SOLVING THE KNAPSACK PROBLEM VIA Z-TRANSFORM

JEAN B. LASSERRE AND EDUARDO S. ZERON

Abstract. Given vectors $a, c \in \mathbb{Z}^n$ and $b \in \mathbb{Z}$, we consider the (unbounded) knapsack optimization problem $\mathbb{P}: \min\{c'x \,|\, a'x = b;\, x \in \mathbb{N}^n\}$. We compute the minimum value p^* using techniques from complex analysis, namely Cauchy 's Residue Theorem to integrate a function in $\mathbb{C}^2$, and the $\mathbb{Z}$-transform of an appropriate function related to $\mathbb{P}$. The computational complexity depends on $s := \sum_{j=1}^n a_j$, not on the magnitude of b as in dynamic programming based approaches. We also completely characterize the number of solutions with value less than p, as a function of p.

1. Introduction

Given integer vectors $a, c \in \mathbb{Z}^n$ and an integer $b \in \mathbb{Z}$, we consider the *unbounded knapsack* optimization problem

$$\mathbb{P}: \quad p^* := \min\{c'x \,|\, a'x = b;\, x \in \mathbb{N}^n\}, \tag{1.1}$$

which is known to be NP-hard.

In this paper we propose an exact method to compute p^* which differs from previous known approaches. The primary goal here is not to compete with the efficient heuristics already available for hard knapsack problems as developed in e.g. Babaev et al. [1] or Chung [5] and the many references therein, not to mention the powerful LLL-type lattice reduction techniques of Lenstra, Lenstra, and Lovász for 0-1 knapsack problems in cryptography (see e.g. Schnorr and Hörner [8]). The proposed method brings some new insight into the problem and shows how simple techniques from complex analysis (widely used in number theory but not in optimization) can help understand and solve some discrete optimization problems (a similar technique was used in Lasserre and Zeron [10] to yield an algorithm for computing the volume of a convex polytope, and in Lasserre and Zeron [12] for solving a class of multivariate integration problems). We briefly recall that with a function $f : \mathbb{N} \to \mathbb{R}$ one may associate its (one-sided) $\mathbb{Z}$-transform $F : \mathbb{C} \to \mathbb{C}$, defined by

$$z \mapsto F(z) := \sum_{n=0}^{\infty} f(n) z^{-n},$$

assumed to be well-defined on a appropriate domain $|z| > r$ for some $r > 0$. Assuming that $f(n) = 0$ for $n < 0$, one may retrieve the value $f(n)$ from the complex integral

$$f(n) = \frac{1}{2\pi i} \int_{|z|=\gamma} F(z) z^{n-1}\, dz, \qquad n \in \mathbb{N}, \tag{1.2}$$

where $\gamma > r$ is fixed, arbitrary (see e.g. Debnath [7, Chap. 10]). For many cases of interest, Cauchy 's Residue Theorem is a powerful technique to compute the integral (1.2). The above also extends to the multi-dimensional case.

We reduce the original problem to a *counting problem* in a related lattice polytope as in [11]. We then use counting techniques based on generating functions as described in Brion and Vergnes [3, 4]. This technique uses the generating function of the function $(b,p)\mapsto f(b,p)$ which counts the *integral* points in the polytope $\{a'x=b; c'x\leq p; x\in\mathbb{R}^n\}$. It can be interpreted as a *dual* technique of those described in Barvinok and Pommersheim [2] (see also Diaz and Robbins [9]) as we work in the space of *dual* variables associated with the (non trivial) constraints of the polytope instead of working with the generating function in the original space $\mathbb{R}^n$. The idea can be summarized as follows. Consider the convex polytope

$$\Omega(b,p) := \{x\in\mathbb{R}^n_+ \,|\, a'x=b; \quad c'x\leq p\}, \tag{1.3}$$

and the function $(b,p)\mapsto f(b,p)$ that counts the number of integral points $x\in\mathbb{N}^n$ in $\Omega(b,p)$. Therefore, since the function $p\mapsto f_b(p):=f(b,p)$ is nonnegative and nondecreasing, for any fixed $b\in\mathbb{Z}$, we only need to detect the first value $p=p^*$ for which $f_b(p)\neq 0$; which, as we show below, can be done without knowledge of the function itself. To do this

- (a) we first provide a very simple closed-form expression of the two-dimensional $\mathbb{Z}$-transform $F(z_1,z_2)$ of $f(b,p)$.

