Basis Reduction and the Complexity of Branch-and-Bound

Gábor Pataki* Mustafa Tural† Erick B. Wong ‡

Abstract

The classical branch-and-bound algorithm for the integer feasibility problem

$$(0.1)\qquad \text{Find} \quad \bar{x} \in Q \cap \mathbb{Z}^n, \text{ with} \quad Q = \left\{ x \mid \begin{pmatrix} \ell_1 \\ \ell_2 \end{pmatrix} \leq \begin{pmatrix} A \\ I \end{pmatrix} x \leq \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} \right\}$$

has exponential worst case complexity.

We prove that it is surprisingly efficient on reformulations of (0.1), in which the columns of the constraint matrix are short and near orthogonal, i.e., a reduced basis of the generated lattice: when the entries of A are from $\{1, \dots, M\}$ for a large enough M, branch-and-bound solves almost all reformulated instances at the root node. For all A matrices we prove an upper bound on the width of the reformulations along the last unit vector.

Our results generalize the results of Furst and Kannan on the solvability of subset sum problems; also, we prove them via branch-and-bound, an algorithm traditionally considered inefficient from the theoretical point of view.

We use two main tools: first, we find a bound on the size of the branch-and-bound tree based on the norms of the Gram-Schmidt vectors of the constraint matrix. Second, building on the ideas of Furst and Kannan, we bound the number of integral matrices for which the shortest nonzero vectors of certain lattices are long.

We explore practical aspects of these results. We compute numerical values of M which guarantee that 90 and 99 percent of the reformulated problems solve at the root: these turn out to be surprisingly small when the problem size is moderate. We also confirm with a computational study that random integer programs become easier, as the coefficients grow.

1 Introduction and Main Results.

The Integer Programming (IP) feasibility problem asks whether a polyhedron Q contains an integral point. Branch-and-bound, which we abbreviate as B&B is a classical solution method, first proposed by Land and Doig in [20]. It starts with Q as the sole subproblem (node). In a general step, one chooses a subproblem Q', a variable x_i, and creates nodes $Q' \cap \{x | x_i = \gamma\}$, where γ ranges over all possible integer values of x_i. We repeat this until all subproblems are shown to be empty, or we find an integral point in one of them.

B&B (and its version used to solve optimization problems) enhanced by cutting planes is a dependable algorithm implemented in most commercial software packages. However, instances in [14, 8, 13, 17, 3, 4] show that it is theoretically inefficient: it may take an exponential number of subproblems to prove the infeasibility of simple knapsack problems. While B&B is inefficient in the worst case, Cornuéjols et al. in [10] developed useful computational tools to give an early estimate on the size of the B&B tree in practice.

Since IP feasibility is NP-complete, one can ask for polynomiality of a solution method only in fixed dimension. All algorithms that achieve such complexity rely on advanced techniques. The algorithms of Lenstra [22] and Kannan [15] first round the polyhedron (i.e., apply a transformation to make it have a spherical appearance), then use basis reduction to reduce the problem to a provably small number of smaller dimensional subproblems. On the subproblems the algorithms are applied recursively, e.g., rounding is done again. Generalized basis reduction, proposed by Lovász and Scarf in [23] avoids rounding, but needs to solve a sequence of linear programs to create the subproblems.

There is a simpler way to use basis reduction in integer programming: preprocessing (0.1) to create an instance with short and near orthogonal columns in the constraint matrix, then simply feeding it to an IP solver. The first such reformulation method, that we call the nullspace reformulation, was proposed by Aardal, Hurkens and Lenstra for equality constrained integer programs in [2], and further studied in [1]. The rangespace reformulation of Krishnamoorthy and Pataki [17] applies to general integer programs. We describe these below, assuming that A is an integral matrix with m rows and n columns, and the w_i and ℓ_i are integral vectors.

The rangespace reformulation of (0.1) is

$$(1.2)\qquad \text{Find} \quad \bar{y} \in Q_R \cap \mathbb{Z}^n, \text{ with} \quad Q_R = \left\{ y \mid \begin{pmatrix} \ell_1 \\ \ell_2 \end{pmatrix} \leq \begin{pmatrix} A \\ I \end{pmatrix} U y \leq \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} \right\},$$

where U is a unimodular matrix computed to make the columns of the constraint matrix a reduced basis of the

*Department of Statistics and Operations Research, University of North Carolina at Chapel Hill

