EUCLIDES Y LA PROGRAMACION MATEMATICA

Jesús Agustín Cano Garcés*

RESUMEN

El problema de encontrar el máximo común divisor de n números enteros dados, $c^1, c^2, \ldots, c^n$ se plantea como un problema de Programación en números enteros y se utiliza una versión modificada del algoritmo de las formas acotantes de Glover para resolverlo. Como solución, el algoritmo produce el mcd $\{c^1, c^2, \ldots, c^n\}$ y además un conjunto de coeficientes enteros $x_1, x_2, \ldots, x_n$ tales que mcd $\{c^1, c^2, \ldots, c^n\} = c^1x_1 + c^2x_2 + \ldots + c^nx_n$.

Además, el hecho de interpretar este problema como uno de Programación Matemática proporciona adicionalmente una expresión para calcular <u>todos</u> los conjuntos de valores enteros $x_1, x_2, \ldots, x_n$ que satisfacen.

$$\text{mcd } \{c^1, c^2, \ldots, c^n\} = c^1x_1 + c^2x_2 + \ldots + c^nx_n .$$

I. INTRODUCCION

Es bien conocido el algoritmo de Euclides para determinar el máximo común divisor de dos enteros no nulos c^1 y c^2; basta deter

* Profesor Titular, Facultad de Ciencias, U.N.A.M.

minar una sucesión de residuos, cada uno de los cuales resulta ser una combinación lineal de c^1 y c^2 y el máximo común divisor será el último residuo diferente de cero que así se haya encontrado. En [1] se hace notar además, que se puede suponer que c^1 y c^2 son enteros positivos y que el procedimiento se extiende para resolver el problema de determinar el máximo común divisor de un conjunto finito de enteros positivos $c^1, c^2, \dots, c^n$, el cual será denotado como:

$$\text{mcd } \{c^1, c^2, \dots, c^n\}$$

El propósito fundamental de este artículo es mostrar que este problema se puede plantear como uno de programación en números enteros. El problema de la programación en números enteros, denotado PPNE, es un caso particular del problema general de la Programación Matemática y puede describirse como sigue (ver [2]). Determinar los valores de $x_1, x_2, \dots, x_n$ que hagan mínimo el valor de z,

$$z = c^1 x_1 + c^2 x_2 + \dots + c^n x_n$$

y que satisfagan al mismo tiempo un sistema de ecuaciones,

$$\begin{aligned}
a_1^1 x + a_1^2 x_2 + \dots + a_1^n x_n &= b_1 \\
a_2^1 x_1 + a_2^2 x_2 + \dots + a_2^n x_n &= b_2 \\
\\
a_m^1 x_1 + a_m^2 x_2 + \dots + a_m^n x_n &= b_m
\end{aligned}$$

y las restricciones adicionales,

$$x_j \geq 0$$

$$x_j \in Z,\ j = 1,2,\ldots,n,$$

donde c^j, a_i^j y b_i son coeficientes reales dados.

En notación matricial, se puede escribir abreviadamente,

$$\text{PPNE} \ldots \quad \begin{array}{c} \text{Min } z = cx \\ \text{s.c.} \\ Ax = b \\ x \geq 0 \\ x \in Z^n \end{array}$$

La otra finalidad para la cual ha sido escrito este artículo es describir un método para resolver el PPNE de entre los muchos que existen, y así proporcionar al lector que carezca de ella, una somera visión de esta rama de las Matemáticas Aplicadas. Para el caso de los lectores que ya hayan tenido contacto con la programación matemática, servirá como una ilustración en cuanto a las relaciones de esta con otras ramas de las Matemáticas.

II. FORMULACION DEL PROBLEMA

El problema consiste, como se ha esbozado ya en la introducción, en determinar el máximo común divisor de números enteros positivos dados, $c^1, c^2, \ldots, c^n$. En esta sección se demostrará que este problema se resuelve utilizando un modelo de programación entera. Con este fin, se define

$$C = \{c \mid c = \sum_{j=1}^{n} c^j x_j,\ x_j \in Z\ j=1,2,\dots,n\},$$

es decir, el conjunto de todas las combinaciones lineales, con coeficientes enteros, de los números enteros dados c^1, c^2, ..., c^n. También, se denotará

$$\text{mcd } C$$

a cualquier entero c^* que satisfaga las siguientes condiciones:

i) Si $c \in C$ entonces $c^* \mid c$

ii) Si $c' \in Z$, $c' \mid c\ \forall\, c \in C$, entonces $c' \mid c^*$

Proposición 1.

