m\times m}$ and $N \in \mathbb{Z}^{n\times n}$, any $Y \in \mathbb{Z}^{m\times n}$ can be written as

$$Y = M\Lambda N, \tag{8}$$

with $\Lambda \in \mathbb{Z}^{m\times n}$.

PROOF. This is obvious by taking $\Lambda = M^{-1}YN^{-1}$, which is integral. □

For details about the Smith normal form of a matrix used in the next two lemmas, see the appendix and, for example, Newman (1972).

LEMMA 2.3. *Consider the lattice $\{\underline{x} \in \mathbb{Z}^n : C\underline{x} = \underline{0}\}$, where $C \in \mathbb{Z}^{m\times n}$, $m \le n$, and* $\operatorname{rank}(C) = m$. *Let $Y = (\underline{y}^1, \dots, \underline{y}^{n-m}) \in \mathbb{Z}^{n\times(n-m)}$ be a set of solutions of $C\underline{x} = \underline{0}$, then the* *following statements are equivalent*:

(i) *The Smith normal form of* Y *is* $\binom{I}{0}$.

(ii) Y *is an integer basis of the lattice.*

Proof. This result appears to be known, but for completeness, a proof is given in the appendix. □

Lemma 2.4. *A matrix* $Y \in \mathbb{Z}^{n\times(n-m)}$ *whose Smith normal form is* $\binom{I}{0}$ *can be extended to a unimodular matrix.*

Proof. There exist unimodular matrices M and N such that

$$Y = (M_1\ M_2)\begin{pmatrix} I \\ 0 \end{pmatrix} N,$$

with $M_1 \in \mathbb{Z}^{n\times(n-m)}$, $M_2 \in \mathbb{Z}^{n\times m}$. Thus, we have that

$$Y = M_1 N.$$

Now, consider the completion $(Y\ M_2)$, we have that

$$(Y\ M_2) = (M_1 N\ M_2) = (M_1\ M_2)\begin{pmatrix} N & 0 \\ 0 & I \end{pmatrix}.$$

Thus,

$$|\det(Y\ M_2)| = |\det M||\det N||\det I| = 1,$$

and M_2 completes Y as a unimodular matrix. □

Proof of Theorem 2.1. By using the two lemmas, we know that we can complete $\underline{\underline{\alpha}}$ and $\underline{\underline{\beta}}$ into unimodular matrices. We denote these completions by $\underline{\underline{\alpha}}^c$ and $\underline{\underline{\beta}}^c$. Therefore, by Observation 2.2, $X \in \mathbb{Z}^{m\times n}$ can be expressed as

$$X = \begin{pmatrix} \underline{\underline{\beta}} & \underline{\underline{\beta}}^c \end{pmatrix}\begin{pmatrix} \Lambda_1 & \Lambda_2 \\ \Lambda_3 & \Lambda_4 \end{pmatrix}\begin{pmatrix} \underline{\underline{\alpha}} \\ \underline{\underline{\alpha}}^c \end{pmatrix},$$

or expanding

$$\begin{aligned} X &= \begin{pmatrix} \underline{\underline{\beta}}\Lambda_1 + \underline{\underline{\beta}}^c\Lambda_3 & \underline{\underline{\beta}}\Lambda_2 + \underline{\underline{\beta}}^c\Lambda_4 \end{pmatrix}\begin{pmatrix} \underline{\underline{\alpha}} \\ \underline{\underline{\alpha}}^c \end{pmatrix} \\ &= \left(\underline{\underline{\beta}}\Lambda_1 + \underline{\underline{\beta}}^c\Lambda_3\right)\underline{\underline{\alpha}} + \left(\underline{\underline{\beta}}\Lambda_2 + \underline{\underline{\beta}}^c\Lambda_4\right)\underline{\underline{\alpha}}^c. \end{aligned}$$

Recall that each solution of (4) can be written in both forms (5) and (6). From the necessary condition (6), we see that X must be a combination of the columns of $\underline{\underline{\alpha}}$. Because $\underline{\underline{\alpha}}$ and $\underline{\underline{\alpha}}^c$ are linearly independent, $\underline{\underline{\beta}}\Lambda_2 + \underline{\underline{\beta}}^c\Lambda_4 = \underline{\underline{0}}$. However, now, because the columns of $\underline{\underline{\beta}}$ and $\underline{\underline{\beta}}^c$ are linearly independent, we can conclude that, for each solution X of (4),

$$\Lambda_2 = \Lambda_4 = \underline{\underline{0}}.$$

Identically, by taking the condition (5), we can conclude that

$$\Lambda_3 = \Lambda_4 = \underline{\underline{0}}.$$

Hence,

$$X = \begin{pmatrix} \underline{\underline{\beta}} & \underline{\underline{\beta}}^c \end{pmatrix}\begin{pmatrix} \Lambda_1 & \underline{\underline{0}} \\ \underline{\underline{0}} & \underline{\underline{0}} \end{pmatrix}\begin{pmatrix} \underline{\underline{\alpha}} \\ \underline{\underline{\alpha}}^c \end{pmatrix},$$

and the set of solutions of (4) can be characterized as

$$X = \underline{\underline{\beta}}\Lambda_1\underline{\underline{\alpha}}$$

for a $\Lambda_1 \in \mathbb{Z}^{(m-L)\times(n-K)}$. Conversely, it is clear that every X of this form is a member of (4). □

We have a general form of the vectors of (4). Now, we introduce some classical notions that allow us to simplify notation.

Definition 2.1. Given a matrix Y, $\text{vec}(Y)$ denotes the column composed of the first column of Y followed by the second, etc.

Definition 2.2. The Kronecker product of two matrices $C \in \mathbb{R}^{m\times n}$ and $D \in \mathbb{R}^{p\times q}$ is

$$C \otimes D = \begin{pmatrix} c_{11}D & \cdots & c_{1n}D \\ \vdots & \ddots & \vdots \\ c_{m1}D & \cdots & c_{mn}D \end{pmatrix},$$

belonging to $\mathbb{R}^{mp\times nq}$.

Proposition 2.5. *For matrices C, Y, D such that CYD exists,*

$$\text{vec}(CYD) = (D^T \otimes C)\,\text{vec}(Y).$$

Proof. See, for example, Lancaster and Tismenetsky (1985). □

Proposition 2.6. $(\underline{\underline{\alpha}}^T \otimes \underline{\underline{\beta}})$ *is a basis for the vectorized solutions of* (4).

