Selected Parts of Solving Sparse System over Z_2 via Block Lanczos Algorithm

Mgr. Marek Sýs, Ing. Vladislav Novák

KAIVT FEI STU BRATISLAVA

Faktorizácia metódou GNFS

- 1. fáza - výber vhodného polynómu
- 2. fáza - preosievanie
- **3. fáza - spracovanie matice exponentov**
- 4. fáza - výpočet faktorov podľa nájdených závislostí

Hľadanie lineárne závislých stĺpcov

= riešenie sústavy rovníc: $\boxed{B\,x = 0}$

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

rozmery matice B [r × n], kde r < n

n = 500 000 až 7 000 000

Výber vhodnej metódy

- Gaussova eliminačná metóda a jej modifikácie
  - vždy nájde výsledok
  - zložitosť: $O(n^3)$
- Wiedemannova metóda
  - výsledok iba s určitou pravdepodobnosťou
  - zložitosť: $O(n^2)$
- Lanczosova metóda
  - výsledok iba s určitou pravdepodobnosťou
  - zložitosť: $O(n^2)$

Lanczosova metóda nad poľom konečnej charakteristiky

- $A\,x = u$, kde $u \neq 0$

  A - symetrická matica

- B x = 0

Predpríprava: $B\,x = 0 \rightarrow A\,x' = u$

1. symetrická matica A

- $A = B^T B$

Predpríprava: $B\,x = 0 \rightarrow A\,x' = u$

2. nenulový člen na pravej strane

- zvolíme náhodné y
- budeme hľadať riešenie sústavy $A\,(x'-y) = 0$
- $A\,(x'-y) = 0 \quad \Rightarrow \quad Ax' - Ay = 0 \quad \Rightarrow$
  $\Rightarrow \quad Ax' = Ay,$
  po substitúcii: $u = Ay$
  $Ax' = u \neq 0$
- po vypočítaní x' pre sústavu $Ax' = u$
  ľahko určíme x pre sústavu $Ax = 0 \qquad x = x' - y$

Predpríprava: $B\,x = 0 \rightarrow A\,x' = u$

- Niektoré riešenia sústavy:

  $A\,x = 0$

  sú riešením aj:

  $B\,x = 0$

Bloková Lanczosova metóda nad poľom konečnej charakteristiky

- vektory x,y nahradíme maticami X,Y
- *namiesto sústavy* $A\,x = A\,y$
  riešime sústavu $A\,X = A\,Y$
  (môžeme nájsť viacero riešení)
- pre pole Z_2: rozmery matíc X,Y: $[n \times N]$,
  kde N = 16, 32, 64, ...

Popis algoritmu

1. vygenerovanie *Y*
2. iteračná časť (takmer 100% výpočtového času)

$$V_{i+1} = AV_iS_iS_i^T + V_iD_{i+1} + V_{i-1}E_{i+1} + V_{i-2}F_{i+1}$$

$$X_A = \Sigma\,(V_i\,W_i^{inv}\,V_i^T\,V_0)$$

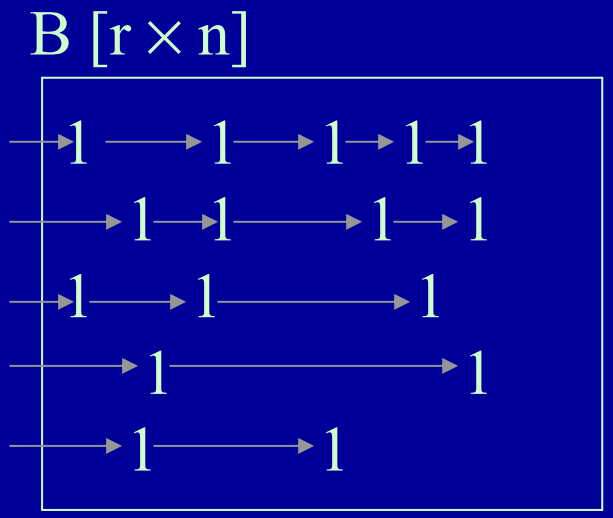
3. záverečné vyhľadanie niekoľkých skupín lineárne závislých stĺpcov v matici *B* Gaussovou eliminániou matice s malým počtom stĺpcov

Reprezentácia matíc

- prvky matíc patria do Z_2
- $B\ [r \times n]$ - veľmi málo nenulových prvkov
  $\Rightarrow$ reprezentácia zoznamami jednotiek

- $AV = B^T(BV)$

  $A = B^TB$



Reprezentácia matíc

- Ostatné matice sú rozmerov $[N \times N]$, alebo $[n \times N]$ (N je počet bitov integera)
  $\Rightarrow$ reprezentované pol'om integerov

