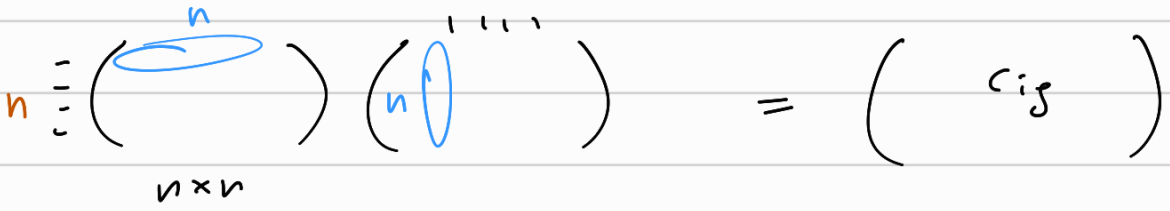
Moltiplicazione matrice per matrice / 16-05

Consideriamo matrici quadrate



$$A \; B = C$$

Effettua n moltiplicazioni di $n \times n$ elementi $= O(n^3)$

Esistono algoritmi detti galattici che utilizzano grandi costanti per cui se $n = 2$ non ovvio n^3 ma qualcosa di meno per cui il costo non è 8 ma 7

L'idea è voler verificare, date le matrici A, B, C $n \times n$ se $AB = C$ n grande

Costruiamo un vettore r-dimensionale $= \{0,1\}^n$

Il prodotto è associativo fra vettori e matrici:

$$(AB)\vec{r} = A(B\vec{r}) = A\vec{s} = \vec{t}$$

avevo non necessario di calcolare A e B fra loro per trovare $AB\vec{r}$

$(-)(|) = (\cdot)$ $\quad O(n^2)$

$0 = n \times n$

$C\vec{r} = \vec{u}$

MC Matrix Multiplication (A, B, C)

Input: A, B, C
Output: "$AB \neq C$" oppure "probabilmente $AB = C$"

- Campiona $\vec{r}$ uniformemente: $\{0,1\}^n$

$\vec{s} \leftarrow B\vec{r}$
$\vec{t} \leftarrow A\vec{s}$
$\vec{u} \leftarrow C\vec{r}$
if $\vec{u} = \vec{t}$
    then return "prob $AB = C$"
else
    return $AB \neq C$

Qual è la prob. che generando un vettore a caso, più volte, con matrici diverse ottengo lo stesso risultato?

Se $AB \neq C$

$p(A(B\vec{r}) = C\vec{r}) \leq \frac{1}{2}$ limite superiore

$AB \neq C \rightarrow D = AB - C \neq 0$ sse $\exists$ un $d_{ij} \neq 0$

d_{ij} $A(B\vec{r}) - C\vec{r} = D\vec{r}$

ottengo nullo se:

$d_{13} \neq 0$

$\begin{pmatrix} \cdots & & \end{pmatrix} \begin{pmatrix} \vdots \\ \vec{r} \end{pmatrix}$ se $\vec{r}$ ha uno zero dentro allora d_{ij} è zero

$d_{13} = 5$, z_3 è 1 e la somma è -5 $\rightarrow$ ho $d_{i3} = 0$

$$\sum_{k=1}^{r} d_{ik} z_k = \sum_{k \neq 3} d_{ik} z_k + d_{i3} z_3$$

$$\| \quad y$$

se $d_{i3} \neq 0$, ho come risultato 0 se $z_3 = 0$ $\rightarrow \frac{1}{2} \cdot p(y=0)$

$$p(y + d_{i3} z_3 = 0) = p(\overset{0}{y} + d_{i3} z_3 = 0 \mid y = 0)\, p(y=0) +$$

$$+ p(y + d_{i3} z_3 = 0 \mid y \neq 0)\, p(y \neq 0)$$

$= 0$ se la somma è $-y$ ($\Leftrightarrow z_3 = 1$)

$p''(d_{i3} z_3 = -y)$

dipende da
$P(A) = P(A|B)P(B) + P(A|\neg B)P(\neg B)$

$$p(d_{i3} z_3 = -y \wedge z_3 = 1) \leq \tfrac{1}{2} p(y \neq 0)$$

ovvero $p(y + d_{i3} z_3 = 0) \leq \frac{1}{2} p(y=0) + \frac{1}{2} p(y \neq 0)$

Confronto di file o stringhe dalle impronte digitali

$\pi(x)$ n° di numeri primi $\leq x \in \mathbb{R}^+$ con $\ln x$

$\rightarrow \pi(x) \sim \frac{x}{\ln x}$ ovvero $\lim_{x \to \infty} \frac{\pi(x)}{x/\ln x} = 1$

Nonostante cresca la differenza $\pi(x) - x/\ln x$
la convergenza rimane a 1

Quindi come stima useremo $x/\ln x$ come n° di primi $\leq x$

Dato un n, quanti sono i suoi fattori primi sapendo che $n < 2^{\ell}$?

Poiché 2 è il più piccolo num. primo, $\forall \ell \in \mathbb{N}$
→ ho al più ℓ fattori primi

$\ell = 2^{30}$ quanti bit ho

a file di Alice
b file di Bob

$2 \ln \ell = 60$

p num primo a caso $< \ell^2$

$f(a) = a \bmod p$ fingerprint (impronta digitale)

se $p = 3$

se $\ell = 2^5 = 32 \bmod 3 =$ n° del messaggio inviato

$f(b) = b \bmod p$ $|f(a) - f(b)| \bmod p$

→ $\neq 0$ file diversi
→ $= 0$ file probabilmente uguali

ℓ bit con ℓ molto grande

es Alice 00101111 = 47 il file usato come numero 8 bit → $\ell = 2^3$
Bob 00101011 = 43

prendo un p : $2 < p < 64$ es 17

ℓ^2

A: $47 \bmod 17 \to 13$

B: $43 \bmod 17 \to 9$

↓

fingerprint del messaggio

se la distanza fra i numeri è 17 va male

$|a-b| \leq 2^{\ell}$ quantità di bit

↓

differenza "fra f.'ti" intesa come numeri

Quanti sono i fattori primi di $|a-b|$?

sono al più ℓ per $|a-b|$

$|47-43|$

Quanti per $|2-\ell^2|$ sono $\frac{x}{\ln x}$ ovvero $\frac{\ell^2}{2 \ln \ell} \to \ln \ell^2$

probabilità = $\frac{\ell^{\pi \text{ fattori primi (al più)}}}{\frac{\ell^2}{2 \ln \ell}} = \frac{2 \ln \ell}{\ell}$

pochi fattori primi, tale rapporto restituisce una p bassa

se ℓ cresce la p di errore diminuisce, es. x figabit $\ell = 30$

} ovvero è poco probabile che per $a \neq b$ io abbia "prob uguali"

$P(2^{30}) = \frac{2 \ln 2^{30}}{2^{30}} = \frac{60 \ln 2}{2^{30}} < \frac{2^6}{2^{30}} = 2^{-24} < 10^{-7}$ errore poco probabile