Proof. Applying Proposition 2.7 to the matrix X given by Theorem 2.1, we obtain

$$\text{vec}(X) = (\underline{\underline{\alpha}}^T \otimes \underline{\underline{\beta}})\,\text{vec}(\Lambda). \quad \square$$

So in other words, a basis for $\mathscr{L}$ is obtained by taking the Kronecker product of the bases $\underline{\underline{\alpha}}$ and $\underline{\underline{\beta}}$ of $\mathscr{L}_A$ and $\mathscr{L}_B$, respectively.

Example. Consider the following linear system with $m = 3$ and $n = 4$.

$$\left.\begin{aligned} &x_{11} + x_{21} + x_{31} = 0 \\ &x_{12} + x_{22} + x_{32} = 0 \\ &x_{13} + x_{23} + x_{33} = 0 \\ &x_{14} + x_{24} + x_{34} = 0 \end{aligned}\right\} \text{Equations } BX = \underline{\underline{0}}$$

$$\left.\begin{aligned} &x_{11} + x_{12} + x_{13} + x_{14} = 0 \\ &16x_{11} + 57x_{12} + 23x_{13} + 66x_{14} = 0 \\ &x_{21} + x_{22} + x_{23} + x_{24} = 0 \\ &16x_{21} + 57x_{22} + 23x_{23} + 66x_{24} = 0 \\ &x_{31} + x_{32} + x_{33} + x_{34} = 0 \\ &16x_{31} + 57x_{32} + 23x_{33} + 66x_{34} = 0 \end{aligned}\right\} \text{Equations } XA = \underline{\underline{0}}$$

$$x_{ij} \in \mathbb{Z}, \quad \text{for } i = 1, \ldots, 3 \text{ and } j = 1, \ldots, 4.$$

The set of solutions form a lattice $\mathscr{L} = \{X \in \mathbb{Z}^{3\times 4} : XA = 0, BX = 0\}$, with

$$A = \begin{pmatrix} 1 & 16 \\ 1 & 57 \\ 1 & 23 \\ 1 & 66 \end{pmatrix}, \quad B = (1\ 1\ 1) \quad \text{and} \quad X = \begin{pmatrix} x_{11} & x_{12} & x_{13} & x_{14} \\ x_{21} & x_{22} & x_{23} & x_{24} \\ x_{31} & x_{32} & x_{33} & x_{34} \end{pmatrix}.$$

By Proposition 2.6, an integer basis can be found by computing the integer bases of the two lattices separately. First of all, we consider the lattice $\mathscr{L}_B$

$$(1\ 1\ 1)\begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = 0, \quad y_1, y_2, y_3 \in \mathbb{Z}.$$

It is readily verified that

$$\underline{\underline{\beta}} = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \end{pmatrix}^T$$

is an integer basis of $\mathscr{L}_B$ (such a basis can be found by basis reduction). Similarly, for the lattice $\mathscr{L}_A$,

$$(y_1\ y_2\ y_3\ y_4)\begin{pmatrix} 1 & 16 \\ 1 & 57 \\ 1 & 23 \\ 1 & 66 \end{pmatrix} = (0\ 0), \quad y_1, y_2, y_3, y_4 \in \mathbb{Z},$$

an integer basis

$$\underline{\underline{\alpha}} = \begin{pmatrix} -1 & -4 & 2 & 3 \\ 10 & -3 & -11 & 4 \end{pmatrix}$$

is obtained. Taking the Kronecker product of the two bases, we obtain that

$$(\underline{\underline{\alpha}}^T \otimes \underline{\underline{\beta}}) = \begin{pmatrix} -1 & 1 & 0 & -4 & 4 & 0 & 2 & -2 & 0 & 3 & -3 & 0 \\ 0 & -1 & 1 & 0 & -4 & 4 & 0 & 2 & -2 & 0 & 3 & -3 \\ 10 & -10 & 0 & -3 & 3 & 0 & -11 & 11 & 0 & 4 & -4 & 0 \\ 0 & 10 & -10 & 0 & -3 & 3 & 0 & -11 & 11 & 0 & 4 & -4 \end{pmatrix}^T$$

is a basis of the lattice $\mathscr{L}$.

3. A reduced basis of $\mathscr{L}$. In this section, we show that, up to a reordering of the vectors, the basis constructed by computing the Kronecker product of reduced bases of the small lattices is itself reduced. Observe that each row of the Kronecker product of the two matrices $\underline{\underline{\alpha}}$ and $\underline{\underline{\beta}}$ is the Kronecker product of a row (basis vector) of $\underline{\underline{\alpha}}$ with a column of $\underline{\underline{\beta}}$ (basis vector). We also need to take scalar products of such vectors.

PROPOSITION 3.1. *Let $\underline{v}^1 := \underline{\gamma}^1 \otimes \underline{\delta}^1$ and $\underline{v}^2 := \underline{\gamma}^2 \otimes \underline{\delta}^2$ with $\underline{\gamma}^i \in \mathbb{R}^n$ and $\underline{\delta}^i \in \mathbb{R}^m$. Then*

$$\langle \underline{v}^1, \underline{v}^2 \rangle = \langle \underline{\gamma}^1, \underline{\gamma}^2 \rangle \langle \underline{\delta}^1, \underline{\delta}^2 \rangle,$$

where $\langle \underline{x}, \underline{y} \rangle$ denotes the scalar product.

PROOF.

$$\begin{aligned} \langle \underline{v}^1, \underline{v}^2 \rangle &= \langle (\gamma_1^1 \underline{\delta}^1, \ldots, \gamma_n^1 \underline{\delta}^1), (\gamma_1^2 \underline{\delta}^2, \ldots, \gamma_n^2 \underline{\delta}^2) \rangle \\ &= \gamma_1^1 \gamma_1^2 \langle \underline{\delta}^1, \underline{\delta}^2 \rangle + \cdots + \gamma_m^1 \gamma_m^2 \langle \underline{\delta}^1, \underline{\delta}^2 \rangle \\ &= \langle \underline{\gamma}^1, \underline{\gamma}^2 \rangle \langle \underline{\delta}^1, \underline{\delta}^2 \rangle. \quad \square \end{aligned}$$

We also need to work with reduced bases.