- (b) we the show that the partial integration of F w.r.t. the variable z_1 associated with the constraint $a'x=b$, yields the $\mathbb{Z}$-transform G_b of $f_b(p)$.

- (c) the $\mathbb{Z}$-transform G_b is a rational fraction $P(z_2)/Q(z_2)$ of the remaining variable z_2; and thus, with simple arguments, it follows that p^* is just the difference of the degrees of P and Q. We also analyze the practical computation of P and Q.

From a computational point of view, the relevant quantities are the number N of positive entries a_j's in the knapsack constraint and the sum $s:=\sum_{j=1}^n a_j$. The magnitude of b is irrelevant. Hence, one can solve several problems with different b's without redoing most computations.

Finally, we also show that the function $f_b(p)$ has the following characterization. It can be written as the sum of a function $w(p)$ which takes *finitely many* values and a polynomial $P(p)$ of degree m, with *periodic* coefficients. The period γ is the least common multiple of the absolute value of some 2×2 sub-determinants of the matrix $[a|b]$. Therefore, the number of solutions with value less than $p=t\gamma$ is of the order t^m.

2. Main result

Let $\mathbb{Z}$ and $\mathbb{N}$ denote the sets of integers and natural numbers respectively (we consider 0 to be a natural number), and let x' denote the transpose of any vector $x\in\mathbb{R}^n$.

Consider the function $f:\mathbb{Z}^2\to\mathbb{N}$ defined by

$$(b,p) \mapsto f(b,p) := |\,\mathbb{N}^n\cap\{x\,|\,a'x=b;\, c'x\leq p\}\,| \tag{2.1}$$

(where $|A|$ denotes the cardinality of A). That is, f *counts* the integral points in the convex rational polytope (1.3).

Next, for fixed $b\in\mathbb{Z}$, let $f_b:\mathbb{Z}\to\mathbb{N}$ be the function

$$p \mapsto f_b(p) := f(b,p). \tag{2.2}$$

Since f_b is obviously non-negative and non-decreasing, with p^* as in (1.1), we have

$$p^* = c'x^* \quad\Leftrightarrow\quad f_b(p^*)\geq 1 \quad\text{and}\quad f_b(p)=0 \quad \forall\, p<p^*. \tag{2.3}$$

Moreover, let $F : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$ be the two-sided $\mathbb{Z}$-transform of f, that is,

$$z \mapsto F(z_1, z_2) := \sum_{j,k\in\mathbb{Z}} f(j,k) z_1^{-j} z_2^{-k}, \tag{2.4}$$

for $(z_1, z_2) \in \Gamma \subset \mathbb{C}^2$.

Theorem 2.1. *Let $(a, c) \in \mathbb{Z}^n \times \mathbb{Z}^n$ and assume that $p^* > -\infty$.*

(a) *For every $z \in \mathbb{C}^2$ such that*

$$|z_2| > 1 \quad and \quad |z_1^{a_j} z_2^{c_j}| > 1 \quad \forall j = 1, \ldots, n, \tag{2.5}$$

we have

$$F(z_1, z_2) = \frac{z_2}{z_2 - 1} \prod_{j=1}^{n} \left(1 - z_1^{-a_j} z_2^{-c_j}\right)^{-1}. \tag{2.6}$$

