JOURNAL OF COMBINATORIAL THEORY (A) **13**, 170–175 (1972)

On the Number of Solutions to a Diophantine Equation

BRUCE FAALAND*

Graduate School of Business, University of Washington, Seattle, Washington 98105

Communicated by G. B. Dantzig

Received April 13, 1970

Let $A_1, ..., A_r, \bar{x}_1, ..., \bar{x}_r$, and A be known positive integers. Let $f(A)$ be the number of integer solutions $(x_1, ..., x_r)$ satisfying the Diophantine equation

$$\sum_{j=1}^{r} A_j x_j = A$$

and the conditions $0 \leqslant x_j \leqslant \bar{x}_j$, $j = 1, ..., r$. This paper expresses $f(A)$ recursively as a linear function of $f(0), f(1), ..., f(A\text{-}1)$.

INTRODUCTION

Mignosi [5] obtained the number of non-negative integer solutions to the equation

$$\sum_{j=1}^{r} A_j x_j = A, \tag{1}$$

where $A_1, ..., A_r$ and A are known positive integers. Implicit in equation (1) is the requirement that

$$x_j \leqslant \left[\frac{A}{A_j}\right], \qquad j = 1, ..., r,$$

where $[t]$ denotes the largest integer less than or equal to t. This paper generalizes Mignosi's result by obtaining the number of integer solutions satisfying

$$\sum_{j=1}^{r} A_j x_j = A, \qquad 0 \leqslant x_j \leqslant \bar{x}_j, \qquad j = 1, ..., r, \tag{2}$$

where $\bar{x}_j$, $j = 1, ..., r$, are arbitrary positive integers.

* This research was supported by the Office of Naval Research and the National Science Foundation. Reproduction in whole or in part is permitted for any purpose of the United States Government.

The problem of finding the number of integer solutions to (2) is of particular interest in integer programming. For example, it can be shown that on any integer programming problem which may be solved by the Bound-and-Scan Algorithm [4], the number of solutions to an equation of type (2) is an upper bound on the number of iterations required by the algorithm to solve the problem.

An integer solution to (2) may also be interpreted as a partition of A composed of x_j parts of size A_j, $j = 1,..., r$, where at most $\bar{x}_j$ parts of size A_j are available for the partition. In the special case in which no upper bounds are specified, where $A = r$, and where $A_j = j$ $(j = 1,..., r)$, the solutions to (2) are called unrestricted partitions of A (see [2]). In another special case, where the A_j are required only to be distinct, the number of solutions to (2) has as an upper bound the number of unrestricted partitions of A (usually designated by $p(A)$). While the calculation of the number of solutions to (2) for large A may not be practical in certain cases, asymptotic results are well known for $p(A)$ [3].

The Number of Solutions

THEOREM. *Let $f(A)$ denote the number of integer solutions to* (2) *and* $P_j \equiv A_j(\bar{x}_j + 1)$, $j = 1,..., r$. *Define*

$$Q_k \equiv \sum_{\substack{j=1\\ j \ni A_j | k}}^{r} A_j - \sum_{\substack{j=1\\ j \ni P_j | k}}^{r} P_j, \qquad k = 1,..., A. \tag{3}$$

Then $f(0) = 1$ *and*

$$f(k) = \frac{1}{k} \sum_{m=1}^{k} Q_m f(k-m), \qquad k = 1,..., A. \tag{4}$$

Proof. Clearly $f(0) = 1$ because only the solution $x_1 = \cdots = x_r = 0$ satisfies (2) if $A = 0$. In general, $f(k)$ is the coefficient of v^k in

$$\sum_{k=0}^{\infty} f(k)\, v^k = \prod_{j=1}^{r} \left(\sum_{m=0}^{\bar{x}_j} v^{mA_j} \right). \tag{5}$$

It is well known that, for every $b \neq 1$,

$$\sum_{j=0}^{r} b^j = \frac{1 - b^{r+1}}{1 - b},$$

and, if $|b| < 1$,

$$\sum_{j=0}^{\infty} b^j = \frac{1}{1-b}.$$

Therefore (5) may be written as

$$1 = \sum_{k=0}^{\infty} f(k)\, v^k \cdot \prod_{j=1}^{r} \frac{(1 - v^{A_j})}{(1 - v^{P_j})}. \tag{6}$$

Taking the logarithm of each side of (6) and then the derivative with respect to v gives

$$\sum_{j=1}^{r} \left(\frac{A_j v^{A_j - 1}}{1 - v^{A_j}} - \frac{P_j v^{P_j - 1}}{1 - v^{P_j}} \right) = \frac{\sum_{k=1}^{\infty} k f(k)\, v^{k-1}}{\sum_{k=0}^{\infty} f(k)\, v^k}.$$

Now use the expansion of

$$\frac{1}{1 - v^{A_j}} \quad \text{and} \quad \frac{1}{1 - v^{P_j}}$$

to obtain the relationship

$$\sum_{j_1=0}^{\infty} \left\{ A_1 v^{A_1(j_1+1)-1} - P_1 v^{P_1(j_1+1)-1} \right\} + \cdots + \sum_{j_r=0}^{\infty} \left\{ A_r v^{A_r(j_r+1)-1} - P_r v^{P_r(j_r+1)-1} \right\}$$

$$= \frac{\sum_{k=1}^{\infty} k f(k)\, v^{k-1}}{\sum_{k=0}^{\infty} f(k)\, v^k}. \tag{7}$$

Consider the coefficient Q_j of v^{j-1} on the left side of (7):

$$Q_j = \sum_{m \in K_j} A_m - \sum_{m \in L_j} P_m,$$

where $K_j = \{m\colon 1 \leqslant m \leqslant r$ and there exists an integer $j_m \geqslant 0 \ni A_m(j_m + 1) = j\}$
$= \{m\colon 1 \leqslant m \leqslant r$ and $A_m \mid j\}$, and
$L_j = \{m\colon 1 \leqslant m \leqslant r$ and there exists an integer $j_m \geqslant 0 \ni P_m(j_m + 1) = j\}$
$= \{m\colon 1 \leqslant m \leqslant r$ and $P_m \mid j\}$.