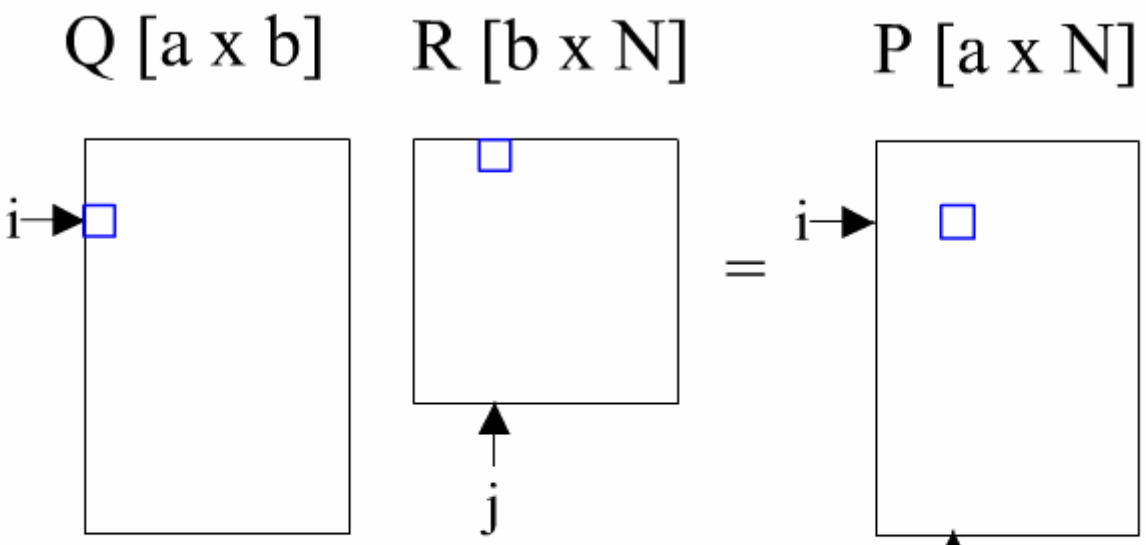
$V\,[N \times N]$

011100010110
110101010001
100110100101
011100010110
101000100011
011100010110

$V\,[n \times N]$

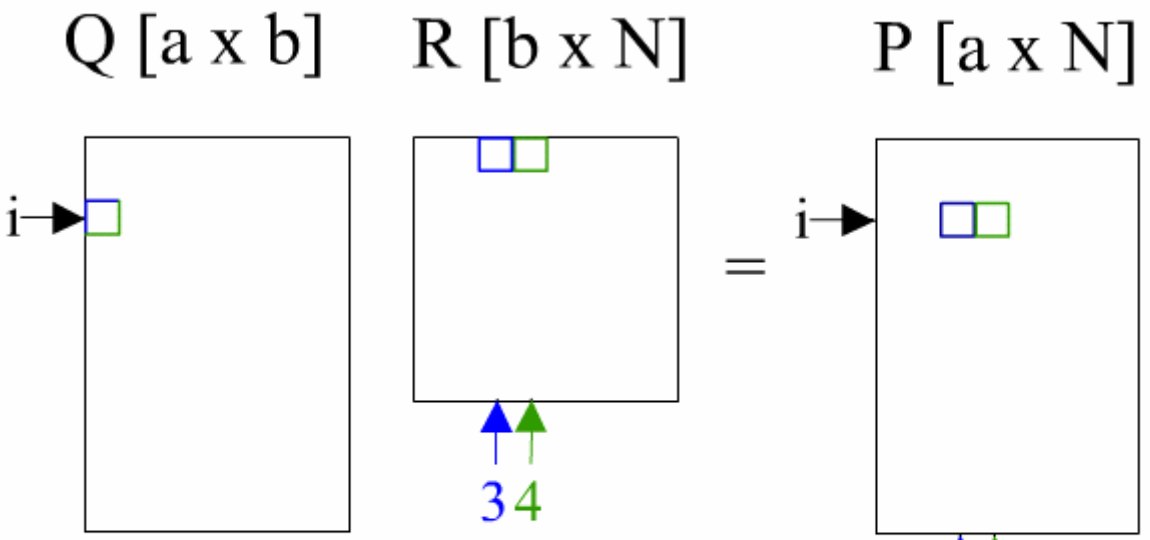
011100010110
110101010001
100110100101
011100010110
101000100011
011100010110
110001010011
011100010110
011100010110
110101010001
100110100101
011100010110