†Institute for Mathematics and its Applications, University of Minnesota

‡Department of Mathematics, University of British Columbia

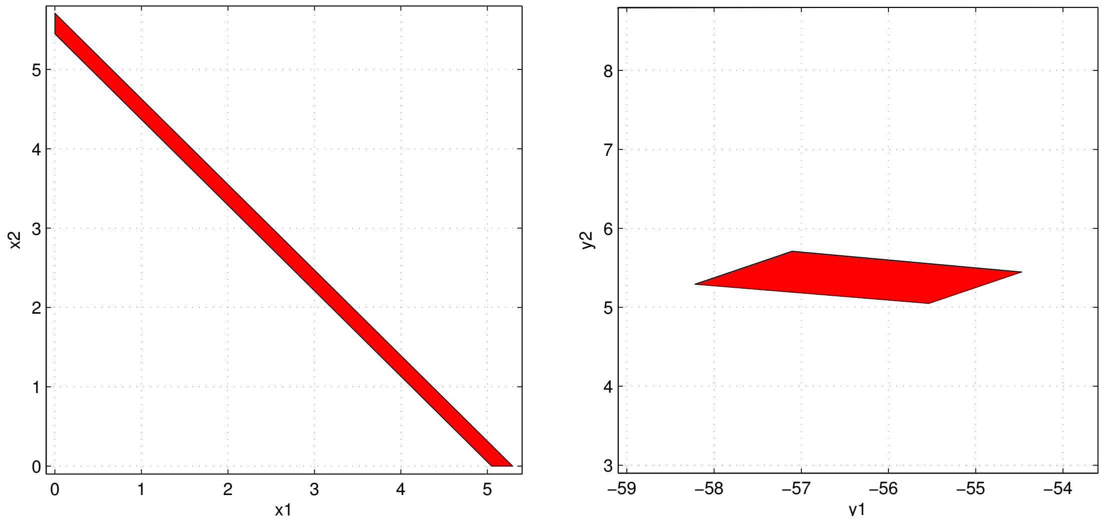

Figure 1: The polyhedron of Example 1 before and after the reformulation

generated lattice.

The nullspace reformulation is applicable when $w_1 = \ell_1$. Assuming that the rows of A are linearly independent, it is

$$(1.3)\qquad \begin{array}{rl} \text{Find} & \bar{y} \in Q_N \cap \mathbb{Z}^{n-m}, \text{ with} \\ Q_N = & \{\, y \mid \ell_2 - x_0 \le By \le w_2 - x_0 \,\}, \end{array}$$

where $x_0 \in \mathbb{Z}^n$ satisfies $Ax_0 = \ell_1$, and the columns of B are a reduced basis of the lattice $\{\, x \in \mathbb{Z}^n \mid Ax = 0 \,\}$.

We analyze the use of Lenstra-Lenstra-Lovász (LLL) (see [21]), and reciprocal Korkhine-Zolotarev (RKZ) reduced bases (see [18]) in the reformulations, and use Korkhine-Zolotarev (KZ) reduced bases [15, 16] in our computational study. We will review the relevant properties of these bases in Section 2.

When Q_R is computed using LLL reduction, we call it the LLL-rangespace reformulation of Q, and abusing notation we also call (1.2) the LLL-rangespace reformulation of (0.1). Similarly we talk about LLL-nullspace, RKZ-rangespace, and RKZ-nullspace reformulations.

Example. The polyhedron

$$(1.4)\qquad \begin{array}{rcl} 207 \le & 41x_1 + 38x_2 & \le 217 \\ 0 \le & x_1, x_2 & \le 10 \end{array}$$

is shown on the first picture of Figure 1. It is long and thin, and defines an infeasible and relatively difficult integer feasibility problem for B&B, as branching on either x_1 or x_2 yields 6 subproblems. Lenstra's and Kannan's algorithms would first transform this polyhedron to make it more spherical; generalized basis reduction would solve a sequence of linear programs to find the direction $x_1 + x_2$ along which the polyhedron is thin.

The LLL-rangespace reformulation is

$$(1.5)\qquad \begin{array}{rcl} 207 \le & -3x_1 + 8x_2 & \le 217 \\ 0 \le & -x_1 - 10x_2 & \le 10 \\ 0 \le & x_1 + 11x_2 & \le 10 \end{array}$$

shown on the second picture of Figure 1: now branching on y_2 proves integer infeasibility. (A similar example was given in [17]).

The reformulation methods are easier to describe, than, say Lenstra's algorithm, and are also successful in practice in solving several classes of hard integer programs: see [2, 1, 17]. For instance, the original formulations of the marketshare problems of Cornuéjols and Dawande in [9] are notoriously difficult for commercial solvers, while the nullspace reformulations are much easier to solve as shown by Aardal et al. in [1].

However, they seem difficult to analyze in general. For an overview of previous results, we need the following concepts: if Q is a polyhedron and z is an integral vector, then the width, and integer width of Q along z are

$$\text{width}(z, Q) = \max_{x \in Q} \{\langle z, x\rangle\} - \min_{x \in Q} \{\langle z, x\rangle\}, \text{ and}$$

$$\text{iwidth}(z, Q) = \left\lfloor \max_{x \in Q} \{\langle z, x\rangle\} \right\rfloor - \left\lceil \min_{x \in Q} \{\langle z, x\rangle\} \right\rceil + 1.$$

The quantity $\text{iwidth}(z, Q)$ is the number of subproblems generated, when branching on the hyperplane $\langle z, x\rangle$ in seeking to find an integral point in Q. In particular, $\text{iwidth}(z, Q) = 0$ implies that Q has no integral point.