Sea c^* el mínimo entero positivo que pertenece a C. Entonces $c^* = \text{mcd } C$.

Demostración

Es claro que el conjunto C contiene enteros positivos y entonces contiene un elemento que es el mínimo entero positivo, el cual se denota c^* y que es de la forma

$$c^* = \sum_{j=1}^{n} c^j x_j^*$$

para un cierto conjunto de enteros x_1^* , x_2^* , ..., x_n^* .

Hay que demostrar que c^* satisface las propiedades i) y ii) enunciadas anteriormente.

Sea $c \in C$ un elemento cualquiera; existen x_1, x_2, ..., x_n enteros tales que

$$c = \sum_{j=1}^{n} c^j x_j$$

De acuerdo al algoritmo de Euclides, dados dos enteros en este caso c y c^*, existen enteros q y r tales que

$$c = c^* q + r, \quad 0 \le r < c^*$$

es decir,

$$\sum_{j=1}^{n} c^j x_j = q \sum_{j=1}^{n} c^j x_j^* + r,$$

o sea

$$\sum_{j=1}^{n} c^j (x_j - q x^*_j) = r$$

Como

$$(x_j - q x_j^*) \in Z \quad j=1,2,...,n$$

se tiene que

$$r \in C$$

Y como c^* es el mínimo entero positivo en C, entonces

$$r = 0$$

$$\therefore c^* | c$$

Para probar la segunda parte, supóngase que existe $c' \in \mathbb{Z}$ tal que

$$c'|c \qquad \forall \quad c \in C;$$

puesto que

$$c^* \in C, \quad \text{se tendrá}$$

$$c'|\ c^*$$

Para justificar la escritura

$$c^* = \text{mcd } C$$

es necesario probar la unicidad del mcd C, lo cual es una cuestión trivial y se omite.

Proposición 2.

$$c^* = \text{mcd } \{c^1,\ c^2, \ldots, c^n\}$$

Demostración:

Cada uno de los enteros positivos dados pertenece al conjunto C, pues basta tomar $x_j = 1$, $x_i = 0$, $i \neq j$ para poder escribir

$$c^j = \sum_{i=1}^{n} c^i x_i$$

Entonces, de acuerdo a la proposición anterior, se sabe que

$$c^*|c^j \quad \text{para cada} \quad j=1,2,\ldots,\ n$$

Ahora, suponiendo que c' es un divisor común de los enteros $c^1,\ c^2, \ldots, c^n$, se tiene

$$c^j = c'd^j, \qquad d^j \in Z, \quad j=1,2,\ldots,n$$

y substituyendo el valor de c^j en la expresión de c^* se tendrá

$$c^* = \sum_{j=1}^{n} c^j x^*_j \; = \; c' \sum_{j=1}^{n} d^j x^*_j$$

y como

$$\sum_{j=1}^{n} d^j x^*_j \qquad \in \quad Z$$

entonces

$$c' \mid c^*$$

Esta afirmación, aunada al hecho de que c^* es un divisor común de los enteros $c^1, c^2, \ldots, c^n$, permite concluir

$$c^* = \text{mcd}\ \{c^1, c^2, \ldots, c^n\}$$

En virtud de estas dos proposiciones, el problema se reduce a determinar el mínimo entero positivo del conjunto C, y esto se puede hacer resolviendo el siguiente PPNE.