DEFINITION 3.1. Given r linearly independent vectors $(\underline{b}^j) \in \mathbb{R}^n$, $(\underline{b}^j)_{j=1,\ldots,r}$ is a reduced basis if

(i) $|\mu_{ij}| \le \frac{1}{2}$ for all $i < j$,

(ii) $\|\hat{\underline{b}}^{j+1} + \mu_{j,j+1} \hat{\underline{b}}^{j}\|^2 \ge \frac{3}{4} \|\hat{\underline{b}}^{j}\|^2$ for $1 \le j \le r-1$, where $\mu_{ij} = \langle \underline{b}^j, \hat{\underline{b}}^i \rangle / \langle \hat{\underline{b}}^i, \hat{\underline{b}}^i \rangle$, and $(\hat{\underline{b}}^j)_{j=1,\ldots,r}$ is the Gram-Schmidt orthogonalization of $(\underline{b}^j)_{j=1,\ldots,r}$.

For the rest of this section, we study the integral basis $V = (\underline{v}^{pq}) = (\underline{\alpha}^p \otimes \underline{\beta}^q)$ constructed in §2, where $(\underline{\alpha}^p)_{p=1}^P$ and $(\underline{\beta}^q)_{q=1}^Q$ are now *reduced* bases with $P = n - K$ and $Q = m - L$. Let $(\hat{\underline{\alpha}}^p)_p$, $(\hat{\underline{\beta}}^q)_q$ denote the Gram-Schmidt orthogonalization of the bases $(\underline{\alpha}^p)_p$ and $(\underline{\beta}^q)_q$, respectively, with Gram-Schmidt coefficients denoted μ^α and μ^β, respectively.

We now consider possible orderings of the set V of basis vectors. Throughout this section $(p, q) < (p', q')$ means that $p \le p'$, $q \le q'$, and $(p, q) \ne (p', q')$. On the other hand, $(i, j) \prec (i', j')$ means that v^{ij} comes before $v^{i'j'}$ in the ordering.

Definition 3.2. A total ordering of the basis V is called *a monotone ordering* if, for any distinct pair of vectors $\underline{v}^{pq}$ and $\underline{v}^{p'q'}$ with $(p, q) < (p', q')$, $\underline{v}^{pq}$ precedes $\underline{v}^{p'q'}$ in the ordering (or $(p, q) \prec (p', q')$).

Proposition 3.2. *For any monotone ordering, $\prec$ of the integral basis V, $(\hat{\underline{v}}^{pq}) = (\hat{\underline{\alpha}}^p \otimes \hat{\underline{\beta}}^q)$ is the Gram-Schmidt orthogonalization of V.*

Proof. Clearly, $\hat{\underline{v}}^{11} = \underline{v}^{11} = \underline{\alpha}^1 \otimes \underline{\beta}^1 = \hat{\underline{\alpha}}^1 \otimes \hat{\underline{\beta}}^1$. We then proceed by induction on $\prec$. We have

$$\begin{aligned}
\hat{\underline{\alpha}}^p \otimes \hat{\underline{\beta}}^q &= \left(\underline{\alpha}^p - \sum_{i=1}^{p-1} \mu^\alpha_{ip} \hat{\underline{\alpha}}^i\right) \otimes \left(\underline{\beta}^q - \sum_{j=1}^{q-1} \mu^\beta_{jq} \hat{\underline{\beta}}^j\right) \text{ by the Gram-Schmidt procedure}\\
&= \underline{v}^{pq} - \underline{\alpha}^p \otimes \left(\sum_{j=1}^{q-1} \mu^\beta_{jq} \hat{\underline{\beta}}^j\right) - \left(\sum_{i=1}^{p-1} \mu^\alpha_{ip} \hat{\underline{\alpha}}^i\right) \otimes \underline{\beta}^q + \sum_{i=1}^{p-1}\sum_{j=1}^{q-1} \mu^\alpha_{ip}\mu^\beta_{jq} (\hat{\underline{\alpha}}^i \otimes \hat{\underline{\beta}}^j)\\
&= \underline{v}^{pq} - \left(\hat{\underline{\alpha}}^p + \sum_{k=1}^{p-1} \mu^\alpha_{kp} \hat{\underline{\alpha}}^k\right) \otimes \left(\sum_{j=1}^{q-1} \mu^\beta_{jq} \hat{\underline{\beta}}^j\right) - \left(\sum_{i=1}^{p-1} \mu^\alpha_{ip} \hat{\underline{\alpha}}^i\right)\left(\hat{\underline{\beta}}^q + \sum_{l=1}^{q-1} \mu^\beta_{lq} \hat{\underline{\beta}}^l\right)\\
&\quad + \sum_{i=1}^{p-1}\sum_{j=1}^{q-1} \mu^\alpha_{ip}\mu^\beta_{jq} (\hat{\underline{\alpha}}^i \otimes \hat{\underline{\beta}}^j)\\
&= \underline{v}^{pq} - \sum_{(i,j)<(p,q)} \tilde{\mu}_{ij} (\hat{\underline{\alpha}}^i \otimes \hat{\underline{\beta}}^j).
\end{aligned}$$

Now by induction, $\hat{\underline{v}}^{ij} = \hat{\underline{\alpha}}^i \otimes \hat{\underline{\beta}}^j$ for all $(i, j) \prec (p, q)$. Because $(i, j) < (p, q)$ implies $(i, j) \prec (p, q)$, it follows that

$$\hat{\underline{v}}^{ij} = \hat{\underline{\alpha}}^i \otimes \hat{\underline{\beta}}^j \quad \text{for all } (i, j) < (p, q).$$

Hence,

$$\hat{\underline{\alpha}}^p \otimes \hat{\underline{\beta}}^q = \underline{v}^{pq} - \sum_{(i,j)<(p,q)} \tilde{\mu}_{ij} \hat{\underline{v}}^{ij}. \tag{9}$$

We now need to show that $\hat{\underline{\alpha}}^p \otimes \hat{\underline{\beta}}^q$ is orthogonal to all the $\hat{\underline{v}}^{ij}$ with $(i, j) \prec (p, q)$. Indeed, we have

$$\begin{aligned}
\langle (\hat{\alpha}^p \otimes \hat{\beta}^q), \hat{v}^{ij} \rangle &= \langle \hat{\underline{\alpha}}^p \otimes \hat{\underline{\beta}}^q, \hat{\underline{\alpha}}^i \otimes \hat{\underline{\beta}}^j \rangle \quad \text{for all } (i, j) \prec (p, q)\\
&= \langle \hat{\alpha}^p, \hat{\alpha}^i \rangle \langle \hat{\beta}^q, \hat{\beta}^j \rangle \quad \text{by Proposition 3}\\
&= 0 \quad \text{for all } (i, j) \prec (p, q),
\end{aligned}$$

because either $i \ne p$ or $j \ne q$. □

Let us remark that in expression (9), only the indices $(i,j) < (p,q)$ have a corresponding μ nonzero. This leads to the following observation.