Krishnamoorthy and Pataki in [17] studied knapsack problems with a constraint vector a having a given decomposition $a = \lambda p + r$, with p and r integral vectors, and λ an integer, large compared to $\| p \|$ and $\| r \|$. They proved

$$\text{width}(e_n, Q_R) \le \text{width}(p, Q), \tag{1.6}$$

$$\text{iwidth}(e_n, Q_R) \le \text{iwidth}(p, Q), \tag{1.7}$$

and analogous results for the nullspace reformulation.

These inequalities partially explain why the reformulation techniques are effective: considering (1.6), note that width(p, Q) is small, due to λ being large, i.e., p being near parallel to the constraint vector. Also, for a wide variety of problems iwidth$(p, Q) = 0$, but branching on the individual variables would need an exponential number of B&B nodes: as (1.7) shows, for these problems branching on the last variable in Q_R proves infeasibility at the root node. In other words, the effect of branching on $\langle p, x \rangle$ in Q is mimicked by branching on a single variable in Q_R.

In a general analysis, one could hope for proving polynomiality of B&B on the reformulations of (0.1) when the dimension is fixed. This seems difficult. However, we give a different and perhaps even more surprising complexity analysis. It is in the spirit of Furst and Kannan's work in [12] on subset sum problems and builds on a generalization of their Lemma 1 to bound the fraction of integral matrices for which the shortest nonzero vectors of certain corresponding lattices are short. We also use an upper bound on the size of the B&B tree, which depends on the norms of the Gram-Schmidt vectors of the constraint matrix. We introduce necessary notation and state our results, then give a comparison with [12].

When a statement is true for all, but at most a fraction of $1/2^n$ of the elements of a set S, we say that it is true for *almost all* elements. The value of n will be clear from the context. *Reverse B&B* is B&B branching on the variables in reverse order starting with the one of highest index. We assume $w_2 > \ell_2$ and for simplicity of stating the results we also assume $n \ge 5$. For positive integers m, n, and M we denote by $G_{m,n}(M)$ the set of matrices with m rows and n columns, and the entries drawn from $\{1, \dots, M\}$. We denote by $G'_{m,n}(M)$ the subset of $G_{m,n}(M)$ consisting of matrices with linearly independent rows, and let

$$\chi_{m,n}(M) = \frac{|G'_{m,n}(M)|}{|G_{m,n}(M)|}. \tag{1.8}$$

It is shown by Martin and Wong in [24], and by Bourgain et al. in [6] that $\chi_{m,m}(M)$ (and therefore also $\chi_{m,n}(M)$ for $m \le n$) are of the order $1 - o(1)$. In this paper we will use $\chi_{m,n}(M) \ge 1/2$ for simplicity. In the proof of Proposition 1.2, however, we will use a stronger statement, Lemma 1.1, whose proof is given in the full paper.

LEMMA 1.1. *For positive integers m, n, and M with $m \le n$,*

$$\chi_{m,n}(M) \ge 1 - \frac{1}{(M-1)M^{n-m}}. \tag{1.9}$$

□

For matrices (and vectors) A and B, we write $(A; B)$ for $\begin{pmatrix} A \\ B \end{pmatrix}$. For an m by n integral matrix A with independent rows we write gcd(A) for the greatest common divisor of the m by m subdeterminants of A. If B&B generates at most one node at each level of the tree, we say that it solves an integer feasibility problem at the root node.

The main results of the paper follow.

THEOREM 1.1. *The following hold.*

(1) If $M \ge (2n \,\| (w_1; w_2) - (\ell_1; \ell_2) \|)^{n/m+1}$, then for almost all $A \in G_{m,n}(M)$ reverse B&B solves the RKZ-rangespace reformulation of (0.1) at the root node.

(2) If $M \ge (12(n-m) \,\| w_2 - \ell_2 \|)^{n/m}$, then for almost all $A \in G'_{m,n}(M)$ reverse B&B solves the RKZ-nullspace reformulation of (0.1) at the root node.

□

The proofs also show that when M obeys the above bounds, then Q has at most one element for almost all $A \in G_{m,n}(M)$ (or almost all $A \in G'_{m,n}(M)$). Note that when n/m is fixed and the problems are binary, the magnitude of M required is a polynomial in n.

THEOREM 1.2. *The conclusions of Theorem 1.1 hold for the LLL-reformulations, if the bounds on M are*

$$(2^{(n+4)/2} \,\| (w_1; w_2) - (\ell_1; \ell_2) \|)^{n/m+1},$$

and

$$(2^{(n-m+4)/2} \,\| w_2 - \ell_2 \|)^{n/m},$$

respectively. □

Furst and Kannan in [12] based on Lagarias' and Odlyzko's [19] and Frieze's [11] work show that the subset sum problem is solvable in polynomial time using a simple iterative method for almost all weight vectors in $G_{1,n}(M)$ and all right hand sides, when M is sufficiently large and a reduced basis of the orthogonal lattice of the weight vector is available. Their bound on M is

$$M \geq 2^{(3/2)n \log n + 5n}, \tag{1.10}$$

when the basis is RKZ reduced, and

$$M \geq 2^{n^2/2+2n} n^{3n/2}, \tag{1.11}$$

when it is LLL reduced.

