1. Publicação nº	2. Versão	3. Data	5. Distribuição
INPE-3687-PRÉ/834		*Out., 1985*	☐ Interna ☒ Externa
4. Origem *DIN/DEP*	Programa *POPES/INFOR*		☐ Restrita

6. Palavras chaves - selecionadas pelo(s) autor(es)
EQUAÇÃO DIOFANTINA LINEAR
ALGORITMO PSEUDOPOLINOMIAL
MATRIZ DE MIGNOSI

7. C.D.U.: *519.87*

8. Título *INPE-3687-PRE/834*

UM ALGORITMO PSEUDOPOLINOMIAL PARA A EQUAÇÃO DIOFANTINA LINEAR

10. Páginas: *07*

11. Última página: *05*

12. Revisada por

L. Antonio N. Lorena

9. Autoria *Nei Yoshihiro Soma*
Horacio Hideki Yanasse

Assinatura responsável

13. Autorizada por

Marco Antonio Raupp
Diretor Geral

14. Resumo/Notas

Apresenta-se um algoritmo pseudopolinomial que resolve equações diofantinas lineares. Este algoritmo baseia-se em observações colhidas sobre a matriz de Mignosi.

15. Observações

Trabalho apresentado no 8º CNMAC - Congresso Nacional de Matemática Aplicada e Computacional, Florianópolis, 16 a 20 de Setembro de 1985.

ABSTRACT

A pseudo-polynomial algorithm that solves linear diophantine equations is presented. This algorithm is based on observations from the Mignosi matrix.

UM ALGORITMO PSEUDOPOLINOMIAL PARA A EQUAÇÃO DIOFONTINA LINEAR

Nei Yoshihiro Soma

Horácio Hideki Yanasse

Instituto de Pesquisas Espaciais - INPE

Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq

Caixa Postal 515 - 12200 - São José dos Campos - SP - Brasil

O Problema de Partições (PP) surge com Leibnitz em uma carta endereçada a Bernoulli em 1669, e grande matemáticos como Euler, Cauchy, Schur e Gauss desenvolveram investigações sobre este problema. O PP consiste na determinação do número de soluções naturais da Equação: $a_1x_1+...+a_nx_n=b$, onde b e a_i, i=1,...,n são números naturais. Sem perda de generalidade admite-se $a_n>...>a_1>0$.

Este problema surge em um grande número de situações práticas, veja-se por exemplo em Kluyver e Salkin (1975).

A importância da proposição de Algoritmos eficientes decorre do fato de que este problema, como notam Garey e Johnson (1979), é NP-Completo; o melhor método para sua resolução foi proposto por Gilmore e Gomory (1966), cuja ordem de convergência é dada por $O(nb)$ e o espaço de requisições por $O(b)$.

O Algoritmo proposto baseia-se no trabalho de Mignosi (1908) que mostra que o número de soluções naturais (C_b) da equação $a_1x_1+\ldots+a_nx_n=b$, $a_i \in N$, $j=1,\ldots,n$; é $C_b=(-1)^b/b!\ \det(M)$,

onde:

$$M = \begin{bmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(b-1) & \sigma(b) \\ -(b-1) & \sigma(1) & \cdots & \sigma(b-2) & \sigma(b-1) \\ & -(b-2) & \ddots & \vdots & \vdots \\ & & \ddots & \sigma(1) & \sigma(2) \\ & & & -1 & \sigma(1) \end{bmatrix}$$

e $\sigma(j)$ é dado por:

$$\sigma(j) \triangleq \begin{cases} \sum\limits_{i \in I(j)} a_i \quad , & I(j) \triangleq \{i \mid a_i \text{ divide } j\} \\ 0 \quad , & \text{caso contrário.} \end{cases}$$

Um outro resultado referente ao trabalho de Mignosi é:

Se $C_b \neq 0$, então $\det M/b! \in \mathbf{N}$.

Para saber se o PP possui pelo menos uma solução com base nos dois resultados acima, basta verificar se $\det M \neq 0$ ou, equivalentemente, se o posto da matriz M é b.

Dadas às características da matriz M (isto é, todos os elementos acima da diagonal principal inclusive são não-negativos, pois $\sigma(j) \geq 0$; em uma mesma diagonal estes têm os mesmos valores; a diagonal abaixo da principal tem valores negativos e os outros elementos são nulos), mostra-se que o posto de M pode ser encontrado através de operações elementares das colunas de 1 a b-1 com a b-ésima.

