Algoritmo Freivalds

Teoría de Algoritmos I (75.29 / 95.06)

Ing. Víctor Daniel Podberezski
vpodberezski@fi.uba.ar

Verificador de multiplicador de matrices

Sea:

las Matrices A y B de nxn

la matriz C,

$$\left\{ A \right\} \times \left\{ B \right\} \stackrel{?}{=} \left\{ C \right\}$$

Queremos <u>verificar</u>

C = A x B

Algoritmos de multiplicación conocidos

Algoritmos de multiplicación:

“naive”: $O(n^3)$

Strassen (1969): $O\left(n^{\log_2 7}\right)$

Le Gall (2014): $O(n^{2,37286})$

…

?? (??): $O(n^w)$, $w \geq 2$

(!) Cuanto menor w, mayor la constante k del algoritmo (recién para n muy grandes hay ganancia real en su aplicación)

Algoritmo Freivalds

Sea un vector r [1..n]

Tal que $r_i = \{0,1\}$ con equiprobabilidad para todo i

Calcular:

$D = A \times (Bxr) - (Cxr)$

Si D = vector cero => AxB es <u>probablemente</u> C (retorna "si")

Si D ≠ vector cero => AxB <u>NO</u> es c (retorna "no")

$$\left\{ D \right\} = \left\{ A \right\} \times \left(\left\{ B \right\} \left\{ r \right\} \right) - \left(\left\{ C \right\} \left\{ r \right\} \right)$$

Algoritmo Freivalds (cont.)

Es un algoritmo de tipo Montecarlo

La complejidad en tiempo es $O(N^2)$

Si AxB= C => Pr[resp=si] = 1

Esta afirmación es trivial. Para cualquier r seleccionado (AxB)xr=(C)xr

Si AxB ≠ C => Pr[resp=si] ≤ ½

Requiere una demostración

Falsos positivos

Afirmación:

Si $AB \neq C \Rightarrow Prob[ABr \neq Cr] \geq ½$

Hipotesis:

Sea $D = AB - C$ tal que $D \neq 0$

Queremos mostrar que hay muchos r tal que $Dr \neq 0$, específicamente $Prob[Dr \neq 0] \geq ½$ para un r elegido aleatoriamente

Probaremos que para cada $Dr = 0$ donde $D \neq 0$, existe un r' tal que $Dr' \neq 0$ y $D \neq 0$

Falso positivo

Negativo

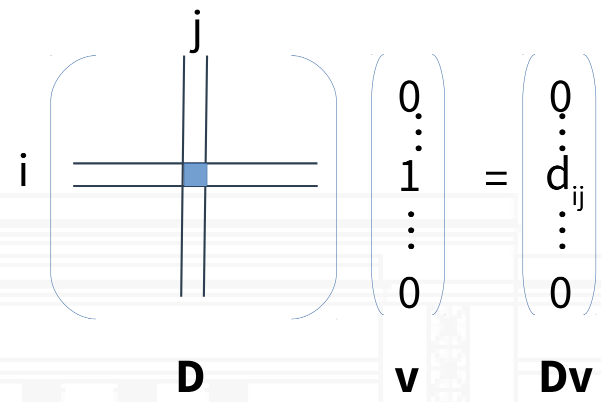
Falsos positivos (cont.)

$D = AB - C \neq 0$

Existe i,j tal que $d_{ij} \neq 0$

Seleccionamos un vector v con v_j=1 y $v_{x \neq j}$ =0

Vemos que Dxv = Dv ≠ 0



Sea cualquier r que pueda ser elegido aleatoreamente por el algoritmo tal que Dr=0,

Sea r’ = r + v => Dr’ = D(r+v) = 0 + Dv ≠ 0

r con r’ tienen una relacion de 1 a 1 (al tener solo 1 elemento “switcheado”

Por lo tanto el numero de r’ / Dr’ ≠ 0 ≥ numero de r / Dr=0

Finalmente Prob[Dr ≠ 0] ≥ ½

Ejemplo

$$A = \begin{Bmatrix} 2 & 3 \\ 3 & 4 \end{Bmatrix} \quad B = \begin{Bmatrix} 1 & 0 \\ 1 & 2 \end{Bmatrix} \quad C = \begin{Bmatrix} 6 & 5 \\ 8 & 7 \end{Bmatrix}$$

Falso positivo!

$$r = \begin{Bmatrix} 1 \\ 1 \end{Bmatrix} \Rightarrow \begin{Bmatrix} 2 & 3 \\ 3 & 4 \end{Bmatrix} \left(\begin{Bmatrix} 1 & 0 \\ 1 & 2 \end{Bmatrix} \begin{Bmatrix} 1 \\ 1 \end{Bmatrix} \right) - \begin{Bmatrix} 6 & 5 \\ 8 & 7 \end{Bmatrix} \begin{Bmatrix} 1 \\ 1 \end{Bmatrix} = \begin{Bmatrix} 0 \\ 0 \end{Bmatrix}$$

Resp: “Si”

$$r = \begin{Bmatrix} 1 \\ 0 \end{Bmatrix} \Rightarrow \begin{Bmatrix} 2 & 3 \\ 3 & 4 \end{Bmatrix} \left(\begin{Bmatrix} 1 & 0 \\ 1 & 2 \end{Bmatrix} \begin{Bmatrix} 1 \\ 0 \end{Bmatrix} \right) - \begin{Bmatrix} 6 & 5 \\ 8 & 7 \end{Bmatrix} \begin{Bmatrix} 1 \\ 0 \end{Bmatrix} = \begin{Bmatrix} -1 \\ -1 \end{Bmatrix}$$

Resp: “No”

Basta encontrar una respuesta en “no” para determinar que AxB ≠ C.

Margen de error

Para disminuir la posibilidad de los falsos positivos podemos ejecutar k veces el mismo

- El orden de complejidad será $O(kn^2)$
- La probabilidad de falso positivo sera $\leq 1/2^k$

Cuanto mayor k, la probabilidad tiende a cero

- Si k=n, la complejidad pasa a ser n^3

.UBA fiuba

FACULTAD DE INGENIERÍA

Presentación realizada en Junio de 2020