Princíp násobenia matíc



$$P_{i,j}=\Sigma_k(Q_{i,k}\,R_{k,j})$$

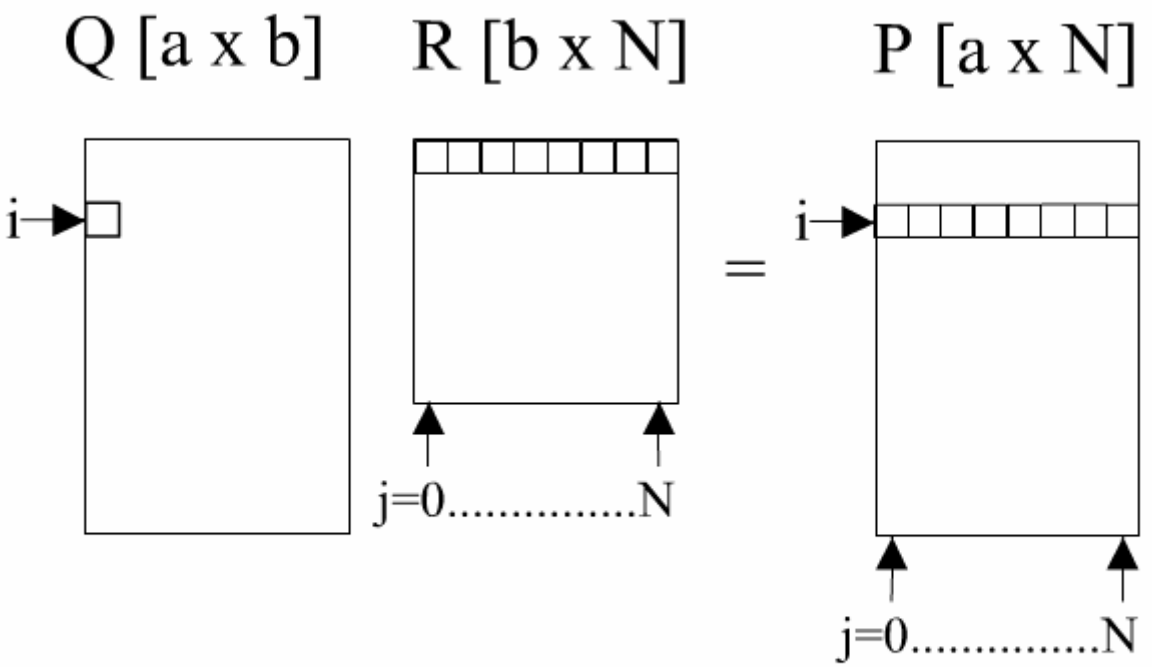
Princíp násobenia matíc



$P_{i,3}=\Sigma_k(Q_{i,k}\,R_{k,3})$