$$\text{Min } z = c^1x_1 + c^2\ x_2 + \ldots + c^n x_n$$

$$\text{s.c.} \qquad c^1x_1 + c^2x_2 + \ldots + c^n x_n \geq 1$$

$$x_j \in Z, \quad j=1,2,\ldots,n$$

Como se ve, este PPNE difiere ligeramente del planteamiento general de un PPNE, ya que la única restricción de este problema no es una igualdad y además los variables pueden - tomar valores negativos. Para subsanar la primera discrepancia, basta restar una variable, denominada variable de holgura y que debe tomar valores enteros no negativos, con lo cual el problema quedará planteado como sigue:

$$\text{Min } z = c^1x_1 + c^2x_2 + \ldots + c^nx_n$$

s.c.

$$c^1x_1 + c^2x_2 + \ldots + c^nx_n - x_{n+1} = 1$$

$$x_{n+1} \geq 0$$

$$x_j \in Z, \quad j=1,2,\ldots,n+1.$$

Respecto a la condición que se impone en el planteamiento general del PPNE, de que los variables tomen valores no negativos, se verá que puede hacerse a un lado si se modifica adecuadamente el algoritmo que se presenta en la siguiente sección y que sirve para resolver el problema.

III. UN METODO PARA RESOLVER EL PPNE

El método que se propone aquí para resolver el PPNE es debido a Glover (ver [3]) y pertenece a una clase de métodos denominados Métodos de los Planos Cortantes.

La idea principal en estos algoritmos consiste en resolver primeramente el problema, sin tomar en cuenta las restricciones

$$x_j \in Z, \quad j=1,2,\ldots,n$$

utilizando técnicas de programación lineal. Si la solución a este problema relajado es tal que los valores de las variables son enteros, entonces será también la solución óptima al PPNE. Si este no es el caso, entonces se añaden restricciones, tales que cualquier conjunto de valores enteros de los variables que satisfagan las restricciones iniciales, también satisfarán las adicionales, eliminando al mismo tiempo la solución no entera de la que se había partido (ver [8]).

De un punto de vista geométrico, estos métodos pueden describirse diciendo que primeramente se resuelve el problema sobre un conjunto convexo de soluciones factibles; si la solución no corresponde a un punto con coordenadas enteras, entonces se añade un hiperplano que corta una parte de este conjunto convexo, sin eliminar los puntos con coordenadas enteras que se hallaban dentro, pero eliminando al mismo tiempo, la solución no entera que se tenía.

El Método de Glover resuelve el problema siguiente:

$$\begin{aligned} \text{Min} \quad & z = cx \\ \text{s.c.} \quad & Ax = b \\ & x \geq 0 \\ & x \in Z^n \end{aligned}$$

donde

A , una matriz mxn de rango m,

c , un vector 1xn y

b , un vector mx1, son dados.

Se puede demostrar (ver [5]), que si el problema tiene una solución óptima finita, entonces existe un subconjunto de variables llamadas no básicas y cuyos índices pertenecen a un conjunto que se denomina J, $J \subset \{1,2,\ldots,n\}$ y tales que se puede escribir

(1) ... $x = \alpha + \beta x_J$,

donde

$$x = \begin{bmatrix} z \\ \cdots \\ x_J \\ \cdots \\ x_I \end{bmatrix} \quad \alpha = \begin{bmatrix} zo \\ \cdots \\ 0 \\ \cdots \\ \overline{x}_I \end{bmatrix} \quad \beta = \begin{bmatrix} c^J - z_J \\ \cdots \\ U \\ \cdots \\ -y_I{}^J \end{bmatrix}$$

y donde

zo es el valor de la función objetivo

$\overline{x}_I$ es un vector de valores de las variables básicas en esa solución.

$c^J - z_J$ es el vector de costos reducidos de las variables no básicas.

U es una matriz identidad de rango (n-m)

$I = \{1,2,\ldots,n\} - J$

Para poder aplicar el algoritmo de Glover se supone que se ha escrito el problema en la forma (1) y que satisface las siguientes condiciones:

$$\alpha i \in \mathbf{Z}$$

$$\beta_i^j \in \mathbf{Z} \qquad i = 1,2,\ldots,n$$

$$\beta^j > 0 \qquad j \in J$$

donde se denota que un vector es lexicográficamente positivo

$$\beta^j > 0$$

si la primera componente no nula del vector es positiva, y además no es el vector nulo.