Também mostra-se que, para fins da determinação do posto da matriz M, o valor dos $\sigma(j)$ não é importante, podendo este ser um número real positivo qualquer quando $\sigma(j) \neq 0$. O importante é a posição relativa dos elementos não-nulos em M (para maiores detalhes veja-se Soma, no prelo).

Note-se que a partir da coluna b é possível gerar toda a matriz de Mignosi deslocando os valores para posições imediatamente superiores.

De uma análise detalhada da matriz de Mignosi e da determinação de seu posto, chegou-se a uma matriz H em que se associam no máximo $\underline{n}$ índices, da seguinte forma:

$$H = \begin{bmatrix} \sigma'(1) & \sigma'(2) & \cdots & \sigma'(b-1) & \sigma'(b) \\ -1 & \sigma'(1) & \cdots & \sigma'(b-2) & \sigma'(b-1) \\ & -1 & \ddots & & \vdots \\ & & \ddots & \ddots & \sigma'(2) \\ & & & -1 & \sigma'(1) \end{bmatrix}$$

onde $\sigma'(a_i)=j$, para $j=1,\dots,n$ e $\sigma'(i)=0$ para $i\neq a_j$; $i=1,\dots,b$

Define-se uma transformação T, $T(H)=H'\stackrel{\Delta}{=}[\underline{H}_1 \vdots \dots \vdots \underline{H}_j \vdots \dots \vdots \underline{H}_b']$, onde:

$$H^1_{i,b} \stackrel{\Delta}{=} \begin{cases} H_{i,b} & \text{para} \quad H_{i,j} = 0 \quad \text{ou} \quad b \geq i \geq j+1 \\ & \text{e} \\ H_{i,j} & \text{se} \quad H_{i,j} \neq 0 \end{cases}$$

$$j \stackrel{\Delta}{=} 1 + \max_{t=2,\dots t_1} \{t \mid H_{t,b} \neq 0\} \text{ e } t_1 \text{ é pré-determinado.}$$

Após k transformações do tipo T, onde inicialmente $t_1=b$ e t_1 é decrescido de 1 a cada aplicação de transformação, tem-se:

$$\underbrace{T_0T_0\dots{}_0T(H)}_{k \text{ vezes}} = \underbrace{T_0T_0\dots{}_0T(H')}_{k-1 \text{ vezes}} = \dots = T(H^{k-1}) = H^k.$$

Interrompem-se as transformações quando a matriz H^k apresentar $H^k_{1,b} \neq 0$, ou quando houver mais de $((b-a_1)/2)+1$ posições não-nulas, donde se conclui que $p(M)=b$, ou ainda quando $t_1=a_1-1$ (donde se conclui que não há soluções naturais).

Detalhes do porque da matriz H e da transformação T podem ser abstraídas de Soma (no prelo).

No pior caso, o número de operações até a obtenção da matriz H^k final é dada por $O(H^k) = O(n(b-a_1)-\sum_{j=i}^{n} a_i)$ e o espaço de requisições, por $O(b-2a_1)$. A idéia da finitude do método, bem como suas ordens, está em Soma e Yanasse (1985) que utilizam abordagem similar para resolver o problema da mochila. Com base nesta mesma idéia pode-se sugerir outras transformações que dão origem a algoritmos diferentes para o PP, mas de mesma ordem, que na prática podem ter desempenhos melhores do que com a transformação T.

BIBLIOGRAFIAS

GAREY, M.R.; JOHNSON, D.S. *Computers and intractability - A Guide to the theory of NP-completeness*. San Francisco, W.H. Freeman, 1979.

GILMORE, P.; GOMORY, R. The theory and computation of knapsack functions. *Operations Research*, 14:1045-1074, 1966.

KLUYVER, C.A.; SALKIN, H.M. The knapsack problem: a survey. *Naval Research Logistics Quarterly*, 2(1):127-144, 1975.

MIGNOSI, G. Sulla Equazione Lineare Indeterminata. *Periodico di Matematica*, 23:173-176, 1908.

SOMA, N.Y. *Um Algoritmo exato para o problema da mochila*. Dissertação de Mestrado em Análise de Sistemas e Aplicações. São José dos Campos, INPE, jun. 1985 (no prelo).

SOMA, N.Y.; YANASSE, H.H. *A new enumeration scheme to the knapsack problem*. Apresentado na School on Combinatorial Optimization, Rio de Janeiro, 8-19 de julho de 1985.