Our bounds obtained by letting $m = 1$ in Theorems 1.1 and 1.2 are comparable, as far as the size of M, i.e., $\lceil \log(M+1) \rceil$ is concerned. With RKZ reduction, both the bounds in Theorem 1.1 and the one in (1.10) require the size of M to be $O(n \log n)$. With LLL reduction, our bounds in Theorem 1.2 and the one in (1.11) require the size of M to be $O(n^2)$. Hence, our results generalize the solvability results of [12] from subset sum problems to bounded integer programs; also, we prove them via branch-and-bound, an algorithm considered inefficient from the theoretical point of view.

Proposition 1.1 gives another indication why the reformulations are relatively easy. One can observe that $\det(AA^T)$ can be quite large even for moderate values of M, if $A \in G_{m,n}(M)$ is a random matrix with $m \leq n$, although we could not find any theoretical studies on the subject. For instance, for a random $A \in G_{4,30}(100)$ we found $\det(AA^T)$ to be of the order 10^{18}.

While we cannot give a tight upper bound on the size of the B&B tree in terms of this determinant, we are able to bound the width of the reformulations along the last unit vector for any A (i.e., not just almost all).

Proposition 1.1. *If Q_R is computed using RKZ reduction, then*

$$\text{width}(e_n, Q_R) \leq \frac{\sqrt{n}\, \| (w_1; w_2) - (\ell_1; \ell_2) \|}{\det(AA^T + I)^{1/(2n)}}. \tag{1.12}$$

Also, if A has independent rows, and Q_N is computed using RKZ reduction, then

$$\text{width}(e_{n-m}, Q_N) \leq \frac{\gcd(A)\sqrt{n-m}\, \| w_2 - \ell_2 \|}{\det(AA^T)^{1/(2(n-m))}}. \tag{1.13}$$

The same results hold for the LLL-reformulations, if $\sqrt{n}$ and $\sqrt{n-m}$ are replaced by $2^{(n-1)/4}$ and $2^{(n-m-1)/4}$, respectively.

□

Remark 1.1. *As described in Section 5 of [17], and in [26] for the nullspace reformulation, directions achieving the same widths exist in Q, and they can be quickly computed. For instance, if p is the last row of U^{-1}, then* $\text{width}(e_n, Q_R) = \text{width}(p, Q)$.

A practitioner of integer programming may ask for the value of Theorems 1.1 and 1.2. Proposition 1.2 and a computational study put these results into a more practical perspective. Proposition 1.2 shows that when m and n are not too large, already fairly small values of M guarantee that the RKZ-nullspace reformulation (which has the smallest bound on M) of the majority of binary integer programs get solved at the root node.

Proposition 1.2. *Suppose that m and n are chosen according to Table 1, and M is as shown in the third column. Then for at least 90% of $A \in G'_{m,n}(M)$ and*

n	m	M for 90 %	M for 99 %
20	10	99	124
30	20	31	35
40	30	21	23
50	40	18	19
30	10	3478	4378
40	20	229	256
50	30	93	100
40	10	169000	212758
50	20	1844	2069
60	30	410	442
70	40	193	205

Table 1: Values of M to make sure that the RKZ-nullspace reformulation of 90 or 99 % of the instances of type (1.14) solve at the root node

all b right hand sides, reverse B&B solves the RKZ-nullspace reformulation of

$$\begin{aligned} Ax &= b \\ x &\in \{0,1\}^n \end{aligned} \tag{1.14}$$

at the root node. The same is true for 99% of $A \in G'_{m,n}(M)$, if M is as shown in the fourth column.

□

Note that 2^{n-m} is the best upper bound one can give on the number of nodes when B&B is run on the original formulation (1.14); also, randomly generated IPs with $n - m = 30$ are nontrivial even for commercial solvers.

According to Theorems 1.1 and 1.2, random integer programs with coefficients drawn from $\{1, \ldots, M\}$ should get easier, as M grows. Our computational study confirms this somewhat counterintuitive hypothesis on the family of marketshare problems of Cornuéjols and Dawande in [9].

We generated twelve 5 by 40 and twelve 10 by 40 matrices with entries drawn from $\{1,\ldots,M\}$ with $M = 100, 1000,$ and 10000 (this is 72 matrices overall), set $b = \lfloor Ae/2 \rfloor,$ where e is the vector of all ones, and constructed the instances of type (1.14), and

$$(1.15)\qquad \begin{array}{rcl} b - e \ \leq & Ax & \leq \ b \\ x & \in & \{0,1\}^n. \end{array}$$

The latter of these are a relaxed version, which correspond to trying to find an almost-equal market split.

Table 2 shows the average number of nodes (rounded to the nearest integer) that the commercial IP solver CPLEX 9.0 took to solve the rangespace reformulation of the inequality- and the nullspace reformulation of the equality-constrained 5 by 40 problems. Analogous results are listed in Table 3 for the 10 by 40 instances.

M	EQUALITY	INEQUALITY
100	17532	38885
1000	1254	22900
10000	201	1976

Table 2: Average number of B&B nodes to solve the inequality- and equality-constrained marketshare problems. Here $m = 5,$ and $n = 40$.