La última de estas condiciones indica que se principia considerando una solución que es óptima, pero que posiblemente no satisface algunas de las condiciones de no negatividad sobre las variables. Es decir, el método va determinando soluciones enteras que son óptimas pero no factibles, hasta encontrar la solución factible óptima.

Supóngase que existe una ecuación tal que

$$x_i = \alpha i + \sum_{j \in J} \beta_i^j \, x_j$$

con

$$\alpha_i < 0 \, ,$$

$$(2) \ldots \qquad \beta_i^k > 0 \, ,$$

$$\beta_i^j \leq 0 \, , \quad j \in J, \quad j \neq k.$$

Como se debe imponer la condición de no negatividad sobre la variable x_i, entonces se impondrá

$$\sum_{j \in J} \beta_i^j x_j \geq -\alpha i > 0$$

de la cual necesariamente se debe tener

$$\beta_i^k x_k \geq -\alpha i$$

es decir

$$x_k \geq \frac{-\alpha i}{\beta_i^k}$$

para cualquier solución factible del problema. Si además se requieren únicamente soluciones enteras, entonces esta condición es equivalente a

$$x_k \geq \left\lceil \frac{-\alpha i}{\beta_i^k} \right\rceil > 0$$

donde $\lceil Y \rceil$ indica el menor entero que es mayor o igual a Y. Esta restricción es un plano cortante, pues no elimina ninguna solución entera factible y en cambio hace que la solución entera que se tenía, y que no es factible, sea eliminada.

Sin embargo, no siempre se cuenta con ecuaciones que satisfagan (2) y es necesario hacer ciertas transformaciones al sistema de ecuaciones para obtenerlas. Así, sea un índice $\ell \in \{1,2,\ldots,n\}$ tal que

$$x_\ell = \alpha_\ell + \sum_{j \in J} \beta_\ell^j \, x_j$$

con

$$\alpha_\ell < 0$$

y sea

$$J^+ = \{ j \in J \mid \beta_\ell^j > 0 \}$$

Se selecciona entre los índices que pertenecen a J^+, al índice k tal que

$$\beta^k = \min_{j \in J^+} \{\beta^j\}$$

donde el mínimo se considera en el sentido lexicográfico.

Dividiendo la ecuación entre β_ℓ^k y considerando el hecho que x_ℓ debe ser no negativo, se tiene

$$\sum_{\substack{j \in J \\ j \neq k}} \left(\frac{\beta_\ell^j}{\beta_\ell^k}\right) x_j + x_k \geq \frac{-\alpha_\ell}{\beta_\ell^k}$$

y definiendo una variable x_k' como sigue

$$(3)\ldots \quad x_k' = \sum_{\substack{j \in J^+ \\ j \neq k}} \left| \frac{\beta_\ell^j}{\beta_\ell^k} \right| x_j + x_k$$

se despeja x_k de esta ecuación y se elimina del sistema, obteniendo una nueva representación

$$x = \alpha' + \beta' x_{J'}$$

donde

$$(4)\ldots \quad \begin{aligned} \alpha' &= \alpha \\ (\beta^j) &= \beta^j \quad , \quad j \notin J^+ \\ (\beta^j)' &= \beta^j - \left\lceil \frac{\beta^j_\ell}{\beta^k_\ell} \right\rceil \beta^j \quad , \quad j \in J^+ \ , \ j \neq k \\ (\beta^k)' &= \beta^k \end{aligned}$$

Es claro de estas fórmulas de transformación que la nueva - ecuación donde aparece x_ℓ satisface (2) y se puede entonces generar el plano cortante correspondiente. Si a la nueva variable x'_k se le redenomina x_k teniendo en consideración que esta x_k no es la misma variable que la anterior, sino que están ligadas por la relación (3), se tendrá

$$x_k \geq \left\lceil \frac{-\alpha_\ell}{\beta^k_\ell} \right\rceil = q$$

Agregando este plano cortante al sistema, junto con la variable de holgura correspondiente y utilizando el método dual lexicográfico para reoptimizar el problema, se obtiene una nueva representación