(b) *Fix $\alpha_1, \alpha_2 \in \mathbb{R}$ such that $\alpha_2 > 1$ and $\alpha_1^{a_j} \alpha_2^{c_j} > 1$ for $j = 1, \ldots, n$. Then*

$$f(b, p) = \frac{1}{(2\pi i)^2} \int_{|z_1|=\alpha_1} \int_{|z_2|=\alpha_2} z_1^{b-1} z_2^{p-1} F(z_1, z_2)\, dz_1\, dz_2. \tag{2.7}$$

Proof. Let $(z_1, z_2) \in \mathbb{C}^2$

$$\begin{aligned} F(z_1, z_2) &= \sum_{j,k\in\mathbb{Z};\ a'x=j,\ c'x\le k} z_1^{-j} z_2^{-k} = \sum_{x\in\mathbb{N}^n} z_1^{-a'x} \sum_{k=c'x}^{\infty} z_2^{-k} \\ &= \frac{z_2}{z_2 - 1} \sum_{x\in\mathbb{N}^n} z_1^{-a'x} z_2^{-c'x} \quad \text{if} \quad |z_2| > 1 \\ &= \frac{z_2}{z_2 - 1} \prod_{j=1}^{n} \left(1 - z_1^{-a_j} z_2^{-c_j}\right)^{-1} \quad \text{[if (2.5) holds.]} \end{aligned}$$

Point (b) follows from Cauchy 's Residue Theorem (see e.g. Conway [6]). It remains to prove that the domain (2.5) is not empty. Since $p^* > -\infty$, the recession cone of the polytope $\Omega(b, p)$ in (1.3), i.e.,

$$\{x \in \mathbb{R}^n \,|\, x \ge 0, \quad a'x = 0, \quad c'x \le 0\},$$

reduces to the singleton $\{0\}$; equivalently $\Omega(b, p)$ is compact. Therefore, it immediately follows from an adapted version of Farkas Lemma due to Carver, that the cone

$$\Omega^* := \{\lambda_1, \lambda_2 \in \mathbb{R} \,|\, \lambda_2 > 0; \quad a_j\lambda_1 + c_j\lambda_2 > 0 \quad \forall j = 1, \ldots, n\}$$

is not empty (e.g. see Schrijver [13, (33), p. 95]). We may then take $(\alpha_1, \alpha_2) := (e^{\lambda_1}, e^{\lambda_2})$ for some arbitrary $(\lambda_1, \lambda_2) \in \Omega^*$. □

2.1. **Computing $f(b, p)$.** From equation (2.7), we can directly calculate the value of $f(b, p)$ at each point (b, p) by computing a double integral.

However, we need *not* compute the double integral defined in (2.7) in order to determine the minimal value p^* in (1.1). We can instead use implicit properties of the $\mathbb{Z}$-transform and proceed as follows.

Fix $\alpha_1, \alpha_2 \in \mathbb{R}$ such that $\alpha_2 > 1$ and $\alpha_1^{a_j} \alpha_2^{c_j} > 1$ for $j = 1, \ldots, n$; next, calculate the following integral, where $b \in \mathbb{Z}$ is fixed;

$$G_b(z_2) := \frac{1}{2\pi i} \int_{|z_1|=\alpha_1} z_1^{b-1} F(z_1, z_2)\, dz_1. \tag{2.8}$$

Obviously, $G_b(z_2)$ is well defined for $\alpha_2 - \epsilon < |z_2| < \alpha_2 + \epsilon$ and $\epsilon > 0$ *small enough*. Moreover, we can express (2.8) as an infinite sum by using definition (2.4) for $F(z_1, z_2)$, which yields

$$\begin{aligned} G_b(z_2) &= \sum_{j,k\in\mathbb{Z}} f(j,k) z_2^{-k} \frac{1}{2\pi i} \int_{|z_1|=\alpha_1} z_1^{b-j-1} dz_1 \\ &= \sum_{k\in\mathbb{Z}} f(b,k) z_2^{-k} = \sum_{k\in\mathbb{Z}} f_b(k) z_2^{-k}. \end{aligned} \tag{2.9}$$

Notice that from (2.9), $G_b(z_2)$ is the $\mathbb{Z}$-transform of $p \mapsto f_b(p)$ for every fixed $b \in \mathbb{Z}$. On the other hand, after calculating (2.8), it immediately follows that $G_b(z_2)$ is a rational function, say

$$G_b(z_2) := \frac{P(z_2)}{Q(z_2)}, \tag{2.10}$$

for some real polynomials P and Q. If $P \equiv 0$ then $f_b(p) = 0$ for all $p \in \mathbb{Z}$, and so $p^* = +\infty$; that is, the equation $a'x = b$ has no integer solution $x \in \mathbb{N}^n$.