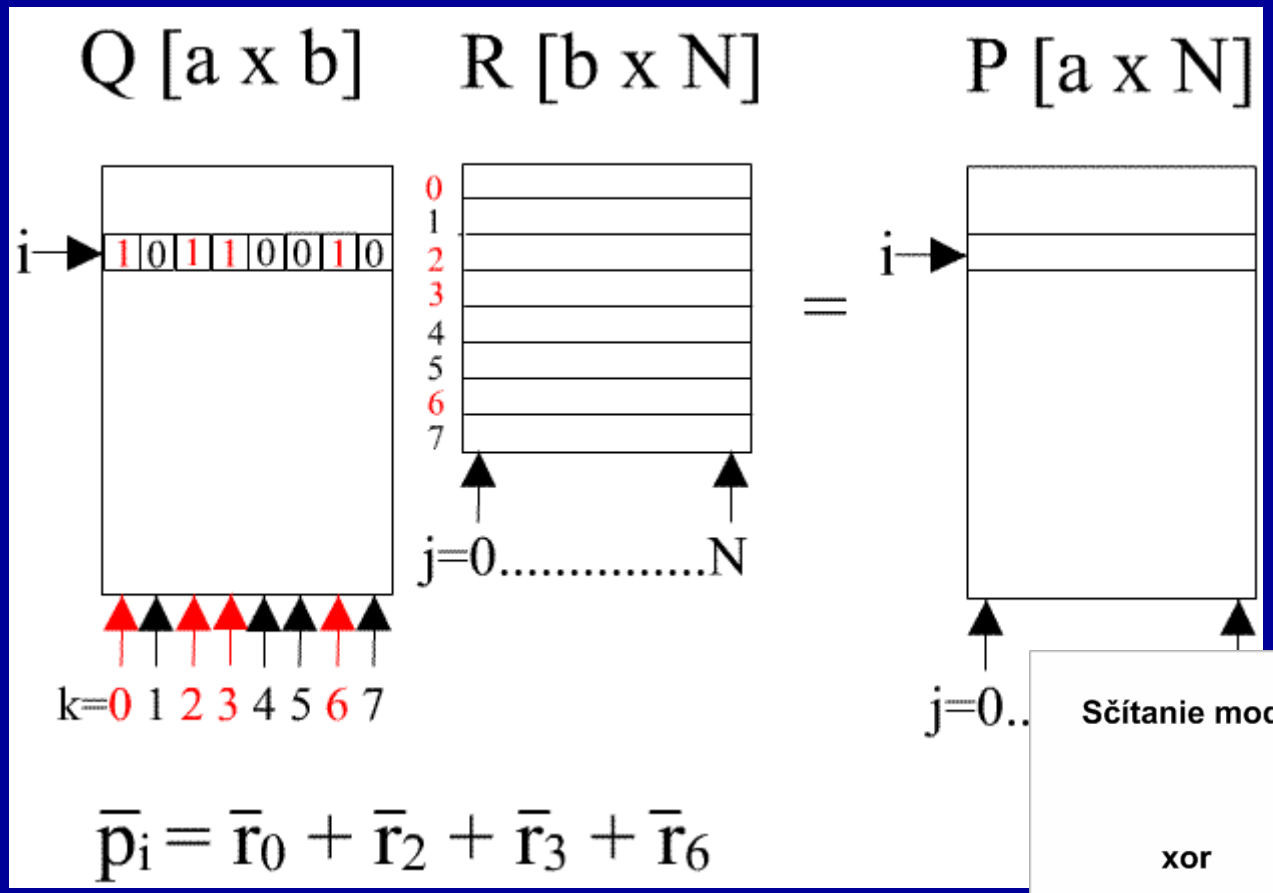
$P_{i,4}=\Sigma_k(Q_{i,k}\,R_{k,4})$

Princíp násobenia matíc



$$\bar{p}_i = \Sigma_k(Q_{i,k}\,\bar{r}_k)$$

Princíp násobenia matíc