$$x = \alpha' + \beta' x_J$$

con

$$\alpha' = \alpha + q\beta^k$$

$$(\beta^j)' = \beta^j \quad , \quad j \in J$$

Para asegurar la convergencia del método, se necesita que en cada interación las columnas de la matriz β queden lexicograficamente positivas (ver [6]). Si se denomina μ_j al mayor entero tal que

$$\beta^j - \mu_j \beta^k \geq 0$$

entonces de (4), vemos que las columnas de β quedan lexicopositivas si

$$\mu_j \geq \left[\frac{\beta_\ell^j}{\beta_\ell^k} \right] , \quad j \in J^+$$

Para tomar en cuenta este hecho, se define

$$p_j = \min \left\{ \left[\frac{\beta_\ell^j}{\beta_\ell^k} \right] , \quad \mu_j \right\} , \; j \in J^+$$

y se utiliza como ecuación adicional en lugar de (3)

$$x_k' = \sum_{\substack{j \in J^+ \\ j \neq k}} p_j x_j + x_k$$

Si al hacer la transformación correspondiente, no se satisface (2), entonces se repite el procedimiento hasta que finalmente se satisfagan estas condiciones.

Resumiendo, el algoritmo de Glover puede presentarse como sigue:

(0) Escribir el problema en la forma

$$X = \alpha + \beta X_J$$

con $\alpha i \in Z$

$\beta_i^j \in Z$ $\quad\quad$ $i=1,2,\ldots,n$, $j \in J$

$\beta^j > 0$

(1) Calcular

$$\alpha_\ell = \min_{i=1,\ldots,n} \{\alpha_i\}$$

- Si $\alpha_\ell \geq 0$, entonces la solución es la buscada. Terminar.

- Si $\alpha_\ell < 0$, ir al paso (2).

(2) Sea $J^+ = \{j \in J \mid \beta_\ell^j > 0\}$

- Si $J^+ = \emptyset$, entonces el problema no tiene soluciones enteras factibles. Terminar.
- Si $J^+ \neq \emptyset$ ir al paso (3).

(3) Sea $k \in J^+$ tal que

$$\beta^k = \underset{j \in J^+}{\ell\text{-min}} \{\beta^j\}$$

Calcular μ_j como se definió más arriba

y calcular $\left\lfloor \dfrac{\beta_\ell^j}{\beta_\ell^k} \right\rfloor$, $j \in J^+$. Ir al paso (4)

(4) Sea

$$P_j = \min \left\{ \left[\frac{\beta_\ell^j}{\beta_\ell^k} \right], \mu_j \right\}, \; j \in J^+.$$

Transformar el sistema utilizando

$$\alpha' = \alpha$$

$$(\beta^j)' = \beta^j \quad , \; j \notin J^+ - \{k\}$$

$$(\beta^j)' = \beta^j - P_j \beta^k \quad , \; j \in J^+ - k$$

Llamar α y β a las matrices así obtenidas.

- Si $\left[\frac{\beta_\ell^j}{\beta_\ell^k} \right] \leq \mu_j \quad \forall \; j \in J^+$

Calcular $q = \left[\frac{-\alpha_\ell}{\beta_\ell^k} \right]$ y hacer una transformación adicional utilizando

$$\alpha' = \alpha + q\beta^k$$

$$\beta' = \beta$$

Llamar nuevamente α y β a las nuevas matrices e ir al paso (1)

- Si existe $j \in J^+$ tal que $\left[\frac{\beta_\ell^j}{\beta_\ell^k} \right] > \mu_j$ entonces ir al paso (1).