Now define the number:

$$p_o := \text{degree}(Q) - \text{degree}(P), \tag{2.11}$$

where P and Q are given on (2.10). It is easy to see that

$$\begin{aligned} \lim_{|z_2|\to\infty} z_2^{p_o} G_b(z_2) &\neq 0 \quad \text{and} \\ \lim_{|z_2|\to\infty} z_2^{p} G_b(z_2) &= 0 \quad \text{whenever} \quad p < p_o. \end{aligned}$$

Hence, recalling the expression (2.9) of $G_b(z_2)$, we can conclude that

$$f(b, p_o) \neq 0 \quad \text{and} \quad f(b,p) = 0 \quad \text{whenever} \quad p < p_o.$$

The preceding constitutes a proof of the following result.

Theorem 2.2. *Let $p^* > -\infty$ be the minimum value of $\mathbb{P}$ in (1.1) and let P and Q be as in (2.10). Then*
(a) $p^* = +\infty$ *if $P \equiv 0$ (the equation $a'x = b$ has no integral solution $x \in \mathbb{N}^n$).*
(b) *if $P \not\equiv 0$ one has*

$$p^* := \text{degree}(Q) - \text{degree}(P). \tag{2.12}$$

2.2. **Practical computation.** We can calculate polynomials P and Q in (2.10) by directly integrating (2.8) using Cauchy 's Residue Theorem (see e.g. Conway [6]); however, we next introduce some observations that make calculations easier.

First we need to locate the poles of $F(z_1, z_2)$ with respect to z_1. These poles are given by $\xi_{jk} = e^{2\pi i k/a_j} z_2^{-c_j/a_j}$, for $k = 1, \ldots, |a_j|$ and $j = 1, \ldots, n$. Besides, recall that we are setting $|z_1| = \alpha_1 > 0$ and $|z_2| = \alpha_2 > 1$ with $\alpha_1^{a_j} \alpha_2^{c_j} > 1$. Hence, only the poles ξ_{jk} with $k = 1, \ldots, a_j$ and a_j strictly positive are located *inside* the integration path $|z_1| = \alpha_1$, because $|\xi_{jk}| = \alpha_2^{-c_j/a_j} < \alpha_1$ only if $a_j > 0$.

Thus, we only need to consider the poles $\xi_{jk} = e^{2\pi i k/a_j} z_2^{-c_j/a_j}$ with $a_j > 0$ in order to integrate (2.8). We will suppose from now on that at least one entry of a is strictly positive, and we order the components of a such that $a_j > 0$ if $j = 1, \ldots, N$ and $a_j \leq 0$ if $j = N+1, \ldots, n$.

Moreover, with no loss of generality, we may assume that $b \geq 0$ (otherwise consider the equality $-a'x = -b$), and that $F(z_1, z_2)$ has only simple poles (with respect to z_1) located inside the integration path $|z_1| = \alpha_1$. This happens whenever none of the 2×2 determinants

$$\Delta_{ij} := \begin{vmatrix} a_i & c_i \\ a_j & c_j \end{vmatrix} \tag{2.13}$$

vanishes for $i, j = 1, \ldots, N$.