Sčítanie modulo 2

1 0 0 1 0 1 1 1

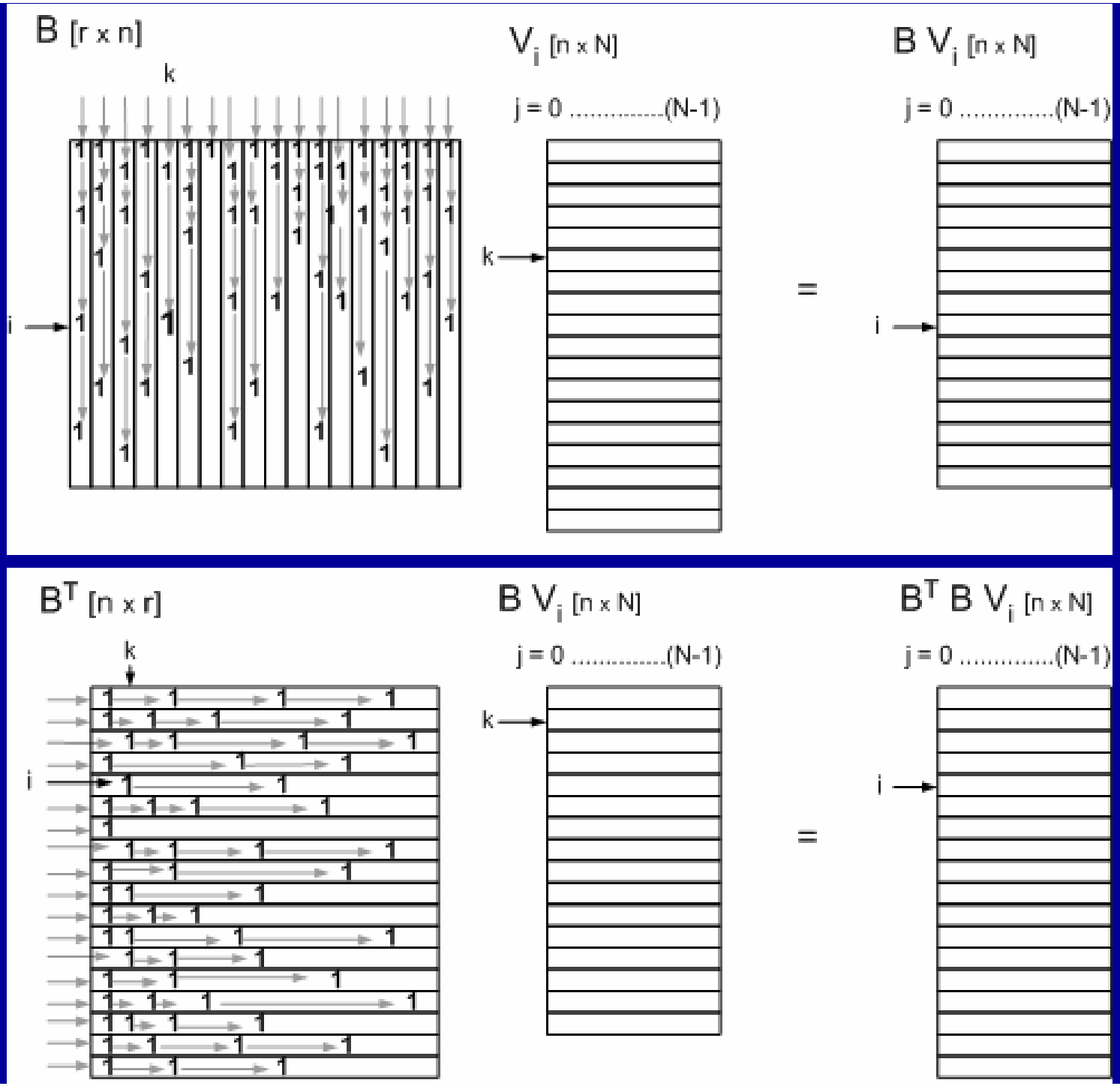
xor 0 1 0 1 1 1 0 0

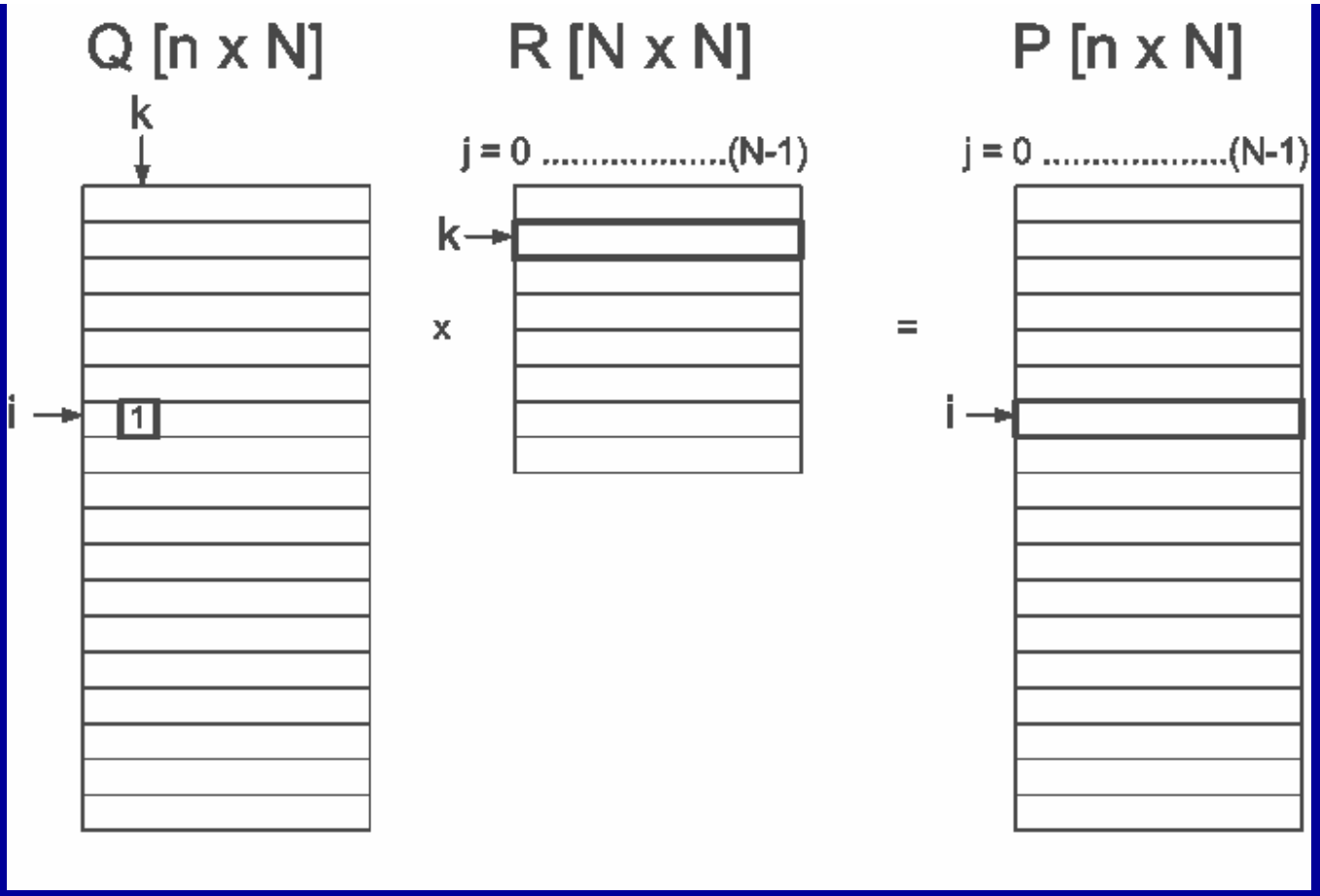
1 1 0 0 1 0 1 1

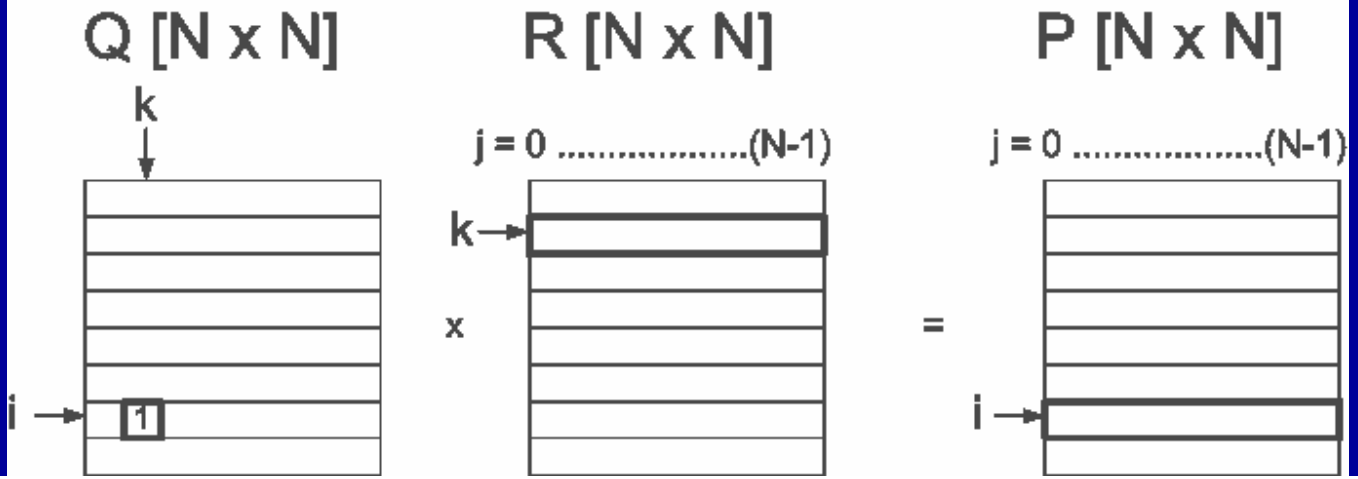