OBSERVATION 3.3. For a monotone ordering on V,

$$\mu_{(i,j)(p,q)} = 0 \qquad \text{for all } (i,j) \prec (p,q) \text{ with } (i,j) \not< (p,q).$$

PROPOSITION 3.4. *For any monotone ordering of the basis V, condition* (i) *of Definition* 3.1 *of a reduced basis is satisfied.*

PROOF. Let (p_1,q_1), (p_2,q_2) be a pair of indices, with $(p_1,q_1) \prec (p_2,q_2)$. If $(p_1,q_1) \not< (p_2,q_2)$, $\mu_{(p_1,q_1)(p_2,q_2)} = 0$ by Observation 3.3. Let us now consider $(p_1,q_1) < (p_2,q_2)$. We have

$$\begin{aligned}
\mu_{(p_1,q_1)(p_2,q_2)} &= \frac{\langle \underline{v}^{p_2q_2}, \hat{\underline{v}}^{p_1q_1}\rangle}{\langle \hat{\underline{v}}^{p_1q_1}, \hat{\underline{v}}^{p_1q_1}\rangle}\\
&= \frac{\langle \underline{\alpha}^{p_2}, \hat{\underline{\alpha}}^{p_1}\rangle \langle \underline{\beta}^{q_2}, \hat{\underline{\beta}}^{q_1}\rangle}{\langle \hat{\underline{\alpha}}^{p_1}, \hat{\underline{\alpha}}^{p_1}\rangle \langle \hat{\underline{\beta}}^{q_1}, \hat{\underline{\beta}}^{q_1}\rangle} \quad \text{by Proposition 3}\\
&= \mu^{\alpha}_{p_1p_2}\mu^{\beta}_{q_1q_2}.
\end{aligned}$$

Now as $(\underline{\alpha}^j)$ and $(\underline{\beta}^i)$ are reduced bases, $|\mu^{\alpha}_{p_1p_2}|, |\mu^{\beta}_{q_1q_2}| \le \frac{1}{2}$, and, thus

$$\begin{aligned}
|\mu_{(p_1,q_1)(p_2,q_2)}| &= |\mu^{\alpha}_{p_1p_2}|\,|\mu^{\beta}_{q_1q_2}|\\
&\le \frac{1}{4}. \quad \square
\end{aligned}$$

Now, we need to refine the ordering of the basis V to satisfy condition (ii) of Definition 3.1.

DEFINITION 3.3. A monotone ordering of the basis V is called *regular* if whenever $\underline{v}^{p_1q_1}$ directly precedes $\underline{v}^{p_2q_2}$ in the ordering and $(p_1,q_1) \not< (p_2,q_2)$, $\|\hat{\underline{v}}^{p_1q_1}\| \le \|\hat{\underline{v}}^{p_2q_2}\|$.

PROPOSITION 3.5. *If the basis V has a regular monotone ordering, it is a reduced basis.*

PROOF. It suffices to show that the condition (ii) of Definition of a reduced basis is satisfied. Consider two pairs, (p_1,q_1), (p_2,q_2), where (p_1,q_1) directly precedes (p_2,q_2) in the ordering. There are two cases.

Case 1. $(p_1,q_1) < (p_2,q_2)$. Because the ordering is monotone, this implies that either $p_2 = p_1+1$ and $q_1 = q_2$ or $p_1 = p_2$ and $q_2 = q_1+1$. Suppose that, without loss of generality, $p_2 = p_1+1$ and $q_1 = q_2$.

$$\begin{aligned}
&\left\| \hat{\underline{v}}^{p_1+1,q_1} + \mu_{(p_1,q_1)(p_1+1,q_1)}\hat{\underline{v}}^{p_1q_1}\right\|^2\\
&\quad = \left\| \hat{\underline{\alpha}}^{p_1+1} \otimes \hat{\underline{\beta}}^{q_1} + \frac{\langle \underline{\alpha}^{p_1+1}, \hat{\underline{\alpha}}^{p_1}\rangle \langle \underline{\beta}^{q_1}, \hat{\underline{\beta}}^{q_1}\rangle}{\langle \hat{\underline{\alpha}}^{p_1}, \hat{\underline{\alpha}}^{p_1}\rangle \langle \hat{\underline{\beta}}^{q_1}, \hat{\underline{\beta}}^{q_1}\rangle}(\hat{\underline{\alpha}}^{p_1} \otimes \hat{\underline{\beta}}^{q_1})\right\|^2\\
&\quad = \left\| \hat{\underline{\alpha}}^{p_1+1} \otimes \hat{\underline{\beta}}^{q_1} + \mu^{\alpha}_{p_1,p_1+1}(\hat{\underline{\alpha}}^{p_1} \otimes \hat{\underline{\beta}}^{q_1})\right\|^2 \quad \text{because } \langle \underline{\beta}^{q_1}, \hat{\underline{\beta}}^{q_1}\rangle = \langle \hat{\underline{\beta}}^{q_1}, \hat{\underline{\beta}}^{q_1}\rangle\\
&\quad = \left\| (\hat{\underline{\alpha}}^{p_1+1} + \mu^{\alpha}_{p_1,p_1+1}\hat{\underline{\alpha}}^{p_1}) \otimes \hat{\underline{\beta}}^{q_1}\right\|^2\\
&\quad = \left\| \hat{\underline{\alpha}}^{p_1+1} + \mu^{\alpha}_{p_1,p_1+1}\hat{\underline{\alpha}}^{p_1}\right\|^2 \left\|\hat{\underline{\beta}}^{q_1}\right\|^2\\
&\quad \ge \frac{3}{4}\|\hat{\underline{\alpha}}^{p_1}\|^2 \left\|\hat{\underline{\beta}}^{q_1}\right\|^2 \qquad \text{since } (\underline{\alpha}^j) \text{ is reduced}\\
&\quad = \frac{3}{4}\left\|\hat{\underline{\alpha}}^{p_1} \otimes \hat{\underline{\beta}}^{q_1}\right\|^2 = \frac{3}{4}\|\hat{\underline{v}}^{p_1q_1}\|^2.
\end{aligned}$$

Case 2. $(p_1, q_1) \nless (p_2, q_2)$

By Observation 3.3, we know that $\mu_{(p_1,q_1)(p_2,q_2)} = 0$. So

$$\begin{aligned}\|\hat{\underline{v}}^{p_2q_2} + \mu_{(p_1,q_1)(p_2,q_2)}\hat{\underline{v}}^{p_1q_1}\|^2 &= \|\hat{\underline{v}}^{p_2q_2}\|^2\\ &\geq \|\hat{\underline{v}}^{p_1q_1}\|^2 \quad \text{as the ordering is regular}\\ &> \frac{3}{4}\|\hat{\underline{v}}^{p_1q_1}\|^2. \quad \square\end{aligned}$$

We now present an algorithm to construct a regular monotone ordering of the basis V.