Para ejemplificar la utilización de este algoritmo, se resolverá el siguiente problema:

$$\begin{aligned} \text{Min} \quad z = {} & X_1 + 2X_2 \\ \text{s.c.} \quad & 3X_1 + X_2 \geq 6 \\ & 4X_1 + 5X_2 \geq 20 \\ & 2X_2 \geq 3 \\ & X_1 , X_2 \geq 0 \\ & X_1 , X_2 \in \mathbb{Z} \end{aligned}$$

El conjunto de puntos que satisfacen este conjunto de restricciones está representado en la gráfica 1. Para poder aplicar el algoritmo, se necesita convertir en ecuaciones cada una de las desigualdades propuestas, esto mediante la utilización de variables de holgura que se denominan X_3, X_4 y X_5. Así, el problema se replantea como

$$\begin{aligned} \text{Min} \quad z = {} & X_1 + 2X_2 \\ \text{s.c.} \quad & 3X_1 + X_2 - X_3 = 6 \\ & 4X_1 + 5X_2 - X_4 = 20 \\ & 2X_2 - X_5 = 3 \\ & \left.\begin{array}{l} X_j \geq 0 \\ X_j \in \mathbb{Z} \end{array}\right. \quad j=1,\ldots,5. \end{aligned}$$

Ahora para escribir este sistema en la forma

$$x = \alpha + \beta X_J$$

se escoge $J = \{1,2\}$ y únicamente se presentan α y β en forma tabular, con lo que se obtiene,

z	0	1	2
X_1	0	1	0
X_2	0	0	1
X_3	-6	3	1
X_4	-20	4	5
X_5	-3	0	2

representación que satisface los requerimientos del paso (0) del algoritmo,

(1) $\ell = 4 \qquad \alpha_\ell = -20$

(2) $J^+ = \{1,2\}$

(3) $k = 1 \quad , \quad \mu_1 = 1, \ \mu_2 = 1 \ , \left[\dfrac{\beta_4^1}{\beta_4^1}\right] = \left[\dfrac{4}{4}\right] = 1, \ \left[\dfrac{\beta_4^2}{\beta_4^1}\right] = \left[\dfrac{5}{4}\right] = 2$

(4) $P_1 = 1 \quad , \ P_2 = 1$

y se obtiene la siguiente tabla

z	0	1	1
X_1	0	1	-1
X_2	0	0	1
X_3	-6	3	-2
X_4	-20	4	1
X	-3	0	2

Puesto que $\left[\frac{\beta_4^2}{\beta_4^1}\right] > \mu_2$, entonces la solución permanece sin cambiar y se va nuevamente al paso (1) del algoritmo.

(1) $\ell = 4$, $\alpha_\ell = -20$

(2) $J^+ = \{1,2\}$

(3) $k = 2$, $\mu_1 = 1$, $\mu_2 = 1$, $\left[\frac{\beta_4^1}{\beta_4^2}\right] = \left[\frac{4}{1}\right] = 4$, $\left[\frac{\beta_4^2}{\beta_4^2}\right] = \left[\frac{1}{1}\right] = 1$

(4) $P_1 = 1$, $P_2 = 1$

y se obtiene

z	0	0	1
X_1	0	2	-1
X_2	0	-1	1
X_3	-6	5	-2
X_4	-20	3	1
X_5	-3	-2	2

Para la siguiente interación,

(1) $\ell=4$, $\alpha_4 = -20$

(2) $J^{+} = \{1,2\}$

(3) $k=2$, $\mu_1=1$, $\mu_2 \rightarrow \infty$, $\left\lceil \dfrac{\beta_4^1}{\beta_4^1} \right\rceil = \left\lceil \dfrac{3}{3} \right\rceil = 1$, $\left\lceil \dfrac{\beta_4^2}{\beta_4^1} \right\rceil = \left\lceil \dfrac{1}{3} \right\rceil = 1$

(4) $P_1=1$, $P_2=1$, $q = \left\lceil \dfrac{-(-20)}{3} \right\rceil = 7$

obteniendo la siguiente tabla, la cual tiene asociada otra - solución entera no factible, representada en la gráfica 1 como el segundo punto que toca la trayectoria flechada,

z	0	0	1
X_1	14	2	-3
X_2	-7	-1	2
X_3	29	5	-7
X_4	1	3	-2
X	-17	-2	4

Esta nueva solución se obtuvo al agregar una cortadura que eliminaba la anterior, pero que conservaba las soluciones enteras factibles dicha cortadura está dada por

$$2X_1 + 3\,X_2 \geq 7$$

y también se ilustra en la gráfica 1.