Princíp násobenia matíc

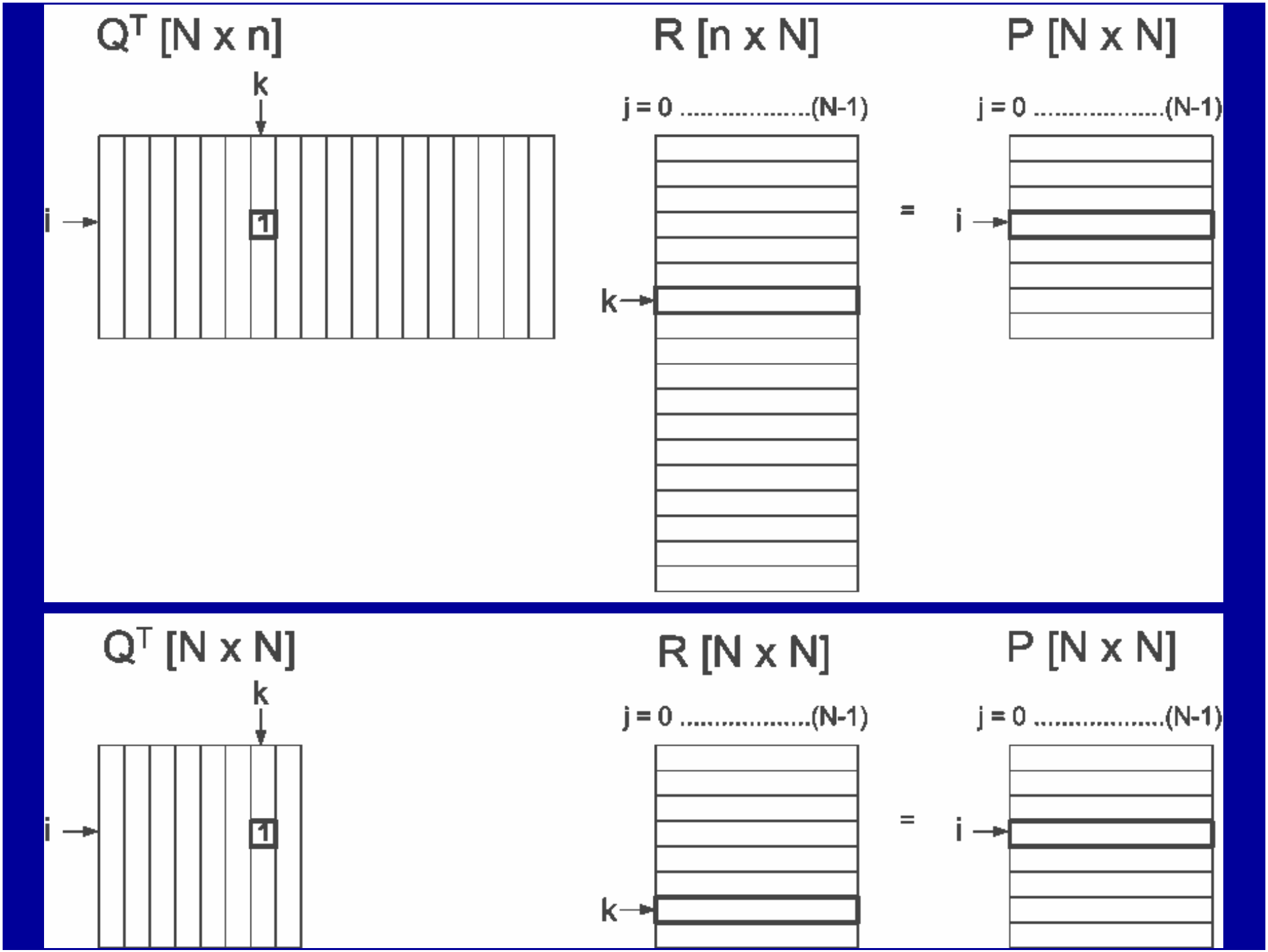
$$P_{i,j} = \sum_k Q_{i,k} R_{k,j} \qquad \Rightarrow \qquad \vec{p}_i = \sum_k Q_{i,k} \vec{r}_k$$