Definition 3.4. Given a vector $\underline{v}^{pq} \in V$, the *direct successors* of $\underline{v}^{pq}$ are the vectors $\underline{v}^{p+1,q}$ and $\underline{v}^{p,q+1}$ (if they exist), and the *predecessors* are the vectors $\underline{v}^{p'q'}$ with $(p', q') < (p, q)$.

Ordering Algorithm. RB is an ordered set of vectors from V. $\mathscr{S}$ is a set of vectors from V.

```
Initialization:    $RB := \{\underline{v}^{11}\}$
                   $\mathscr{S} := \{\underline{v}^{12}, \underline{v}^{21}\}$.
Loop:              While $\mathscr{S} \neq \varnothing$ do
                       Choose $\underline{v} \in \mathscr{S}$ such that $\underline{v} = \arg\min\{\|\hat{\underline{x}}\| : x \in \mathscr{S}\}$
                       $RB := RB \cup \{\underline{v}\}$
                       $\mathscr{S} := \mathscr{S} \setminus \{\underline{v}\}$
                       Add to $\mathscr{S}$ any direct successor of $\underline{v}$
                       that has all its predecessors in $RB$.
                   end
Return $RB$ in order.
```

Proposition 3.6. *The ordering algorithm terminates with a regular monotone ordering of V.*

Proof. The monotonicity is obvious because of the criterion of selection of vectors entering $\mathscr{S}$. Indeed, if $(p, q) < (p', q')$, a vector $\underline{v}^{p'q'}$ cannot come before $\underline{v}^{pq}$ because it cannot enter $\mathscr{S}$ until $\underline{v}^{pq}$ is in RB.

Now we have to prove the regularity. On each loop, we choose a vector $\underline{v} \in \mathscr{S}$. None of the remaining vectors in $\mathscr{S}$ are direct successors of $\underline{v}$, and all of the vectors that are added to $\mathscr{S}$ during the loop are direct successors of $\underline{v}$. Therefore, on the following loop, either we choose a vector $\underline{w}$ that is not a direct successor of $\underline{v}$, and thus $\|\hat{\underline{w}}\| \geq \|\hat{\underline{v}}\|$ because $\underline{v}$ was chosen ahead of $\underline{w}$ on the previous loop, or we choose a vector $\underline{w}$ that is a direct successor of $\underline{v}$. Therefore, the condition of regularity is satisfied.

Finally, we have to check that the algorithm terminates with $|RB| = |V|$. On each loop, exactly one vector is added to RB. So the algorithm has to stop. Suppose now that the algorithm terminates with $RB \subset V$. Select $p := \min\{p : \exists\, j \text{ with } \underline{v}^{pj} \notin RB\}$. Now select $q := \min\{q : \underline{v}^{pq} \notin RB\}$. Clearly, $\underline{v}^{pq}$ can be added to $\mathscr{S}$ because $\underline{v}^{p-1,q} \in RB$ (or $p = 1$) and $\underline{v}^{p,q-1} \in RB$ (or $q = 1$) and, thus, all its direct predecessors are in RB. Therefore, $\mathscr{S} \neq \varnothing$ and the algorithm cannot have ended, a contradiction. So $|RB| = |V|$. $\square$

Theorem 3.7. *RB is a reduced basis of the lattice $\mathscr{L}$.*

To end this section, we observe that stronger properties hold for the reduced basis $\mathscr{L}$ than for a general reduced basis. The next two propositions give the results for a general lattice (Lenstra et al. 1982) and for $\mathscr{L}$, respectively.

Proposition 3.8. *Let $(\underline{\gamma}^k)_{k=1}^r$ be a reduced basis of a r-dimensional lattice $\mathscr{L}_\gamma$ in $\mathbb{R}^n$. Then,*

(i) $\|\underline{\gamma}^1\| \leq 2^{(r-1)/4}(\det \mathscr{L}_\gamma)^{\frac{1}{r}}$

(ii) $\|\underline{\gamma}^1\| \leq 2^{(r-1)/2} \min\{\|\underline{w}\| : \underline{w} \in \mathscr{L}_\gamma, \underline{w} \neq \underline{0}\}$

(iii) $\prod_{k=1}^{r} \|\underline{\gamma}^k\| \leq 2^{r(r-1)/4} \det(\mathscr{L}_\gamma)$.

PROPOSITION 3.9. *For the reduced basis* $(\underline{v}^{pq})_{p=1,\dots,P,\ q=1,\dots,Q}$ *of* $\mathscr{L}$,

(i) $\|\underline{v}^{11}\| \leq 2^{(P+Q-1)/4}(\det \mathscr{L})^{\frac{1}{PQ}}$.

(ii) $\|\underline{v}^{11}\| \leq 2^{(P+Q)/2} \min\{\|\underline{w}\| : \underline{w} \in \mathscr{L}, \underline{w} \neq 0\}$.

(iii) $\prod_{p=1}^{P} \prod_{q=1}^{Q} \|\underline{v}^{pq}\| \leq 2^{PQ(P+Q-2)/4} \det \mathscr{L}$.