Indeed, computation gets simplified for we then have the following decomposition into simple fractions; setting $s := \sum_{j=1}^{N} a_j$ we have that $s > 0$ and :

$$\begin{aligned} \frac{F(z_1, z_2)}{z_1} &= \frac{z_1^{s-1}\, z_2}{z_2 - 1} \prod_{j=1}^{n} \left(z_1^{a_j} - z_2^{-c_j} \right)^{-1} \\ &= \sum_{j=1}^{N} \frac{A_j(z_1, z_2)}{z_1^{a_j} - z_2^{-c_j}} + \frac{A_0(z_1, z_2)}{\prod_{j>N}(1 - z_1^{|a_j|} z_2^{-c_j})}, \end{aligned}$$

where, for all $j = 0, 1, \ldots, N$,
- $A_j(., z_2)$ is a polynomial with respect to z_1, and
- $A_j(z_1, .)$ is a rational function with respect to z_2.

The coefficients of A_j can be calculated either symbolically or numerically by solving a linear system of s variables. The latter because one knows in advance that the the denominator of $A_j(z_1, .)$ is of the form $z_2^{\beta_k}(z_2 - 1) \prod_{i \neq j}(z^{\Delta_{ij}} - 1)$ with Δ_{ij} as in (2.13). Moreover, the degree of $A_j(., z_2)$ with respect to z_1 is less than a_j for $j = 1, \ldots, N$, and so,

$$A_j(z_1, z_2) = \sum_{k=0}^{a_j - 1} A_{jk}(z_2)\, z_1^k \quad \text{for all} \quad j = 1, \ldots, N,$$

where each coefficient $A_{jk}(z_2)$ is a rational function of z_2 with real coefficients. On the other hand, the integral (2.8) depends only on the poles located inside the integration path. Therefore,

$$G_b(z_2) = \sum_{j=1}^{N} \sum_{k=0}^{a_j - 1} \frac{A_{jk}(z_2)}{2\pi i} \int_{|z_1| = \alpha_1} \frac{z_1^{k+b}}{z_1^{a_j} - z_2^{-c_j}}\, dz_1. \tag{2.14}$$

Notice that the term z_1^b does not introduce any new pole at zero because we are supposing b to be greater than or equal to zero. Finally, each one of previous integrals can be easily calculated to get (recall that $|z_1^{a_j} z_2^{b_j}| = \alpha_1^{a_j} \alpha_2^{c_j} > 1$),

$$\begin{aligned} \frac{1}{2\pi i} \int_{|z_1| = \alpha_1} \frac{z_1^{k+b}}{z_1^{a_j} - z_2^{-c_j}}\, dz_1 &= \frac{1}{2\pi i} \int_{|z_1| = \alpha_1} \frac{z_1^{k+b-a_j}}{1 - z_1^{-a_j} z_2^{-c_j}}\, dz_1 \\ &= \sum_{x \geq 0} \frac{z_2^{-c_j x}}{2\pi i} \int_{|z_1| = \alpha_1} z_1^{k+b-(x+1)a_j}\, dz_1 \\ &= \begin{cases} z_2^{-c_j x} & \text{if } x = \frac{k+b+1}{a_j} - 1 \in \mathbb{N}, \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

Thus, (2.14) can be rewritten, for $b \geq 0$, as follows

$$G_b(z_2) = \sum_{j=1}^{N} \sum_{k=0}^{a_j - 1} \begin{cases} A_{jk}(z_2) z_2^{-c_j x} & \text{if } x = \frac{k+b+1}{a_j} - 1 \in \mathbb{N}, \\ 0 & \text{otherwise.} \end{cases} \tag{2.15}$$