M	EQUALITY	INEQUALITY
100	20	1350
1000	5	72
10000	0	9

Table 3: Average number of B&B nodes to solve the inequality- and equality-constrained marketshare problems. Here $m = 10,$ and $n = 40$.

Since RKZ reformulation is not implemented in any software that we know of, we used the Korkhine-Zolotarev (KZ) reduction routine from the NTL library [27]. For brevity we only report the number of B&B nodes and not the actual computing times.

With $m = 5$, and $n = 40$, all equality-constrained instances turned out to be infeasible, except two, corresponding to $M = 100$. Among the inequality constrained problems there were fifteen feasible ones: all twelve with $M = 100$ and three with $M = 1000$. Since infeasible problems tend to be harder, this explains the more moderate decrease in difficulty as we go from $M = 100$ to $M = 1000$. With $m = 10$, and $n = 40$, all instances were infeasible.

Two remarks are in order. First, in the original marketshare problems in [9] n is always equal to $10(m-1)$: we generated problems with more constraints for more variety. Second, CPLEX reports that a problem solves with 0 B&B nodes, if it gets solved by cutting planes, and preprocessing only, and this is what happens for most of the equality constrained problems, when $m = 10$ and $n = 40$.

Overall, Tables 2 and 3 confirm the theoretical findings of the paper: the reformulations of random integer programs become easier as the size of the coefficients grow.

In Section 2 we introduce further notation and give the proof of Theorems 1.1 and 1.2.

2 Further Notation and Proofs

A lattice is a set of the form

$$(2.16)\qquad L = \mathbb{L}(B) = \{\, Bx \,|\, x \in \mathbb{Z}^r \,\},$$

where B is a real matrix with r independent columns, called a *basis* of L and r is called the *rank* of L.

The Euclidean norm of a shortest nonzero vector in L is denoted by $\lambda_1(L)$, and Hermite's constant is

$$(2.17)\quad C_j = \sup\left\{ \frac{\lambda_1(L)^2}{(\det L)^{2/j}} \,|\, L \text{ is a lattice of rank } j \right\}.$$

We define

$$(2.18)\qquad \gamma_i = \max\{\, C_1, \ldots, C_i \,\}.$$

A matrix A defines two lattices that we are interested in:

$$(2.19)\quad L_R(A) = \mathbb{L}(A; I),\ L_N(A) = \{x \in \mathbb{Z}^n | Ax = 0\},$$

where we recall that $(A; I)$ is the matrix obtained by stacking A on top of I.

Given independent vectors $b_1, \ldots, b_r$, the vectors $b_1^*, \ldots, b_r^*$ form the Gram-Schmidt orthogonalization of $b_1, \ldots, b_r$, if $b_1^* = b_1$, and b_i^* is the projection of b_i onto the orthogonal complement of the subspace spanned by $b_1, \ldots, b_{i-1}$ for $i \geq 2$. We have

$$(2.20)\qquad b_i = b_i^* + \sum_{j=1}^{i-1} \mu_{ij} b_j^*,$$

with

$$(2.21)\qquad \mu_{ij} \;=\; \langle b_i, b_j^* \rangle / \, \| b_j^* \|^2 \qquad (1 \leq j < i \leq r).$$

We do not define LLL and RKZ reducedness formally, only collect their properties that we will use below:

LEMMA 2.1. *Suppose that $b_1, \ldots, b_r$ is a basis of the lattice L with Gram-Schmidt orthogonalization $b_1^*, \ldots, b_r^*$. Then*

(1) if $b_1, \ldots, b_r$ is RKZ reduced, then

$$\| b_i^* \| \geq \lambda_1(L)/C_i, \tag{2.22}$$

and

$$\| b_r^* \| \geq (\det L)^{1/r}/\sqrt{r}. \tag{2.23}$$

(2) if $b_1, \ldots, b_r$ is LLL reduced, then

$$\| b_i^* \| \geq \lambda_1(L)/2^{(i-1)/2}, \tag{2.24}$$

and

$$\| b_r^* \| \geq (\det L)^{1/r}/2^{(r-1)/4}. \tag{2.25}$$

Proof. Statements (2.22) and (2.23) are proven in [18], and (2.24) is shown in [21]. We now consider the inequalities

$$\| b_i^* \| \leq 2^{(r-i)/2} \| b_r^* \| \quad (i = 1, \ldots, r), \tag{2.26}$$

which hold when the basis is LLL reduced. Multiplying them, and using $\| b_1^* \| \ldots \| b_r^* \| = \det L$ gives (2.25). □

LEMMA 2.1. *Let P be a polyhedron*

$$P = \{ y \in \mathbb{R}^r \mid \ell \leq By \leq w \}, \tag{2.27}$$

and $b_1^*, \ldots, b_r^*$ the Gram-Schmidt orthogonalization of the columns of B. When reverse B&B is applied to P, the number of nodes on the level of y_i is at most

$$\left(\left\lfloor \frac{\| w - \ell \|}{\| b_i^* \|} \right\rfloor + 1 \right) \ldots \left(\left\lfloor \frac{\| w - \ell \|}{\| b_r^* \|} \right\rfloor + 1 \right). \tag{2.28}$$