PROOF. We prove only (iii). The other proofs are similar.
From Proposition 3.8,

$$\prod_{p=1}^{P} \|\underline{\alpha}^p\| \leq 2^{P(P-1)/4} \det(\mathscr{L}_A), \tag{10}$$

and

$$\prod_{q=1}^{Q} \|\underline{\beta}^q\| \leq 2^{Q(Q-1)/4} \det(\mathscr{L}_B). \tag{11}$$

For the lattice $\mathscr{L}$,

$$\begin{aligned}
\prod_{p=1}^{P} \prod_{q=1}^{Q} \|\underline{v}^{pq}\| &= \prod_{p=1}^{P} \prod_{q=1}^{Q} \|\underline{\alpha}^p\| \|\underline{\beta}^q\| \\
&= \left(\prod_{p=1}^{P} \|\underline{\alpha}^p\|\right)^Q \left(\prod_{q=1}^{Q} \|\underline{\beta}^q\|\right)^P \\
&\leq 2^{QP(P-1)/4}(\det \mathscr{L}_A)^Q 2^{PQ(Q-1)/4}(\det \mathscr{L}_B)^P \qquad (12) \\
&\leq 2^{PQ(P+Q-2)/4} \det \mathscr{L}, \qquad (13)
\end{aligned}$$

where the inequality (12) comes from the inequalities (10) and (11), and the inequality (13) comes from the fact that $\det \mathscr{L} = (\det \mathscr{L}_A)^Q (\det \mathscr{L}_B)^P$. □

Thus, we see that if we want to find the shortest vector of the lattice, (ii) shows that we obtain a guarantee that $\|\underline{v}^{11}\| \leq 2^{(P+Q)/2} \min\{\|\underline{w}\| : \underline{w} \in \mathscr{L}, \underline{w} \neq 0\}$ while the general bound is $\|\underline{v}^{11}\| \leq 2^{(PQ-1)/2} \min\{\|\underline{w}\| : \underline{w} \in \mathscr{L}, \underline{w} \neq 0\}$.

4. The banker's problem.

4.1. Theoretical point of view. Here, we show how the results of §2 can be used to tackle the banker's problem. Specifically, we want to solve the problem.

Problem 4.1.

$$\begin{aligned}
\min \quad & \sum_{i=1}^{m} \frac{|s_i|}{d_i} \\
\text{s.t.} \quad & \sum_{i=1}^{m} x_{ij} = c_j && \text{for } j = 1, \dots, n \\
& \sum_{j=1}^{n} x_{ij} = d_i && \text{for } i = 1, \dots, m \\
& \sum_{j=1}^{n} p_j x_{ij} + s_i = d_i \frac{\sum c_j p_j}{\sum d_i} && \text{for } i = 1, \dots, m \\
& x \in \mathbb{Z}_+^{mn}, \quad s \in \mathbb{Z}^m.
\end{aligned} \tag{14}$$

We rescale the last set of equations so that all the coefficients and variables are integer, which yields

$$\Big(\sum d_k\Big)\sum_{j=1}^{n} p_j x_{ij} + \tilde{s}_i = d_i\bigg(\sum_{j=1}^{n} c_j p_j\bigg).$$

We can see that this system is of the form studied in §2, except for the additional variables s_i. However, the system still has the same structure. Indeed, taking

$$X = \begin{pmatrix} x_{11} & \cdots & x_{1n} & \tilde{s}_1 \\ \vdots & \ddots & \vdots & \vdots \\ x_{m1} & \cdots & x_{mn} & \tilde{s}_m, \end{pmatrix}$$

$$A = \begin{pmatrix} 1 & \cdots & 1 & 0 \\ (\sum d_i)p_1 & \cdots & (\sum d_i)p_n & 1 \end{pmatrix}^T$$

and $B = (1 \ \cdots \ 1)$, we get the system (14), with one more equation, namely $\sum_{i=1}^{m} \tilde{s}_i = 0$. However, every solution of (14) automatically satisfies this equation.

To use the method of Aardal et al. (2000), we need the two reduced bases $\underline{\underline{\alpha}}$ and $\underline{\underline{\beta}}$ of $\mathscr{L}_A$ and $\mathscr{L}_B$, respectively, and also an integer solution $X = Q$ to the equation system of (14) with the nonnegativity constraints on $\underline{\underline{x}}$ dropped (which can be easily found by inspection). Now, the MIP to be solved in Step 2 becomes

$$\begin{aligned} \min\ & \sum_i \frac{\tilde{s}_i^+}{d_i \sum_k d_k} + \sum_i \frac{\tilde{s}_i^-}{d_i \sum_k d_k} \\ \text{s.t.}\ & \begin{pmatrix} x_{11} & \cdots & x_{1n} & \tilde{s}_1^+ - \tilde{s}_1^- \\ \vdots & \ddots & \vdots & \vdots \\ x_{m1} & \cdots & x_{mn} & \tilde{s}_m^+ - \tilde{s}_m^- \end{pmatrix} = Q + \underline{\underline{\beta}}\Lambda\underline{\underline{\alpha}} \\ & \underline{\underline{x}}, \underline{\tilde{s}}^+, \underline{\tilde{s}}^- \geq 0,\ \Lambda \in \mathbb{Z}^{(m-L)\times(n-K)}. \end{aligned}$$

4.2. Computational results. Our set of test instances are randomly generated feasible instances of the banker's problem with expected profits uniformly distributed between 5 and 105, based on a real instance. The supplies are uniformly distributed between 1 and 50, and the demands are randomly generated while maintaining $\sum_i d_i = \sum_j a_j$. In all of the computations, LiDIA (1999) was used to calculate the reduced bases and Cplex, Version 6.6, to solve the MIPs, both running on a Sun SPARC Ultra 60.

In Table 1, we compare the basis reduction approach with the direct MIP approach on five relatively small instances. The basis reduction approach permits us to solve all of the instances within a few seconds. On the other hand, none of the instances were solved by the direct MIP approach because, for each instance, memory problems were encountered after more than 1 hour. In fact, the linear programming relaxations stay at zero throughout the enumeration tree (column LB = *lower bound*), but good feasible solutions are found (column UB = *upper bound*).

In Table 2, we compare the computation times of the basis composition approach using the product of two small reduced bases and the direct basis reduction approach. For both approaches, Time part 1 is the time in seconds to construct the alternative MIP formulation

TABLE 1. Comparison of direct MIP or basis reduction

Sizes		*Basis reduction*			*Direct MIP approach*		
n	*m*	*Time* *B&B*	*LB*	*UB*	*Time* *B&B*	*LB*	*UB*
16	5	1	1.5×10^{-2}		***	0	1.5×10^{-2}
16	5	1	2.5×10^{-2}		***	0	2.5×10^{-2}
16	5	0	8.9×10^{-3}		***	0	8.9×10^{-3}
16	5	1	1.4×10^{-2}		***	0	1.4×10^{-2}
16	5	1	1.7×10^{-2}		***	0	1.7×10^{-2}

***Memory limit reached. Average time, 2 hours.

by computing the integral basis of the homogeneous system, and Time B&B is the time spent to prove optimality with Cplex. For both approaches, the variable selection rule used in Cplex is “pseudoreduced costs” because it leads to better and more stable results. For the direct basis reduction approach, we observe that the time required for basis reduction becomes a limiting factor as the problem gets bigger. On the other hand, using the composite basis approach, the time required in the MIP step slightly increases. This suggests that the product vectors are perhaps not as short as those from direct basis reduction. However, if we consider the total computation time, it is always more interesting to use the composite basis approach.