Example 2.3. Consider Problem (1.1) in $\mathbb{R}^3$ with vectors $a = (2, 3, -5)$ and $c = (1, -1, 2)$. Thus, F in Theorem 2.1 is given by

$$\frac{F(z_1, z_2)}{z_1} = \frac{z_1^4\, z_2}{(z_2 - 1)(z_1^2 - z_2^{-1})(z_1^3 - z_2)(1 - z_1^5 z_2^{-2})},$$

and $|z_1| = \alpha_1 > 0$, $|z_2| = \alpha_2 > 1$, with $\alpha_1^2\alpha_2 > 1$, $\alpha_1^3\alpha_2^{-1} > 1$ and $\alpha_1^{-5}\alpha_2^2 > 1$. Hence, we can set $\alpha_1 = 2$ and $\alpha_2 = 6$. Moreover, since the determinant

$$\begin{vmatrix} 2 & 3 \\ 1 & -1 \end{vmatrix} \neq 0,$$

we have the expansion

$$\begin{aligned} \frac{F(z_1, z_2)}{z_1} &= \frac{z_2^4 + z_2^6 + z_2^7 + (z_2^4 + z_2^5 + z_2^7)z_1 + (z_2^3 + z_2^5 + z_2^7)z_1^2}{(z_2 - 1)^2(z_2^5 - 1)(z_1^3 - z_2)} \\ &\quad - \frac{z_2^5 + z_2^{12} + (z_2^8 + z_2^{10})z_1}{(z_2 - 1)(z_2^5 - 1)(z_2^9 - 1)(z_1^2 - z_2^{-1})} \\ &\quad + \frac{A_0(z_1, z_2)}{(z_2 - 1)^2(z_2^9 - 1)(1 - z_1^5 z_2^{-2})}. \end{aligned}$$

Thus, $N = 2$, $a_1 = 2$, $a_2 = 3$, and:

$$A_{10}(z_2) = -\frac{z_2^5 + z_2^{12}}{(z_2 - 1)(z_2^5 - 1)(z_2^9 - 1)},$$

$$A_{11}(z_2) = \frac{-z_2^8 - z_2^{10}}{(z_2 - 1)(z_2^5 - 1)(z_2^9 - 1)}; \quad A_{20}(z_2) = \frac{z_2^4 + z_2^6 + z_2^7}{(z_2 - 1)^2(z_2^5 - 1)},$$

$$A_{21}(z_2) = \frac{z_2^4 + z_2^5 + z_2^7}{(z_2 - 1)^2(z_2^5 - 1)}; \quad A_{22}(z_2) = \frac{z_2^3 + z_2^5 + z_2^7}{(z_2 - 1)^2(z_2^5 - 1)}.$$

Finally, if for instance $b := 10$, we get

$$\begin{aligned} G_{10}(z_2) &= A_{11}(z_2)z_2^{-5} + A_{21}(z_2)z_2^3 \\ &= \frac{-z_2^3 + z_2^4 - z_2^5 + z_2^6 + z_2^7 + z^9 + z_2^{11} + z_2^{12} + z_2^{14}}{(z_2 - 1)^2(z_2^9 - 1)}. \end{aligned} \tag{2.16}$$

Thus, the minimum value $p^* = -3$, which can be checked to be exact.

Remark 2.4. It is important to emphasize that in contrast to dynamic programming based approaches, the computational complexity does *not* depend on the magnitude of b. Indeed, b is only involved in (2.15) to get the final expression of $G_b(z_2)$. The relevant parameters are

- the number N of positive entries a_j
- the sum $s := \sum_{j=1}^n a_j$.

2.3. **Further characterization.** We have already seen that $G_b(z_2)$ is the $\mathbb{Z}$-transform of $f_b(p)$, cf. (2.9), where $f_b(p)$ counts the integral points in the convex polytope $\Omega(b, p)$ for b *fixed*. Moreover, the function $G_b(z_2) = P(z_2)/Q(z_2)$ is rational, cf. (2.10), and we can determine where its poles are located.