By the definition of Q_j,

$$\sum_{j=1}^{\infty} Q_j v^{j-1} = \frac{\sum_{k=1}^{\infty} k f(k)\, v^{k-1}}{\sum_{k=0}^{\infty} f(k)\, v^k}. \tag{8}$$

Multiplying both sides of (8) by $\sum_{k=0}^{\infty} f(k)\, v^k$ results in

$$\sum_{k=1}^{\infty} \left\{ \sum_{m=1}^{k} Q_m f(k-m) \right\} v^{k-1} = \sum_{k=1}^{\infty} k f(k)\, v^{k-1}. \tag{9}$$

Equating coefficients of v^{k-1} in (9) yields the desired expression for $f(k)$.

Some Computational Considerations

Given that $Q_1, \ldots, Q_A$ have been determined, one may obtain $f(A)$ by finding $f(k)$ for $k = 1, \ldots, A$, in that order, by (4). This calculation involves

$$1 + 2 + \cdots + A = \frac{A(A+1)}{2}$$

integer multiplications and A integer divisions. The following method for calculating $Q_1, \ldots, Q_A$ involves only addition and comparison operations:

Step 1. Initialize $Q_1 = \cdots = Q_A = 0$.
Step 2. Set $j = 1$.
Step 3. Set SUM $= 0$.
Step 4. Reset SUM $=$ SUM $+ A_j$.
Step 5. If SUM $> A$, go to Step 7.
Step 6. Reset $Q_{\text{SUM}} = Q_{\text{SUM}} + A_j$. Go to Step 4.
Step 7. Set SUM $= 0$.
Step 8. SUM $=$ SUM $+ P_j$.
Step 9. If SUM $> A$, go to Step 11.
Step 10. Reset $Q_{\text{SUM}} = Q_{\text{SUM}} - P_j$. Go to Step 8.
Step 11. Reset $j = j + 1$. If $j \leqslant r$, go to Step 3.
Step 12. END.

The above procedure has the advantage of avoiding the $2rA$ divisions which would have to be made if $Q_1, \ldots, Q_A$ were calculated directly.

The calculation of $f(A)$ directly from (4) is not practical for large A because of the number of multiplications required. In the application to integer programming mentioned above, A is chosen to be the integer part of the largest of $(r-1)$ positive numbers, each of which, according to Hillier [4, p. 652], "tends to be very small (the order of magnitude of one)." Therefore, in this case one would expect that A would usually be small enough to make the calculation of $f(A)$ practical.

In applications in which A is large, the following technique may be used to reduce the number of multiplications. For $j = 1,\ldots, r$, let

$$Z_j = \begin{cases} P_j, & \text{if } P_j \leqslant A, \\ A_j, & \text{otherwise,} \end{cases} \tag{10}$$

and let T be the least common multiple of $Z_1,\ldots, Z_r$. For any integer $k \leqslant A$ there exist unique integers t, q satisfying

$$k = tT + q,$$

where $t \geqslant 0$ and $0 \leqslant q < T$. By (3), $Q_k = Q_q$, so that the Q_m terms ($m = 1,\ldots, A$) are periodic with period T, and (4) becomes

$$f(k) = \frac{1}{k}\left(\sum_{m=1}^{q} Q_m \sum_{i=0}^{t} f(k - m - iT) + \sum_{m=q+1}^{T} Q_m \sum_{i=0}^{t-1} f(k - m - iT)\right), \qquad k = 1,\ldots, A. \tag{11}$$

If $T \geqslant A$, no advantage is gained by (11). However, if $T < A$, $T(T+1)/2$ multiplications and T divisions are needed to calculate $f(0), f(1),\ldots, f(T)$ from (4), but only $T(A - T)$ multiplications and $(A - T)$ divisions to obtain $f(T+1),\ldots, f(A)$ from (11), or

$$AT - \frac{T(T-1)}{2}$$

multiplications and A divisions in all.

For example, consider finding the number of nonnegative integer solutions to the equation

$$x_1 + 3x_2 + 2x_3 = 1000, \qquad x_1 \leqslant 5. \tag{12}$$

In (12), $Z_1 = 6$, $Z_2 = 3$, $Z_3 = 2$, so $T = 6$, and $A = 1000$. The calculation of $f(1000)$ by (4) directly would require 500,500 multiplications, but by (11) only 5,985.

If both A and T are large, the enumeration of all solutions of the Diophantine equation (2) may require fewer calculations than the calculations needed in (4) (see [1]). If, in addition, r is close to A and if the $\bar{x}_i$ are large, the asymptotic results for $p(A)$ would be a good approximation. Clearly, it would be very useful to have asymptotic results for $f(A)$.

REFERENCES

1. W. A. BLANKINSHIP, Algorithm 288, solution of simultaneous linear Diophantine equations [F4], *Comm. ACM* **9** (1966), 514.
2. H. GUPTA, Partitions—a survey, *J. Res. Nat. Bur. Standards Sect. B*, January-March, 1970.
3. M. HALL, "Combinatorial Theory," Chapt. 4, Blaisdell, Waltham, Mass., 1967.
4. F. S. HILLIER, A Bound-and-Scan Algorithm for pure integer linear programming with general variables, *Operations Res.* **17** (1969), 638–679.
5. G. MIGNOSI, Sulla equazione lineare indeterminata, *Period. Mat.* **23** (1908), 173–176.