Proof. First we show

$$\text{width}(e_r, P) \leq \| w - \ell \| \, / \, \| b_r^* \| . \tag{2.29}$$

Let $y_{r,1}$ and $y_{r,2}$ denote the maximum and the minimum of y_r over P. Writing $\bar{B}$ for the matrix composed of the first $r-1$ columns of B and b_r for the last column, it holds that there is $y_1, y_2 \in \mathbb{R}^{r-1}$ such that $\bar{B}y_1 + b_r y_{r,1}$ and $\bar{B}y_2 + b_r y_{r,2}$ are in P. So

$$\begin{aligned} \| w - \ell \| &\geq \| (\bar{B}y_1 + b_r y_{r,1}) - (\bar{B}y_2 + b_r y_{r,2}) \| \\ &= \| \bar{B}(y_1 - y_2) + b_r(y_{r,1} - y_{r,2}) \| \\ &\geq \| b_r^* \| \, |y_{r,1} - y_{r,2}| \\ &= \| b_r^* \| \, \text{width}(e_r, P) \end{aligned}$$

holds, and so does (2.29).

After branching on $y_r, \ldots, y_{i+1}$, each subproblem is defined by a matrix formed of the first i columns of B, and bound vectors, which are translates of ℓ and w by the same vector. Hence the above proof implies that the width along e_i in each of these subproblems is at most

$$\| w - \ell \| \, / \, \| b_i^* \|, \tag{2.30}$$

and this completes the proof. □

Our Lemma 2.2 builds on Furst and Kannan's Lemma 1 in [12], with part (2) also being a direct generalization.

LEMMA 2.2. *Let $r > 0$. Then*

(1) the fraction of $A \in G_{m,n}(M)$ with $\lambda_1(L_R(A)) \leq r$ is at most

$$\frac{(2\lfloor r \rfloor + 1)^{n+m}}{M^m}.$$

(2) the fraction of $A \in G'_{m,n}(M)$ with $\lambda_1(L_N(A)) \leq r$ is at most

$$\frac{(2\lfloor r \rfloor + 1)^{n}}{M^m \chi_{m,n}(M)}.$$

Proof. We first prove (2). For v, a fixed nonzero vector in $\mathbb{Z}^n$, consider the equation

$$Av = 0. \tag{2.31}$$

There are at most $M^{m(n-1)}$ matrices in $G'_{m,n}(M)$ that satisfy (2.31): if the components of $n-1$ columns of A are fixed, then the components of the column corresponding to a nonzero entry of v are determined from (2.31).

The number of vectors in $\mathbb{Z}^n$ with norm at most r is at most $(2\lfloor r \rfloor + 1)^n$: if $v \in \mathbb{Z}^n$ satisfies $\| v \| \leq r$, then $|v_i| \leq r$ for all i, hence $|v_i| \leq \lfloor r \rfloor$ for all i. Also, the number of matrices in $G'_{m,n}(M)$ is $M^{mn}\chi_{m,n}(M)$. Therefore the sought ratio is bounded by

$$\frac{(2\lfloor r \rfloor + 1)^n M^{m(n-1)}}{M^{mn}\chi_{m,n}(M)} = \frac{(2\lfloor r \rfloor + 1)^n}{M^m \chi_{m,n}(M)}.$$

For (1), note that $(v_1; v_2) \in \mathbb{Z}^{m+n}$ is a nonzero vector in $L_R(A)$, iff $v_2 \neq 0$ and

$$Av_2 = v_1. \tag{2.32}$$

An argument like the one in the proof of (2) shows that for fixed $(v_1; v_2) \in \mathbb{Z}^{m+n}$ with $v_2 \neq 0$, there are at most $M^{m(n-1)}$ matrices in $G_{m,n}(M)$ that satisfy (2.32).

The number of vectors in $\mathbb{Z}^{n+m}$ with norm at most r is at most $(2\lfloor r \rfloor + 1)^{n+m}$, and the number of matrices in $G_{m,n}(M)$ is M^{mn}. Hence the ratio we are interested in is bounded by

$$\frac{(2\lfloor r \rfloor + 1)^{n+m} M^{m(n-1)}}{M^{mn}} = \frac{(2\lfloor r \rfloor + 1)^{n+m}}{M^m}.$$

□

Proof of Theorems 1.1 and 1.2. For part (1) in Theorem 1.1, let $b_1^*, \dots, b_n^*$ be the Gram-Schmidt orthogonalization of the columns of $(A; I)U$. Lemma 2.1 implies that reverse B&B solves (1.2) at the root, if

$$\| b_i^* \| > \| (w_1; w_2) - (\ell_1; \ell_2) \| \tag{2.33}$$

for $i = 1, \dots, n$. Let us now recall the definition of C_i from (2.17), and of γ_i from (2.18). Since the columns of $(A; I)U$ form an RKZ reduced basis of $L_R(A)$, (2.22) implies

$$\| b_i^* \| \geq \lambda_1(L_R(A))/C_i. \tag{2.34}$$

So (2.33) holds, when

$$\lambda_1(L_R(A)) > C_i \, \| (w_1; w_2) - (\ell_1; \ell_2) \| \tag{2.35}$$

does for $i = 1, \dots, n$, which is in turn implied by

$$\lambda_1(L_R(A)) > \gamma_n \, \| (w_1; w_2) - (\ell_1; \ell_2) \| . \tag{2.36}$$