The poles $\{\xi_{jk}\}$ of $F(z_1, z_2)$ w.r.t. to z_1 are given by $\xi_{jk} = e^{2\pi ik/a_j} z_2^{-c_j/a_j}$, for $k = 1, \ldots, |a_j|$ and $j = 1, \ldots, n$. Notice that we could be counting the same pole several times, so let Ξ be the set of all different poles ξ_{jk} whose absolute value is less than α_1. We can calculate integral (2.8) by using Cauchy 's Residue Theorem, i.e.,

$$G_b(z_2) \;=\; \sum_{\xi_{jk}\in\Xi} \mathrm{Res}(z_1^{b-1}F,\, \xi_{jk}) \;+\; \mathrm{Res}(z_1^{b-1}F,\, 0). \tag{2.17}$$

Recalling that $\mathrm{Res}(z_1^{b-1}F,\, 0) = 0$ whenever $b \geq 1$, (e.g. see Conway [6]); and if m is the multiplicity of the pole $z_1 = \xi_{jk}$,

$$\mathrm{Res}(z_1^{b-1}F, \xi_{jk}) \;=\; \frac{1}{(m-1)!}\,\frac{d^{m-1}}{dz_1^{m-1}}\left[(z_1-\xi_{jk})^m z_1^{b-1}F(z_1,z_2)\right]_{z_1=\xi_{jk}}.$$

Now it is easy to see that the denominator of each residue $\mathrm{Res}(z_1^{b-1}F,\cdot)$ has factors only of the form z_2^{β}, (z_2-1) or $(\xi_{jk}^{a_l} - z_2^{-c_l})$ with $j \neq l$, we only need to recall the definition (2.6) of F. Thus, by adding terms in (2.17) and recalling that $G_b = P/Q$, we can deduce that $Q(z_2)$ has a factorization into terms which are only of the form z_2^{β}, (z_2-1) or $(z_2^{|c_j a_l - c_l a_j|} - 1)$.

For instance, back to Example 2.3, we may indeed check that $G_{10}(z_2)$ in (2.16) factorizes into terms of the form $(z_2^s - 1)$, where s is the absolute value of some 2×2 determinant of the matrix

$$\begin{bmatrix} 2 & 1 \\ 3 & -1 \\ -5 & 2 \end{bmatrix}.$$

Therefore, from the integration of $G_b(z_2)$, the function $p \mapsto f_b(p)$ can be characterized as follows: It is the sum of

- a function $p \mapsto w(p)$ which is equal to zero outside a finite interval $[s_1, s_2] \in \mathbb{Z}$. That is, $w(p) = 0$ if $p < s_1$ or $p > s_2$.

- a *polynomial* $p \mapsto P^*(p)$ whose degree m is the multiplicity of the pole $z_2 = 1$ in $G_b(z_2)$, minus 1, and whose coefficients are *periodic*.

If all the entries $\{a_j\}$ are positive then the polynomial P^* is a constant for the knapsack polytope $\{x \in \mathbb{R}^n \mid a'x = b\}$ has a finite number of integral points (b is fixed).

For instance, consider again Example 2.3. We can decompose G_b into simple fractions :

$$\begin{aligned} G_b(z_2) \;&=\; z_2^3 \,+\, 2z_2^2 \,+\, 4z_2 \,+\, \frac{181\,z_2}{27\,(z_2-1)} \,+\, \frac{10\,z_2}{3\,(z_2-1)^2} \,+ \\ &\quad \frac{5\,z_2}{9\,(z_2-1)^3} \,-\, \frac{z_2^2+2z_2}{27\,(z_2^2+z_2+1)} \,+\, \frac{z_2^6-z_2^2}{3\,(z_2^6+z_2^3+1)} \end{aligned}$$

Thus, $f_{10}(p) = w(p) + P^*(p)$, with

$$w(p) \;=\; \begin{cases} 1 & \text{if } p=-3, \\ 2 & \text{if } p=-2, \\ 4 & \text{if } p=-1, \\ 0 & \text{otherwise,} \end{cases}$$

$$P^*(p) \;=\; \begin{cases} \frac{5p(p-1)}{18} + \frac{10p}{3} + e_0(p) & \text{if } p \geq 0, \\ 0 & \text{otherwise,} \end{cases}$$

where $e_0(p)$ is the only periodic coefficient of P^*, with period $\gamma = 9$. Notice that the leading term of polynomial P^* has degree 2 because the pole $z_2 = 1$ has multiplicity 3.