Typy násobení matíc

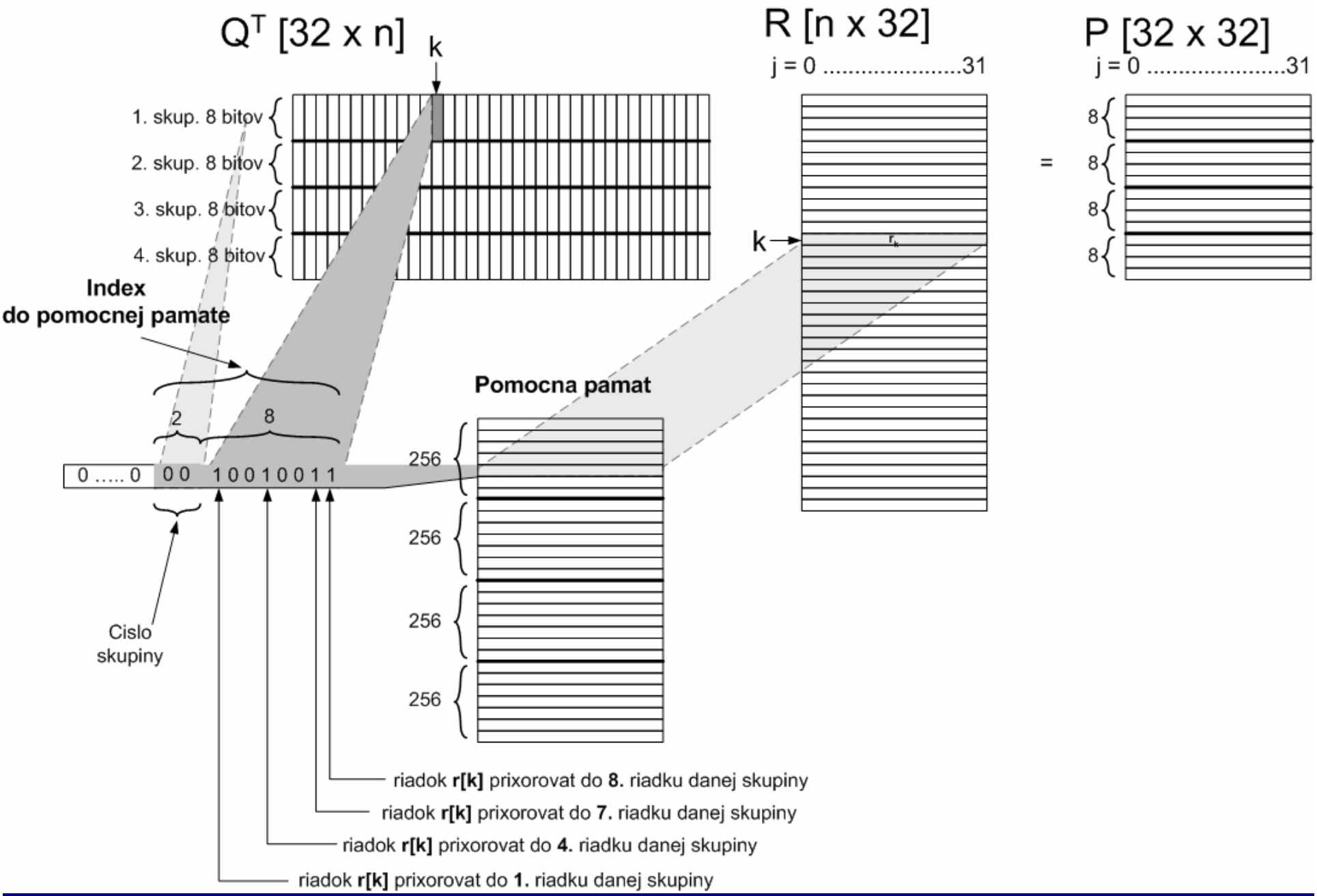

B [r x n]
k
i
V_i [n x N]
j = 0 .....(N-1)
k
=
B V_i [n x N]
j = 0 .....(N-1)
i
B^T [n x r]
k
i
B V_i [n x N]
j = 0 .....(N-1)
k
=
B^T B V_i [n x N]
j = 0 .....(N-1)
i