En el cuadro 1, se dan las tablas que se obtienen durante las siguientes iteraciones del algoritmo hasta obtener la solución factible óptima. Cada una de ellas representa soluciones enteras no factibles que se van aproximando a la solución óptima y se han representado también en la gráfica 1, así como las cortaduras que se van añadiendo al problema.

Cuadro 1.

	5	0	1	5	0	1	6	0	1	6	0	1	7	0	1	7	0	1
X_1	-1	2	-3	5	2	-3	2	2	-3	4	2	-3	1	2	-3	3	2	-3
X_2	3	-1	2	0	-1	2	2	-1	2	1	-1	2	3	-1	2	2	-1	2
X_3	-6	5	-7	9	5	-7	2	5	-7	7	5	-7	0	5	-7	5	5	-7
X_4	-9	3	-2	0	3	-2	-2	3	-2	1	3	-2	-1	3	-2	2	3	-2
X_5	3	-2	4	-3	-2	4	1	-2	4	-1	-2	4	3	-2	4	1	-2	4

IV MODIFICACION AL METODO DE GLOVER

Para poder resolver el problema planteado en II, será necesario modificar en parte el algoritmo de Glover, para considerar el hecho que las variables $X_1, X_2, \ldots, X_n$ no necesitan ser no negativas. - Además, ahora el renglón donde aparece **z** coincide con el renglón --

donde aparece x_{n+1} y una vez que se logre tener un solo elemento positivo ahí, se tendrá una desigualdad del tipo

$$\beta_{n+1}^{k}\ x_k \geq -\alpha_{n+1} \quad , \quad \text{es decir,}$$

$$x_k \geq \left\lceil \frac{-\alpha_{n+i}}{\beta_{n+1}^{k}} \right\rceil$$

que deberá ser satisfecha necesariamente por cualquier solución - entera factible y además se busca minimizar

$$z = \beta_{n+1}^{k}\ x_k$$

que da como solución trivial

$$x_k = 1$$

$$z = \beta_{n+1}^{k}$$

donde x_k no es necesariamente la misma $_k$ del comienzo.

Así, el algoritmo modificado será como sigue:

(0) Escribir el problema en la forma

$$x = \alpha + \beta x_J$$

con

$$\alpha_i \in Z$$

$$\beta_i^j \in Z \qquad i = 1,2,\ldots,n+1$$

$$\beta^j > 0 \qquad j \in J$$

lo cual se puede hacer en forma tabular como sigue:

z	0	c^1	c^2	$\cdots$	c^n
x_1	0	1	0	$\ldots$	0
x_2	0	0	1	$\ldots$	0
.	.				
.	.				
.	.				
x_n	0	0	0	$\ldots$	1
x_{n+1}	-1			$\ldots$	

(1) $\alpha_\ell \equiv \alpha_{n+1} < 0$ Ir al paso (2)

(2) Sea $J^+ = \{j \epsilon J \mid \beta^j_{n+1} > 0\}$

(3) Sea $k \epsilon J^+$

tal que

$$\beta^k_{n+1} = \min_{j \epsilon J^+} \{\beta^j_{n+1}\}$$

calcular

$$P_j = \left\lfloor \frac{\beta^j_{n+1}}{\beta^k_{n+1}} \right\rfloor \quad , \quad j \epsilon J^+$$

donde $\lfloor X \rfloor$ denota al mayor entero menor o igual a **X**.

- Si $|J^+| > 1$ ir al paso (4)
- Si $|J^+| \leq 1$ ir al paso (5)

(4) Transformar el sistema utilizando

$$\alpha' = \alpha$$

$$(\beta^j)' = \beta^j \quad , \quad j \notin J^+ - \{k\}$$

$$(\beta^j)' = \beta^j - P_j \beta^k \ , \ j \in J^+ - \{k\}$$

Llamar α y β a las matrices así obtenidas a ir al paso (1)