Thus, when $p > s_2$ is a multiple $t\gamma$ of the period γ, the function $f_b(t\gamma)$ is the polynomial $t \mapsto P^*(t\gamma)$ that we call the *Ehrhart polynomial* of the polytope $\Omega_b(t\gamma)$. However, observe that $\Omega_b(t\gamma)$ is *not* the dilated polytope $\{tx;\, x \in \Omega_b(\gamma)\}$ and $\Omega_b(\gamma)$ is not an integer polytope in general (as in the usual definition of the Ehrhart polynomial of a dilated polytope). But still, $f_b(t\gamma)$ is a polynomial. It also follows that the number of admissible solutions with value less than $t\gamma$, $t \in \mathbb{N}$, is of the order t^m.

3. Conclusion

We have provided a new approach for solving the knapsack problem. Using the $\mathbb{Z}$-transform of a related function of two variables, the problem is solved by computing the (partial) $\mathbb{Z}$-inverse transform w.r.t. one of the variables via Cauchy's Residue Theorem. From a computational point of view, the relevant quantity is the number N of positive entries a_j in the knapsack constraint and the sum $s := \sum_{j=1}^n a_j$. In contrast to dynamic programming based methods, the magnitude of b is irrelevant. In addition, this approach permits to characterize the function that counts the number of integral points in the polytope $\{a'x = b;\, c'x \leq p;\, x \geq 0\}$, as a function of the threshold value p.

References

[1] D. Babaev, F. Glover and J. Ryan. A new knapsack solution approach by integer equivalent aggregation and consistency determination, *INFORM J. Comp.* **9** (1997), 43–50.
[2] A.I. Barvinok, J.E. Pommersheim. An algorithmic theory of lattice points in polyhedra, in *New Perspectives in Algebraic Combinatorics*, MSRI Publications **38** (1999), 91–147.
[3] M. Brion, M.Vergne. Lattice points in simple polytopes, *J. Amer. Math. Soc.* **10** (1997), 371–392.
[4] M. Brion, M.Vergne. Residue formulae, vector partition functions and lattice points in rational polytopes. *J. Am. Math. Soc.* **10**, No.4, 797–833.
[5] C-S. Chung, M.S. Hung and W.O. Rom. A hard knapsack problem, *Naval Res. Log.* **35** (1988), 85–98.
[6] J.B. Conway. *Functions of a complex variable I*, 2nd ed., Springer, New York, (1978).
[7] L. Debnath. *Integral Transforms and Their Applications*, CRC Press, Boca Raton, 1995.
[8] C-P. Schnorr, H. Hörner. Attacking the Chor-Rivest Cryptosystem by Improved Lattice Reduction, in: *Theory and Application of Cryptographic Techniques*, Lectures Notes in Computer Sciences **921**, Springer, 1995, pp. 1–12.
[9] R. Diaz and Sinai Robins. The Ehrhart polynomial of a lattice n-simplex, *ERA Amer. Math. Soc.* **2**, No 1, August 1996.
[10] J.B. Lasserre, E.S. Zeron. A Laplace transform algorithm for the volume of a convex polytope. *J. of the ACM*, to appear.
[11] J.B. Lasserre, E.S. Zeron. On counting integral points in a convex polytope. Technical report # 01353 (2001), LAAS-CNRS, Toulouse, France.
[12] J.B. Lasserre, E.S. Zeron. Solving a class of multivariate integration problems via Laplace techniques. *Appl. Math. (Warsaw)* **28** (2001), 391–405.
[13] A. Schrijver. *Theory of Linear and Integer Programming*, John Wiley & Sons, Chichester, 1986.

LAAS-CNRS, 7 avenue du Colonel Roche, 31 077 Toulouse cédex 4, France
E-mail address: lasserre@laas.fr

Depto. Matemáticas, CINVESTAV-IPN, Apdo. Postal 14-740, Mexico D.F. 07000, México
E-mail address: eszeron@math.cinvestav.mx