Let ϵ be a real number between 0 and 1. By Lemma 2.2, the fraction of $A \in G_{m,n}(M)$ matrices for which (2.36) does *not* hold is at most ϵ, when

$$\frac{(2\lfloor \gamma_n \, \| (w_1; w_2) - (\ell_1; \ell_2) \| \rfloor + 1)^{n+m}}{M^m} \leq \epsilon,$$

i.e., when

$$M \geq \frac{(2\lfloor \gamma_n \, \| (w_1; w_2) - (\ell_1; \ell_2) \| \rfloor + 1)^{(n+m)/m}}{\epsilon^{1/m}}. \tag{2.37}$$

Using the known estimate $\gamma_n \leq 1 + n/4$ (see for instance [25]) , setting $\epsilon = 1/2^n$, and doing some algebra with (2.37) yields the required result.

The proof of part (2) of Theorem 1.1 is along the same lines: now $b_1^*, \dots, b_{n-m}^*$ is the Gram-Schmidt orthogonalization of the columns of B, which is an RKZ reduced basis of $L_N(A)$. Lemma 2.1 and the reducedness of B implies that reverse B&B solves (1.3) at the root, if

$$\lambda_1(L_N(A)) > \gamma_{n-m} \, \| w_2 - \ell_2 \| . \tag{2.38}$$

Again, letting ϵ be a real number between 0 and 1, Lemma 2.2 implies that the fraction of matrices in $G'_{m,n}(M)$ which do not satisfy (2.38) is at most ϵ, if

$$\frac{(2\lfloor \gamma_{n-m} \, \| w_2 - \ell_2 \| \rfloor + 1)^n}{M^m \chi_{m,n}(M)} \leq \epsilon,$$

that is, when

$$M \geq \frac{(\lfloor 2\gamma_{n-m} \, \| w_2 - \ell_2 \| \rfloor + 1)^{n/m}}{\epsilon^{1/m} (\chi_{m,n}(M))^{1/m}}. \tag{2.39}$$

Then simple algebra and using $\chi_{m,n}(M) \geq 1/2$ completes the proof.

The proof of Theorem 1.2 is an almost verbatim copy, now using the estimate (2.24) to lower bound $\| b_i^* \|$. □

Proof of Proposition 1.1. Let $b_1^*, \dots, b_n^*$ be the Gram-Schmidt orthogonalization of the columns of $(A; I)U$. Using (2.29) in the proof of Lemma 2.1 gives

$$\text{width}(e_n, Q_R) \leq \frac{\| (w_1; w_2) - (\ell_1; \ell_2) \|}{\| b_n^* \|}. \tag{2.40}$$

Next, from (2.23) we obtain

$$\| b_n^* \| \geq \frac{(\det L_R(A))^{1/n}}{\sqrt{n}}. \tag{2.41}$$

Also, the the definition of $L_R(A)$ implies

$$\det L_R(A) = \det(AA^T + I)^{1/2}, \tag{2.42}$$

and combining these three inequalities proves (1.12).

The proof of (1.13) is analogous, but now we need to use

$$\det L_N(A) = \det(AA^T)^{1/2} / \gcd(A), \tag{2.43}$$

whose proof can be found in [7] for instance. To prove the claims about the LLL-reformulations, we need to use (2.25) (in place of (2.23)) to lower bound $\| b_n^* \|$ or $\| b_{n-m}^* \|$. □

Proof of Proposition 1.2. Let $N(n, r)$ denote the number of integral points in the n-dimensional ball of radius r. In the previous proofs we used $(2\lfloor r \rfloor + 1)^n$ as an upper bound for $N(n, r)$. The proof of Part (2) of Theorem 1.1 actually implies that when

$$M \geq \frac{(N(n, \gamma_{n-m} \, \| w_2 - \ell_2 \|)^{1/m}}{\epsilon^{1/m} (\chi_{m,n}(M))^{1/m}}, \tag{2.44}$$

then for all, but at most a fraction of ϵ of $A \in G'_{m,n}(M)$ reverse B&B solves the RKZ-nullspace reformulation of (1.14) at the root node.

With $\| w_2 - \ell_2 \| = \sqrt{n}$ we would like to compute the smallest M that satisfies (2.44) for small values of n and m. First, we use Blichfeldt's upper bound [5]

$$C_i \leq \frac{2}{\pi} \Gamma\left(\frac{i+4}{2}\right)^{2/i}, \tag{2.45}$$

to conclude

$$\gamma_{n-m} \leq \frac{2}{\pi}\Gamma\left(\frac{n-m+4}{2}\right)^{2/(n-m)}. \tag{2.46}$$

Plugging (2.46) and (1.9) into (2.44) gives a valid lower bound for M. We use the values $\epsilon = 0.1$ and $\epsilon = 0.01$ and dynamic programming to exactly find the values of $N(n, r)$, to obtain Table 1.