In Table 3, we run some larger instances with just the composite basis approach as the direct approach is now too time consuming. It appears that for the banker’s problem, the difficulty depends on the number m of clients. Instances with $m = 15$ are more difficult than instances with $m = 8$, even for large n. As m approaches 20, proving optimality becomes difficult.

TABLE 2. Comparison of constructed and direct basis reduction

Sizes		*Composite basis*				*Direct basis reduction*			
n	*m*	*Time* *part 1*	*Time* *B&B*	*LB*	*UB*	*Time* *part 1*	*Time* *B&B*	*LB*	*UB*
22	9	1	1	3.6×10^{-2}		552	2	3.6×10^{-2}	
22	9	1	2	5×10^{-2}		527	1	5×10^{-2}	
22	9	1	3	6×10^{-2}		632	1	6×10^{-2}	
22	9	1	1	3.4×10^{-2}		554	1	3.4×10^{-2}	
22	9	1	1	3.4×10^{-2}		519	1	3.4×10^{-2}	
30	12	1	12	8.3×10^{-2}		4121	669	8.3×10^{-2}	
30	12	1	***	5.5×10^{-2}	6.7×10^{-2}	3955	7	5.5×10^{-2}	
30	12	1	36	6.4×10^{-2}		4315	8	6.4×10^{-2}	
30	12	1	10	6.6×10^{-2}		4003	16	6.6×10^{-2}	
30	12	1	11	7.5×10^{-2}		4438	5	7.5×10^{-2}	
15	15	1	24	2.1×10^{-1}		1110	10	2.1×10^{-1}	
15	15	1	438	1.9×10^{-1}		1241	6	1.9×10^{-1}	
15	15	1	12	2.1×10^{-1}		1415	23	2.1×10^{-1}	
15	15	1	128	2.2×10^{-1}		1416	9	2.2×10^{-1}	
15	15	1	123	3.1×10^{-1}		1083	6	3.1×10^{-1}	
60	8	2	11	1.1×10^{-2}		10252	2	1.1×10^{-2}	
60	8	2	7	9.5×10^{-3}		10482	6	9.5×10^{-3}	
60	8	2	17	1.3×10^{-2}		11223	7	1.3×10^{-2}	
60	8	2	7	1.4×10^{-2}		10965	6	1.4×10^{-2}	

***More than 1 hour.

TABLE 3. Critical sizes of the problems solved by this method

Sizes		*Composite basis approach*			
n	*m*	*Times* *B&B*	*LB*	*UB*	*GAP*
50	15	156	6.4×10^{-2}		
50	15	140	4.4×10^{-2}		
50	15	57	5.2×10^{-2}		
50	15	$***$	5.37×10^{-2}	5.48×10^{-2}	2%
50	15	118	4.5×10^{-2}		
30	20	$***$	2×10^{-1}	6.6×10^{-1}	69%
30	20	$***$	8.54×10^{-2}	6.8×10^{-1}	88%
30	20	1177	2.2×10^{-1}		
30	20	409	1.1×10^{-1}		
30	20	$***$	2×10^{-1}	2.4×10^{-1}	17%

***More than 1 hour.

5. Conclusions. The special structure of the linear integer system, or the corresponding lattice $\mathscr{L}$, is crucial in the results obtained here. It is natural to ask whether there are other structured linear integer programs for which a similar decomposition approach can be developed.

Theoretically, another interesting question arises. If $\underline{\alpha}^1$ and $\underline{\beta}^1$ are the shortest vectors in the lattices $\mathscr{L}_A$ and $\mathscr{L}_B$, respectively, $\underline{\alpha}^1 \otimes \underline{\beta}^1$ is the shortest vector in $\mathscr{L}$ among all the vectors of the form $\underline{\alpha} \otimes \underline{\beta}$ with $\underline{\alpha} \in \mathscr{L}_A$ and $\underline{\beta} \in \mathscr{L}_B$. How close is this vector to being the shortest vector in $\mathscr{L}$?

More generally, a satisfying explanation of when the approach of Aardal et al. (2000) is likely to be effective is still lacking.

Another question is more computational. Step 1 of the Aardal et al. (2000) approach leads to a reduced basis and, thus, an ordered set of columns. However, the ordering plays no obvious role in the solution of the mixed-integer program in Step 2. Some limited experiments (Aardal et al. 2000, Louveaux 1999) have been carried out using priorities in an attempt to decide whether to branch on the first or last vector in the basis, but more seems to be needed. It would also be interesting to test whether the composite basis for $\mathscr{L}$ is a shorter basis than that produced by the direct reduced basis approach.

Acknowledgments. The authors thank Paul Van Dooren for suggesting appropriate notation and the structure of the proof of Theorem 2.1. The work of the first author is supported by the Belgian National Fund for Scientific Research (FNRS). Research carried out as part of Project TMR-DONET nr. ERB FMRCX-CT98-0202 of the European Union. This paper presents research results of the Belgian Program on Interuniversitary Poles of Attraction initiated by the Belgian State, Prime Minister's Office, Science Policy Programming. The scientific responsibility is assumed by the authors.

Appendix. In Proposition A.1, we present the basic results about Smith normal form, and we prove Lemma 2.3, characterizing when a set of integer vectors forms an integral basis of the null space of a matrix.

PROPOSITION A.1. (SMITH NORMAL FORM). *Let A be an integer matrix from $\mathbb{Z}^{m\times n}$ with $m \geq n$ and* $\operatorname{rank}(A) = r$. *There exist unimodular matrices $U \in \mathbb{Z}^{m\times m}$ and $V \in \mathbb{Z}^{n\times n}$ such that*

$$UAV = \begin{pmatrix} s_1 & & & & & \\ & \ddots & & & & \\ & & s_r & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \\ & & \underline{\underline{0}} & & & \end{pmatrix},$$

with $s_1|s_2|\dots|s_r$. For $1 \leq k \leq r$, $\Pi_{i=1}^{k} s_i$ is the gcd of the determinants of all $k \times k$ submatrices of A.