(5) Calcular $q = \left\lceil \frac{-\alpha_{n+1}}{\beta^k_{n+1}} \right\rceil = 1$ y transformar la tabla, utilizando

$$\alpha' = \alpha + q\beta^k$$

$$\beta' = \beta$$

La solución es óptima, terminar. Entonces se tiene

$$\text{mcd } \{c^1, c^2, \ldots, c^n\} = \alpha_0$$

y además se tiene un conjunto de coeficientes $X_1, X_2, \ldots, X_n$ que proporcionan α_0

$$\alpha_0 = \sum_{j=1}^{n} c^j \alpha_j$$

Aún más, se tiene toda una familia de combinaciones lineales que producen α_0, y que están dados por

$$X_i = \alpha_i + \sum_{j\in J} \beta_i^j Y_j \quad , \; i=1,2,\ldots,n$$

donde Y_j son constantes cualesquiera, $j\in J$, excepto para el índice j que está asociado a la última constante positiva de la ecuación de X_{n+1}, que debe tener un valor de 0.

Ejemplo: Calcular el máximo común divisor de 6, 15 y 24.

Se plantea el problema equivalente

$$\text{Min } z = 6X_1 + 15X_2 + 24X_3$$

$$\text{s.c.} \quad 6X_1 + 15X_2 + 24X_3 - X_4 = 1$$

$$X_4 \geq 0$$

$$X_j \in Z \quad , \quad j = 1,\ldots,4.$$

y se obtiene la siguiente sucesión de tablas que se presentan en el Cuadro 2.

CUADRO 2.

z	0	6	15	24	0	6	3	0	0	0	3	0	3	0	3	0
X_1	0	1	0	0	0	1	-2	-4	0	5	-2	-4	-2	5	-2	-4
X_2	0	0	1	0	0	0	1	0	0	-2	1	0	1	-2	1	0
X_3	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1
X_4	-1	6	15	24	-1	6	3	0	-1	0	3	0	2	0	3	0

De este último cuadro se obtiene la solución

$$\text{mcd } \{6,15,24\} = 3$$

$$3 = -2\ (6) + 1\ (15) + 0\ (24)$$

Además una clase de coeficientes viene dada por

$$X_1 = -2 + 5Y_1 - 2Y_2 - 4Y_3$$

$$X_2 = 1 - 2Y_1 + Y_2$$

$$X_3 = \qquad\qquad\qquad Y_3$$

$$Y_2 = 0$$

Y_1, Y_3 enteros arbitrarios.

Es interesante hacer notar que los procedimientos computacionales que han aparecido en la literatura (Ver [7] y [8]) hacen el énfasis en la obtención de los valores de $X_1, X_2, \ldots, X_n$ que son los coeficientes de la combinación lineal que proporcionan

$$\text{mcd } \{c^1, c^2, \ldots, c^n\}$$

utilizando algoritmos que proporcionan esencialmente la misma sucesión de tablas que se presentan en este trabajo, pero no utilizan el hecho de que dicha información puede utilizarse para obtener una expresión general para todas las posibles soluciones a

$$\text{mcd } \{c^1, c^2, \ldots, c^n\} = c^1x_1 + c^2x_2 + \ldots + c^nx_n$$

Así, interpretando el problema de encontrar el máximo común divisor de números enteros dados, como un problema de PNE, y utilizando el método adecuado para resolverlo, se obtiene una información más completa en cuanto al conjunto de soluciones.

BIBLIOGRAFIA

1. Weiss, Marie J. y Dubisch R., *"Higher Algebra for the undergraduate"*, John Wiley and Sons, 1962.

2. Simonnard, M. *"Linear programming"*, Prentice Hall, 1966.

3. Glover, F. *"A new foundation for a simplified primal integer programming algorithm"*, Operations Research. Vol. 16, Nº 4, 1968.

4. Garfinkel S. Robert y Nemhauser L. George, *"Integer Programming"*, John Wiley and Sons, 1972.

5. Greenberg H. *"Integer programming"* Academic Press, 1971.

6. Zionts S. *"Linear and integer programming"* Prentice Hall 1974.

7. Blankinship, W. A. *"A new version of the Euclidean Algorithm"*, American Mathematical Monthly, Vol. 70, 1963.

8. Bradley, G. H. *"Algorithm and bound for the greatest common divisor of n integers"*, Communications of the A.C.M. Vol. 13, No. 7, 1970.