We note that in general $N(n, r)$ is hard to compute, or find good upper bounds for; however for small values of n and r a simple dynamic programming algorithm finds the exact value quickly. □

Acknowledgement We thank Van Vu for pointing out reference [6]. We are very grateful to Greg Martin for discussions leading to the proof of Lemma 1.1.

References

[1] Karen Aardal, Robert E. Bixby, Cor A. J. Hurkens, Arjen K. Lenstra, and Job W. Smeltink. Market split and basis reduction: Towards a solution of the Cornuéjols-Dawande instances. *INFORMS Journal on Computing*, 12(3):192–202, 2000.

[2] Karen Aardal, Cor A. J. Hurkens, and Arjen K. Lenstra. Solving a system of linear Diophantine equations with lower and upper bounds on the variables. *Mathematics of Operations Research*, 25(3):427–442, 2000.

[3] Karen Aardal and Arjen K. Lenstra. Hard equality constrained integer knapsacks. *Mathematics of Operations Research*, 29(3):724–738, 2004.

[4] Karen Aardal and Arjen K. Lenstra. Erratum to: Hard equality constrained integer knapsacks. *Mathematics of Operations Research*, 31(4):846, 2006.

[5] Hans Frederik Blichfeldt. A new principle in the geometry of numbers, with some applications. *Transactions of the American Mathematical Society*, 15(3):227–235, 1914.

[6] Jean Bourgain, Van H. Vu, and Philip Matchett Wood. On the singularity probability of discrete random matrices. *Journal of Functional Analysis*, to appear.

[7] J. W. S. Cassels. *An introduction to the geometry of numbers*. Springer, 1997.

[8] Vašek Chvátal. Hard knapsack problems. *Operations Research*, 28(6):1402–1411, 1980.

[9] Gérard Cornuéjols and Milind Dawande. A class of hard small 0–1 programs. *INFORMS Journal on Computing*, 11(2):205–210, 1999.

[10] Gérard Cornuéjols, Miroslav Karamanov, and Yanjun Li. Early estimates of the size of branch-and-bound trees. *INFORMS Journal on Computing*, 18(1):86–96, 2006.

[11] Alan Frieze. On the Lagarias-Odlyzko algorithm for the subset sum problem. *SIAM Journal on Computing*, 15:536–540, 1986.

[12] Merrick Furst and Ravi Kannan. Succinct certificates for almost all subset sum problems. *SIAM Journal on Computing*, 18:550 – 558, 1989.

[13] Zonghao Gu, George L. Nemhauser, and Martin W. P. Savelsbergh. Lifted cover inequalities for 0–1 integer programs: Complexity. *INFORMS J. on Computing*, 11:117–123, 1998.

[14] Robert G. Jeroslow. Trivial integer programs unsolvable by branch-and-bound . *Mathematical Programming*, 6:105–109, 1974.

[15] Ravi Kannan. Minkowski's convex body theorem and integer programming. *Mathematics of Operations Research*, 12(3):415–440, 1987.

[16] A. Korkine and G. Zolotarev. Sur les formes quadratiques. *Mathematische Annalen*, 6:366–389, 1873.

[17] Bala Krishnamoorthy and Gábor Pataki. Column basis reduction and decomposable knapsack problems. *Discrete Optimization*, 6:242–270, 2009.

[18] Jeffrey C. Lagarias, Hendrik W. Lenstra, and Claus P. Schnorr. Korkine-Zolotarev bases and successive minina of a lattice and its reciprocal lattice. *Combinatorica*, 10(4):333–348, 1990.

[19] Jeffrey C. Lagarias and Andrew M. Odlyzko. Solving low-density subset sum problems. *Journal of ACM*, 32:229–246, 1985.

[20] A. H. Land and Alison G. Doig. An automatic method for solving discrete programming problems. *Econometrica*, 28:497–520, 1960.

[21] Arjen K. Lenstra, Hendrik W. Lenstra, Jr., and László Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261:515–534, 1982.

[22] Hendrik W. Lenstra, Jr. Integer programming with a fixed number of variables. *Mathematics of Operations Research*, 8:538–548, 1983.

[23] László Lovász and Herbert E. Scarf. The generalized basis reduction algorithm. *Mathematics of Operations Research*, 17:751–764, 1992.

[24] Greg Martin and Erick B. Wong. Almost all integer matrices have no integer eigenvalues. *The American Mathematical Monthly*, 116:588–598, 2009.

[25] Jacques Martinet. *Perfect Lattices in Euclidean Spaces*. Springer-Verlag, Berlin, 2003.

[26] Sanjay Mehrotra and Zhifeng Li. On generalized branching methods for mixed integer programming. *Research Report, Department of Industrial Engineering, Northwestern University*, 2004.

[27] Victor Shoup. NTL: A Number Theory Library, 1990. http://www.shoup.net.