PROPOSITION A.2. *Consider the system $C\underline{x} = \underline{0}$, where $C \in \mathbb{Z}^{m\times n}$ with $m \leq n$ and* $\operatorname{rank}(C) = m$. *Let $Y \in \mathbb{Z}^{n\times(n-m)}$ be a set of solutions of $C\underline{x} = \underline{0}$, then the following statements are equivalent*:

(i) *The Smith normal form of Y is $\binom{I}{0}$.*

(ii) *Y is an integer basis of all the integer solutions of $C\underline{x} = \underline{0}$.*

PROOF. (ii) ⇒ (i) As $\operatorname{rank}(Y) = n - m$, there exist two unimodular matrices U and V such that

$$Y = U \begin{pmatrix} s_1 & & \\ & \ddots & \\ & & s_{n-m} \\ & \underline{\underline{0}} & \end{pmatrix} V,$$

with $U \in \mathbb{Z}^{n\times n}$ and $V \in \mathbb{Z}^{(n-m)\times(n-m)}$ and $s_{n-m} \geq 1$. As V is unimodular, its inverse exists, and we can write

$$YV^{-1} = U \begin{pmatrix} s_1 & & \\ & \ddots & \\ & & s_{n-m} \\ & \underline{\underline{0}} & \end{pmatrix}.$$

Then,

$$U \begin{pmatrix} s_1 & & \\ & \ddots & \\ & & s_{n-m} \\ & 0 & \end{pmatrix} = \left(s_1\underline{u}^1 \cdots s_{n-m}\underline{u}^{n-m}\right) \tag{15}$$

is also an integer basis of the integer solutions of $C\underline{x} = \underline{0}$ because it is obtained by multiplying a basis by the unimodular matrix V. So $s_{n-m}\underline{u}^{n-m}$ is a solution of $C\underline{x} = \underline{0}$, and $\underline{u}^{n-m}$ is an integral solution as well. However, it lies only in the basis (15) if $s_{n-m} = 1$. Hence, $s_{n-m} = 1$ and $s_i = 1$ for $i = 1, \dots, n - m$ by the divisibility property of the Smith normal form.

(i) ⇒ (ii). There exists a basis of all the integer solutions of $C\underline{x} = \underline{0}$. Let us call it W. By hypothesis, we can find two unimodular matrices $U \in \mathbb{Z}^{n\times n}$ and $V \in \mathbb{Z}^{(n-m)\times(n-m)}$ such that

$$UYV = \begin{pmatrix} I_{n-m} \\ \underline{\underline{0}}_{m\times(n-m)} \end{pmatrix}. \tag{16}$$

As each column of Y is a solution of $C\underline{x} = \underline{0}$, each of them is an integer combination of the columns of W. Thus, there exists a nonsingular integer matrix $\Lambda \in \mathbb{Z}^{(n-m)\times(n-m)}$ such that

$$Y = W\Lambda. \tag{17}$$

To prove that Y is an integer basis of the solutions of $C\underline{x} = \underline{0}$, we just have to prove that this matrix Λ is unimodular. We now show that ΛV is unimodular. Let S be its Smith normal form, so

$$P\Lambda VQ = S,$$

with P and Q unimodular. Rewriting (16), we now have

$$UW\Lambda V = UWP^{-1}SQ^{-1} = \begin{pmatrix} I \\ \underline{\underline{0}} \end{pmatrix}.$$

As U and Q^{-1} are unimodular, the Smith normal form of $WP^{-1}S$ is $\binom{I}{\underline{\underline{0}}}$. In $WP^{-1}S$, all the elements of the last column are multiples of the last element of the diagonal of S, and thus $s_{n-m} = 1$. Therefore, the Smith normal form of ΛV is $\binom{I}{\underline{\underline{0}}}$ and ΛV is unimodular. Therefore, Λ is unimodular and Y is a basis. □

References

Aardal, K., R. E. Bixby, C. A. J. Hurkens, A. K. Lenstra, J. W. Smeltink. 2000. Market split and basis reduction: Towards a solution of the Cornuéjols-Dawande instances. *J. Comput.* **12**(3) 192–202.

———, C. A. J. Hurkens, A. K. Lenstra. 2000. Solving a system of linear diophantine equations with lower and upper bounds on the variables. *Math. Oper. Res.* **25**(3) 427–442.

Cohen, H. 1996. *A Course in Computational Algebraic Number Theory*. Springer-Verlag, Berlin, Germany.

Joux, A. 1998. La réduction de réseaux en cryptographie. Ph.D. thesis, Ecole Polytechnique, Palaiseau, France.

Lancaster, P., M. Tismenetsky. 1985. The theory of matrices, 2nd ed. *Computer Science and Applied Mathematics*. Academic Press, Inc., Orlando, FL.

Lenstra, A. K., H. W. Lenstra, L. Lovász. 1982. Factoring polynomials with rational coefficients. *Mathematische Annalen* **261** 515–534.

LiDIA. 1999. A library for computational number theory. *http://www.informatik.th-darmstadt.de/TI/LiDIA*. TH Darmstadt/Universität des Saarlandes, Fachbereich Informatik, Institut für Theoretische Informatik, Darmstadt, Germany.

Louveaux, Q. 1999. Résolution de problèmes d'optimisation en nombres entiers par un algorithme de réduction de base dans les treillis. *Mémoire de la Faculté des Sciences Appliquées*. Université catholique de Louvain, Louvain, Belgium.

Nemhauser, G. L., L. A. Wolsey, 1988. *Integer and Combinatorial Optimization*. John Wiley and Sons, New York.

Newman, M. 1972. Integral matrices. *Pure and Applied Mathematics: A Series of Monographs and Textbooks*, vol. 45. Academic Press, New York.

Schrijver, A. 1986. *Theory of Linear and Integer Programming*. John Wiley and Sons, Chichester, U.K.

Williams, H. P. 1993. *Model Building in Mathematical Programming*. John Wiley and Sons, Chichester, U.K.

Q. Louveaux: INMA and CORE, Université catholique de Louvain, 34 Voie du Roman Pays, Louvain-la-Neuve, B-1348 Belgium; e-mail: louveaux@core.ucl.ac.be

L. A. Wolsey: INMA and CORE, Université catholique de Louvain, 34 Voie du Roman Pays, Louvain-la-Neuve, B-1348 Belgium; e-mail: wolsey@core.ucl.ac.be