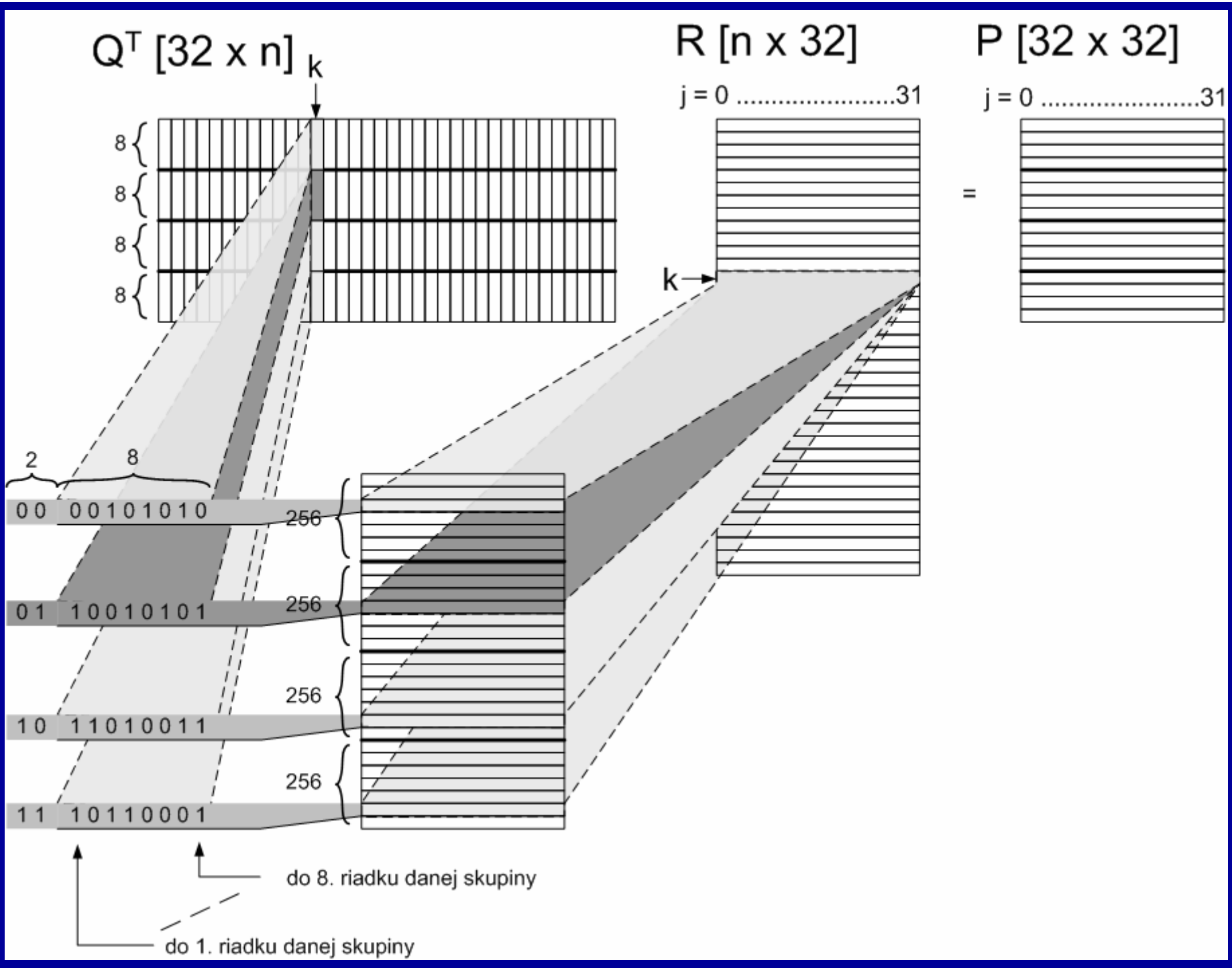

Q [n x N]
R [N x N]
P [n x N]
k
j = 0 .....(N-1)
k
x
=
i
1
i


Q [N x N]
R [N x N]
P [N x N]
k
j = 0 .....(N-1)
k
x
=
i
1
i


Q^T [N x n]
k
i
1
R [n x N]
j = 0 .....(N-1)
k
=
P [N x N]
j = 0 .....(N-1)
i
Q^T [N x N]
k
i
1
R [N x N]
j = 0 .....(N-1)
k
=
P [N x N]
j = 0 .....(N-1)
i

Zrýchlenie násobenia matíc


Q^T [32 x n]
k
1. skup. 8 bitov
2. skup. 8 bitov
3. skup. 8 bitov
4. skup. 8 bitov
Index
do pomocnej pamate
2
8
0 0
0 0
1 0 0 1 0 0 1 1
Cislo
skupiny
Pomocna pamat
256
256
256
256
R [n x 32]
j = 0 31
k
r_k
=
P [32 x 32]
j = 0 31
8
8
8
8
riadok r[k] prixorovat do 8. riadku danej skupiny
riadok r[k] prixorovat do 7. riadku danej skupiny
riadok r[k] prixorovat do 4. riadku danej skupiny
riadok r[k] prixorovat do 1. riadku danej skupiny


Q^T [32 x n] k
R [n x 32]
P [32 x 32]
j = 0 31
j = 0 31
=
k
8
8
8
8
2
8
0 0 0 0 1 0 1 0 1 0
0 1 1 0 0 1 0 1 0 1
1 0 1 1 0 1 0 0 1 1
1 1 1 0 1 1 0 0 0 1
256
256
256
256
do 8. riadku danej skupiny
do 1. riadku danej skupiny

Paralelný Blokový Lanczosov algoritmus

- násobenie matice B bitovo reprezentovanou maticou
- násobenie „dlhých“ bitovo reprezentovaných matíc
- prenášanie veľkého množstva údajov

Ďakujem za pozornosť